Proving e-voting mixnets in the CCSA model: zero-knowledge proofs and rewinding

Anonymous authors

***Abstract*—Mixnets are crucial components of electronic voting protocols, used to mix the ballot box before the tally. Mixnets should ensure two somewhat antithetic properties: preservation of the list of ballots, and privacy. Unfortunately, proving that mixnets ensure the desired properties requires both complex cryptographic primitives (zero-knowledge proofs, commitments schemes) and proof techniques (mainly rewinding). Hence, such proofs are at the same time highly desirable but quite complex to get. In order to achieve such complex formal proofs, we focus on the quite recent Computationally Complete Symbolic Attacker logics, which handles computational security proofs with first-order logic, abstracting most probabilities and explicit reductions. Said differently, it provides precise and subtle computational reasoning, while not requiring too much expertise from the user who setup the proof. In the present work, we enrich the logic to be able to deal with zero-knowledge proofs and rewinding techniques, and provide the first complete formal proof of Terelius-Wikström mixnet protocol.**

***Index Terms*—mixnet, zero-knowledge proof, rewinding, formal proof, Computationally Complete Symbolic Attacker**

I. Introduction

Electronic voting (e-voting) protocols are more and more used for widespread applications, from professional to political elections in direct democracy, as for example in Switzerland. Therefore, depending on the criticality of the elections, we need them to provide robust security guarantees. In broad terms, such protocols should achieve two main properties: verifiability and privacy. Roughly speaking, verifiability ensures that all the ballots in the ballot box have indeed been counted during the tally (*universal verifiability*) and that each voter can verify if his ballot is present in the ballot box (*individual verifiability*). While specific definitions may vary, privacy broadly ensures that no adversary can link ballots to voters. This is why such protocols involve some permutation step of the ballots, e.g. with the help of *mixnets*, which we focus on in this work.

More generally, e-voting protocols are composed of three main steps. They begin with a setup, where a server is prepared (by an authority commitee) to host the election. Later, during the voting phase, voters submit their votes into a public *ballot box*. Finally, as soon as the voting delay expires, authorities join together to perform the tally, which may lead to more or less complex computations and issues. For simple tallies, e.g. when only sums are involved, homomorphic encryption can be enough to compute the result. However, for more complex tallies, e.g. when voters are asked to rank candidates, we need to mix the ballot box to safely decrypt the ballots and then compute the tally without compromising ballots-voters unlinkability. One solution to this issue is to use *mixnets*.

A *mixnet* is composed of several connected *mix-servers* acting as authorities. Each mix-server takes as input the encrypted list of ballots, and produces as output a permutation (going with a re-encryption) of these ballots. Regarding the main security properties we want e-voting protocols to guarantee, we expect two security properties from mixnets:

- *Verifiability*: A dishonest mixnet should not be able to convince an honest verifier that the output list is a re-encrypted permutation of the input list when it is not the case. In particular, as the output list is indeed a permutation of the input list, no ballot can be dismissed nor duplicated. This preserves both individual and universal verifiability properties.
- *Permutation secrecy*: An honest mixnet should ensure that no adversary can link votes from the output list with votes from the input list.

To achieve these security properties, mixnets rely on advanced cryptographic constructions, e.g. zero-knowledge proofs and commitment schemes, with complex interactions between them. Consequently, proof techniques required by these protocols are quite intricate. Indeed, they are based on complex cryptographic reductions techniques (e.g. rewinding) and complex interactions between cryptographic and algebraic results.

Formally proving security properties of e-voting protocols is a huge task, and some results have already been achieved. In particular, some protocols involving simple tallies have been completely proved [1], whereas more complex ones using mixnets still need efforts to be completely proved. For some of them, partial proofs exist, assuming for example that the involved mixnets are ideal [2]. Formally proving security properties of real-life mixnets remains somewhat of a blind spot in the overall proofs of complex e-voting protocols, mainly because of the complexity of the underlying proofs. In particular, we need to handle *zero-knowledge* proofs, which implies to manage *rewinding* techniques to get the associated witnesses (in our case, the witnesses will be the permutations used to mix the ballot box). This means that we have to “get back into the past of the adversary’s actions and make them choose another way, a kind of fork paradigm”. This implies that we have to manage very precisely adversary knowledge and behaviour, and cannot consider them as a black box. Other probabilistic aspects also lead to subtleties, and we need to be able to manage them through formal models which need to be precise, expressive and sound. Getting all this at the same time is necessary to get comprehensive proofs that we can trust.

A. Related work

Terelius-Wikström mixnet protocol (a variant of mixnet protocol that is used in the e-voting protocol Belenios [3]) has been originally proposed in [4], [5], with a sketch of handmade cryptographic proof of the proposed constructions, and a particular focus on algebraic properties, but without formalizing the rewinding step linked to the zero-knowledge proofs, and assuming that the adversary produces as many proof transcripts as needed to extract a number of witnesses.

Our goal is to supplement this work by providing a formal computational proof of this protocol security properties, Formal security proofs of cryptographic protocols are usually based on one among two main paradigms. The first one is the *symbolic model*, Based on first-order logic, it has led to several well-known tools and to successful protocols analyses, even for mixnets, as in [6], [7]. However, symbolic models consider cryptographic constructions as black-boxes with perfect security, making them unsuitable to capture the subtleties of rewinding arguments. The second approach, known as *computational model*, takes into account the ability for the attackers to break cryptographic primitives with some probability of success, e.g. considering them as Probabilistic Polynomial-Time Turing Machines. Several such frameworks have been proposed and developed. The well-known CryptoVerif tool [8] provides a mechanized way to handle general reductions techniques, but for intrinsic reasons is unfortunately not able to handle rewinding techniques. Other approaches, based on probabilistic Hoare logic (e.g. leading to the EasyCrypt tool [9]) could be more suitable for our purpose. Unfortunately, even if recent advances allow rewinding in EasyCrypt [10], performing complex proofs of protocols using advanced cryptographic techniques remains very complex and time consuming with this kind of tools, making them ill-suited for our goal.

In the present work, we focus on a third paradigm, namely the *Computationally Complete Symbolic Attacker* (CCSA) model [11], [12]. This model aims to take benefits of both previous paradigms: using a first-order logic, it abstracts (and then ease) most probabilitic and complexity theoretic reasoning, but provides at the same time strong cryptographic guarantees by giving a probabilistic semantics to this logic. These benefits rely on the central predicate $u \sim v$, encoding the fact that the probability, for a probabilistic polynomial-time adversary, to distinguish the computational interpretations of the terms u and v is negligible. In order to perform a proof in this model, one has to provide elementary axioms in this logic to capture the properties of the cryptographic constructions (their computational interpretation should be proven sound), and perform the proof with the help of these axioms. A correct proof then provides guarantees against a computational attacker. This logic, which has been implemented in the Squirrel proof assistant [13], allows relatively simple proofs of complex protocols (for example key-management APIs [14]), with very limited work on proving soundness of the axioms. Notably, the soundness proofs are small and relatively easy to check, and the remainder of the reasoning is pure first-order reasoning. Today, neither CCSA nor Squirrel can handle rewinding techniques, but it is precisely the goal of the present work to supplement previous works by providing all the material to be able to reason with rewinding techniques and zero-knowledge proofs within the CCSA logic, hence providing all the necessary reasoning techniques to prove mixnets security formally.

Other efforts have already been made to formalize such proofs with logics. In particular, [15], [16] propose a model of Terelius-Wikström mixnet in Coq (now Rocq) using the CertiCrypt project [17]. These proofs focus on properly capturing all the associated probabilistic arguments, but exclude rewinding. More precisely, their models are low-level ones and, then, more precise than ours when studying the algebraic properties (which we mostly axiomatize), providing a lot of confidence in the algebraic reasoning and justifying in particular the proof of permutation. However, they do not model rewinding at all and, thus, miss some adversarial selection argument, as discussed later. These works are complementary to ours, and provide us confidence that our axiomatization of algebraic properties is correct, while our work ensures that the rewinding step of the proof is correct A final remark is that their work provides verified running code, which is not the case of our work.

Our work heavily relies on the properties of interactive zero-knowledge protocols, and more precisely on Σ-protocols. A number of works aim at proving that such interactive zero-knowledge protocols or Σ-protocols precisely satisfy intended properties [18], [19], [20], [21], [22], considering them at the atomic primitive level. Among these works, some lead to implementations into formal tools as CertiCrypt, ZKCrypt, CryptHOL, EasyCrypt and SSProve. But, none of them addresses larger protocols using Σ-protocols at a macro level, and we adopt here a complementary approach where we assume that the zero-knowledge or Σ-protocols satisfy the intended properties, formalize them as building blocks used to build larger protocols, and then prove that the overall protocol using them satisfies another set of properties. The aforementioned works give a strong fondation for our hypotheses.

Finally, few works aim at formalizing rewinding for computationally sound logics targeting cryptographic reasoning. Notably, [10] aims at formalizing rewinding for EasyCrypt logic's. However, proofs in EasyCrypt are notoriously intricated as soon as the reductions become complex, and capturing the nested rewinding steps — which is necessary here — would be a rather complex problem in this logic. By contrast, we provide here a relatively simple proof thanks to our formalization of adversarial success. Concerning our choice of framework, we point out that in EasyCrypt all reductions must be explicit, leading to heavier and less Human readable long proofs (in terms of lines of code). In particular, adversarial executions are explicit in the number of times the rewinding has to be executed. Our CCSA formalization of the rewinding technique abstracts it inside the semantics of our axiom, making it much easier to handle for the user. Besides, EasyCrypt provides concrete security analysis, but makes computations on probabilities explicit. This makes it more precise, but leads to heavier and less Human readable proofs (in terms of lines of code).

B. Contributions

The goal of our work is twofold: firstly, to the best our our knowledge, we provide the first complete and precise proof of Terelius-Wikström mixnet protocol; secondly, we provide a formalization of rewinding and other reasoning techniques in the CCSA logic, which can be reused in any other formal analysis involving it. More precisely:

- We provide (and prove) axioms for the algebraic properties needed for the proof.
- We provide the first CCSA axiomatization of zero-knowledge proofs, commitment schemes and re-encryption.
- We provide a new construction that allows to capture rewinding in the CCSA logic. Natively, the original CCSA logic only allows reasoning on globally negligible (or globally non-negligible) events, meaning that one can only reason on probabilities on the whole sampling space, but it cannot handle conditional probabilities. However, rewinding requires reasoning on the probability of a certain event *knowing* that an execution point has been reached. Therefore, we introduce a new construction in the CCSA logic that captures that a certain formula is true with non-negligible probability knowing that another formula is true. Additionally, we provide axioms addressing interactions between this construction and the usual global CCSA formulas. With this enrichment of the CCSA logic, we are able to capture the rewinding argument.

To our knowledge, our work is the first one to provide a framework providing complete and precise formal proofs of not-idealized mixnets.

C. Outline

Our paper is organized as follows. We first provide in Section II an overview of Terelius-Wikström mixnet protocol, to give a flavor of its intrinsic nature. Then, we introduce in Section III some background on the CCSA logic, and show in Section IV how we use it to formalize the cryptographic primitives and properties involved in Terelius-Wikström protocol. Then, Section V is dedicated to a more detailed presentation of the protocol, which includes CCSA logic formalizations. At this point, all the ingredients are set to expose our proofs of verifiability in Section VI and permutation secrecy in Section VII. The article ends in Section VIII with a summary of our contributions and future work directions. We provide more technical details on the proofs and supplementary material in appendices.

II. Terelius-Wikström mixnet protocol in a nutshell

We provide in this section an overview of Terelius-Wikström protocol [5], [4]. A more precise description is provided in Appendix B. Before presenting the protocol, we need to introduce some notation. From now on, N will denote a natural number and $p_\eta \in \mathbb{N}^*$ will be a prime number of size at least η, *i.e.* we have $\log_2 p_\eta \geqslant \eta$. Moreover, $\mathbb{G}_{p_\eta}$ refers to a cyclic group of order p_η, and $\mathbb{F}(p_\eta)$ refers to the Galois field of order p_η. We denote by $\langle \cdot \mid \cdot \rangle$ the standard scalar product over $\mathbb{F}(p_\eta)^N$: for all vectors $\mathbf{x} = (x_1, \dots, x_N), \mathbf{y} = (y_1, \dots, y_N) \in \mathbb{F}(p_\eta)^N$, we have $\langle \mathbf{x} \mid \mathbf{y} \rangle = \sum_{i=1}^N x_i y_i$. We denote by $\mathbf{1}$ the unit vector $\mathbf{1} = (1, \dots, 1) \in \mathbb{F}(p_\eta)^N$. Finally, we define $\circledast$ to be the following operator on vectors: for two vectors $\mathbf{x} = (x_1, \dots, x_N), \mathbf{y} = (y_1, \dots, y_N) \in \mathbb{F}(p_\eta)^N$, $\mathbf{x} \circledast \mathbf{y} = \prod_{i=1}^N x_i^{y_i}$. In Terelius-Wikström mixnet protocol, permutations are represented as matrices. More precisely, if $\pi \in \mathfrak{S}_N$ is a permutation of length N, its representation in the form of a matrix is $M_\pi = \left(m_{i,j}^{(\pi)}\right)_{1 \leqslant i,j \leqslant N}$ where, for all $i, j \in [\![1; N]\!]$, $m_{i,j}^{(\pi)} = \delta_{i\pi(j)}$ (where $\delta_{i\pi(j)} = 1$ when $i = \pi(j)$). We define the predicate $\mathbf{perm}_N\ M_\pi$ to hold when M_π is a permutation matrix.

Terelius-Wikström mixnet protocol is split into two parts, an *offline* one and an *online* one. First, at the same time as the election setup, during the *offline phase*, each mix-server chooses a random permutation $\pi \xleftarrow{\$} \mathfrak{S}_N$ and publishes a *commitment* to the matrix M_π representing this permutation π. In other words, each mix-server chooses a random vector $\mathbf{s} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ and publishes the value $\mathbf{a} \leftarrow \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, M_\pi\, ; \mathbf{s})$ where the commitment algorithm $\mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}$ is based on Pedersen's commitment scheme. In doing so, each mix-server publicly promises to use the permutation π without revealing it. Later, just before the tally of the election, the *online phase* will consist of the ballot box mixing procedure, which goal is to erase the link between ballots and voters, ensuring ballot privacy. During this phase, each mix-server takes on its turn the list of ballots in the ballot box $\mathbf{b}^{(\mathrm{in})}$, and outputs a permutted and re-randomized version of this list of ballots $\mathbf{b}^{(\mathrm{out})}$. Besides, each phase of the protocol comes with a zero-knowledge proof attesting that the target property is satisfied.

Before going deeper into details, let us point out the properties that any mix-server should satisfy:

- **(Correctness)** When both mix-server and verifier are honest, a mix-server must keep the content of each ballot untouched, and the proof transcripts produced by the mix-server must be accepted by the verifier. More precisely, the decryption of the input list of ballots and the decryption of the output list of ballots are equal as multisets. Actually, as this property has been shown in [4] and [16], we will not linger on it.
- **(Permutation secrecy)** When the mix-server is honest but the verifier is dishonest, *i.e.* is controlled by an adversary $\mathcal{A}$, the mix-server blurs the link between the output list of ballots and the input one. That is, the adversary $\mathcal{A}$ cannot link ballots to voters.
- **(Verifiability)** This property aims to verify that a mix-server does not cheat, under the assumptions that the mix-server is controlled by an adversary $\mathcal{A}$ and the verifier is

honest. More precisely, it is achieved if $\mathcal{A}$ cannot produce any proof transcript accepted by the verifier while the decryption of the output list of ballots is not a permutation (up to re-encryption) of the input one.

III. The CCSA logic

We briefly recall in this section the very key concepts of the Computationally Complete Symbolic Attacker (CCSA) logic [12]. This logic is a first-order logic built on (higher-order) terms, using *names* to denote random samplings, and a subset of functions to represent the adversarial computations. These terms are interpreted as random variables over the randomness of both the protocol and the adversary, and represent the interactions between the protocol and the adversary. Formulas are built on top of two main predicates: $[\phi]$ which denotes that a formula (a term of type **bool**) is true with overwhelming probability, and $\mathbf{u} \sim \mathbf{v}$ that states that no probabilistic polynomial-time adversary can distinguish between the distributions of the lists of terms $\mathbf{u}$ and $\mathbf{v}$ with non-negligible probability.

A. Terms

Types in the CCSA logic are built on a set of *base types* $\mathbb{T}$ using the usual type arrow $\rightarrow$. Notably, we assume that *base types* include at least **bool**, **nat**, **real** and **msg** (this latter to model bitstrings). A *type structure* $\mathbb{M}$ defines an interpretation $\llbracket\tau\rrbracket^{\eta}_{\mathbb{M}}$ for each base type $\tau \in \mathbb{T}$ and security parameter η. The interpretation of standard types is the standard one, and function types are defined as usual. A type is said to be *finite* if, for any η, its interpretation is finite.

The terms considered in the CCSA logic are simply-typed λ-terms built upon a set of variables $\mathcal{X}$:

$$t ::= x \mid t\ t\ |\lambda(x : \tau).t \mid \forall(x : \tau).t$$

Variables represent function arguments, logical variables and function symbols (e.g. cryptographic functions) declared in an *environment*.

An *environment* consists in variable declarations $(x : \tau)$ and variable definitions $(x : \tau = t)$. We assume that environments declare at least the standard boolean operations (e.g. $\wedge, \vee$), integer operations, real operations, and a number of standard functions (in particular an **if** **then** construct). Note that environments allow for well-founded recursive definitions.

A *model* $\mathbb{M}$ for a term structure $\mathcal{E}$ consists, for every η, of two sets of random tapes: $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ (the *honest* randomness) and $\mathbb{T}^{\mathsf{a}}_{\mathbb{M},\eta}$ (the *adversarial* randomness). It defines, for every declared variable $(x : \tau)$ and every security parameter η, a $\llbracket\tau\rrbracket^{\eta}_{\mathbb{M}}$ valued random variable $\rho \in \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta} \times \mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta} \mapsto \llbracket x\rrbracket^{\eta,\rho}_{\mathbb{M}}$. This interpretation $\llbracket\cdot\rrbracket^{\eta,\rho}_{\mathbb{M}}$ is naturally lifted to terms. We require that usual functions are interpreted in the standard way.

Example 1. *For all $n \in \llbracket 1; N\rrbracket$, for all $i \in \llbracket 1; n\rrbracket$, we define term $\mathbf{i}$ to be the i-th canonical vector $\mathbf{u}_i \in \mathbb{F}(p_\eta)^n$ where, for all $j \in \llbracket 1; n\rrbracket$, $(\mathbf{u}_i)_j = \delta_{ij}$. Therefore, we have $\llbracket\mathbf{i}\rrbracket^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = \mathbf{u}_i$ for all security parameter η and all random tape $\rho \in \mathbb{T}$.*

We call *names* a subset $\mathcal{N} \subset \mathcal{X}$ of variables, which represents honest random samplings. Names can only be declared in an environment, and are of type $\tau_0 \rightarrow \tau_b$ where τ_b is a base type. Names are interpreted as a sequence of *independent identically distributed random samplings* from the honest randomness $\mathbb{T}^{\mathsf{h}}_{\mathbb{M},\eta}$ to τ_b. This means that we require that two different names, or the same name used with two different indices, do not "use" the same part of the random tape. Contrary to [12], we do not require that τ_0 is a finite type, however we require that all formulas involving names are guarded by a condition ensuring that they only use, for every η, a finite number of indices, which achieves the same effect. This allows us to define a recursive term of type **nat** $\rightarrow$ **msg** that returns a list of randomnesses of arbitrary size. It is then only used under the assumption that its argument is bounded for every η.

B. Formulas

Formulas of the CCSA logic are standard first-order formulas built on top of the first-order terms, with predicates designed to capture cryptographic reasoning. We write $\tilde{\vee}, \tilde{\wedge}, \tilde{\exists}, \ldots$ for the usual global logical connectors, in order to distinguish them from their local counterparts that appear in terms. The semantics of the logic is the usual first-order semantics, where $\mathbb{M} \models F$ means that F holds in $\mathbb{M}$.

We now recall the definition of the main predicates of the CCSA logic given in [12]. To capture cryptographic properties, we need to define what is a small enough success probability for the adversary.

Definition 1. *A function $f : \mathbb{N} \rightarrow \mathbb{R}$ is* negligible *if for all polynomials P, we asymptotically have $f(\eta) \leq \frac{1}{P(\eta)}$.*

Predicate $[\phi]$ denotes the fact that the formula ϕ (*i.e.* a term of type **bool**) is almost always true. Precisely, $\mathbb{M} \models [\phi]$ holds when $\eta \mapsto \Pr_\rho\left[\ \llbracket\phi\rrbracket^{\rho;\eta}_{\mathbb{M}}\ \right]$ is negligible in η.

Predicate $\sim$ captures computational indistinguishability. If $\mathbf{u}$ and $\mathbf{v}$ are lists of terms with matching types, $\mathbf{u} \sim \mathbf{v}$ holds if, for any probabilistic polynomial-time Turing machine $\mathcal{A}$,

$$\left|\Pr_\rho\left[\ \mathcal{A}(1^\eta, \llbracket\mathbf{u}\rrbracket^{\rho;\eta}_{\mathbb{M}}, \rho_a)\ \right] - \Pr_\rho\left[\ \mathcal{A}(1^\eta, \llbracket\mathbf{v}\rrbracket^{\rho;\eta}_{\mathbb{M}}, \rho_a)\ \right]\right|$$

is negligible in η. Note that $\mathcal{A}$ is given access to the adversarial randomness from the model.

Predicate $\mathbf{adv}(u)$ expresses that the term u can be computed by the adversary in polynomial time. Predicate **det** states that a term does not depend on randomness (i.e. is a constant for each η). Predicate $\mathbf{pbound}(u)$ states, for a term of type **nat**, that $\llbracket u\rrbracket^{\rho;\eta}_{\mathbb{M}}$ is bounded by a polynomial in η.

The logic given in [12] is equiped with a proof system that allows to reason at two levels: the *local* level (i.e. for a fixed randomness), and *global* level (i.e. first-order reasoning on the predicates given above). A *global* judgement $\mathcal{E}; \Theta \vdash F$ states that F is entailed by global hypotheses Θ in environment $\mathcal{E}$:

$$\models \mathcal{E}; \Theta \vdash F \text{ if } \models (\tilde{\bigwedge}\Theta) \tilde{\rightarrow} F.$$

A *local* judgement $\mathcal{E};\Theta;\Gamma \vdash \phi$ states that under global hypotheses Θ, Γ almost always entails ϕ (a term of type **bool**):

$$\models \mathcal{E};\Theta;\Gamma \vdash \phi \text{ if } \models (\tilde{\bigwedge}\Theta)\tilde{\rightarrow}[(\wedge\Gamma) \rightarrow \phi].$$

In order to ensure that terms never need to be evaluated on unbounded randomnesses, and thus that all probabilities are well defined, we ensure that all formulas appearing in our proofs satisfy the following syntactic condition: for every term k used as index for names in ϕ or F, we have $\mathbf{pbound}(k)$ as a global hypothesis.

The proof system proposed in [12] also provides generic reasoning rules for logical connectives, together with a number of rules dealing with simple properties of the predicates which we do not recall here.

IV. Modelling cryptographic properties

We provide axioms for cryptographic constructions needed to model the protocol. First, we model *commitment schemes* to reveal only a fingerprint of the permutation used. Then, we model Σ-*protocols*, a kind of interactive zero-knowledge proofs used to prove the good behavior of a mixnet. Finally, we model an abstraction of the shuffle performed by a mix-server, with so-called *shuffle-friendly* maps. In this section, we focus only on how to model these cryptographic constructions in the CCSA logics. For readers who are not familiar with these advanced cryptographic objects, we provide detailed definitions and security properties statements in Appendix A.

A. Commitment schemes

Commitment schemes are used to commit to an information without revealing it directly; the committed information is first sealed and can eventually be revealed later, but its value cannot be modified between commitment and opening steps. We denote by $\mathcal{M}$ the set of messages we commit to. More formally, a *commitment scheme for a set of messages* $\mathcal{M}$ is a pair of algorithms $\mathbb{KS}[\mathcal{M}] = (\mathbf{gencomkey}, \mathbf{com})$ where

- $[\![\mathbf{gencomkey}]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$ defines an algorithm which outputs a commitment key ck and defines the set $\mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$ of randoms used to commit, as well as the set $\mathcal{K}_{\mathcal{M}}$ of commitment messages.
- $\mathbf{com} : \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg}$ is a deterministic algorithm outputting commitment message a; it takes as inputs a commitment key ck, a message $m \in \mathcal{M}$ and a randomness $r \in \mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$.

A commitment scheme has two cryptographic properties: the *hiding* property and the *binding* property. For both properties, the commitment key ck is honestly computed by a setup oracle.

- **(Hiding property)** The *hiding* property states that for any given commitment message a, no polynomial-time adversary can break a to obtain an opening information (m, r) such that $a = \mathbf{com}\ ck\ m\ r$. The underlying cryptographic game $\text{Hiding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}(\eta, \rho\,;\,\beta)$ is a classic left-right game with some secret bit $\beta \in \{0,1\}$ and can be found in Appendix A. An adversary against this game is given by a pair of probabilistic polynomial-time adversaries $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}})$ such that $\mathcal{A}_{\mathsf{setup}}$ generates a challenge consisting of two messages $m_0, m_1 \in \mathcal{M}$ with $m_0 \neq m_1$, while $\mathcal{A}_{\mathsf{guess}}$ tries to guess β from the output of the commitment oracle, which has committed to message m_β. $\mathcal{A}$ wins the game $\text{Hiding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}(\eta, \rho\,;\,\beta)$ when β is correctly guessed by $\mathcal{A}_{\mathsf{guess}}$. We formalize this property by the rule G.Com:Hide (see Fig. 1).
- **(Binding property)** The *binding* property states that a commitment message a can only be opened to a single message m, the one used to compute a. Identifying the function **com** with a hash function, we see this property as the collision resistance property usually set for hash functions. Therefore, the idea behind the cryptographic game $\text{Binding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}(\eta, \rho)$ is to leave the choice of challenge messages to the adversary $\mathcal{A}$. They have to produce two messages $m_1, m_2 \in \mathcal{M}$ with two randoms $r_1, r_2 \in \mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$, and send these two pairs (m_1, r_1) and (m_2, r_2) to the commitment oracle, which produces honest commitments $c_1, c_2 \in \mathcal{K}_{\mathcal{M}}$ from these two pairs. The adversary $\mathcal{A}$ wins the game $\text{Binding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}(\eta, \rho)$ when $c_1 = c_2$ but $(m_1, r_1) \neq (m_2, r_2)$. We formalize this rule by L.Com:Bind (see Fig. 1).

B. Σ-protocols

Let $\mathcal{R} \subset \mathcal{PP}_{\mathcal{R}} \times \mathcal{X}_{\mathcal{R}} \times \mathcal{W}_{\mathcal{R}}$ be a polynomial-time computable relation. For triplets $(\sigma, x, w) \in \mathcal{R}$, we denote by $\sigma \in \mathcal{PP}_{\mathcal{R}}$ the *public parameter*, by $x \in \mathcal{X}_{\mathcal{R}}$ the *statement*, and by $w \in \mathcal{W}_{\mathcal{R}}$ the *witness*. We define the set $\mathcal{L}_{\mathcal{R}}(\sigma) \overset{\text{def}}{=} \{x \in \mathcal{X}_{\mathcal{R}} \mid \exists\, w \in \mathcal{W}_{\mathcal{R}}, (\sigma, x, w) \in \mathcal{R}\}$ to be the language set of the binary relation $\mathcal{R}$. Besides, given a security parameter $\eta \in \mathbb{N}^*$ and a random tape $\rho \in \mathbb{T}$, the property $[\![\mathbf{zkp\text{-}rel}_{\mathcal{R}}\ \sigma\ x\ w]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$ holds for a public parameter σ, a statement x and a witness w when $([\![\sigma]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}, [\![x]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}, [\![w]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}) \in \mathcal{R}$. A Σ-*protocol for the computable relation* $\mathcal{R}$ is a 3-message protocol $\Sigma_{\mathcal{R}}$ between two agents, a prover $\mathcal{P}$ and a verifier $\mathcal{V}$. These agents and the setup phase $\mathcal{S}$ are formalized as probabilistic polynomial-time Turing machines. Note that the statement x is a public input of both $\mathcal{P}$ and $\mathcal{V}$, while the witness w is known only by $\mathcal{P}$. The prover $\mathcal{P}$ first sends a so-called *commit message* to initiate the interaction. Then, the verifier $\mathcal{V}$ sends back a random *challenge* (chosen *uniformly at random* in the challenge space), to which $\mathcal{P}$ responds. A Σ-protocol $\Sigma_{\mathcal{R}}$ is then defined by three functions $\mathbf{zkp\text{-}com}_{\mathcal{R}}$, $\mathbf{zkp\text{-}res}_{\mathcal{R}}$ and $\mathbf{zkp\text{-}verif}_{\mathcal{R}}$, corresponding to executions of honests prover $\mathcal{P}$ and verifier $\mathcal{V}$:

- $\mathbf{zkp\text{-}com}_{\mathcal{R}} : \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg}$ computes, from an input $(\sigma, x, w) \in \mathcal{R}$, a *commit message* α;
- $\mathbf{zkp\text{-}res}_{\mathcal{R}} : \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg}$ computes a *response message* $z(c)$ from an input $(\sigma, x, w) \in \mathcal{R}$ and a *challenge* c;
- $\mathbf{zkp\text{-}verif}_{\mathcal{R}} : \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{msg} \rightarrow \mathbf{bool}$ takes as input a public parameter σ, a statement x and a *proof transcript* $\langle \alpha, c, z(c) \rangle$ and outputs a Boolean $b : \mathbf{bool}$ whether or not the verifier is convinced by the proof transcript.

For ease of notation, we will use function $\textbf{zkp-prove}_{\mathcal{R}} : \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg}$ as a macro for

$$\textbf{zkp-prove}_{\mathcal{R}}\ \sigma\ x\ w\ (r\ i) \overset{\text{def}}{=} \langle \textbf{zkp-com}_{\mathcal{R}}\ \sigma\ x\ w, r\ i, \textbf{zkp-res}_{\mathcal{R}}\ \sigma\ x\ w\ (r\ i)\rangle.$$

We denote by $\Big(\mathcal{P}(w) \rightleftharpoons^{(\Sigma)}_{\mathcal{R}} \mathcal{V}\Big)(\sigma, x)$ *the* Σ*-protocol interaction* between the prover $\mathcal{P}$ and the verifier $\mathcal{V}$ as described above by the macro $\textbf{zkp-prove}_{\mathcal{R}}$. Note that functions $\textbf{zkp-prove}_{\mathcal{R}}$ and $\textbf{zkp-verif}_{\mathcal{R}}$ must satisfy $\textbf{zkp-verif}_{\mathcal{R}}\ \sigma\ x\ (\textbf{zkp-prove}_{\mathcal{R}}\ \sigma\ x\ w\ (r\ i)) = \top$. Besides, a Σ-protocol must satisfy the two following properties:

- **(Special-soundness)** $\Sigma_{\mathcal{R}}$ is said to be *special-sound* when there exists a polynomial-time extractor $\mathcal{E}_{\mathcal{R}}$ given by the function $\textbf{zkp-extract}_{\mathcal{R}} : \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg}$, such that the witness extraction is possible when two proof transcripts $\mathfrak{p}_{\mathcal{R}}^{(i)} \overset{\text{def}}{=} \langle \alpha, c_i, z(c_i)\rangle$, $i \in \{1, 2\}$, are accepted by the verifier for the same commitment message α but for different challenges $c_1 \neq c_2$. Informally, $\Sigma_{\mathcal{R}}$ is special-sound when any prover producing a proof accepted by the verifier for the witness-statement pair $(\sigma, x, w) \in \mathcal{R}$ "knows" the witness w. We formalize this rule by L.Σ-P:SpSound (see Fig. 1).
- **(Honest-Verifier Zero-Knowledge)** This property is surely the trickiest one. The key idea is to state that any proof accepted by an honest verifier $\mathcal{V}$ leaks no information about a witness w of a witness-statement triplet $(\sigma, x, w) \in \mathcal{R}$. More precisely, $\Sigma_{\mathcal{R}}$ is said to be *honest-verifier zero-knowledge* (HVZK) when there exists a polynomial-time simulator $\mathcal{S}\mathsf{im}_{\mathcal{R}}$ (given by the function $\textbf{zkp-sim}_{\mathcal{R}} : \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg}$) such that, on a public parameter σ, a statement $x \in \mathcal{L}_{\mathcal{R}}(\sigma)$ and a random challenge c, outputs an accepting interaction $\langle \alpha, c, z\rangle$ with the same probability distribution as honest interactions $\Big(\mathcal{P}(w) \rightleftharpoons^{(\Sigma)}_{\mathcal{R}} \mathcal{V}(c)\Big)(\sigma, x)$ between the honest prover $\mathcal{P}$ and the honest verifier $\mathcal{V}$ where w is the witness for the statement x (*i.e.* $(\sigma, x, w) \in \mathcal{R}$) and where the verifier $\mathcal{V}$ must send the challenge c. We formalize this property by the rule G.Σ-P:HVZK (see Fig. 1).

In the case of Terelius-Wikström protocol, we define a family of Σ-protocols $(\Sigma_{\mathcal{R}}(\mathbf{e}))_{\mathbf{e} \in \mathbb{F}(p_\eta)^N}$ for a family of binary relations $(\mathcal{R}(\mathbf{e}))_{\mathbf{e} \in \mathbb{F}(p_\eta)^N}$, each Σ-protocol and relation being associated to a specific vector $\mathbf{e} \in \mathbb{F}(p_\eta)^N$. For a given vector $\mathbf{e}$, the corresponding Σ-protocol is defined by adding a first challenge vector $\mathbf{e}$ sent by the verifier at the very beginning of the Σ-protocol, the following steps being those of a standard Σ-protocol, but for a relation depending on $\mathbf{e}$.

C. Shuffle-friendly *maps*

In their works, Terelius-Wikström generalize the rerandomization of the encryption and potential partial decryption performed by a mix-server, by a so-called *shuffle-friendly* map $\phi_{\mathbb{CS}}$. Formally, each ballot in the ballot box is encrypted using a cryptosystem $\mathbb{CS}$ allowing re-encryption (typically, an homomorphic cryptosystem is well-suited to encrypt ballots).

To achieve semantic security, the encryption algorithm $\mathrm{Enc}_{\mathbb{CS}}$ is a (see Fig. 1) non-deterministic algorithm using some random r as randomness: for a plaintext $m \in \mathcal{M}_{\mathbb{CS}}$ the encryption of m under the public key $pk = \mathtt{pk}_{\mathbb{CS}}(sk)$ is $c = \mathrm{Enc}_{\mathbb{CS}}(pk, m\,; r)$,where $r \overset{\$}{\leftarrow} \mathcal{R}_{\mathbb{CS}}$ is chosen uniformly at random. From this ciphertext c, we re-encrypt the plaintext m without decrypting the ciphertext, by multiplying c by the encryption of 1 using another random value $r' \overset{\$}{\leftarrow} \mathcal{R}_{\mathbb{CS}}$. That is, if c' is the new ciphertext, then the re-encryption algorithm $\mathrm{ReEnc}_{\mathbb{CS}}$ computes: $c' = \mathrm{ReEnc}_{pk}(c\,; r') \overset{\text{def}}{=} c \cdot \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,; r')$. A ciphertext c is said to be *well-formed for a secret key sk* when c can be decrypted with the secret key sk. We denote it $\textbf{wf\_ctxt}\ sk\ c$, and this means:

$$[\![\textbf{wf\_ctxt}\ sk\ c]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1 \iff \mathrm{Dec}_{\mathbb{CS}}([\![sk]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}, [\![c]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}) \neq \bot$$

We extend this predicate to ciphertexts lists $\mathbf{c}$ of length n as expected: $\textbf{wf\_ctxt}_n\ sk\ \mathbf{c} \leftrightarrow \bigwedge_{i=1}^{n}(\textbf{wf\_ctxt}\ sk\ \langle \mathbf{c} \mid \mathbf{i}\rangle)$. A map $\phi_{\mathbb{CS}} : \mathcal{PK}_{\mathbb{CS}} \times \mathcal{C}_{\mathbb{CS}} \times \mathcal{R}_{\mathbb{CS}} \longrightarrow \mathcal{C}_{\mathbb{CS}}$ is called *a shuffle-friendly map for a cryptosystem* $\mathbb{CS}$ if it defines an homomorphic map, *i.e.*, for all public key $pk \in \mathcal{PK}_{\mathbb{CS}}$, for all ciphertexts $c, c' \in (\mathcal{C}_{\mathbb{CS}}, \cdot)$ using the public key pk, and for all randomnesses $r, r' \in (\mathcal{R}_{\mathbb{CS}}, +)$, we have $\phi_{\mathbb{CS}}(pk, c \cdot c'\,; r + r') = \phi_{\mathbb{CS}}(pk, c\,; r) \cdot \phi_{\mathbb{CS}}(pk, c'\,; r')$. We model these *shuffle-friendly* maps $\phi_{\mathbb{CS}}$ in the CCSA model by supplying a function $\textbf{shuf-map}_{\phi_{\mathbb{CS}}} : \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg} \rightarrow \textbf{msg}$. Roughly speaking, two different modes can be considered, separately or together: re-encryption or partial decryption. In the CCSA logic, we denote by $\textbf{dec}_{\mathbb{CS}}$ the decryption predicate of a single ciphertext, and by $\textbf{dec-list}^{(n)}_{\mathbb{CS}}$ the decryption of a ciphertexts list of length n.

To be used in a mixnet protocol, a *shuffle-friendly* map $\phi_{\mathbb{CS}}$ must satisfy the following three properties.

- **(Decryption preservation)** Firstly, $\phi_{\mathbb{CS}}$ must keep the content of each ballot untouched. For this property, we assume that the public key pk is honestly computed from a secret key sk, *i.e.* we have $pk = \mathtt{pk}_{\mathbb{CS}}\ sk$. Therefore, we say that $\phi_{\mathbb{CS}}$ *preserves decryption* when, for all ciphertexts $c, c' \in \mathcal{C}_{\mathbb{CS}}$ such that, if (i) c is an encryption of a message $m \in \mathcal{M}_{\mathbb{CS}}$ under public key pk, and (ii) there exists a random value $r' \in \mathcal{R}_{\mathbb{CS}}$ such that $c' = \phi_{\mathbb{CS}}(pk, c\,; r')$, then we have $\mathrm{Dec}_{\mathbb{CS}}(sk, c') = \mathrm{Dec}_{\mathbb{CS}}(sk, c) = m$. This proves the soundness of rule L.Sfm:Correct (see Fig. 1). Notice that for each new definition of a *shuffle-friendly* map, one has to prove that this new map satisfies the decryption preservation property.
- **(Associated Zero-Knowledge Proof)** Secondly, we want to get a Σ-protocol $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$ proving that a ciphertext $c' \in \mathcal{C}_{\mathbb{CS}}$ is computed with $\phi_{\mathbb{CS}}$ from a ciphertext $c \in \mathcal{C}_{\mathbb{CS}}$ and a random value $r' \in \mathcal{R}_{\mathbb{CS}}$. This property can be characterized by an associated relation $\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$, called *shuffle-friendly* map relation, which is given by

$$(pk, (c, c'), r') \in \mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}} \overset{\text{def}}{\iff} c' = \phi_{\mathbb{CS}}(pk, c\,; r').$$

- **(Indistinguishability of $\phi_{\mathbb{CS}}$ output)** Finally, we do not want $\phi_{\mathbb{CS}}$ to leak any information about the supplied ciphertext $c \in \mathcal{C}_{\mathbb{CS}}$. Let $c, c' \in \mathcal{C}_{\mathbb{CS}}$ be two ciphertexts such that $c' = \phi_{\mathbb{CS}}(pk, c\,;\,r')$ and $c = \mathrm{Enc}_{\mathbb{CS}}(pk, m\,;\,r)$, where $m \in \mathcal{M}_{\mathbb{CS}}$ is a message and $r, r' \in \mathcal{R}_{\mathbb{CS}}$ are random values. We need to make sure that no adversary can distinguish whether c' has been computed by $\phi_{\mathbb{CS}}$ from a ciphertext $c_0 \in \mathcal{C}_{\mathbb{CS}}$ or some other $c_1 \in \mathcal{C}_{\mathbb{CS}}$. Therefore, we define a new cryptographic game $\text{Ind-CCA}^{\mathcal{A}}_{\phi_{\mathbb{CS}},\,\textbf{valid}}(\eta, \rho\,;\,\beta)$ to be a left-right game with some secret $\beta \in \{0, 1\}$. An adversary against this game is given by a pair of probabilistic polynomial-time adversaries $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}})$. The first sub-adversary $\mathcal{A}_{\mathsf{setup}}$ generates two ciphertexts $c_0, c_1 \in \mathcal{C}_{\mathbb{CS}}$ with $c_0 \neq c_1$ and a proof v that these ciphertexts satisfy the **valid** predicate, which is an over-approximation property of the well-formed predicate **wf_ctxt**: **valid** $(\mathrm{pk}_{\mathbb{CS}}\ sk)\ c\ v \rightarrow$ **wf_ctxt** $sk\ c$. We extend this predicate to ciphertexts list $\mathbf{c}$ in the following way:

$$\textbf{valid}_n\ (\mathrm{pk}_{\mathbb{CS}}\ sk)\ \mathbf{c}\ v \rightarrow \textbf{wf\_ctxt}_n\ sk\ \mathbf{c} \\ \wedge \bigwedge_{1 \leqslant i < j \leqslant n} (\textbf{len}\ \langle \mathbf{c} \mid \mathbf{i} \rangle = \textbf{len}\ \langle \mathbf{c} \mid \mathbf{j} \rangle)$$

  Then, the second sub-adversary $\mathcal{A}_{\mathsf{guess}}$ tries to guess β from the output of the oracle which applies $\phi_{\mathbb{CS}}$ on ciphertext c_β. Adversary $\mathcal{A}$ wins the game $\text{Ind-CCA}^{\mathcal{A}}_{\phi_{\mathbb{CS}},\,\textbf{valid}}(\eta, \rho\,;\,\beta)$ when β is correctly guessed by $\mathcal{A}_{\mathsf{guess}}$. When $\mathcal{A}$ wins the game with negligible advantage, the rule G.Sfm:IndCCA (see Fig. 1) is sound.

V. CCSA logic to prove Terelius-Wikström mixnet protocol

Now we have given general background about the protocol and some formalizations of the cryptographic primitives and properties, we dive into this section in the core of our contributions and show how to precisely formalize and prove the security properties of the protocol with the CCSA logic. Notice that we will not details proofs of soundness of CCSA rules here. They can be found in Appendix D, alongside a figure which recap all the rules we need.

A. Linking the protocol description with the CCSA logic

a) A more precise description: To define a commitment scheme for a matrix, we first define a commitment scheme for vectors in $\mathbb{F}(p_\eta)^N$ based on Pedersen's commitment scheme. Then, the commitment algorithm **com-mat** for a matrix in $\mathsf{Mat}_N(\mathbb{F}(p_\eta))$ is based on this commitment scheme for vectors **com-vec** with the exception that the randomness space is $\mathbb{F}(p_\eta)^N$ and the commitment space is $\mathbb{G}^N_{p_\eta}$. For a matrix M, a commitment key ck and a random vector $\mathbf{s}$, the commitment message $\mathbf{a} =$ **com-mat** $ck\ M\ \mathbf{s}$ to matrix M is defined by $\langle \mathbf{a} \mid \mathbf{i} \rangle \overset{\text{def}}{=}$ **com-vec** $ck\ (M \cdot \mathbf{i})\ \langle \mathbf{s} \mid \mathbf{i} \rangle$. Both above-mentioned commitment schemes are *perfectly hiding* and *computationally binding* under the *Discrete Logarithm* assumption for the group $\mathbb{G}_{p_\eta}$. During the *offline* phase, each mix-server must produce a valid commitment message to the secret permutation matrix it chose. The corresponding zero-knowledge proof proving this step is based on an algebraic result of characterization of a permutation matrix. Indeed, a matrix $M \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))$ is a permutation matrix if and only if (i) $M \cdot \mathbf{1} = \mathbf{1}$ and (ii) for all vector $\mathbf{e} = (e_1, \ldots, e_N) \in \mathbb{F}(p_\eta)^N$, $\prod_{i=1}^N (M \cdot \mathbf{e})_i = \prod_{i=1}^N e_i$.

Definition 2 (Correct commitment relation)**.** *Let* $\mathbf{a} \in \mathbb{G}^N_{p_\eta}$ *be a vector. Let* $ck \leftarrow \mathrm{Gen}_{\mathbb{F}(p_\eta)^N}(1^\eta, N) \in \mathbb{G}^{N+1}_{p_\eta}$ *be a commitment key of Pedersen commitment scheme* $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$*. Let* $\mathbf{e} \in \mathbb{F}(p_\eta)^N$ *be a vector. We define* $\mathcal{R}^{\mathit{com}}(\mathbf{e})$ *to be the* relation of correct commitment for vector $\mathbf{e}$*:*

$$((ck, \mathbf{e}), \mathbf{a}, (t, \mathbf{e}', k)) \in \mathcal{R}^{\mathit{com}}(\mathbf{e}) \\ \overset{\mathit{def}}{\Longleftrightarrow} \begin{cases} \mathbf{a} \circledast \mathbf{1} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{1}\,;\,t) \\ \wedge\ \mathbf{a} \circledast \mathbf{e} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'\,;\,k) \\ \wedge\ \prod_{i=1}^N e'_i = \prod_{i=1}^N e_i. \end{cases}$$

During the *online* phase, a mix-server has to use the same permutation (than the one picked up and committed during the *offline* phase) to permute the input list of ballots and transform it thanks to the *shuffle-friendly* map $\phi_{\mathbb{CS}}$. We define the following relation of correct shuffle.

Definition 3 (Correct shuffle relation)**.** *Let* $\mathbf{a} \in \mathbb{G}^N_{p_\eta}$ *be a vector of size* N*. Let* $ck \leftarrow \mathrm{Gen}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(1^\eta, N) \in \mathbb{G}^{N+1}_{p_\eta}$ *be a commitment key for the Pedersen commitment scheme* $\mathbb{KS}[\mathsf{Mat}_N(\mathbb{F}(p_\eta))]$*. Let* $(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(1^\eta) \in \mathbb{F}(p_\eta) \times \mathcal{PK}_{\mathbb{CS}}$ *be a key pair and* $\phi_{\mathbb{CS}}$ *be a* shuffle-friendly *map for the cryptosystem* $\mathbb{CS}$*. Let* $\mathbf{c}, \mathbf{c}' \in \mathcal{C}^N_{\mathbb{CS}}$ *be two lists of ciphertexts. Let* $\mathbf{e} \in \mathbb{F}(p_\eta)^N$ *be a vector. We define* $\mathcal{R}^{\mathit{shuffle}}_{\phi_{\mathbb{CS}}}(\mathbf{e})$ *to be the* relation of correct shuffle for vector $\mathbf{e}$*:*

$$((ck, pk, \mathbf{e}), (\mathbf{a}, \mathbf{c}, \mathbf{c}'), (\mathbf{e}', k, u)) \in \mathcal{R}^{\mathit{shuffle}}_{\phi_{\mathbb{CS}}}(\mathbf{e}) \\ \overset{\mathit{def}}{\Longleftrightarrow} \begin{cases} \mathbf{a} \circledast \mathbf{e} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'\,;\,k) \\ \wedge\ (pk, (\mathbf{c} \circledast \mathbf{e}, \mathbf{c}' \circledast \mathbf{e}'), u) \in \mathcal{R}^{\mathit{map}}_{\phi_{\mathbb{CS}}}. \end{cases}$$

Again, if $\mathbf{a}$ is a commitment message to a matrix M, we get $M \cdot \mathbf{e} = \mathbf{e}'$ from the first equality and the binding property. Hence, by an algebraic argument (that we will explain later), we conclude the existency, with overwhelming probability, of a vector of random values $\mathbf{r} = (r_i)_{i=1}^N \in \mathbb{F}(p_\eta)^N$ such that we have, for all $i \in [\![1; N]\!]$, $c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\,r_i)$. For ease of notation, we denote by $\textbf{shuffle}_{\phi_{\mathbb{CS}}}\ pk\ \mathbf{c}\ \pi\ \mathbf{r}$ the function outputting the ciphertexts list term $\mathbf{c}'$ with the semantics defined above. Concrete definitions of Σ-protocols for both relations of correct commitment $\mathcal{R}^{\mathsf{com}}(\mathbf{e})$ and of correct shuffle $\mathcal{R}^{\mathsf{shuffle}}_{\phi_{\mathbb{CS}}}(\mathbf{e})$ can be found in [4].

b) Formalization and axiomatization in the CCSA logic: We model the execution of Terelius-Wikström shuffle protocol in the CCSA logic with the help of a macro $\textbf{mix}_{\phi_{\mathbb{CS}}}/4$, considered as a function symbol of arity 4. More precisely, for a permutation matrix term π : $\textbf{matrix}_N$, for a commitment key parameter term ck : **comkey**, for a public key term $(\mathrm{pk}_{\mathbb{CS}}\ sk)$: **pkey**, and a pair of ciphertexts list and bitstring

G.Com:Hide

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, m_1, m_2) \qquad \mathcal{E};\Theta \vdash [\Psi^{r,i}_{\textsf{fresh}}(\mathbf{u}, m_1, m_2) \wedge \Psi^{ck,n}_{\textsf{comkey}}(\mathbf{u}, m_1, m_2)]}{\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{com}\ (ck\ n)\ m_1\ (r\ i) \sim \mathbf{u}, \mathbf{com}\ (ck\ n)\ m_2\ (r\ i)}$$

L.Com:Bind

$$\frac{\begin{array}{c}\mathcal{E};\Theta \vdash \mathbf{adv}(m_1, m_2, r_1, r_2) \qquad \mathcal{E};\Theta;\Gamma \vdash \Psi^{ck,n}_{\textsf{comkey}}(m_1, m_2)\\ \mathcal{E};\Theta;\Gamma \vdash \mathbf{com}\ (ck\ n)\ m_1\ r_1 = \mathbf{com}\ (ck\ n)\ m_2\ r_2\end{array}}{\mathcal{E};\Theta;\Gamma \vdash m_1 = m_2}$$

L.Σ-P:SpSound

$$\frac{\begin{array}{c}\mathcal{E};\Theta \vdash \mathbf{adv}(x, \mathfrak{p}^{(1)}_{\mathcal{R}}(c_1), \mathfrak{p}^{(2)}_{\mathcal{R}}(c_2)) \qquad \mathcal{E};\Theta;\Gamma \vdash c_1 \neq c_2\\ \mathcal{E};\Theta;\Gamma \vdash \bigwedge_{i\in\{1,2\}} \mathbf{zkp\text{-}verif}_{\mathcal{R}}\ (\sigma\ s)\ x\ \mathfrak{p}^{(i)}_{\mathcal{R}}(c_i)\end{array}}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{zkp\text{-}rel}_{\mathcal{R}}\ (\sigma\ s)\ x\ (\mathbf{zkp\text{-}extract}_{\mathcal{R}}\ (\sigma\ s)\ x\ \mathfrak{p}^{(1)}_{\mathcal{R}}(c_1)\ \mathfrak{p}^{(2)}_{\mathcal{R}}(c_2))}$$

G.Σ-P:HVZK

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, x, w) \qquad \mathcal{E};\Theta \vdash [\Psi^{r,i}_{\textsf{fresh}}(\mathbf{u}, x, w)]}{\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{zkp\text{-}prove}_{\mathcal{R}}\ (\sigma\ s)\ x\ w\ (r\ i) \sim \mathbf{u}, \mathbf{zkp\text{-}sim}_{\mathcal{R}}\ (\sigma\ s)\ x\ (r\ i)}$$

L.Sfm:Correct

$$\frac{\begin{array}{c}\mathcal{E};\Theta;\Gamma \vdash \mathbf{wf\_ctxt}\ sk\ c\\ \mathcal{E};\Theta;\Gamma \vdash \exists\, v.\ c' = \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ c\ v\end{array}}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{dec}_{\mathbb{CS}}\ sk\ c = \mathbf{dec}_{\mathbb{CS}}\ sk\ c'}$$

G.Sfm:IndCCA

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, c, v) \qquad \mathcal{E};\Theta \vdash [\Psi^{sk,t_0}_{\textsf{skey}}(\mathbf{u}, c, v) \wedge \Psi^{r,i}_{\textsf{fresh}}(\mathbf{u}, c, v)]}{\begin{array}{r}\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{if\ valid}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ v\ \mathbf{then\ shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ (r\ i)\\ \sim\ \mathbf{u}, \mathbf{if\ valid}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ v\ \mathbf{then\ shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ (\mathbf{0}\ (\mathbf{len}\ c))\ (r\ i)\end{array}}$$

For the rule L.Σ-P:SpSound, notation $\mathfrak{p}^{(i)}_{\mathcal{R}}(c_i)$ stands for the triplet term $\langle \alpha, c_i, z(c_i)\rangle$. For definitions of $\Psi^{r,i}_{\textsf{fresh}}(\mathbf{u}, m_1, m_2)$-like properties, see Appendix C. Roughly, it is used to ensure that the adversary does not know secret values like private keys.

Fig. 1. New cryptographic rules in CCSA

term $(\mathbf{c}, v) : \mathcal{C}^N_{\mathbb{CS}} \times \mathbf{msg}$, the term $\mathbf{mix}_{\phi_{\mathbb{CS}}}\ \pi\ ck\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c}, v)$ is a macro for the following sequence of terms:

$$\begin{array}{l}\mathbf{mix}_{\phi_{\mathbb{CS}}}\ \pi\ ck\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c}, v) \overset{\text{def}}{=} \mathbf{a}_\pi, \mathbf{e}_\pi\ t_1, (r_\pi\ j), \mathfrak{p}_\pi(\pi),\\ \quad \mathbf{if\ valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \mathbf{then}\\ \qquad\qquad\qquad \langle (\mathbf{r}\ l), \mathbf{c}'_\pi, (\mathbf{e}_\phi\ t_2), (r_\phi\ p), \mathfrak{p}_\phi(\pi)\rangle\end{array}$$

where

$$\begin{aligned}\mathbf{a}_\pi &\overset{\text{def}}{=} \mathbf{com\text{-}mat}\ ck\ \pi\ (\mathbf{s}\ i),\\ \mathfrak{p}_\pi(\pi) &\overset{\text{def}}{=} \mathbf{zkp\text{-}prove}_\pi\ (ck, \mathbf{e}_\pi\ t_1)\ \mathbf{a}_\pi\ w_\pi\ (r_\pi\ j),\\ \mathbf{c}'_\pi &\overset{\text{def}}{=} \mathbf{shuffle}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ \mathbf{c}\ \pi\ (\mathbf{r}\ l),\\ \mathfrak{p}_\phi(\pi) &\overset{\text{def}}{=} \mathbf{zkp\text{-}prove}_\phi\ (ck, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_\phi\ t_2)\ (\mathbf{a}_\pi, \mathbf{c}, \mathbf{c}'_\pi)\ w_\phi\ (r_\phi\ p).\end{aligned}$$

The (only) trace of the protocol is frame, defined as

$$\begin{array}{l}(ck\ n), (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k)), \pi, \mathbf{c}, v,\\ \qquad\qquad \big(\mathbf{mix}_{\phi_{\mathbb{CS}}}\ \pi\ (ck\ n)\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c}, v)\big).\end{array}$$

B. Algebraic properties

Proofs of verifiability strongly rely on some algebraic properties. Firstly, once enough witnesses have been extracted and have given enough equations to fully determine a matrix M and a vector $\mathbf{s}$ such that $\mathbf{a} = \mathbf{com\text{-}vec}\ ck\ M\ \mathbf{s}$ (if M is of size N, we need N equations and therefore N witnesses), we can solve the system of equations with a function $\mathbf{solve} : \mathbf{msg} \to \mathbf{msg} \to \mathbf{msg} \to (\mathbf{msg} \times \mathbf{msg})$ that outputs M and $\mathbf{s}$. This function's semantics corresponds to an adaptation of the Gaussian elimination, which is polynomial-time. For all $i \in [\![1; N]\!]$, the witness $(t, \mathbf{e}'_i, k_i) \in \mathcal{W}_{\mathcal{R}}$ for the relation of correct commitment $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_i)$ associated with the vector $\mathbf{e}_i \in \mathbb{F}(p_\eta)^N$ gives the following equation on matrix M: $\mathbf{a} \circledast \mathbf{e}_i = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'_i\,;\,k_i)$.

Actually, we have enough equations, *i.e.* we have N equations, when the vectors family $(\mathbf{e}_i)_{i=1}^N$ defines a basis of the vector space $\mathbb{F}(p_\eta)^N$, which is expressed by $\mathbf{basis}_N\ (\mathbf{e}_i)_{i=1}^N$ in the CCSA logic. As $\dim(\mathbb{F}(p_\eta)^N) = N$, we only need a free family, which is achieved with overwhelming probability for any family of vectors chosen uniformly and independently at random. Therefore, we formalize the opening of the commitment value $\mathbf{a}$ by the rule L.Open (see Fig. 2).

Secondly, once we get matrix M, we use the characterization of a permutation matrix to show that this matrix indeed represents a permutation. This characterization states that M is a permutation matrix *if and only if* the two following equations hold: (i) $M \cdot \mathbf{1} = \mathbf{1}$ and (ii) when $\mathbf{e}$ is chosen uniformly at random in $\mathbb{F}(p_\eta)^N$, then $\prod_{i=1}^N (M \cdot \mathbf{e})_i = \prod_{i=1}^N e_i$. In the CCSA model, we denote this last product operation by the function $\mathbf{prod}_N$. Actually, to model this characterization result in the CCSA model, the second condition (ii) is a bit twisted, and instead of Condition (ii), we use Equation

$$(ii') \quad \forall\, \mathbf{e} \in \mathbb{F}(p_\eta)^N, \prod_{i=1}^N (M \cdot \mathbf{e})_i = \prod_{i=1}^N e_i.$$

We characterize a permutation matrix in the CCSA logic by the rule L.π:Charac (see Fig. 2). Equations (ii) and (ii') are equivalent thanks to the *Schwartz-Zippel* lemma [23], [24], which states that, for $f_d \in \mathbb{F}(p_\eta)[X_1, \ldots, X_N]$ a non-zero multivariate polynomial of total degree $d \in \mathbb{N}$ over $\mathbb{F}(p_\eta)$ and for $\mathbf{e} \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^N$ a vector chosen uniformly at random in the vector space $\mathbb{F}(p_\eta)^N$, then $\Pr_{\mathbf{e} \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^N}\Big[\ f_d(\mathbf{e}) = 0\ \Big] \leqslant \frac{d}{p_\eta^N}$. This result can be formalized by L.Sz (see Fig. 2).

Finally, to show that matrix M has indeed been used to shuffle the input list of ciphertexts, the second zero-knowledge proof shows that for any $\mathbf{e} \in \mathbb{F}(p_\eta)^N$ chosen uniformly at random we have: $\exists\, u \in \mathbb{F}(p_\eta), \mathbf{c}' \circledast (M \cdot \mathbf{e}) = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}\,;\,u)$. By studying the set $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$ given by

$$\begin{array}{l}\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} = \big\{\mathbf{e} \in \mathbb{F}(p_\eta)^N \mid\\ \qquad\qquad \exists\, v \in \mathbb{F}(p_\eta), \mathbf{c}' \circledast (M_\pi \cdot \mathbf{e}) = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}\,;\,v)\big\},\end{array}$$

we show the equivalence between the two following properties

1) $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} = \mathbb{F}(p_\eta)^N$;
2) When vectors $\mathbf{e} \in \mathbb{F}(p_\eta)^N$ are chosen uniformly at random, we have: $\Pr_{\mathbf{e} \xleftarrow{\$} \mathbb{F}(p_\eta)^N}\left[\, \mathbf{e} \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} \,\right] > \frac{1}{p_\eta}$.

We formalize it in rule L.SFM:CHARAC (see Fig. 2).

C. Security properties

Now, let us focus on security properties. In both following properties, the commitment key parameter ck is honestly computed by the setup algorithm **gencomkey** and is publicly sent on the network to all agents. Details of corresponding cryptographic games can be found in Appendix B.

- (***Verifiability***) This property is studied under the assumption that the mix-server is controlled by an adversary $\mathcal{A}$ and the verifier behaves honestly. Intuitively, the verifiability property ensures that, as long as the mix-server provides proofs that are accepted by the verifier, the decryption of the output list of ballots is a permutation of the decryption of the input one. We state this property in the CCSA model as

$$\mathcal{E};\varnothing \vdash \left[\begin{array}{ll} & \mathbf{zkp\text{-}verif}_{\pi}\ (ck\ n, \mathbf{e}_\pi\ t_1)\ \mathbf{a}\ \langle \alpha_\pi, (r_\pi\ l), z_\pi(r_\pi)\rangle \\ \wedge & \mathbf{zkp\text{-}verif}_{\phi_{\mathbb{CS}}}\ (ck\ n, \mathrm{pk}_{\mathbb{CS}}\ (sk\ k), \mathbf{e}_\phi\ t_2)\ (\mathbf{a}, \mathbf{c}, \mathbf{c}') \\ & \qquad\qquad\qquad \langle \alpha_\phi, (r_\phi\ p), z_\phi(r_\phi)\rangle \\ \wedge & \mathbf{wf\_ctxt}_N\ (sk\ k)\ \mathbf{c} \\ & \rightarrow \\ & \mathbf{wf\_ctxt}_N\ (sk\ k)\ \mathbf{c}' \\ \wedge & \mathbf{eqm}_N\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ (sk\ k)\ \mathbf{c})\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ (sk\ k)\ \mathbf{c}') \end{array}\right]$$

  where $\mathbf{eqm}_N$ is the predicate standing for equality of lists as multisets.
- (***Permutation secrecy***) This property is studied under the assumption that the mix-server behaves honestly while the verifier is controlled by an adversary $\mathcal{A}$. The idea of the secrecy property is to show that there is no way for $\mathcal{A}$ to identify the permutation used by the mix-server if the mix-server behaves accordingly to the protocol. Let $\mathsf{frame}_{\mathsf{init}}$ denote the initial knowledge of the adversary and let Θ_{init} be the initial global context of formulas defined by

$$\mathsf{frame}_{\mathsf{init}} \overset{\text{def}}{=} (ck\ n), (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k)), \pi, \mathrm{id}, \mathbf{c}, v \quad \text{and}$$
$$\Theta_{\mathsf{init}} \overset{\text{def}}{=} [\Psi^{ck,n}_{\mathsf{comkey}}(\mathsf{frame}_{\mathsf{init}})], [\Psi^{sk,k}_{\mathsf{skey}}(\mathsf{frame}_{\mathsf{init}})]$$

  We formalize the permutation secrecy property in the CCSA logic by the following property

$$\mathcal{E};\Theta_{\mathsf{init}} \vdash \mathsf{frame}_{\mathsf{init}}, \mathbf{mix}_{\phi_{\mathbb{CS}}}\ \pi\ (ck\ n)\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c}, v)$$
$$\sim \mathsf{frame}_{\mathsf{init}}, \mathbf{mix}_{\phi_{\mathbb{CS}}}\ \mathrm{id}\ (ck\ n)\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c}, v)$$

VI. PROOF OF VERIFIABILITY

Let us remind that in the case of the verifiability property, the adversary $\mathcal{A}$ controls the mix-server while the verifier $\mathcal{V}$ behaves honestly. This property is a trace property, *i.e.* at the very end of the mix-server protocol, we check whether or not the verifiability property holds for the obtained trace, by considering all the messages exchanged between $\mathcal{A}$ and $\mathcal{V}$. More precisely, the full trace $\mathsf{frame}_{\mathsf{verif}}$ is given by

$$\mathsf{frame}_{\mathsf{verif}} \overset{\text{def}}{=} (ck\ n), \mathbf{a}, (\mathbf{e}_\pi\ t_1), \alpha_\pi, (r_\pi\ l), z_\pi(r_\pi),$$
$$sk, \mathbf{c}, \mathbf{c}', v, (\mathbf{e}_\phi\ t_2), \alpha_\phi, (r_\phi\ p), z_\phi(r_\phi)$$

where

- terms $\mathbf{a}$, α_π, $z_\pi(r_\pi)$, $(sk, \mathbf{c}, \mathbf{c}', v)$, α_ϕ, and $z_\phi(r_\phi)$ are computed by $\mathcal{A}$;
- while terms $(ck\ n)$, $(\mathbf{e}_\pi\ t_1)$, $(r_\pi\ l)$, $(\mathbf{e}_\phi\ t_2)$, and $(r_\phi\ p)$ are honestly computed by $\mathcal{V}$.

A. Sketch of verifiability proof

To prove the verifiability property, we first need to extract N witnesses for the commitment relation $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_i)$, for a vector basis $(\mathbf{e}_i)_{i=1}^N$ sent by the verifier. These witnesses are used to extract the matrix M contained in the commitment message $\mathbf{a} \in \mathbb{G}^N_{p_\eta}$. Then, by extracting one last witness for the commitment relation $\mathcal{R}^{\mathsf{com}}(\mathbf{e})$, we use the *binding* property of the commitment scheme $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ to show that M satisfies both (i) $M \cdot \mathbf{1} = \mathbf{1}$ and (ii) $\mathbf{prod}_N\ (M \cdot X) = \mathbf{prod}_N\ X$, hence concluding that M is a permutation. Finally, we extract a witness for the shuffle relation $\mathcal{R}^{\mathsf{shuffle}}_{\phi_{\mathbb{CS}}}(\mathbf{e})$, concluding that both ciphertexts lists $\mathbf{c}$ and $\mathbf{c}'$ are linked by the *shuffle-friendly* map $\phi_{\mathbb{CS}}$, meaning that for all $i \in [\![1;N]\!]$, we have the following property: $\exists\, r_i \in \mathbb{F}(p_\eta), c'_{M(i)} = \phi_{\mathbb{CS}}(\mathrm{pk}_{\mathbb{CS}}(sk), c_i\ ;\ r_i)$. Those last equations imply, by correctness of *shuffle-friendly* maps, the equality of lists $\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}(sk, \mathbf{c})$ and $\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}(sk, \mathbf{c}')$ as multisets, which is the property we wanted to prove.

To be able to extract witnesses, rewinding is necessary. Roughly speaking, this technique states that one can run the adversary $\mathcal{A}$ *twice*: $\mathcal{A}$ is run a first time, then we rewind them to a previous state, and finally run them a second time from this state. The rewinding argument is used in two different contexts. The first one is linked to the witness extraction from a Σ-protocol using the special-soundness property. As a reminder, the idea behind the special-soundness property is that: if we get two different proof transcripts for the same commitment message, then we can extract the witness for the associated relation. The second one is linked to the rebuilding of the matrix committed in the vector $\mathbf{a}$, where we need N independent linear equations. Note that if the first use of rewinding mentioned above can be abstracted as a black-box, the second one cannot. Indeed, to be able to apply the solver of linear equations system **solve**, the family of vectors $(\mathbf{e}_i)_{i=1}^N$ used to extract witnesses, and then to get the linear equations system, has to be a free family. However, even if the probability for a vector family to be free is overwhelming, the verifier must generate more than N vectors, because the adversary $\mathcal{A}$ may not give an accepted proof transcript for all the vectors produced by $\mathcal{V}$. As a matter of fact, $\mathcal{A}$ sort of *chooses* which vectors they will answer to.

B. Rewinding in the CCSA logic

The main issue when formalizing the proof is precisely how to properly formalize the rewinding argument. As mentioned

L.Open

$$\frac{\mathcal{E};\Theta;\Gamma \vdash \mathbf{basis}_N\ (\mathbf{e}_i)_{i=1}^{N} \qquad \mathcal{E};\Theta;\Gamma \vdash \bigwedge_{i=1}^{N} (\mathbf{a} \circledast \mathbf{e}_i = \textbf{com-vec}\ ck\ \mathbf{e}'_i\ k_i)}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \textbf{com-mat}\ ck\ M\ \mathbf{s}}$$

L.π:Charac

$$\frac{\mathcal{E};\Theta;\Gamma \vdash M \cdot \mathbf{1} = \mathbf{1} \qquad \mathcal{E};\Theta;\Gamma \vdash \mathbf{prod}_N\ (M \cdot X) - \mathbf{prod}_N\ X = \mathbf{0}}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{perm}_N\ M}$$

L.Sz

$$\frac{\mathcal{E};\Theta;\Gamma \vdash \Psi^{\mathbf{x},t_0}_{\mathsf{fresh}}(P) \qquad \mathcal{E};\Theta;\Gamma \vdash P(\mathbf{x}\ t_0) = 0}{\mathcal{E};\Theta;\Gamma \vdash P = \mathbf{0}}$$

L.Sfm:Charac

$$\frac{\begin{array}{c}\mathcal{E};\Theta;\Gamma \vdash \mathbf{perm}_N\ \pi \qquad \mathcal{E};\Theta;\Gamma \vdash \Psi^{\mathbf{e},t}_{\mathsf{fresh}}(\mathbf{c},\mathbf{c}',\pi) \\ \mathcal{E};\Theta;\Gamma \vdash \exists\, v.\ \mathbf{c}' \circledast (\pi \cdot (\mathbf{e}\ t)) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ pk\ (\mathbf{c} \circledast (\mathbf{e}\ t))\ v\end{array}}{\mathcal{E}, (\mathbf{x} : \mathbf{msg});\Theta;\Gamma \vdash \exists\, v_{\mathbf{x}}.\ \mathbf{c}' \circledast (\pi \cdot \mathbf{x}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ pk\ (\mathbf{c} \circledast \mathbf{x})\ v_{\mathbf{x}}}$$

In L.Open rule terms M and $\mathbf{s}$ are defined as follows: $(M, \mathbf{s}) \overset{\text{def}}{=} \textbf{solve}\ \mathbf{a}\ (\mathbf{e}_i)_{i=1}^{N}\ (\mathbf{e}'_i, k_i)_{i=1}^{N}$.

Fig. 2. New algebraic rules in CCSA

above, rewinding gets back to a past state of the adversary's computation, and run the attack process again from this state. In our case, it is used to obtain a number of proof transcripts in order to apply the special-soundness property.

Rewinding is neither a fully local construction (we need the adversary to succeed with non-negligible probability), nor a fully global one (we rewind from a state of the protocol where a portion of the randomness is fixed). In order to capture rewinding in the CCSA model, we therefore introduce two new predicates, which precisely quantify the probability of success of the adversary, globally and from a specific execution point.

First, we capture the fact that a formula is true with probability at least g. This predicate offers a quantitative version of what already exists in the CCSA framework, but with explicit lower bounds for the adversary. For a formula ϕ : **bool** and a real parameter g : **real** with **non-negl**(g), we define the global predicate ${}_{g}[\phi]$ with the following semantics:

$$[\![{}_{g}[\phi]]\!]_{\mathbb{M}\,:\,\mathcal{E}} \overset{\text{def}}{=} \forall\, \eta \in \mathbb{N}^*, \Pr_\rho \Big[\ [\![\phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big] \geqslant \mathbb{E}_\rho\big([\![g]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$

Notice that, if g is non-negligible, we have:

G.$\tilde{\neg}$:Charac

$$\frac{}{\mathcal{E};\Theta \vdash \tilde{\neg}\ [\neg\, \phi] \ \tilde{\Leftrightarrow}\ \tilde{\exists}\ (g : \mathbf{real}).\ \textbf{non-negl}(g)\ \tilde{\wedge}\ {}_{g}[\phi]}$$

The proof is quite straightforward, as if $\neg\phi$ is false with non-negligible probability, then there exists a non-negligible g such that ϕ is true with probability g.

In order to capture rewinding, we also need a local version of this predicate, quantifying the success probability of the adversary when part of the protocol state is fixed. Therefore, given a property $\phi : \tau_1 \to \cdots \to \tau_p \to$ **bool** and parameter g : **real** with **non-negl**(g), we define the **low-bound** predicate with the following semantics:

$$\begin{array}{l}\forall\, \eta \in \mathbb{N}^*, \forall\, \rho \in \mathbb{T}, [\![\textbf{low-bound}\ g\ \phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \overset{\text{def}}{=} \\ \qquad \Pr_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}},\ i \in [\![1;p]\!]} \Big[\ [\![\phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r_1, \ldots, r_p)\ \Big] \geqslant \mathbb{E}_{\rho'}\big([\![g]\!]^{\eta\,;\,\rho'}_{\mathbb{M}\,:\,\mathcal{E}}\big).\end{array}$$

This predicate captures the probability that a formula ϕ is true with non-negligible probability when part of the randomness used (everything but $r_1, \ldots, r_p$) is fixed.

These two predicates are linked by the following axiom:

G.LB:Intro

$$\frac{\mathcal{E};\Theta \vdash {}_{g}[\phi\ \mathbf{r}]}{\mathcal{E};\Theta \vdash {}_{g/2}[\textbf{low-bound}\ (g/2)\ \phi]}$$

This comes from the following fact: for a $\phi(r, s)$ property to be true with probability g, there needs to be enough values of r where the probability over s that $\phi(r, s)$ is true is large.

In fact, these axioms imply a nicer one that will be really helpful in our proofs:

G.LB:Elim

$$\frac{\mathcal{E};\Theta \vdash \tilde{\forall}\, g : \mathbf{real}.\ \textbf{non-negl}(g)\ \tilde{\wedge}\ \mathbf{det}(g)\ \tilde{\rightarrow}\ [\textbf{low-bound}\ g\ \phi \rightarrow \phi\ \mathbf{r} \rightarrow \psi\ \mathbf{r}]}{\mathcal{E};\Theta \vdash [\phi\ \mathbf{r} \rightarrow \psi\ \mathbf{r}]}$$

This axiom allows us to introduce **low-bound** conditions when proving a security property of the form $\phi \to \psi$. This is crucial for using rewinding, as rewinding is only allowed for properties that are true with non-negligible probabilities. We can now state the rewinding axiom in the CCSA logic:

Axiom 1 (Rewinding)**.** *For all polynomial-time property* $\phi \overset{\text{def}}{=} \lambda x.(\phi\ x) : \tau \to$ ***bool*** [ptime]*, for all non-negligible parameter* g : ***real*** *with* ***non-negl***(g)*, the following rule to catch the rewinding argument* [1] *is sound*

$$\begin{array}{l}\mathcal{E};\Theta \vdash \tilde{\exists}\, \textbf{\textit{select}}^{(n)}_{\mathit{rand}}.\ \tilde{\exists}\, k_g : \textbf{\textit{nat}}.\ \textbf{\textit{det}}(k_g)\ \tilde{\wedge}\ \textbf{\textit{pbound}}(k_g)\ \tilde{\rightarrow} \\ {[\textbf{\textit{low-bound}}\ g\ \phi\ \rightarrow\ \forall\, (t : \textbf{\textit{nat}}).\ (\mathbf{r}_s\ t \in \textbf{\textit{select}}^{(n)}_{\mathit{rand}}\ k_g\ \mathbf{r}_s)\ \rightarrow\ \phi\ (\mathbf{r}_s\ t)]} \\ \tilde{\wedge}\ [\forall\, (t : \textbf{\textit{nat}}).\ (\mathbf{r}_s\ t) \in \textbf{\textit{select}}^{(n)}_{\mathit{rand}}\ k_g\ \mathbf{r}_s\ \rightarrow\ (\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \ldots, \mathbf{r}_s\ k_g\}]\end{array}$$

To prove the soundness of this rewinding axiom, we define an adversarial selection function $\textbf{select}^{(n)}_{\text{rand}} : \mathbf{nat} \to (\mathbf{nat} \to \tau) \to \mathbf{set}_n(\tau)$; studying its complexity provides a concrete value for the natural number term k : **nat** which satisfies both predicates **det**(k) and **pbound**(k). The complete proof can be found in Appendix E.

But, to be able to derive a complete proof, a last ingredient is still missing. Indeed, throughout their proof, Terelius and Wikström assumed that the adversary is not able to influence the distribution of challenges for which rewinding is performed. But we need to address the fact that properties which are true with overwhelming probability are preserved under adversarial

[1] Notice that this axiom closely captures the rewinding argument: as long as a formula is true with non-negligible probability, we have a polynomial-time procedure that produces a given number of quasi-independent witnesses. A crucial point here is that g is assumed to be non-negligible, ensuring that our choice of k is, indeed, polynomial. If we drop that assumption, an exponentially small g would yield an exponential k breaking the reduction.

selection of randomness as defined previously. We address this point with the following rule:

G.SEL

$$\dfrac{\mathcal{E};\Theta\vdash \mathbf{det}(k)\ \tilde{\wedge}\ \mathbf{pbound}(k) \qquad \mathcal{E};\Theta\vdash[\phi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)] \\ \mathcal{E};\Theta\vdash[\forall\,(t:\mathbf{nat}).\ (\mathbf{r}_s\ t)\in \mathbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s \to (\mathbf{r}_s\ t)\in\{\mathbf{r}_s\ 1,\ldots,\mathbf{r}_s\ k\}]}{\mathcal{E};\Theta\vdash[n\leqslant k\to\phi\ (\mathbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]}$$

This rule states that if a property ϕ holds with overwhelming probability over a set of random samplings, then it still holds even if the adversary is allowed to select the randomness from a polynomial-size set. This comes from the fact that in a polynomial-size set of randomness, the probability of finding a subset that invalidates ϕ is negligible. As a short example, $[\mathbf{basis}_N\ (\mathbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]$ holds, meaning that even if the adversary can select randomness in a polynomial-size set, N random vectors still form a basis with overwhelming probability. This is necessary, as the rewinding axiom does not provide uniformly sampled random values. To the best of our knowledge, this argument has been missed in all previous proofs of Terelius-Wikström mixnet protocol.

C. *Verifiability proof*

In this subsection, we give a detailed sketch of the verifiability. The complete proof is given in Appendix F.

Let $\mathsf{frame}_{\mathsf{verif}}$ be the complete trace of Terelius-Wikström protocol, defined as

$$\mathsf{frame}_{\mathsf{verif}} \stackrel{\text{def}}{=} (ck\ n), \mathbf{a}, (\mathbf{e}_\pi\ t_1), \alpha_\pi, (r_\pi\ l), z_\pi(r_\pi), \\ sk, \mathbf{c}, \mathbf{c}', (\mathbf{e}_\phi\ t_2), \alpha_\phi, (r_\phi\ p), z_\phi(r_\phi)$$

Verifiability property states that if the input is well-formed and all zero-knoweldge proofs are successfully verified, then the output list of votes produced by the mix-server is equal (as a multiset) to the input one. In CCSA, we capture this as

$$[\phi\to \mathbf{eqm}_N\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}')]$$

where ϕ is the verifiability condition:

$$\phi \stackrel{\text{def}}{=} \mathbf{zkp\text{-}verif}_\pi\ (ck\ n, \mathbf{e}_\pi\ t_1)\ \mathbf{a}\ \langle\alpha_\pi,(r_\pi\ l),z_\pi(r_\pi)\rangle \\ \wedge\ \mathbf{zkp\text{-}verif}_{\phi_{\mathbb{CS}}}\ (ck\ n, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_\phi\ t_2)\ (\mathbf{a},\mathbf{c},\mathbf{c}') \\ \langle\alpha_\phi,(r_\phi\ p),z_\phi(r_\phi)\rangle \\ \wedge\ \mathbf{wf\_ctxt}_N\ sk\ \mathbf{c}.$$

The CCSA proof sketch is similar to the computational proof [4], but introduces **low-bound** predicates when needed for rewinding steps, and removes them at the end to conclude.

1) Extraction of the committed matrix: The first step of the proof is the extraction of the permutation matrix. This is performed through the extraction of N witnesses $(\mathbf{e}'_i, k_i)_{i=1}^N$ for the relations of correct commitment $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_i)$, where $(\mathbf{e}_i)_{i=1}^N$ is a free family of $\mathbb{F}(p_\eta)^N$; then, for each of these witnesses we build one linear equation involving the committed matrix, and we finally solve the system composed of all these equations.

To do so, we have to handle two rewinding steps. The first one provides a sequence of proofs for vectors $(\mathbf{e}_i)_{i=1}^N$. Then, for each of these vectors, we perform a rewinding on the challenge $r\in\mathbb{F}(p_\eta)$; doing so, we can apply the *special-soundness* axiom and obtain one equation. Hence, to be able to apply the rewinding axiom twice, we need two **low-bound** assumptions: the first one states that there are enough random vectors to rewind; and the second one states that for a chosen vector, there are enough random challenges to rewind. More formally, let us denote by ψ_π the formula

$$\psi_\pi \stackrel{\text{def}}{=} \lambda\mathbf{e}.\ \lambda r.\ \mathbf{zkp\text{-}verif}_\pi\ (ck\ n,\mathbf{e})\ \mathbf{a}\ \langle\alpha_\pi, r, z_\pi(r)\rangle,$$

where both arguments on which we perform rewinding are abstracted. We introduce the following condition allowing for both, nested, rewinding steps

$$\mathbf{low\text{-}bound}\ g\ (\lambda\mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\psi_\pi\ \mathbf{e}))$$

for g, g' : **real**.

Going deeper into the details, let us define $\mathbf{e}_s : \mathbf{nat}\to\mathbf{vect}_N$ and $\mathbf{r}_s : \mathbf{nat}\to\mathbf{chall}_\pi$ to be names (i.e. semantically random nonces) corresponding to sources of random vectors and public random coins in $\mathbb{F}(p_\eta)^*$. With two sequential rewinding axiom applications, we prove the existence of two deterministic and polynomially bounded natural number terms $k_{\mathbf{e}}$: **nat** and $k_{\mathbf{r}}$: **nat**, with $k_{\mathbf{e}}\geqslant N$ and $k_{\mathbf{r}}\geqslant 2$, and two selection functions, such that for all $i\in\llbracket 1;N\rrbracket$ and $j\in\{1,2\}$:

- $\mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s = \{\mathbf{e}_s\ t_i\}_{i=1}^N$, with $t_1,\ldots,t_N$: **nat** pairwise distincts,
- $\mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s = \{\mathbf{r}_s\ r_{i,1}, \mathbf{r}_s\ r_{i,2}\}$, with $r_{i,1}\neq r_{i,2}$,
- and $\psi_\pi\ (\mathbf{e}_s\ t_i)\ (\mathbf{r}_s\ r_{i,j})$.

Therefore, for all $i\in\llbracket 1;N\rrbracket$, we have $\psi_\pi\ (\mathbf{e}_s\ t_i)\ (\mathbf{r}_s\ r_{i,1})$ and $\psi_\pi\ (\mathbf{e}_s\ t_i)\ (\mathbf{r}_s\ r_{i,2})$ with $r_{i,1}\neq r_{i,2}$. Thus, by the *special-soundness* axiom, we get N witnesses $w_\pi(i)$, for all $i\in\llbracket 1;N\rrbracket$, defined by

$$w_\pi(i) \stackrel{\text{def}}{=} \mathbf{zkp\text{-}extract}_\pi\ (ck\ n, \mathbf{e}_s\ t_i)\ \mathbf{a} \\ (\mathfrak{p}^{(i)}_\pi(\mathbf{r}_s\ r_{i,1}))\ (\mathfrak{p}^{(i)}_\pi(\mathbf{r}_s\ r_{i,2}))$$

where $\mathfrak{p}^{(i)}_\pi(c) \stackrel{\text{def}}{=} \langle\alpha_\pi(i), c, z_\pi(i,c)\rangle$. And each witness $w_\pi(i)$ satisfies the property $\mathbf{zkp\text{-}rel}_\pi\ (ck\ n, \mathbf{e}_s\ t_i)\ \mathbf{a}\ (w_\pi(i))$.

Then, using G.SEL and L.BASIS followed by L.OPEN, we get two terms M and $\mathbf{s}$ such that $\mathbf{a}$ is a commitment message to the matrix M, *i.e.* under the **low-bound** described above we have $\mathbf{a} = \mathbf{com\text{-}mat}\ (ck\ n)\ M\ \mathbf{s}$.

2) M is a permutation: We now need to prove that matrix M is indeed a permutation. To do so, we use our characterization of a permutation matrix: we extract a new witness for the relation of correct commitment $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_\pi)$, where vector $\mathbf{e}_\pi$ and matrix M must be independent; then, we can apply *Schwartz-Zippel* rule (L.SZ and G.SEL), and finally conclude that $\mathbf{prod}_N\ (M\cdot X) - \mathbf{prod}_N\ X = \mathbf{0}$. Once again, we need enough random challenges to rewind with vector $\mathbf{e}_\pi$, which implies to add the condition $\mathbf{low\text{-}bound}\ g'\ (\psi_\pi\ \mathbf{e}_\pi)$. Finally, using L.$\pi$:CHARAC, we get $\mathbf{perm}_N\ M$, which concludes the proof.

3) M has been used to shuffle the input ciphertexts list with the shuffle-friendly *map $\phi_{\mathbb{CS}}$:* The last step of the proof consist in proving that the permutation matrix M we have extracted satisfies $\mathbf{a} = \textbf{com-mat}\ (ck\ n)\ M\ \mathbf{s}$, for some vector $\mathbf{s}$. Indeed, we are left with proving that the output ciphertexts list $\mathbf{c}'$ is the *shuffle* of the input ciphertexts list $\mathbf{c}$ for the extracted permutation M. Once again, we need to apply the rewinding axiom, this time to the second *zero-knowledge* proof. We define ψ_ϕ the formula used in the rewinding axiom

$$\psi_\phi \overset{\text{def}}{=} \lambda r.\ \textbf{zkp-verif}_\phi\ (ck\ n, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_\phi\ t_2)\ (\mathbf{a}, \mathbf{c}, \mathbf{c}')\ \langle \alpha_\phi, r, z_\phi(r)\rangle$$

and add the corresponding lower bound condition $\textbf{low-bound}\ g''\ \psi_\phi$. Using the extracted witness, it follows from the properties of *shuffle-friendly* maps that M has been used to shuffle the input ciphertexts list.

4) Putting everything together: We will now prove the verifiability property. To do so, we denote by $\mathcal{H}$ the function defined by

$$\begin{aligned}\mathcal{H} \overset{\text{def}}{=} \lambda \mathbf{e}.\ \lambda r.\ \lambda r'.\ &\textbf{zkp-verif}_\pi\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_\pi, r, z_\pi(r)\rangle \\ \wedge\ &\textbf{zkp-verif}_{\phi_{\mathbb{CS}}}\ (ck\ n, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_\phi\ t_2)\ (\mathbf{a}, \mathbf{c}, \mathbf{c}')\ \langle \alpha_\phi, r', z_\phi(r')\rangle \\ &\wedge\ \textbf{wf\_ctxt}_N\ sk\ \mathbf{c}.\end{aligned}$$

We want to prove the following formula

$$\begin{aligned}[&\mathcal{H}\ (\mathbf{e}_\pi\ t_1)\ (r_\pi\ l)\ (r_\phi\ p) \rightarrow \\ &\qquad \textbf{eqm}_N\ (\textbf{dec-list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})\ (\textbf{dec-list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}')]\end{aligned}$$

As $\mathcal{H}\ (\mathbf{e}_\pi\ t_1)\ (r_\pi\ l)\ r_\phi\ p \rightarrow \psi_\pi\ (\mathbf{e}_\pi\ t_1)\ (r_\pi\ l)$ and $\mathcal{H}\ (\mathbf{e}_\pi\ t_1)\ (r_\pi\ l)\ (r_\phi\ p) \rightarrow \psi_\phi\ (r_\phi\ p)$, we use the three previous results to prove the following property for all deterministic non-negligible parameters $g, g' : \textbf{real}$:

$$\begin{aligned}&\textbf{low-bound}\ g\ (\lambda \mathbf{e}.\ \textbf{low-bound}\ g'\ (\mathcal{H}\ \mathbf{e})) \rightarrow \\ &\quad \textbf{low-bound}\ g'\ (\mathcal{H}\ (\mathbf{e}_\pi\ t_1)) \rightarrow \mathcal{H}\ (\mathbf{e}_\pi\ t_1)\ (r_\pi\ l)\ (r_\phi\ p) \rightarrow \\ &\qquad \textbf{eqm}_N\ (\textbf{dec-list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})\ (\textbf{dec-list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}')\end{aligned}$$

Therefore, by two applications of the elimination rule G.LB:ELIM of predicate **low-bound** (one with parameter g, then another one with parameter g'), we get the desired verifiability property.

VII. PROOF OF PERMUTATION SECRECY

Let $\mathsf{frame}_{\mathsf{init}}$ denote the initial knowledge of the adversary, and let Θ_{init} be the initial global context of formulas:

$$\begin{aligned}\mathsf{frame}_{\mathsf{init}} &\overset{\text{def}}{=} (ck\ n), (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k)), \pi, \mathrm{id}, \mathbf{c}, v \\ \Theta_{\mathsf{init}} &\overset{\text{def}}{=} [\Psi^{ck,n}_{\mathsf{comkey}}(\mathsf{frame}_{\mathsf{init}})], [\Psi^{sk,k}_{\mathsf{skey}}(\mathsf{frame}_{\mathsf{init}})]\end{aligned}$$

For ease of notation, for a permutation σ, we denote by $x_\phi(\sigma)$ the statement $x_\phi(\sigma) \overset{\text{def}}{=} (\mathbf{a}_\sigma, \mathbf{c}, \mathbf{c}'_\sigma)$. By unfolding the definition of the mix predicate $\textbf{mix}_{\phi_{\mathbb{CS}}}$, one has to prove the following indistinguishability property:

$$\begin{aligned}&\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_{\mathsf{init}}, \mathbf{a}_\pi, (\mathbf{e}_\pi\ t_1), (r_\pi\ j), \mathfrak{p}_\pi(\pi), \\ &\textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \langle (\mathbf{r}\ l), \mathbf{c}'_\pi, (\mathbf{e}_\phi\ t_2), (r_\phi\ p), \mathfrak{p}_\phi(\pi)\rangle \\ &\qquad \sim \mathsf{frame}_{\mathsf{init}}, \mathbf{a}_{\mathrm{id}}, (\mathbf{e}_\pi\ t_1), (r_\pi\ j), \mathfrak{p}_\pi(\mathrm{id}), \\ &\textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \langle (\mathbf{r}\ l), \mathbf{c}'_{\mathrm{id}}, (\mathbf{e}_\phi\ t_2), (r_\phi\ p), \mathfrak{p}_\phi(\mathrm{id})\rangle\end{aligned}$$

where

$$\begin{aligned}\mathbf{a}_\sigma &\overset{\text{def}}{=} \textbf{com-mat}\ (ck\ n)\ \sigma\ (\mathbf{s}\ i), \\ \mathfrak{p}_\pi(\sigma) &\overset{\text{def}}{=} \textbf{zkp-prove}_\pi\ \langle ck\ n, \mathbf{e}_\pi\ t_1\rangle\ \mathbf{a}_\sigma\ w_\sigma\ (r_\pi\ j), \\ \mathbf{c}'_\sigma &\overset{\text{def}}{=} \textbf{shuffle}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ \sigma\ (\mathbf{r}\ l),\ \text{and} \\ \mathfrak{p}_\phi(\sigma) &\overset{\text{def}}{=} \textbf{zkp-prove}_\phi\ \langle ck\ n, \mathtt{pk}_{\mathbb{CS}}\ (sk\ k), \mathbf{e}_\phi\ t_2\rangle\ x_\phi(\sigma)\ w_\phi\ (r_\phi\ p).\end{aligned}$$

To prove this security property, and because of dependencies between adversarial computations, we have to use a backtracking strategy using the following order of terms:

$$\begin{aligned}&\mathfrak{p}_\phi(\sigma) \rightsquigarrow (r_\phi\ p, \mathbf{e}_\phi\ t_2) \rightsquigarrow \mathbf{c}'_\sigma \rightsquigarrow (\mathbf{r}\ l) \\ &\qquad\qquad \rightsquigarrow \mathfrak{p}_\pi(\sigma) \rightsquigarrow (r_\pi\ j, \mathbf{e}_\pi\ t_1) \rightsquigarrow \mathbf{a}_\sigma.\end{aligned}$$

More precisely, we use the following arguments.

- For proof transcript terms $\mathfrak{p}_\phi(\sigma)$ and $\mathfrak{p}_\pi(\sigma)$, we use the *Honest-Verifier Zero-Knowledge* hypothesis on both Σ-protocols by applying the corresponding rule G.Σ-P:HVZK. Therefore, we transform function symbols $\textbf{zkp-prove}_{\mathcal{R}}/4$ by simulated ones $\textbf{zkp-sim}_{\mathcal{R}}/3$, which are independent of the respective witnesses. Doing so, the term we obtain only depends on *public data*, and not on the permutation used σ.
- For fresh names computed by the honest verifier (*i.e.* terms $\mathbf{e}_\pi\ t_1$, $r_\pi\ j$, $\mathbf{r}\ l$, $\mathbf{e}_\phi\ t_2$, and $r_\phi\ p$), we use the fresh rule G.$\sim$:FRESH and, then, can simplify the resulting term with rule G.$\sim$:SIMPL.
- For the list of ciphertexts term $\mathbf{c}'_\sigma$, which is computed by applying function symbol $\textbf{shuf-map}_{\phi_{\mathbb{CS}}}/3$, we use the *indistinguishability of $\phi_{\mathbb{CS}}$ output* hypothesis by applying corresponding rule G.SFM:INDCCA.
- Finally, for the commitment value $\mathbf{a}_\sigma$, we use the *hiding* hypothesis for commit function symbol $\textbf{com-mat}/3$, by applying corresponding rule G.COM:HIDE.

More details on this proof can be found in Appendix A.

VIII. CONCLUSION

Many e-voting protocols use mixnets, which are critical to achieve security properties but unfortunately really hard to handle in automatic formal proofs frameworks. In this paper, we propose a complete proof of Terelius-Wikström mixnet protocol in the CCSA logic. To do so, we introduce new predicates, rules and axioms in the logic to be able to handle zero-knowledge proofs and rewinding. To our knowledge, it is the first time that this protocol can be proved in a logical framework, and the first fully precise cryptographic proof of the Terelius-Wikström mixnet.

As future work, we plan to include this new material in Squirrel, the tool implementing the CCSA logic. This will open the way to complete mechanized proofs of e-voting protocols using mixnets. In parallel, since our axiomatization of rewinding is not tailored to our case study, this will also open the way to proofs of other kinds of protocols needing to handle zero-knowledge or rewinding. Our additions to the CCSA logic also open the way for other types of proofs. For example proofs involving the programmable Random Oracle

Model (e.g. the Fiat-Shamir transform) are now attainable as they involve probabilistic arguments which are similar to those needed to catch the rewinding lemma in the CCSA logic.

While the present paper focuses on proving properties of one mix-server, in an e-voting protocol several such mix-servers are run sequentially. The goal is to ensure that privacy holds if at least one is honest, while maintaining verifiability through a chain of mix sevrers. While this is left as further work, we took particular care to ensure that our secrecy and verifiability properties are amenable to sequential composition by guarding the conditions of the input list by an arbitrary **valid** predicate that is also satisfied by the output of a mixserver. Formally integrating mix servers in a larger proof of e-voting protocols will be a significant further work.

References

[1] V. Cortier, C. C. Dragan, F. Dupressoir, and B. Warinschi, "Machine-checked proofs for electronic voting: Privacy and verifiability for belenios," in *CSF*. IEEE Computer Society, 2018, pp. 298–312.

[2] G. Bana, R. Chadha, and A. K. Eeralla, "Formal analysis of vote privacy using computationally complete symbolic attacker," in *ESORICS (2)*, ser. Lecture Notes in Computer Science, vol. 11099. Springer, 2018, pp. 350–372.

[3] V. Cortier, P. Gaudry, and S. Glondu, "Belenios: A simple private and verifiable electronic voting system," in *Foundations of Security, Protocols, and Equational Reasoning*, ser. Lecture Notes in Computer Science, vol. 11565. Springer, 2019, pp. 214–238.

[4] B. Terelius and D. Wikström, "Proofs of restricted shuffles," in *AFRICACRYPT*, ser. Lecture Notes in Computer Science, vol. 6055. Springer, 2010, pp. 100–113.

[5] D. Wikström, "A commitment-consistent proof of a shuffle," in *ACISP*, ser. Lecture Notes in Computer Science, vol. 5594. Springer, 2009, pp. 407–421.

[6] J. Dreier, P. Lafourcade, and D. Mahmoud, "Shaken, not stirred - automated discovery of subtle attacks on protocols using mix-nets," in *USENIX Security Symposium*. USENIX Association, 2024.

[7] S. Post. (2019) Gitlab repository of symbolic proofs for the swisspost e-voting protocol. [Online]. Available: https://gitlab.com/swisspost-evoting/e-voting/e-voting-documentation/-/tree/master/Symbolic-models

[8] B. Blanchet, "A computationally sound mechanized prover for security protocols," *IEEE Trans. Dependable Secur. Comput.*, vol. 5, no. 4, pp. 193–207, 2008.

[9] G. Barthe, B. Grégoire, S. Heraud, and S. Z. Béguelin, "Computer-aided security proofs for the working cryptographer," in *CRYPTO*, ser. Lecture Notes in Computer Science, vol. 6841. Springer, 2011, pp. 71–90.

[10] D. Firsov and D. Unruh, "Reflection, rewinding, and coin-toss in easycrypt," in *CPP*. ACM, 2022, pp. 166–179.

[11] G. Bana and H. Comon-Lundh, "A computationally complete symbolic attacker for equivalence properties," in *CCS*. ACM, 2014, pp. 609–620.

[12] D. Baelde, A. Koutsos, and J. Lallemand, "A higher-order indistinguishability logic for cryptographic reasoning," in *LICS*, 2023, pp. 1–13.

[13] D. Baelde, S. Delaune, C. Jacomme, A. Koutsos, and S. Moreau, "An interactive prover for protocol verification in the computational model," in *SP*. IEEE, 2021, pp. 537–554.

[14] G. Scerri and R. Stanley-Oakes, "Analysis of key wrapping apis: Generic policies, computational security," in *CSF*. IEEE Computer Society, 2016, pp. 281–295.

[15] T. Haines, R. Goré, and B. Sharma, "Did you mix me? formally verifying verifiable mix nets in electronic voting," in *SP*. IEEE, 2021, pp. 1748–1765.

[16] T. Haines, R. Goré, and M. Tiwari, "Machine-checking multi-round proofs of shuffle: Terelius-wikstrom and bayer-groth," in *USENIX Security Symposium*. USENIX Association, 2023, pp. 6471–6488.

[17] G. Barthe, B. Grégoire, and S. Z. Béguelin, "Formal certification of code-based cryptographic proofs," in *POPL*. ACM, 2009, pp. 90–101.

[18] G. Barthe, D. Hedin, S. Zanella-Béguelin, B. Grégoire, and S. Heraud, "A machine-checked formalization of sigma-protocols," in *CSF*. IEEE Computer Society, 2010, pp. 246–260.

[19] J. B. Almeida, M. Barbosa, E. Bangerter, G. Barthe, S. Krenn, and S. Zanella-Béguelin, "Full proof cryptography: verifiable compilation of efficient zero-knowledge protocols," in *CCS*. ACM, 2012, pp. 488–500.

[20] D. Butler, A. Lochbihler, D. Aspinall, and A. Gascón, "Formalising $\varsigma$-protocols and commitment schemes using crypthol," *J. Autom. Reason.*, vol. 65, no. 4, pp. 521–567, 2021.

[21] D. Firsov and D. Unruh, "Zero-knowledge in easycrypt," in *CSF*. IEEE, 2023, pp. 1–16.

[22] P. G. Haselwarter, E. Rivas, A. Van Muylder, T. Winterhalter, C. Abate, N. Sidorenco, C. Hritcu, K. Maillard, and B. Spitters, "Ssprove: A foundational framework for modular cryptographic proofs in coq," *ACM Trans. Program. Lang. Syst.*, vol. 45, no. 3, pp. 15:1–15:61, 2023.

[23] R. Zippel, "Probabilistic algorithms for sparse polynomials," in *EUROSAM*, ser. Lecture Notes in Computer Science, vol. 72. Springer, 1979, pp. 216–226.

[24] J. T. Schwartz, "Fast probabilistic algorithms for verification of polynomial identities," *J. ACM*, vol. 27, no. 4, pp. 701–717, 1980.

[25] V. Shoup, "Sequences of games: a tool for taming complexity in security proofs," *IACR Cryptol. ePrint Arch.*, p. 332, 2004.

[26] M. Manulis and J. Nguyen, "Fully homomorphic encryption beyond IND-CCA1 security: Integrity through verifiability," in *EUROCRYPT (2)*, ser. Lecture Notes in Computer Science, vol. 14652. Springer, 2024, pp. 63–93.

[27] R. Küsters, T. Truderung, and A. Vogt, "Formal analysis of chaumian mix nets with randomized partial checking," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2014, pp. 343–358.

[28] A. Lysyanskaya and L. N. Rosenbloom, "Universally composable σ-protocols in the global random-oracle model," in *TCC (1)*, ser. Lecture Notes in Computer Science, vol. 13747. Springer, 2022, pp. 203–233.

[29] T. Attema, S. Fehr, and M. Klooß, "Fiat-shamir transformation of multi-round interactive proofs (extended version)," *J. Cryptol.*, vol. 36, no. 4, p. 36, 2023.

[30] D. Baelde, C. Fontaine, A. Koutsos, G. Scerri, and T. Vignon, "A probabilistic logic for concrete security," in *CSF*. IEEE, 2024, pp. 324–339.

Appendix

In Appendix A we recall and precise all cryptographic definitions and games this paper is based on. In Appendix B, we recall the specification of Terelius-Wikström shuffle protocol as given in [5], [4]. Finally, our details proofs of security properties for Terelius-Wikström shuffle protocol, and proofs of soundness for the CCSA rules we have added, can be found in the other appendices (Appendices D and F). Appendix E presents details of the rewinding technique and Appendix C presents subterms mechanics and freshness properties used in cryptographic rules.

Appendix A
Cryptographic definitions

In this section, we recall usual definitions of the cryptographic security properties for all the cryptographic constructions we need in this paper.

A. Useful usual cryptographic definitions

Firstly, we recall usual definition of cryptosystems from [25]. A *cryptosystem* $\mathbb{CS}$ is a tuple

$$\mathbb{CS} = \left(\mathcal{PK}_{\mathbb{CS}}, \mathcal{M}_{\mathbb{CS}}, \mathcal{R}_{\mathbb{CS}}, \mathcal{C}_{\mathbb{CS}}, \mathrm{KeyGen}_{\mathbb{CS}}, \mathrm{Enc}_{\mathbb{CS}}, \mathrm{Dec}_{\mathbb{CS}}\right)$$

where

- The sets $\mathcal{PK}_{\mathbb{CS}}$, $\mathcal{M}_{\mathbb{CS}}$, $\mathcal{R}_{\mathbb{CS}}$, and $\mathcal{C}_{\mathbb{CS}}$ are respectively called the *public key space*, the *plaintext space*, the *randomness space*, and the *ciphertext space* for the cryptosystem $\mathbb{CS}$;

- $\mathrm{KeyGen}_{\mathbb{CS}} : \mathbb{N}^* \longrightarrow \mathbb{F}(p_\eta) \times \mathcal{PK}_{\mathbb{CS}}$ is an algorithm takes as input a security parameter $\eta \in \mathbb{N}^*$ and outputs a key pair $(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta)$ where $sk \in \mathbb{F}(p_\eta)$ is the randomly chosen private key of bit-size at least η and $pk \in \mathcal{PK}_{\mathbb{CS}}$ is the corresponding public encryption key defined by some function $\mathtt{pk}_{\mathbb{CS}} : \mathbb{F}(p_\eta) \longrightarrow \mathcal{PK}_{\mathbb{CS}}$;
- $\mathrm{Enc}_{\mathbb{CS}}^{(\eta)} : \mathcal{PK}_{\mathbb{CS}}^{(\eta)} \times \mathcal{M}_{\mathbb{CS}}^{(\eta)} \times \mathcal{R}_{\mathbb{CS}} \longrightarrow \mathcal{C}_{\mathbb{CS}}$ is a deterministic algorithm taking as inputs a public key $pk \in \mathcal{PK}_{\mathbb{CS}}$, a message $m \in \mathcal{M}_{\mathbb{CS}}$, and a randomness $r \in \mathcal{R}_{\mathbb{CS}}$ and outputs a ciphertext $c \leftarrow \mathrm{Enc}_{\mathbb{CS}}^{(\eta)}(pk, m\,;\, r) \in \mathcal{C}_{\mathbb{CS}}$ encrypted with the public key pk ;
- $\mathrm{Dec}_{\mathbb{CS}}^{(\eta)} : \mathbb{F}(p_\eta) \times \mathcal{C}_{\mathbb{CS}}^{(\eta)} \longrightarrow \mathcal{M}_{\mathbb{CS}}^{(\eta)} \sqcup \{\perp\}$ is a deterministic algorithm taking as input a secret key $sk \in \mathbb{F}(p_\eta)$ and a ciphertext $c \in \mathcal{C}_{\mathbb{CS}}$ and try to decrypt it with some secret key $sk \in \mathbb{F}(p_\eta)$. If c was not encrypted with the corresponding public key $pk = \mathtt{pk}_{\mathbb{CS}}(sk)$, the decryption algorithm fails and outputs in this case a special symbol $\perp$ supposed to not belong to the message space $\mathcal{M}_{\mathbb{CS}}$. Otherwise, the decryption algorithm succeeds and outputs the message $m \in \mathcal{M}_{\mathbb{CS}}$ such that $c = \mathrm{Enc}_{\mathbb{CS}}(\mathtt{pk}_{\mathbb{CS}}(sk), m\,;\, r)$ where $r \in \mathcal{R}_{\mathbb{CS}}$.

For a cryptosystem $\mathbb{CS}$, and for all natural number $n \in \mathbb{N}^*$, we define the function $\mathbf{wf}_{\mathbb{CS}}^{(n)} : \mathbb{F}(p_\eta) \times \mathcal{C}_{\mathbb{CS}}^n \longrightarrow \{0,1\}$, called *the well-founded ciphertexts list predicate*, such that the following property holds

$$\begin{aligned}&\forall\, sk \in \mathbb{F}(p_\eta),\ \forall\, (c_i)_{i=1}^n \in \mathcal{C}_{\mathbb{CS}}^n,\\ &\mathbf{wf}_{\mathbb{CS}}^{(n)}\left(sk, (c_i)_{i=1}^n\right) = 1 \overset{\text{def}}{\Longleftrightarrow} \forall\, i \in [\![1;n]\!], \mathrm{Dec}_{\mathbb{CS}}(sk, c_i) \neq \perp.\end{aligned}$$

Definition 4 (Homomorphic cryptosystem)**.** *A* cryptosystem $\mathbb{CS}$ *is called* homomorphic *when*

- *The sets* $(\mathcal{M}_{\mathbb{CS}}, \otimes)$, $(\mathcal{R}_{\mathbb{CS}}, \oplus)$ *and* $(\mathcal{C}_{\mathbb{CS}}, \odot)$ *are Abelian groups ;*
- *For all security parameter* $\eta \in \mathbb{N}^*$*, for all honest key pair* $(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta)$*, the following property holds*

$$\begin{aligned}&\forall\, m_1, m_2 \in \mathcal{M}_{\mathbb{CS}}^{(\eta)},\ \forall\, r_1, r_2 \in \mathcal{R}_{\mathbb{CS}},\\ &\quad \mathrm{Enc}_{\mathbb{CS}}(pk, m_1 \otimes m_2\,;\, r_1 \oplus r_2) =\\ &\qquad \mathrm{Enc}_{\mathbb{CS}}(pk, m_1\,;\, r_1) \odot \mathrm{Enc}_{\mathbb{CS}}(pk, m_2\,;\, r_2).\end{aligned}$$

Besides, we recall two usual cryptographic properties, the *Indistinguishability under Chosen Plaintexts Attack* (Ind-CPA) [26] security property and the *Discrete Logarithm* assumption [25].

1) Indistinguishability under Chosen Plaintexts Attack (Ind-CPA)*:* For an adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}})$, a security parameter $\eta \in \mathbb{N}^*$, a random tape $\rho \in \mathbb{T}$, and a secret bit $\beta \in \{0,1\}$, we define the cryptographic *Indistinguishability under Chosen Plaintexts Attack* game $\text{Ind-CPA}_{\mathbb{CS}}^{\mathcal{A}}(\eta, \rho\,;\, \beta)$ to be the cryptographic game defined in Game 3.

```
Ind-CPA$_{\mathbb{CS}}^{(\mathcal{A}_{setup},\mathcal{A}_{guess})}(\eta, (\rho_h, \rho_a)\,;\, \beta)$ – Ind-CPA property
$(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta\,;\, \rho_h)$ ; $r \xleftarrow{\$} \mathcal{R}_{\mathbb{CS}}$ ;
$(m_0, m_1) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, pk\,;\, \rho_a)$ ;
$c_\beta \leftarrow \mathrm{Enc}_{\mathbb{CS}}(pk, m_\beta\,;\, r)$ ;
$b \leftarrow \mathcal{A}_{\mathsf{guess}}(c_\beta\,;\, \rho_a)$ ;
return $(b = \beta)$.
```

Game 3. Cryptographic game of indistinguishability under chosen plaintexts attack for cryptosystems

We define the *advantage of the adversary* $\mathcal{A}$ *against the indistinguishability under chosen plaintexts attack game* to be the following function

$$\begin{aligned}\forall\, \eta \in \mathbb{N}^*,\ &\mathrm{Adv}_{\text{Ind-CPA}}\left[\mathcal{A} \,\middle|\, \mathbb{CS}\right](\eta) \overset{\text{def}}{=\!=}\\ &\quad \Pr_{\rho \in \mathbb{T}}\left[\ 1 \leftarrow \text{Ind-CPA}_{\mathbb{CS}}^{\mathcal{A}}(\eta, \rho\,;\, \beta)\ \right] \in [0,1].\end{aligned}$$

A cryptosystem $\mathbb{CS}$ is said to *be secure against the indistinguishability under chosen plaintexts attack* when, for all adversary $\mathcal{A}$ against the Ind-CPA game, the function $\mathrm{Adv}_{\text{Ind-CPA}}\left[\mathcal{A} \,\middle|\, \mathbb{CS}\right]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

2) Discrete Logarithm assumption: Let $\mathfrak{G} = (\mathbb{G}_{p_\eta}, g_\eta)_{\eta \in \mathbb{N}^*}$ be a sequence of pairs of cyclic group and generator where, for a security parameter $\eta \in \mathbb{N}^*$, $g_\eta \in \mathbb{G}_{p_\eta}$ is a generator of the cyclic group $\mathbb{G}_{p_\eta}$ of prime order p_η such that $\log_2 p_\eta \geqslant \eta$. For an adversary $\mathcal{A}$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the *Discrete Logarithm Attack game* $\mathrm{DLP}_{\mathfrak{G}}^{\mathcal{A}}(\eta, \rho)$ to be the cryptographic game defined in Game 4.

```
DLP$_{\mathfrak{G}}^{\mathcal{A}}(\eta, (\rho_h, \rho_a))$ – Discrete Logarithm problem
$r \xleftarrow{\$} \mathbb{F}(p_\eta)$ ; $h \leftarrow g_\eta^r \in \mathbb{G}_{p_\eta}$ ;
$\gamma \leftarrow \mathcal{A}(g_\eta, h\,;\, \rho_a)$ ;
return $(r = \gamma)$.
```

Game 4. Cryptographic game of discrete logarithm attack for a sequence of cyclic groups $\mathfrak{G} = (\mathbb{G}_{p_\eta}, g_\eta)_{\eta \in \mathbb{N}^*}$

We define the *advantage of the adversary* $\mathcal{A}$ *against the discrete logarithm game* to be the following function

$$\begin{aligned}\forall\, \eta \in \mathbb{N}^*,\ &\mathrm{Adv}_{\mathrm{DLP}}\left[\mathcal{A} \,\middle|\, \mathfrak{G}\right](\eta) \overset{\text{def}}{=\!=}\\ &\quad \Pr_{\rho \in \mathbb{T}}\left[\ 1 \leftarrow \mathrm{DLP}_{\mathfrak{G}}^{\mathcal{A}}(\eta, \rho)\ \right] \in [0,1].\end{aligned}$$

We say that *the sequence of cyclic groups* $\mathfrak{G} = (\mathbb{G}_{p_\eta}, g_\eta)_{\eta \in \mathbb{N}^*}$ *is secure against the Discrete Logarithm Attack* when the function $\mathrm{Adv}_{\mathrm{DLP}}\left[\mathcal{A} \,\middle|\, \mathfrak{G}\right]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

B. Commitment schemes

In this subsection, we recall definitions of cryptographic security properties for *zero-knowledge* proofs as described in [27]. Let $\mathcal{M}$ be an infinite countable set. A *commitment scheme* $\mathbb{KS}[\mathcal{M}]$ *for the set of messages* $\mathcal{M}$ is a tuple

$$\mathbb{KS}[\mathcal{M}] = \left(\mathcal{PK}_{\mathcal{M}}, \mathcal{R}_{\mathcal{M}}^{\mathsf{com}}, \mathcal{K}_{\mathcal{M}}, \mathrm{Gen}_{\mathcal{M}}, \mathrm{Com}_{\mathcal{M}}\right)$$

such that

- The sets $\mathcal{PK}_{\mathcal{M}}$, $\mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$, and $\mathcal{K}_{\mathcal{M}}$ are respectively called the *commitment key parameter space*, the *randomness space*, and the *commit value space* ;
- The algorithm $\mathrm{Gen}_{\mathcal{M}} : \mathbb{N}^* \longrightarrow \mathcal{PK}_{\mathcal{M}}$ is a probabilistic polynomial-time algorithm which outputs a commitment key $ck \leftarrow \mathrm{Gen}_{\mathcal{M}}(\eta) \in \mathcal{PK}_{\mathcal{M}}$ on input a security parameter $\eta \in \mathbb{N}^*$. This algorithm is called the *generator of commitment parameters for the commitment scheme* $\mathbb{KS}[\mathcal{M}]$;
- Finally, the algorithm $\mathrm{Com}_{\mathcal{M}} : \mathcal{PK}_{\mathcal{M}} \times \mathcal{M} \times \mathcal{R}^{\mathsf{com}}_{\mathcal{M}} \longrightarrow \mathcal{K}_{\mathcal{M}}$ is a deterministic polynomial-time (in the security parameter $\eta \in \mathbb{N}^*$) algorithm which outputs a commitment value $\mathrm{Com}^{(\eta)}_{\mathcal{M}}(ck, m\,;\, r)$ on input a commitment key parameter $ck \in \mathcal{PK}_{\mathcal{M}}$, a message $m \in \mathcal{M}$ and a randomness $r \in \mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$.

Moreover, a commitment scheme $\mathbb{KS}[\mathcal{M}]$ has to satisfies two security properties: the *hiding* and the *binding* properties as defined below. Notice that these two properties *cannot be perfectly verified at the same time*.

1) Hiding property for commitment schemes: For an adversary $\mathcal{A} = \big(\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}}\big)$, a security parameter $\eta \in \mathbb{N}^*$, a random tape $\rho = (\rho_h, \rho_a) \in \mathbb{T}$ (where $\rho_h \in \mathbb{T}^{\mathsf{h}}$ is the *honest random tape* and $\rho_a \in \mathbb{T}^{\mathsf{a}}$ is the *adversarial random tape*), and a secret bit $\beta \in \{0,1\}$, we define the cryptographic *hiding* game $\mathrm{Hiding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}\big(\eta, \rho\,;\, \beta\big)$ to be the cryptographic game defined in Game 5.

```
Hiding$^{(\mathcal{A}_{setup},\mathcal{A}_{guess})}_{\mathbb{KS}[\mathcal{M}]}\big(\eta,(\rho_h,\rho_a)\,;\,\beta\big)$ – Hiding property
$ck \leftarrow \mathrm{Gen}_{\mathcal{M}}(\eta\,;\,\rho_h)$ ; $r \xleftarrow{\$} \mathcal{R}^{\mathsf{com}}_{\mathcal{M}}$ ;
$(m_0, m_1) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, ck\,;\,\rho_a)$ ;
$c_\beta \leftarrow \mathrm{Com}_{\mathcal{M}}(ck, m_\beta\,;\, r)$ ;
$b \leftarrow \mathcal{A}_{\mathsf{guess}}(c_\beta\,;\,\rho_a)$ ;
return $(b = \beta)$.
```

Game 5. Cryptographic game of hiding for commitment schemes

We define the *advantage of the adversary $\mathcal{A}$ against the hiding game* to be the following function

$$\forall \eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{Hiding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big](\eta) \overset{\text{def}}{=} \Pr_{\rho \in \mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Hiding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}\big(\eta, \rho\,;\, \beta\big)\ \Big] \in [0,1].$$

- **(Perfectly hiding)** A commitment scheme $\mathbb{KS}[\mathcal{M}]$ for the message set $\mathcal{M}$ is said to be *perfectly hiding* when, for all adversary $\mathcal{A}$ against the hiding game, we have
$$\forall \eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{Hiding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big](\eta) = 0.$$
- **(Computationally hiding)** A commitment scheme $\mathbb{KS}[\mathcal{M}]$ for the message set $\mathcal{M}$ is said to be *computationally hiding* when, for all adversary $\mathcal{A}$ against the hiding game, the function $\mathrm{Adv}_{\mathrm{Hiding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

2) Binding property for commitment schemes: For an adversary $\mathcal{A}$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the cryptographic *binding game* $\mathrm{Binding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}\big(\eta, \rho\big)$ to be the cryptographic game defined in Game 6.

```
Binding$^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}\big(\eta,(\rho_h,\rho_a)\big)$ – Binding property
$ck \leftarrow \mathrm{Gen}_{\mathcal{M}}(\eta\,;\,\rho_h)$ ;
$(m_1, r_1) \leftarrow \mathcal{A}(\eta, ck\,;\,\rho_a)$ ; $(m_2, r_2) \leftarrow \mathcal{A}(\eta, ck\,;\,\rho_a)$ ;
$a_1 \leftarrow \mathrm{Com}_{\mathcal{M}}(ck, m_1\,;\, r_1)$ ; $a_2 \leftarrow \mathrm{Com}_{\mathcal{M}}(ck, m_2\,;\, r_2)$ ;
if $(m_1 \neq m_2 \wedge a_1 = a_2)$ then $b \leftarrow 1$ else $b \leftarrow 0$ ;
return $b$.
```

Game 6. Cryptographic game of binding for commitment schemes

We define the *advantage of the adversary $\mathcal{A}$ against the binding game* to be the following function

$$\forall \eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{Binding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big](\eta) \overset{\text{def}}{=} \Pr_{\rho \in \mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Binding}^{\mathcal{A}}_{\mathbb{KS}[\mathcal{M}]}\big(\eta, \rho\big)\ \Big] \in [0,1]$$

- **(Perfectly binding)** A commitment scheme $\mathbb{KS}[\mathcal{M}]$ for the message set $\mathcal{M}$ is said to be *perfectly biding* when, for all adversary $\mathcal{A}$ against the biding game, we have
$$\forall \eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{Binding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big](\eta) = 0.$$
- **(Computationally binding)** A commitment scheme $\mathbb{KS}[\mathcal{M}]$ for the message set $\mathcal{M}$ is said to be *computationally binding* when, for all adversary $\mathcal{A}$ against the binding game, the function $\mathrm{Adv}_{\mathrm{Binding}}\big[\mathcal{A} \,\big|\, \mathbb{KS}[\mathcal{M}]\big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

C. Zero-knowledge *proofs and Σ-protocols*

In this subsection, we recall definitions of cryptographic security properties for *zero-knowledge* proofs as described in [28].

1) General case: Let $\mathcal{R} \subseteq \mathcal{PP}_{\mathcal{R}} \times \mathcal{X}_{\mathcal{R}} \times \mathcal{W}_{\mathcal{R}}$ be a computable relation, *i.e.* a relation which can be verified by a Polynomial-time Turing Machine. The sets $\mathcal{PP}_{\mathcal{R}}$, $\mathcal{X}_{\mathcal{R}}$ and $\mathcal{W}_{\mathcal{R}}$ are respectively called *the public parameters space*, *the statements space* and *the witnesses space*. We denote by $\varphi_{\mathcal{R}} : \mathcal{PP}_{\mathcal{R}} \times \mathcal{X}_{\mathcal{R}} \times \mathcal{W}_{\mathcal{R}} \longrightarrow \{0,1\}$ the *polynomially decidable* function such that, for a public parameter $\sigma \in \mathcal{PP}_{\mathcal{R}}$, a statement $x \in \mathcal{X}_{\mathcal{R}}$, and a witness $w \in \mathcal{W}_{\mathcal{R}}$, we have $\varphi_{\mathcal{R}}\big((\sigma, x, w)\big) = 1$ if and only if $(\sigma, x, w) \in \mathcal{R}$.

Let $\mu \in \mathbb{N}$. A *zero-knowledge proof* $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ *for the relation $\mathcal{R}$ with* $(2\mu+1)$ *moves* is a triplet $\mathbb{ZK}^{(\mu)}[\mathcal{R}] = \big(\mathcal{S}, \mathcal{P}, \mathcal{V}\big)$ such that

- Algorithm $\mathcal{S}$ is a special probabilistic polynomial-time algorithm which outputs on a public channel a public parameter $\sigma \in \mathcal{PP}_{\mathcal{R}}$ and a statement $x \in \mathcal{X}_{\mathcal{R}}$ (x is a public data) and outputs on a private channel directly to the algorithm $\mathcal{P}$ a witness $w \in \mathcal{W}_{\mathcal{R}}$ (w is a private data). This algorithm takes as input a security parameter $\eta \in \mathbb{N}^*$

and is called the *setup algorithm for the* zero-knowledge *protocol* $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$.

- Both probabilistic polynomial-time algorithms $\mathcal{P}$, called *the prover*, and $\mathcal{V}$, called *the verifier* define a $(2\mu+1)$-move protocol, where $2\mu+1$ messages are exchanged between the both on a public channel. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $(\sigma, x\,;\,w) \leftarrow \mathcal{S}(\eta)$ be an output of the setup algorithm $\mathcal{S}$. An interaction between $\mathcal{P}$ and $\mathcal{V}$ is given by the sequence of $2\mu+1$ messages $\Big(\mathcal{P}(w) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}\Big)(\eta, \sigma, x) = (m_i)_{i=1}^{2\mu+1}$. All even messages $(m_{2i})_{i=1}^{\mu}$ are sent by the verifier $\mathcal{V}$, are called *the challenge messages* and live respectively in the sets $\big(\mathcal{C}h_{\mathcal{R}}^{(i)}\big)_{i=1}^{\mu}$. All odd messages $(m_{2i+1})_{i=0}^{\mu}$ are sent by the prover $\mathcal{P}$, are called *the commitment messages* and live respectively in the sets $\big(\mathcal{K}_{\mathcal{R}}^{(i)}\big)_{i=0}^{\mu-1}$ except the last one $m_{2\mu+1}$ which is called *the response message* and lives in the set $\mathcal{Z}_{\mathcal{R}}$. We denote by $\mathcal{T}_{\mathcal{R}} = \big(\bigtimes_{i=1}^{\mu}\big(\mathcal{K}_{\mathcal{R}}^{(i-1)} \times \mathcal{C}h_{\mathcal{R}}^{(i)}\big)\big) \times \mathcal{Z}_{\mathcal{R}}$ the *proof transcripts space* of the *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$.
- At the very end of the $(2\mu+1)$-move protocol, the verifier $\mathcal{V}$ outputs a bit $b \in \{0,1\}$ either they are convinced by the messages sent by the prover $\mathcal{P}$ or not. More formally, we define a set $\mathsf{Eq}_{\lambda_{\mathcal{R}}}[\mathbb{ZK}^{(\mu)}[\mathcal{R}]] = \big\{f_i : \mathcal{PP}_{\mathcal{R}} \times \mathcal{X}_{\mathcal{R}} \times \mathcal{T}_{\mathcal{R}} \longrightarrow \{0,1\}\big\}_{i=1}^{\lambda_{\mathcal{R}}}$ of equations with $\lambda_{\mathcal{R}} \in \mathbb{N}^*$ defined by the *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $(\sigma, x\,;\,w) \leftarrow \mathcal{S}(\eta)$ be an output of the setup algorithm $\mathcal{S}$. We denote by $v_{\mathcal{R}}^{\sigma,\,x} : \mathcal{T}_{\mathcal{R}} \longrightarrow \{0,1\}$ the function defined by the following equation.

$$\forall\,(m_i)_{i=1}^{2\mu+1} \leftarrow \Big(\mathcal{P}(w) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}\Big)((\eta, \sigma, x)) \in \mathcal{T}_{\mathcal{R}},$$
$$v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big) = 1 \overset{\text{def}}{\Longleftrightarrow} \forall\,j \in [\![1;\lambda_{\mathcal{R}}]\!], f_i\big(\sigma, x, (m_i)_{i=1}^{2\mu+1}\big) = 1.$$

Hence, at the very end of the $(2\mu+1)$-move protocol, the verifier $\mathcal{V}$ outputs the bit $b = v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big) \in \{0,1\}$.

Besides, a *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ has to satistfy at least three security properties defined below whether or not the prover or the verifier is honest or not.

a) **Completeness *property for zero-knowledge protocols*:** This property describes the case where both prover $\mathcal{P}$ and verifier $\mathcal{V}$ are honest. For an adversary $\mathcal{A}$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the cryptographic *completeness game* $\mathsf{Completeness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho)$ to be the cryptographic game defined in Game 7.

```
$\mathsf{Completeness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}\big(\eta, (\rho_h, \rho_a)\big)$ – Completeness property
$\sigma \leftarrow \mathcal{S}(\eta\,;\,\rho_h)$ ;
$(x, w) \leftarrow \mathcal{A}(\eta, \sigma\,;\,\rho_a)$ ;
$(m_i)_{i=1}^{2\mu+1} \leftarrow \Big(\mathcal{P}(w) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}\Big)(\sigma, x\,;\,\rho_h)$ ;
$b \leftarrow v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big)$ ;
$\mathbf{return}\ \big(\varphi_{\mathcal{R}}\big((\sigma, x, w)\big) \wedge \neg\, b\big)$.
```

Game 7. Cryptographic game of completeness for *zero-knowledge* protocols

We define the *advantage of the adversary $\mathcal{A}$ against the completeness game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathsf{Completeness}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}]\Big](\eta) \overset{\text{def}}{=} \Pr_{\rho \in \mathbb{T}}\Big[\ 1 \leftarrow \mathsf{Completeness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho)\ \Big] \in [0,1].$$

- **(Perfectly complete)** A *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ for the relation $\mathcal{R}$ and with $(2\mu+1)$-move is said to be *perfectly complete* when, for all adversary $\mathcal{A}$ against the completeness game, we have
$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathsf{Completeness}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}]\Big](\eta) = 0.$$
- **(Computationally complete)** A *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ for the relation $\mathcal{R}$ with $(2\mu+1)$-move is said to be *computationally complete* when, for all adversary $\mathcal{A}$ against the completeness game, the function $\mathrm{Adv}_{\mathsf{Completeness}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}]\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

b) **Computational soundness *property for zero-knowledge protocols*:** This property describes the case where the prover $\mathcal{P}$ is dishonest and the verifier $\mathcal{V}$ is honest. For an adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{prove}})$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the cryptographic *soundness game* $\mathsf{Soundness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho)$ to be the cryptographic game defined in Game 8.

```
$\mathsf{Soundness}^{(\mathcal{A}_{setup}, \mathcal{A}_{prove})}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}\big(\eta, (\rho_h, \rho_a)\big)$ – Soundness property
$\sigma \leftarrow \mathcal{S}(\eta\,;\,\rho_h)$ ;
$x \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, \sigma\,;\,\rho_a)$ ;
$(m_i)_{i=1}^{2\mu+1} \leftarrow \Big(\mathcal{A}_{\mathsf{prove}}(\rho_a) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}(\rho_h)\Big)(\sigma, x)$ ;
$b \leftarrow v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big)$ ;
$\mathbf{return}\ \big(x \in \mathcal{L}_{\mathcal{R}}(\sigma) \wedge \neg\, b\big)$.
```

Game 8. Cryptographic game of soundness for *zero-knowledge* protocols

Then, we define the *advantage of the adversary $\mathcal{A}$ against the soundness game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathsf{Sound}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}]\Big](\eta) \overset{\text{def}}{=} \Pr_{\rho \in \mathbb{T}}\Big[\ 1 \leftarrow \mathsf{Soundness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho)\ \Big].$$

A *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ for the relation $\mathcal{R}$ with $(2\mu+1)$-move is said to be *computationally sound* when, for all adversary $\mathcal{A}$ against the soundness game, the function $\mathrm{Adv}_{\mathsf{Sound}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}]\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

c) **Perfect Honest-Verifier Zero-Knowledge *property for zero-knowledge protocols*:** This last property describes the case where the verifier $\mathcal{V}$ is honest but the prover $\mathcal{P}$ is dishonest. For an adversary $\mathcal{A}$, a special probabilistic polynomial-time algorithm $\mathcal{S}\mathsf{im}_{\mathcal{R}}$ called *simulator*, a security parameter $\eta \in \mathbb{N}^*$, a random tape $\rho \in \mathbb{T}$, and a secret bit $\beta \in \{0,1\}$, we define the cryptographic *Honest-Verifier*

Zero-Knowledge game $\mathrm{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{S}\mathsf{im}_{\mathcal{R}}}(\eta, \rho\,;\,\beta)$ to be the cryptographic game defined in Game 9

Then, we define the *advantage of the adversary $\mathcal{A}$ against the Honest-Verifier Zero-Knowledge game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{HVZK}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}],\, \mathcal{S}\mathsf{im}_{\mathcal{R}}\Big](\eta) \overset{\text{def}}{=} \Bigg| \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow \mathrm{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{S}\mathsf{im}_{\mathcal{R}}}(\eta, \rho\,;\,\beta = 0)\ \Big] - \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow \mathrm{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{S}\mathsf{im}_{\mathcal{R}}}(\eta, \rho\,;\,\beta = 1)\ \Big] \Bigg|.$$

A *zero-knowledge* protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ for the relation $\mathcal{R}$ with $(2\mu+1)$-move is said to be *perfectly Honest-Verifier Zero-Knowledge* when, there exists a probabilistic polynomial-time simulator $\mathcal{S}\mathsf{im}_{\mathcal{R}}$ such that, for all adversary $\mathcal{A}$ against the HVZK game, we have the following identity

$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{\mathrm{HVZK}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(\mu)}[\mathcal{R}],\, \mathcal{S}\mathsf{im}_{\mathcal{R}}\Big](\eta) = 0.$$

2) Special case of $\mu = 1$ – Σ-protocols: In the special case of *zero-knowledge* 3-move ($\mu = 1$) protocols, we first define a new cryptographic property stronger than the soundness property, called the *k-special-soundness* [29], for a natural number $k \in \mathbb{N}$, $k \geqslant 2$, defined by the relation $\mathcal{R}$. This property implies the soundness property but also give a "way" to recover the witness from proof transcripts with some additional information. Hence, for an adversary $\mathcal{A}$, a special deterministic polynomial-time algorithm $\mathcal{E}_{\mathcal{R}}$ called *extractor*, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the cryptographic *k-special-soundness game* $k\text{-SpSound}^{\mathcal{A}}_{\mathbb{ZK}^{(1)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}(\eta, \rho)$ to be the cryptographic game defined in Game 10.

Then, we define the *advantage of the adversary $\mathcal{A}$ against the k-special-soundness game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*,\ \mathrm{Adv}_{k\text{-SpSound}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(1)}[\mathcal{R}],\, \mathcal{E}_{\mathcal{R}}\Big](\eta) \overset{\text{def}}{=} \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow k\text{-SpSound}^{\mathcal{A}}_{\mathbb{ZK}^{(1)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}(\eta, \rho)\ \Big].$$

A *zero-knowledge* 3-move protocol $\mathbb{ZK}^{(1)}[\mathcal{R}]$ for the relation $\mathcal{R}$ is said to be *k-special sound* when there exists a deterministic polynomial-time extractor $\mathcal{E}_{\mathcal{R}}$ such that, for all adversary $\mathcal{A}$ against the k-special-soundness game, the function $\mathrm{Adv}_{k\text{-SpSound}}\Big[\mathcal{A} \mid \mathbb{ZK}^{(1)}[\mathcal{R}],\, \mathcal{E}_{\mathcal{R}}\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

Definition 5 (Σ-protocol)**.** *A* Σ-protocol $\Sigma_{\mathcal{R}}$ for a computable relation $\mathcal{R}$ *is a* 3*-move* zero-knowledge *protocol satisfying* (i) *the* perfect (or computational) completeness *property,* (ii) *the* perfect Honest-Verifier Zero-Knowledge *property, and* (iii) *the* k-special-soundness *property for some* $k \in \mathbb{N}$*,* $k \geqslant 2$*.*

D. Shuffle-friendly *maps*

In this subsection, we recall the notion of *shuffle-friendly* map from [5] and extend it.

1) Cryptographic definition: A *shuffle-friendly map* $\phi_{\mathbb{CS}} : \mathcal{PK}_{\mathbb{CS}} \times \mathcal{C}_{\mathbb{CS}} \times \mathcal{R}_{\mathbb{CS}} \longrightarrow \mathcal{C}_{\mathbb{CS}}$ *for the cryptosystem* $\mathbb{CS}$ is an homomorphic map, *i.e.* the following property holds.

$$\forall\, pk \in \mathcal{PK}_{\mathbb{CS}}, \forall\, c, c' \in \mathcal{C}_{\mathbb{CS}}, \forall\, r, r' \in \mathcal{R}_{\mathbb{CS}},\quad \phi_{\mathbb{CS}}(pk, c \cdot c'\,;\, r + r') = \phi_{\mathbb{CS}}(pk, c\,;\, r) \cdot \phi_{\mathbb{CS}}(pk, c'\,;\, r').$$

Besides, a *shuffle-friendly* map $\phi_{\mathbb{CS}}$ has to satisfy the three following security properties.

- **(Decryption preservation)** This property states that the application of a *shuffle-friendly* map have no effect on the decryption of a *valid* ciphertext c, *i.e.* a ciphertext honestly computed. Formally, we say that a *shuffle-friendly map* $\phi_{\mathbb{CS}}$ *achieves the decryption preservation security property* when the following property holds.

$$\forall\,\eta \in \mathbb{N}^*, \forall\,(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta), \forall\, c \in \mathcal{C}_{\mathbb{CS}}, \forall\, r' \in \mathcal{R}_{\mathbb{CS}},\quad \Big[\exists\,(m, r) \in \mathcal{M}_{\mathbb{CS}} \times \mathcal{R}_{\mathbb{CS}},\ c = \mathrm{Enc}_{\mathbb{CS}}(pk, m\,;\, r)\Big] \implies \mathrm{Dec}_{\mathbb{CS}}(sk, \phi_{\mathbb{CS}}(pk, c\,;\, r')) = \mathrm{Dec}_{\mathbb{CS}}(sk, c).$$

- **(Associated *zero-knowledge* proof)** We define

$$\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}} \subseteq \underbrace{\mathcal{PK}_{\mathbb{CS}}}_{\text{Public parameter set}} \times \underbrace{\mathcal{C}^2_{\mathbb{CS}}}_{\text{Statement set}} \times \underbrace{\mathcal{R}_{\mathbb{CS}}}_{\text{Witness set}}$$

to be the *relation of correctness for* shuffle-friendly *maps* $\mathcal{R}^{map}_{\phi_{\mathbb{CS}}}$ defined by

$$(pk, (c, c'), r') \in \mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}} \overset{\text{def}}{\iff} c' = \phi_{\mathbb{CS}}(pk, c\,;\, r').$$

We say that a *shuffle-friendly map* $\phi_{\mathbb{CS}}$ *achieves the associated zero-knowledge proof security property* when there exists a *zero-knowledge* proof $\mathbb{ZK}^{(\mu)}[\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}}]$ for the relation of correctness for *shuffle-friendly* maps $\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$ with $(2\mu+1)$ moves.

- **(Indistinguishability of $\phi_{\mathbb{CS}}$ output)** First, we define a decidable function $v^{(n)}_{\mathbb{CS}} : \mathcal{PK}_{\mathbb{CS}} \times \mathcal{C}^n_{\mathbb{CS}} \times \{0,1\}^* \longrightarrow \{0,1\}$, where $n \in \mathbb{N}^*$, such that, for all public key $pk \in \mathcal{PK}_{\mathbb{CS}}$, for all list of n ciphertexts $(c_i)^n_{i=1} \in \mathcal{C}^n_{\mathbb{CS}}$, for all additional information $v \in \{0,1\}^*$, the following property holds

$$v^{(n)}_{\mathbb{CS}}(pk, (c_i)^n_{i=1}, v) = 1 \overset{\text{def}}{\Longrightarrow} \exists\, sk \in \mathbb{F}(p_\eta), \begin{cases} & pk = \mathtt{pk}_{\mathbb{CS}}(sk) \\ \wedge & \forall\, i \in [\![1; n]\!], \mathrm{Dec}_{\mathbb{CS}}(sk, c_i) \neq \bot. \end{cases} \qquad (\Phi)$$

We call this function $v^{(n)}_{\mathbb{CS}}$ to be the *function of valid ciphertexts for the cryptosystem* $\mathbb{CS}$.
For an adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}})$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the *indistinguishability of $\phi_{\mathbb{CS}}$ output game* $\mathrm{Ind\text{-}CCA}^{\mathcal{A}}_{\phi_{\mathbb{CS}},\, v^{(2)}_{\mathbb{CS}}}(\eta, \rho\,;\,\beta)$ to be the cryptographic game defined in Game 11. Then, we define the *advantage of the adversary $\mathcal{A}$ against the indistinguishability game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*, \mathrm{Adv}_{\mathrm{Ind\text{-}CCA}}\Big[\mathcal{A} \mid \phi_{\mathbb{CS}},\, v^{(2)}_{\mathbb{CS}}\Big](\eta) \overset{\text{def}}{=} \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Ind\text{-}CCA}^{\mathcal{A}}_{\phi_{\mathbb{CS}},\, v^{(2)}_{\mathbb{CS}}}(\eta, \rho\,;\,\beta)\ \Big].$$

$\mathrm{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{S}\mathsf{im}_{\mathcal{R}}}\big(\eta, (\rho_h, \rho_a)\,;\,\beta\big)$ – HVZK property

Case $\beta = 0$	**Case** $\beta = 1$
$\sigma \leftarrow \mathcal{S}(\eta\,;\,\rho_h)$;	$\sigma \leftarrow \mathcal{S}(\eta\,;\,\rho_h)$;
$(x, w, \rho) \leftarrow \mathcal{A}(\eta, \sigma\,;\,\rho_a)$;	$(x, w, \rho) \leftarrow \mathcal{A}(\eta, \sigma\,;\,\rho_a)$;
$(m_i)_{i=1}^{2\mu+1} \leftarrow \Big(\mathcal{P}(w\,;\,\rho_h) \rightleftharpoons_{\mathcal{R}}^{(\mu)} \mathcal{V}(\rho)\Big)(\sigma, x)$;	$(m_i)_{i=1}^{2\mu+1} \leftarrow \mathcal{S}\mathsf{im}_{\mathcal{R}}(\sigma, x, \rho\,;\,\rho_h)$;
$b \leftarrow v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big)$;	$b \leftarrow v_{\mathcal{R}}^{\sigma,\,x}\big((m_i)_{i=1}^{2\mu+1}\big)$;
return $\big(\ \varphi_{\mathcal{R}}\big((\sigma, x, w)\big)\ \wedge\ b\ \big)$.	**return** $\big(\ \varphi_{\mathcal{R}}\big((\sigma, x, w)\big)\ \wedge\ b\ \big)$.

Game 9. Cryptographic game of Honest-Verifier Zero-Knowledge for *zero-knowledge* protocols

k-$\mathrm{SpSound}^{\mathcal{A}}_{\mathbb{ZK}^{(1)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}\big(\eta, (\rho_h, \rho_a)\big)$ – k-special-soundness

```
$\sigma \leftarrow \mathcal{S}(\eta\,;\,\rho_h)$ ;
$\big(x, (\langle \alpha, c_i, z_i \rangle)_{i=1}^{k}\big) \leftarrow \mathcal{A}(\eta, \sigma\,;\rho_a)$ ;
$b_{\neq} \leftarrow \bigwedge_{1 \leqslant i < j \leqslant k} c_i \neq c_j$ ;        $b_v \leftarrow \bigwedge_{i=1}^{k} v_{\mathcal{R}}^{\sigma,\,x}\big(\langle \alpha, c_i, z_i \rangle\big)$ ;
if $(\neg\,(b_{\neq} \wedge b_v))$ then return $0$ ;
$w \leftarrow \mathcal{E}_{\mathcal{R}}(\sigma, x, (\langle \alpha, c_i, z_i \rangle)_{i=1}^{k})$ ;
return $\varphi_{\mathcal{R}}\big((\sigma, x, w)\big)$.
```

Game 10. Cryptographic game of k-special-soundness for *zero-knowledge* protocols

$\text{Ind-CCA}^{(\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}})}_{\phi_{\mathbb{CS}},\, v_{\mathbb{CS}}^{(2)}}\big(\eta, (\rho_h, \rho_a)\,;\,\beta\big)$ – Indistinguishability

```
$(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta\,;\,\rho_h)$ ; $r \xleftarrow{\$} \mathcal{R}_{\mathbb{CS}}$ ;
$((c_0, c_1), v) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, pk\,;\,\rho_a)$ ;
if $\Big(\neg\, v_{\mathbb{CS}}^{(2)}\big(pk, (c_0, c_1), v\big)\Big)$ then return $0$ ;
$c'_\beta \leftarrow \phi_{\mathbb{CS}}(pk, c_\beta\,;\,r)$ ;
$b \leftarrow \mathcal{A}_{\mathsf{guess}}(c'_\beta\,;\,\rho_a)$ ;
return $(b = \beta)$.
```

Game 11. Cryptographic game of output indistinguishability for *shuffle-friendly* maps

We say that a *shuffle-friendly map* $\phi_{\mathbb{CS}}$ *achieves the indistinguishability of its output security property* when, for all function of valid ciphertext $v_{\mathbb{CS}}^{(2)}$ satisfying the property given by Eq. (Φ), for all adversary $\mathcal{A}$, the function $\mathrm{Adv}_{\text{Ind-CCA}}\Big[\mathcal{A}\ \Big|\ \phi_{\mathbb{CS}},\, v_{\mathbb{CS}}^{(2)}\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

*2) A full example – "*re-encryption only*" mode:* As an example of *shuffle-friendly* map, we present the case of "*re-encryption only*" for the El-Gamal cryptosystem discussed in [5]. The *El-Gamal cryptosystem* $\mathbb{EG}$ is defined as follows. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $g \in \mathbb{G}_{p_\eta}$ be a generator of the cyclic group of prime order p_η.

- The set of plaintexts is $\mathcal{M}_{\mathbb{EG}} = \mathbb{G}_{p_\eta}$, the set of public keys is $\mathcal{PK}_{\mathbb{EG}} = \mathbb{G}_{p_\eta}^2$, the set of randomness is $\mathcal{R}_{\mathbb{EG}} = \mathbb{F}(p_\eta)$, and the set of ciphertexts is $\mathcal{C}_{\mathbb{EG}} = \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}$;
- The key generation algorithm $\mathrm{KeyGen}_{\mathbb{EG}} : \mathbb{N}^* \longrightarrow \mathbb{F}(p_\eta) \times \mathbb{G}_{p_\eta}^2$ is a probabilistic polynomial-time algorithm which outputs a random secret key $sk \xleftarrow{\$} \mathbb{F}(p_\eta)$ and the associated public key $pk = (g, g^{sk}) \in \mathbb{G}_{p_\eta}^2$ on input a security parameter $\eta \in \mathbb{N}^*$;
- The encryption algorithm $\mathrm{Enc}_{\mathbb{EG}}$ is given by the following function

$$\begin{array}{rccl} \mathrm{Enc}_{\mathbb{EG}}^{(\eta)}: & \mathbb{G}_{p_\eta}^2 \times \mathbb{G}_{p_\eta} \times \mathbb{F}(p_\eta) & \longrightarrow & \mathbb{G}_{p_\eta}^2 \\ & \big((g, y), m, r\big) & \longmapsto & (g^r, y^r m); \end{array}$$

- The decryption algorithm $\mathrm{Dec}_{\mathbb{EG}}$ is given by the following function

$$\begin{array}{rccl} \mathrm{Dec}_{\mathbb{EG}}^{(\eta)}: & \mathbb{F}(p_\eta) \times \mathbb{G}_{p_\eta}^2 & \longrightarrow & \mathbb{G}_{p_\eta} \\ & \big(sk, (u, v)\big) & \longmapsto & v \cdot u^{-sk}. \end{array}$$

Notice that the *El-Gamal* cryptosystem $\mathbb{EG}$ is an homomorphic cryptosystem and verifies the Ind-CPA security property, because the cyclic group $\mathbb{G}_{p_\eta}$ verifies the *discrete logarithm* assumption. Then, the "*re-encryption only*" *shuffle-friendly* map $\phi_{\mathbb{EG}}^{\mathsf{reenc}}$ for the El-Gamal cryptosystem $\mathbb{EG}$ is defined by the following function

$$\boxed{\begin{array}{rccl} \phi_{\mathbb{EG}}^{\mathsf{reenc}}: & \mathbb{G}_{p_\eta}^2 \times \mathbb{G}_{p_\eta}^2 \times \mathbb{F}(p_\eta) & \longrightarrow & \mathbb{G}_{p_\eta}^2 \\ & \big((g, y), (u, v), r\big) & \longmapsto & (g^r \cdot u, y^r \cdot v). \end{array}}$$

Then, we verify all three mandatory security properties for *shuffle-friendly* maps.

- **(Decryption preservation)** Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\big(sk, (g, g^{sk})\big) \leftarrow \mathrm{KeyGen}_{\mathbb{EG}}(\eta)$ be an El-Gamal key pair. Let $(u, v) \in \mathbb{G}_{p_\eta}^2$ be a ciphertext and $r' \in \mathbb{F}(p_\eta)$ be a random value. We suppose the following property

$$\exists\,(m, r) \in \mathbb{G}_{p_\eta} \times \mathbb{F}(p_\eta), (u, v) = \mathrm{Enc}_{\mathbb{EG}}((g, y), m\,;\,r). \quad (\mathcal{H})$$

Then, we have

$$\begin{array}{lll} \multicolumn{2}{l}{\mathrm{Dec}_{\mathbb{EG}}(sk, \phi_{\mathbb{EG}}^{\mathsf{reenc}}((g, y), (u, v)\,;\,r'))} & \\ \quad = & \mathrm{Dec}_{\mathbb{EG}}\big(sk, (g^{r'} u, y^{r'} v)\big) & \text{(by definition of } \phi_{\mathbb{EG}}^{\mathsf{reenc}}\text{)} \\ \quad = & \mathrm{Dec}_{\mathbb{EG}}\big(sk, (g^{r'} g^{r}, y^{r'} y^{r} m)\big) & \text{(by hypothesis Eq. } (\mathcal{H})\text{)} \\ \quad = & \big(y^{r+r'} m\big) \cdot \big(g^{r+r'}\big)^{-sk} & \text{(by definition of } \mathrm{Dec}_{\mathbb{EG}}\text{)} \\ \quad = & \big(y^{r+r'} m\big) / \big(y^{r+r'}\big) & \\ \quad = & m = \mathrm{Dec}_{\mathbb{EG}}\big(sk, (u, v)\big). & \end{array}$$

Hence, the *decryption preservation* security property is verified by the *shuffle-friendly* map $\phi_{\mathbb{EG}}^{\mathsf{reenc}}$.

- **(Associated *zero-knowledge* proof)** Let $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{EG}}^{\mathsf{reenc}}}$ be the protocol defined as follows in Protocol 1. Hence, this 3-move protocol $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{EG}}^{\mathsf{reenc}}}$ defines a Σ-protocol for the computable relation for *shuffle-friendly* maps $\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{EG}}^{\mathsf{reenc}}}$. Consequently, the *shuffle-friendly* map $\phi_{\mathbb{EG}}^{\mathsf{reenc}}$ verifies the *associated zero-knowledge proof* security property.

```
Protocol 1: $\Sigma$-protocol $\Sigma^{\mathsf{map}}_{\phi^{\mathsf{reenc}}_{\mathbb{EG}}}$ – Correct output for the shuffle-friendly map $\phi^{\mathsf{reenc}}_{\mathbb{EG}}$.

Public Input :  A security parameter $\eta \in \mathbb{N}^*$. A public key $pk = (g, y) \in \mathbb{G}^2_{p_\eta}$. Two ciphertexts $c = (u, v), c' = (u', v') \in \mathbb{G}^2_{p_\eta}$.
Private Input:  A random value $r \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)$ such that $c' = \phi^{\mathsf{reenc}}_{\mathbb{EG}}(pk, c\,;\, r)$.
Begin protocol
    1) (Commitment message) The prover $\mathcal{P}_{\mathsf{map}}$ chooses a random value $s \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)$. Then, $\mathcal{P}_{\mathsf{map}}$ computes $(\alpha, \beta) = (g^s, y^s)$, and hands it to the verifier $\mathcal{V}_{\mathsf{map}}$.
    2) (Challenge message) The verifier $\mathcal{V}_{\mathsf{map}}$ chooses uniformly at random a challenge $\gamma \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^*$ and sends it to $\mathcal{P}_{\mathsf{map}}$.
    3) (Response message) $\mathcal{P}_{\mathsf{map}}$ computes the value $\delta = \gamma \cdot r + s \in \mathbb{F}(p_\eta)$ and sends back to $\mathcal{V}_{\mathsf{map}}$ the response $\delta$.
    4) (Conclusion's bit) The verifier $\mathcal{V}_{\mathsf{map}}$ accepts if and only if the following equations hold.
           $g^\delta = \left(\frac{u}{u'}\right)^\gamma \alpha$   and   $y^\delta = \left(\frac{v}{v'}\right)^\gamma \beta.$
End
```

- **(Indistinguishability of $\phi^{\mathsf{reenc}}_{\mathbb{EG}}$ output)** Let $v^{(2)}_{\mathbb{EG}} : \mathbb{G}^2_{p_\eta} \times \left(\mathbb{G}^2_{p_\eta}\right)^2 \times \{0,1\}^* \longrightarrow \{0,1\}$ be a function of valid ciphertext satisfying the property Eq. (Φ), *i.e.* such that

$$\forall\, pk = (g, y) \in \mathbb{G}^2_{p_\eta}, \forall\, c_0, c_1 \in \mathbb{G}^2_{p_\eta}, \forall\, v \in \{0,1\}^*,$$
$$v^{(2)}_{\mathbb{EG}}\big(pk, (c_0, c_1), v\big) = 1 \implies \exists\, sk \in \mathbb{F}(p_\eta),$$
$$y = g^{sk} \ \wedge \bigwedge_{i \in \{0,1\}} \left(\mathrm{Dec}_{\mathbb{EG}}(sk, c_i) \neq \bot\right). \quad (\mathcal{H})$$

Let $\mathcal{A} = \left(\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}}\right)$ be an adversary. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\rho = (\rho_h, \rho_a) \in \mathbb{T}$ be an adversarial-honest random tapes pair. Let $(sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{EG}}(\eta\,;\, \rho_h)$ be an honest pair of keys for the *El-Gamal* cryptosystem $\mathbb{EG}$ where $pk = (g, y)$ with $y = g^{sk}$. Let $r \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)$ be an honest random value (meaning that r is computed by using the honest random tape ρ_h). Let $\big((c_0, c_1), v\big) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, pk\,;\, \rho_a)$ be an adversarial setup material. Let suppose that we have indeed $v^{(2)}_{\mathbb{EG}}\big(pk, (c_0, c_1), v\big) = 1$. Therefore, by the hypothesis Eq. ($\mathcal{H}$) on the valid ciphertext function $v^{(2)}_{\mathbb{EG}}$, there exists a secret key $sk' \in \mathbb{F}(p_\eta)$ such that $y = g^{sk'}$. However, by definition of y, we have also $y = g^{sk}$. Thus, we have $g^{sk} = g^{sk'}$. By the *discrete logarithm* assumption for the cyclic group $\mathbb{G}_{p_\eta}$, we conclude, with *overwhelming probability*, that $sk = sk'$. Hence, by the hypothesis Eq. ($\mathcal{H}$), we conclude that, for all $b \in \{0,1\}$, $\mathrm{Dec}_{\mathbb{EG}}(sk, c_b) \neq \bot$. Said differently, we have, for all $b \in \{0,1\}$, the existency of a plaintext $m_b \in \mathbb{G}_{p_\eta}$ and a random value $r_b \in \mathbb{F}(p_\eta)$ such that $c_b = \mathrm{Enc}_{\mathbb{EG}}(pk, m_b\,;\, r_b)$. For $b \in \{0,1\}$, let $c'_b \in \mathbb{G}^2_{p_\eta}$ be the ciphertext defined by $c'_b = \phi^{\mathsf{reenc}}_{\mathbb{EG}}(pk, c_b\,;\, r)$. As $\mathbb{EG}$ is an homomorphic cryptosystem, and by definitions of c_b and c'_b, the following property holds

$$\forall\, b \in \{0,1\},\ c'_b = \mathrm{Enc}_{\mathbb{EG}}(pk, m_b\,;\, r + r_b).$$

Because the *El-Gamal* cryptosystem $\mathbb{EG}$ verifies the Ind-CPA security property, we conclude that the following quantity is negligible in the security parameter $\eta \in \mathbb{N}^*$

$$\Big|\, \Pr_{\rho_a \in \mathbb{T}^{\mathsf{a}}}\left[\, 0 \leftarrow \mathcal{A}_{\mathsf{guess}}(c'_0\,;\, \rho_a)\,\right] - \Pr_{\rho_a \in \mathbb{T}^{\mathsf{a}}}\left[\, 1 \leftarrow \mathcal{A}_{\mathsf{guess}}(c'_1\,;\, \rho_a)\,\right] \Big|.$$

Consequently, the function $\mathrm{Adv}_{\text{Ind-CCA}}\left[\mathcal{A} \,\middle|\, \phi^{\mathsf{reenc}}_{\mathbb{EG}},\, v^{(2)}_{\mathbb{EG}}\right]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$, *i.e.* the *shuffle-friendly* map $\phi^{\mathsf{reenc}}_{\mathbb{EG}}$ verifies the *indistinguishability of its output* security property.

Appendix B
Specification of the Terelius-Wikström protocol

Let $\phi_{\mathbb{CS}}$ be a *shuffle-friendly map* for the cryptosystem $\mathbb{CS}$ with ciphertext set denoted by $\mathcal{C}_{\mathbb{CS}}$. Let $N \in \mathbb{N}^*$ be a *constant* natural number. Let $\eta \in \mathbb{N}^*$ be a security parameter and $p_\eta \in \mathbb{N}^*$ be a η-bits size prime, *i.e.* $\log_2 p_\eta \geqslant \eta$. We suppose that the randomness set used by the cryptosystem $\mathbb{CS}$ is the finite field $\mathbb{F}(p_\eta)$ of cardinality p_η.

We define

$$\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}} \subseteq \underbrace{\left(\mathbb{G}^{N+1}_{p_\eta} \times \mathcal{PK}_{\mathbb{CS}}\right)}_{\text{Public parameter set}} \times \underbrace{\left(\mathbb{G}^{N}_{p_\eta} \times \mathcal{C}^{N}_{\mathbb{CS}} \times \mathcal{C}^{N}_{\mathbb{CS}}\right)}_{\text{Statement set}} \times \underbrace{\left(\mathsf{Mat}_N(\mathbb{F}(p_\eta)) \times \mathbb{F}(p_\eta)^N \times \mathbb{F}(p_\eta)^N\right)}_{\text{Witness set}}$$

to be the *relation of the Terelius-Wikström protocol* defined by

$$((ck, pk), (\mathbf{a}, \mathbf{c}, \mathbf{c}'), (\pi, \mathbf{r}, \mathbf{s})) \in \mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}} \overset{\text{def}}{\iff} \begin{cases} \mathbf{a} = \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, \pi\,;\, \mathbf{r}) \\ \forall\, i \in [\![1; N]\!], c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i) \end{cases}$$

To prove this relation with *zero-knowledge* proofs, we define two families of Σ-protocols, one occuring as a preliminary work, called this way the *offline proof*, and the other one occuring only when the election is closed and the result is about to be computed, called this way the *online proof*. Each of these two families have an extra dependency in a random public vector honestly output by the verifier with the honest random tape.

A. Σ-*protocols family for the* offline *phase* $\left(\Sigma_{\mathsf{off}}(\mathbf{e})\right)_{\mathbf{e} \in \mathbb{F}(p_\eta)^N}$

We define

$$\mathcal{R}^{\mathsf{off}} \subseteq \underbrace{\left(\mathbb{G}^{N+1}_{p_\eta}, \mathbb{F}(p_\eta)^N\right)}_{\text{Public parameter set}} \times \underbrace{\mathbb{G}^{N}_{p_\eta}}_{\text{Statement set}} \times \underbrace{\left(\mathbb{F}(p_\eta) \times \mathbb{F}(p_\eta)^N \times \mathbb{F}(p_\eta)\right)}_{\text{Witness set}}$$

to be the *offline relation of the Terelius-Wikström protocol* defined by

$$
\begin{aligned}
&((ck,\mathbf{e}),\mathbf{a},(t,\mathbf{e}',k)) \in \mathcal{R}^{\mathsf{off}}\\
&\overset{\text{def}}{\iff} \begin{cases} & \mathbf{a} \circledast \mathbf{1} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{1}\,;\, t)\\ \wedge & \mathbf{a} \circledast \mathbf{e} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'\,;\, k)\\ \wedge & \prod_{i=1}^N e_i = \prod_{i=1}^N e'_i \end{cases}
\end{aligned}
$$

A Σ-protocol family proving this relation is given by the Protocol 2, according to Terelius-Wikström papers [4].

As shown in the paper [4], we have the following property.

Proposition 1. *On the hypothesis of* perfectly hiding *and* computationally binding *commitment schemes* $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ *and* $\mathbb{KS}[\mathsf{Mat}_N(\mathbb{F}(p_\eta))]$*, and on the hypothesis of* discrete logarithm *assumption on the set of group* $\left(\mathbb{G}_{p_\eta}\right)_{\eta\in\mathbb{N}^*}$*, the following property holds. The* offline proofs *family* $\left(\Sigma_{\mathsf{off}}(\mathbf{e})\right)_{\mathbf{e}\in\mathbb{F}(p_\eta)^N}$ *given by the Protocol 2 is a family of* computationally complete *Σ-protocols for the relation $\mathcal{R}^{\mathsf{off}}$.*

B. Σ-protocols family for the online *phase* $\left(\Sigma_{\mathsf{on}}(\mathbf{e})\right)_{\mathbf{e}\in\mathbb{F}(p_\eta)^N}$

By the property of *associated zero-knowledge proof* verified by the *shuffle-friendly map*, there exists a Σ-protocol $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$ proving the relation for *shuffle-friendly map* $\mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$. We denote by $\alpha^{(\phi_{\mathbb{CS}})}_{\mathsf{map}}$ the probabilistic function outputting a *commitment message* according to the specification of the Σ-protocol $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$ on input a public key $pk \in \mathcal{PK}_{\mathbb{CS}}$, a statement $(c,c') \in \mathcal{C}^2_{\mathbb{CS}}$, and a witness $u \in \mathbb{F}(p_\eta)$. Besides, we denote by $z^{(\phi_{\mathbb{CS}})}_{\mathsf{map}}$ the probabilistic function outputting a *response message* according to $\Sigma^{\mathsf{map}}_{\phi_{\mathbb{CS}}}$ on input a public key $pk \in \mathcal{PK}_{\mathbb{CS}}$, a statement $(c,c') \in \mathcal{C}^2_{\mathbb{CS}}$, a witness $u \in \mathbb{F}(p_\eta)$, a commitment message α and a challenge $\gamma \in \mathbb{F}(p_\eta)^*$. We define

$$
\begin{aligned}
\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}} \subseteq \underbrace{\left(\mathbb{G}^{N+1}_{p_\eta} \times \mathcal{PK}_{\mathbb{CS}} \times \mathbb{F}(p_\eta)^N\right)}_{\text{Public parameter set}} &\times \underbrace{\left(\mathbb{G}^N_{p_\eta} \times \mathcal{C}^N_{\mathbb{CS}} \times \mathcal{C}^N_{\mathbb{CS}}\right)}_{\text{Statement set}}\\
&\times \underbrace{\left(\mathbb{F}(p_\eta)^N \times \mathbb{F}(p_\eta) \times \mathbb{F}(p_\eta)\right)}_{\text{Witness set}}
\end{aligned}
$$

to be the *online relation of the Terelius-Wikström protocol* defined by

$$
\begin{aligned}
&((ck,pk,\mathbf{e}),(\mathbf{a},\mathbf{c},\mathbf{c}'),(\mathbf{e}',k,u)) \in \mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}\\
&\overset{\text{def}}{\iff} \begin{cases} & \mathbf{a} \circledast \mathbf{e} = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'\,;\, k)\\ \wedge & \left(pk, \left(\mathbf{c} \circledast \mathbf{e}, \mathbf{c}' \circledast \mathbf{e}'\right), u\right) \in \mathcal{R}^{\mathsf{map}}_{\phi_{\mathbb{CS}}} \end{cases}
\end{aligned}
$$

A Σ-protocol family proving this relation is given by the Protocol 3, according to Terelius-Wikström papers [4].

As shown in the paper [4], we have the following property.

Proposition 2. *We suppose the* zero-knowledge *proof* $\Sigma^{map}_{\phi_{\mathbb{CS}}}$ *to be a Σ-protocol for the relation* $\mathcal{R}^{map}_{\phi_{\mathbb{CS}}}$*. Then, the* online proofs *family* $\left(\Sigma^{\phi_{\mathbb{CS}}}_{on}(\mathbf{e})\right)_{\mathbf{e}\in\mathbb{F}(p_\eta)^N}$ *given by the Protocol 3 is a family of Σ-protocols for the relation* $\mathcal{R}^{on}_{\phi_{\mathbb{CS}}}$.

Protocol 2: Σ-protocol $\Sigma_{\text{off}}(\mathbf{e})$ – *offline proof* – Correct commitment Σ-protocol using a vector $\mathbf{e} \in \mathbb{F}(p_\eta)^N$

Public Input : A natural number $N \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g,\mathbf{g}) \in \mathbb{G}^{N+1}_{p_\eta}$ for the commitment schemes $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ and $\mathbb{KS}[\mathsf{Mat}_N(\mathbb{F}(p_\eta))]$. Two vectors $\mathbf{a} \in \mathbb{G}^N_{p_\eta}$ and $\mathbf{e} \in \mathbb{F}(p_\eta)^N$.

Private Input: A permutation $\pi \in \Pi_N(\mathbb{F}(p_\eta))$ and a vector of random values $\mathbf{s} \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^N$ such that $\mathbf{a} = \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, \pi\,;\,\mathbf{s})$.

Begin protocol

1) **(Commitment message)** The prover $\mathcal{P}_{\text{off}}(\mathbf{e})$ defines $\mathbf{e}' = \pi \cdot \mathbf{e} \in \mathbb{F}(p_\eta)^N$, $t = \langle \mathbf{1} \mid \mathbf{s}\rangle \in \mathbb{F}(p_\eta)$ and $k = \langle \mathbf{s} \mid \mathbf{e}\rangle \in \mathbb{F}(p_\eta)$. Then, $\mathcal{P}_{\text{off}}(\mathbf{e})$ chooses two vectors of random values $\mathbf{r},\mathbf{s}' \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^N$ and three random values $s_\gamma, s_\delta, s_\epsilon \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)$. We set $B_0 = g_1$ and $\mathcal{P}_{\text{off}}(\mathbf{e})$ computes the following values
$$
\begin{gathered}
\forall\, i \in [\![1;N]\!],\ B_i = g^{r_i} B^{e'_i}_{i-1}, \quad \text{and} \quad \beta_i = g^{s_i} B^{s'_i}_{i-1}\\
\gamma = g^{s_\gamma} \prod_{i=1}^N g_i^{s'_i},\ \delta = g^{s_\delta}, \quad \text{and} \quad \epsilon = g^{s_\epsilon}
\end{gathered}
$$
Finally, $\mathcal{P}_{\text{off}}(\mathbf{e})$ hands to the verifier $\mathcal{V}_{\text{off}}(\mathbf{e})$ the commitment message $\alpha = \left((B_i)_{i=1}^N, \gamma, (\beta_i)_{i=1}^N, \delta, \epsilon\right)$.
2) **(Challenge message)** $\mathcal{V}_{\text{off}}(\mathbf{e})$ chooses uniformly at random a challenge $c \overset{\$}{\leftarrow} \mathbb{F}(p_\eta)^*$ and sends it to $\mathcal{P}_{\text{off}}(\mathbf{e})$.
3) **(Response message)** We set $e''_1 = s_1$ and, for all $i \in [\![2;N]\!]$, $e''_i = e''_{i-1}e'_i + s_i$. Then, $\mathcal{P}_{\text{off}}(\mathbf{e})$ computes the following values in $\mathbb{F}(p_\eta)$:
$$
\begin{gathered}
\forall\, i \in [\![1;N]\!],\ d'_i = ce'_i + s'_i, \quad \text{and} \quad d_i = cr_i + s_i\\
d_\gamma = ck + s_\gamma,\ d_\delta = ct + s_\delta, \quad \text{and} \quad d_\epsilon = ce''_N + s_\epsilon
\end{gathered}
$$
Finally, $\mathcal{P}_{\text{off}}(\mathbf{e})$ sends to $\mathcal{V}_{\text{off}}(\mathbf{e})$ the response message $z(c) = \left((d'_i)_{i=1}^N, d_\gamma, (d_i)_{i=1}^N, d_\delta, d_\epsilon\right)$.
4) **(Conclusion's bit)** The verifier $\mathcal{V}_{\text{off}}(\mathbf{e})$ accepts if and only if the following equations hold:
$$
\begin{gathered}
\left(\mathbf{a} \circledast \mathbf{1} \middle/ \prod_{i=1}^N g_i\right)^c \delta = g^{d_\delta},\\
\left(\mathbf{a} \circledast \mathbf{e}\right)^c \gamma = g^{d_\gamma} \prod_{i=1}^N g_i^{d'_i},\\
\forall\, i \in [\![1;N]\!],\ B_i^c \beta_i = g^{d_i} B^{d'_i}_{i-1},\\
\left(B_N \middle/ g_1^{\prod_{i=1}^N e_i}\right)^c \epsilon = g^{d_\epsilon}.
\end{gathered}
$$

End

Protocol 3: Σ-protocol $\Sigma_{\mathsf{on}}^{\phi_{\mathbb{CS}}}(\mathbf{e})$ – *online proof* – Correct shuffle *zero-knowledge* proof using a *shuffle-friendly map* $\phi_{\mathbb{CS}}$ and a vector $\mathbf{e} \in \mathbb{F}(p_\eta)^N$

Public Input : A natural number $N \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A public key $pk \in \mathcal{PK}_{\mathbb{CS}}$ of a cryptosystem $\mathbb{CS}$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{N+1}$ for the commitment schemes $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ and $\mathbb{KS}[\mathsf{Mat}_N(\mathbb{F}(p_\eta))]$. Two vectors $\mathbf{a} \in \mathbb{G}_{p_\eta}^N$ and $\mathbf{e} \in \mathbb{F}(p_\eta)^N$. Two lists of ciphertexts $\mathbf{c} = (c_i)_{i=1}^N, \mathbf{c}' = (c'_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$.

Private Input: A permutation $\pi \in \Pi_N(\mathbb{F}(p_\eta))$ and a vector of random values $\mathbf{s} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ such that $\mathbf{a} = \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, \pi\,;\, \mathbf{s})$. A vector of random values $\mathbf{r} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ such that, for all $i \in [\![1;N]\!]$, $c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i)$.

Begin protocol

1) **(Commitment message)** The prover $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ defines $\mathbf{e}' = \pi \cdot \mathbf{e} \in \mathbb{F}(p_\eta)^N$, $k = \langle \mathbf{s} \mid \mathbf{e} \rangle \in \mathbb{F}(p_\eta)$, and $u = \langle \mathbf{r} \mid \mathbf{s} \rangle \in \mathbb{F}(p_\eta)$. Then, $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ chooses a vector of random values $\mathbf{s}' \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ and a random value $s_\mu \xleftarrow{\$} \mathbb{F}(p_\eta)$. At this step, $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ computes the following values

$$\lambda = \alpha_{\mathsf{map}}^{(\phi_{\mathbb{CS}})}\big(pk,\, (\mathbf{c} \circledast \mathbf{e}, \mathbf{c}' \circledast \mathbf{e}'),\, u\big),$$
$$\text{and} \quad \mu = g^{s_\mu} \prod_{i=1}^{N} g_i^{s'_i}.$$

Finally, $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ hands to the verifier $\mathcal{V}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ the commitment message $\alpha = (\lambda, \mu)$.

2) **(Challenge message)** $\mathcal{V}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ chooses uniformly at random a challenge $\gamma \xleftarrow{\$} \mathbb{F}(p_\eta)^*$ and sends it to $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$.

3) **(Response message)** $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ computes the following values in $\mathbb{F}(p_\eta)$:

$$d_\lambda = \mathfrak{z}_{\mathsf{map}}^{(\phi_{\mathbb{CS}})}\big(pk,\, (\mathbf{c} \circledast \mathbf{e}, \mathbf{c}' \circledast \mathbf{e}'),\, u,\, \lambda,\, \gamma\big),$$
$$d_\mu = \gamma k + s_\mu, \quad \text{and} \quad \forall\, i \in [\![1;N]\!],\ d'_i = \gamma e'_i + s'_i.$$

Finally, $\mathcal{P}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ sends to $\mathcal{V}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ the response $z = \big(d_\lambda, (d'_i)_{i=1}^N, d_\mu\big)$.

4) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e})$ accepts if and only if the following equations hold:

$$v_{\mathsf{map}}^{pk,\,(\mathbf{c}\circledast\mathbf{e},\ \mathbf{c}'\circledast\mathbf{e}')}\big(\langle \lambda, \gamma, d_\lambda \rangle\big) = 1,$$
$$\text{and} \quad \big(\mathbf{a} \circledast \mathbf{e}\big)^\gamma \mu = g^{d_\mu} \prod_{i=1}^{N} g_i^{d'_i}$$

End

C. 9-move protocol of the Terelius-Wikström shuffle

Based on the two Σ-protocols families $\big(\Sigma_{\mathsf{off}}(\mathbf{e})\big)_{\mathbf{e}\in\mathbb{F}(p_\eta)^N}$, proving the relation $\mathcal{R}^{\mathsf{off}}$, and $\big(\Sigma_{\mathsf{on}}^{\phi_{\mathbb{CS}}}(\mathbf{e})\big)_{\mathbf{e}\in\mathbb{F}(p_\eta)^N}$, proving the relation $\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{on}}$, we define a 9-move shuffle protocol (Protocol 4) following the definition given in [4].

This 9-move protocol achieves both of security properties we expect from a shuffle protocol used by mix-servers of a mixnet protocol[2], namely the *permutation secrecy* and the *verifiability* properties. Now, we give the complete cryptographic definition of both security properties for a shuffle protocol.

1) Permutation secrecy *property:* Informally, we ask $\mathcal{A}$ to generate two permutations π_0 and π_1 in $\mathfrak{S}_N$ and send them to the mix-server. Then, the mix-server secretely chooses one of them, depending on a secret random bit $\beta \in \{0,1\}$, and mixes the ballots with the permutation π_β. At this step, $\mathcal{A}$ takes all the mix-server outputs and tries to guess the secret bit β. $\mathcal{A}$ wins the *permutation secrecy game* $\mathrm{Secrecy}^{\mathcal{A}}\big(1^\eta\,;\,\beta\big)$ if they correctly guess the secret bit β. If they cannot win the game with significant probability, then we consider that the permutation secrecy is guaranteed.

Let $v_{\mathbb{CS}}^{(N)} : \mathcal{PK}_{\mathbb{CS}} \times \mathcal{C}_{\mathbb{CS}}^N \times \{0,1\}^* \longrightarrow \{0,1\}$ a function of valid ciphertexts for the cryptosystem $\mathbb{CS}$ (*i.e.* verifying the property given in Eq. (Φ)). For an adversary $\mathcal{A} = \big(\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{guess}}\big)$, a security parameter $\eta \in \mathbb{N}^*$, a random tape $\rho \in \mathbb{T}$, and a secret bit $\beta \in \{0,1\}$, we define the cryptographic *permutation secrecy game* $\mathrm{Secrecy}_{\mathbb{ZK}^{(4)}[\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{TW}}],\, v_{\mathbb{CS}}^{(N)}}^{\mathcal{A}}\big(\eta, \rho\,;\,\beta\big)$ to be the cryptographic game defined in Game 12.

We define the *advantage of the adversary $\mathcal{A}$ against the permutation secrecy game* to be the following function

$$\forall\,\eta \in \mathbb{N}^*, \mathrm{Adv}_{\mathrm{Secrecy}}\Big[\mathcal{A} \,\Big|\, \mathbb{ZK}^{(4)}[\mathcal{R}_{\mathcal{R}}^{\mathsf{TW}}]\Big]\,(\eta) \overset{\text{def}}{=}$$
$$\Bigg|\, \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Secrecy}_{\mathbb{ZK}^{(4)}[\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{TW}}],\, v_{\mathbb{CS}}^{(N)}}^{\mathcal{A}}\big(\eta, \rho\,;\,\beta = 0\big)\ \Big]$$
$$- \Pr_{\rho\in\mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Secrecy}_{\mathbb{ZK}^{(4)}[\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{TW}}],\, v_{\mathbb{CS}}^{(N)}}^{\mathcal{A}}\big(\eta, \rho\,;\,\beta = 1\big)\ \Big]\,\Bigg|.$$

Hence, we say that *the Terelius-Wikström shuffle protocol achieves permutation secrecy* when, for all function of valid ciphertexts $v_{\mathbb{CS}}^{(N)} : \mathcal{PK}_{\mathbb{CS}} \times \mathcal{C}_{\mathbb{CS}}^N \times \{0,1\}^* \longrightarrow \{0,1\}$, for all (1) adversary $\mathcal{A}$, the function $\mathrm{Adv}_{\mathrm{Secrecy}}\Big[\mathcal{A} \,\Big|\, \mathbb{ZK}^{(4)}[\mathcal{R}_{\mathcal{R}}^{\mathsf{TW}}]\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

2) Verifiability *property:* Roughly speaking, the verifiability property means that $\mathcal{A}$ first outputs a vector $\mathbf{a} \in \mathbb{F}(p_\eta)^N$ along with a proof transcript $\mathfrak{p}_{\mathsf{off}}(\mathbf{e}_\pi)$ showing the relation $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_\pi)$ for some vector $\mathbf{e}_\pi \in \mathbb{F}(p_\eta)^N$ computed by the verifier $\mathcal{V}$. Then, $\mathcal{A}$ outputs two ciphertexts lists $\mathbf{c}, \mathbf{c}' \in \mathcal{C}_{\mathbb{CS}}^N$ of length N and a secret key $sk \in \mathbb{F}(p_\eta)$ along with a proof transcript $\mathfrak{p}_{\mathsf{on}}(\mathbf{e}_\phi)$ showing the relation $\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{shuffle}}(\mathbf{e}_\phi)$ for some other vector $\mathbf{e}_\phi \in \mathbb{F}(p_\eta)^N$. $\mathcal{A}$ wins the *verifiability game*

[2] While we do not prove it here for reasons of conciseness, it follows from the proof that the 9-move protocol $\mathbb{ZK}^{(4)}[\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{TW}}]$ actually satisfies the *computational completeness*, the *knowledge soundness* [29] and the *perfect Honest-Verifier Zero-Knowledge* properties. It is therefore an *argument of knowledge* of the computable relation $\mathcal{R}_{\phi_{\mathbb{CS}}}^{\mathsf{TW}}$.

```
$\mathrm{Secrecy}^{(\mathcal{A}_{setup},\mathcal{A}_{guess})}_{\mathbb{ZK}^{(4)}[\mathcal{R}^{TW}_{\phi_{\mathbb{CS}}}],\, v^{(N)}_{\mathbb{CS}}}\big(\eta, (\rho_h, \rho_a)\,;\,\beta\big)$ – Permutation secrecy property
$ck \leftarrow \mathrm{Gen}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(\eta\,;\,\rho_h)\ ;\ (sk, pk) \leftarrow \mathrm{KeyGen}_{\mathbb{CS}}(\eta\,;\,\rho_h)\ ;$
$\big((\mathbf{c}, v), (\pi_0, \pi_1), \rho\big) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, (ck, pk)\,;\,\rho_a)\ ;$
$\textbf{if}\ \Big(\neg\ \big(v^{(N)}_{\mathbb{CS}}(pk, \mathbf{c}, v)\big)\Big)\ \textbf{then return}\ 0\ ;$
$\overrightarrow{\mathbf{m}}_{\pi_\beta} \leftarrow \Big(\mathcal{P}^{(\phi_{\mathbb{CS}})}_{\mathsf{TW}}\big(\rho_h[\ (\pi \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))) \mapsto \pi_\beta\ ]\big) \rightleftharpoons^{(4)}_{\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}} \mathcal{V}^{(\phi_{\mathbb{CS}})}_{\mathsf{TW}}(\rho)\Big)((ck, pk), \mathbf{c})\ ;$
$b \leftarrow \mathcal{A}_{\mathsf{guess}}(\overrightarrow{\mathbf{m}}_{\pi_\beta}\,;\,\rho_a)\ ;$
$\textbf{return}\ (1 - b \oplus \beta).$
```

Game 12. Cryptographic game of permutation secrecy for the Terelius-Wikström shuffle protocol

$\mathrm{Verif}^{\mathcal{A}}(1^\eta)$ when the proofs are accepted by the verifier, but the decryption of the output ciphertexts list $\mathbf{c}'$ leads to a different decryption than the decryption of the input ciphertexts list $\mathbf{c}$. For an adversary $\mathcal{A} = (\mathcal{A}_{\mathsf{setup}}, \mathcal{A}_{\mathsf{prove}})$, a security parameter $\eta \in \mathbb{N}^*$, and a random tape $\rho \in \mathbb{T}$, we define the cryptographic *verifiability game* $\mathrm{Verifiability}^{\mathcal{A}}_{\mathbb{ZK}^{(4)}[\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}]}(\eta, \rho)$ to be the cryptographic game defined in Game 13.

```
$\mathrm{Verifiability}^{(\mathcal{A}_{setup},\mathcal{A}_{prove})}_{\mathbb{ZK}^{(4)}[\mathcal{R}^{TW}_{\phi_{\mathbb{CS}}}]}\big(\eta, (\rho_h, \rho_a)\big)$ – Verifiability property
$ck \leftarrow \mathrm{Gen}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(\eta\,;\,\rho_h)\ ;$
$(sk, \mathbf{c}) \leftarrow \mathcal{A}_{\mathsf{setup}}(\eta, ck\,;\,\rho_a)\ ;$
$\textbf{if}\ \Big(\neg\ \big(\mathbf{wf}^{(N)}_{\mathbb{CS}}(sk, \mathbf{c})\big)\Big)\ \textbf{then return}\ 0\ ;$
$\overrightarrow{m} \leftarrow \Big(\mathcal{A}_{\mathsf{prove}}(\rho_a) \rightleftharpoons^{(4)}_{\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}} \mathcal{V}^{(\phi_{\mathbb{CS}})}_{\mathsf{TW}}(\rho_h)\Big)((ck, \mathtt{pk}_{\mathbb{CS}}(sk)), \mathbf{c})\ ;$
$\big(\mathbf{a}, \mathbf{e}_{\mathsf{off}}, \alpha_{\mathsf{off}}, \gamma_{\mathsf{off}}, (z_{\mathsf{off}}, \mathbf{c}'), \mathbf{e}_{\mathsf{on}}, \alpha_{\mathsf{on}}, \gamma_{\mathsf{on}}, z_{\mathsf{on}}\big) \leftarrow \overrightarrow{m}\ ;$
$b_{\mathsf{off}} \leftarrow v^{(ck, \mathbf{e}_{\mathsf{off}}),\, \mathbf{a}}_{\mathcal{R}^{\mathsf{off}}}\big(\langle \alpha_{\mathsf{off}}, \gamma_{\mathsf{off}}, z_{\mathsf{off}}\rangle\big)\ ;$
$b_{\mathsf{on}} \leftarrow v^{(ck, \mathtt{pk}_{\mathbb{CS}}(sk), \mathbf{e}_{\mathsf{on}}),\, (\mathbf{a}, \mathbf{c}, \mathbf{c}')}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\big(\langle \alpha_{\mathsf{on}}, \gamma_{\mathsf{on}}, z_{\mathsf{on}}\rangle\big)\ ;$
$\textbf{if}\ (\neg\,(b_{\mathsf{off}} \wedge b_{\mathsf{on}}))\ \textbf{then return}\ 0\ ;$
$\textbf{if}\ \big($ equal_multisets  (decrypt_list $sk$ $\mathbf{c}$)
                                   (decrypt_list $sk$ $\mathbf{c}'$) $\big)$
$\textbf{then return}\ 0\ ;$
$\textbf{else return}\ 1\ ;$
```

Game 13. Cryptographic game of verifiability for the Terelius-Wikström shuffle protocol

We define the *advantage of the adversary $\mathcal{A}$ against the verifiability game* to be the following function

$$\forall\, \eta \in \mathbb{N}^*, \mathrm{Adv}_{\mathrm{Verifiability}}\Big[\mathcal{A}\ \Big|\ \mathbb{ZK}^{(4)}[\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}]\Big](\eta) \stackrel{\mathrm{def}}{=} \Pr_{\rho \in \mathbb{T}}\Big[\ 1 \leftarrow \mathrm{Verifiability}^{\mathcal{A}}_{\mathbb{ZK}^{(4)}[\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}]}(\eta, \rho)\ \Big].$$

Hence, we say that *the Terelius-Wikström shuffle protocol achieves verifiability* when the function $\mathrm{Adv}_{\mathrm{Verifiability}}\Big[\mathcal{A}\ \Big|\ \mathbb{ZK}^{(4)}[\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}]\Big]$ is negligible in the security parameter $\eta \in \mathbb{N}^*$.

Appendix C
Generalised subterms and freshness properties

In this section, we recall definition of generalised subterms from [12]. Let $\mathcal{E}$ be an environment. We define the *generalised subterms set $\mathcal{ST}_{\mathcal{E}}(t)$ of a term t with respect to the environment $\mathcal{E}$* to be a set of triples $(\overrightarrow{\alpha}, \phi, t')$, called *occurrences*, where $\overrightarrow{\alpha}$ is a sequence of typed variables that are freshly bounded, *i.e.* variables bounded in $\overrightarrow{\alpha}$ are not bounded in $\mathcal{E}$. Hence, we define the new environment $\mathcal{E}_\alpha = (\mathcal{E}, \overrightarrow{\alpha})$. Then, terms $\phi : \mathbf{bool}$ and $t' : \tau$ of occurrences in the set $\mathcal{ST}_{\mathcal{E}}(t)$ are *well-typed* terms in the new environment $\mathcal{E}_\alpha$. For a set $\mathbb{S}$ of occurrences, we define

$$[\phi]\mathbb{S} \stackrel{\mathrm{def}}{=} \{(\overrightarrow{\alpha}, \psi \wedge \phi, t)\ |\ (\overrightarrow{\alpha}, \psi, t) \in \mathbb{S}\}$$
$$(x : \tau).\mathbb{S} \stackrel{\mathrm{def}}{=} \{((\overrightarrow{\alpha}, x : \tau), \psi, t)\ |\ (\overrightarrow{\alpha}, \psi, t) \in \mathbb{S}\}.$$

Set of generalised subterms $\mathcal{ST}_{\mathcal{E}}(t)$ is then defined as the smallest set satisfying equations given in Fig. 14.

To give cryptographic or freshness rules in the CCSA logic, we define several special generalised subterms set.

- **(Freshness)** Let $\mathbf{n} : \tau_0 \to \tau$ be a name and let $t_0 : \tau_0$ be a term. Informally, the term $\mathbf{n}\ t_0 : \tau$ is said to be *fresh* in the sequence of terms $\mathbf{u}$ when if for all occurrences of the form $(\overrightarrow{\alpha}, \phi, \mathbf{n}\ t) \in \mathcal{ST}_{\mathcal{E}}(\mathbf{u})$ then $t \neq t_0$. Formally, we first define the *set of formulas in the freshness case* $\Phi^{\mathbf{n}, t_0}_{\textit{fresh}}(\mathbb{S})$ for any set of occurrences $\mathbb{S}$ to be the set defined by

  $$\Phi^{\mathbf{n}, t_0}_{\mathsf{fresh}}(\mathbb{S}) \stackrel{\mathrm{def}}{=} \big\{\big(\forall\, \overrightarrow{\alpha}.\ \psi \to t \neq t_0\big)\ |\ (\overrightarrow{\alpha}, \psi, \mathbf{n}\ t) \in \mathbb{S}\big\}.$$

  Hence, for any sequence of terms $\mathbf{u}$, we denote by $\Psi^{\mathbf{n}, t_0}_{\mathsf{fresh}}(\mathbf{u}, t_0) : \mathbf{bool}$, to be any *well-typed* $\mathbf{bool}$ formula in $\mathcal{E}$ implying the *freshness* of the term $\mathbf{n}\ t_0$. Formally, for all model $\mathbb{M} : \mathcal{E}$ for the environment $\mathcal{E}$, all security parameter $\eta \in \mathbb{N}^*$ and all random tape $\rho \in \mathbb{T}$, we have

  $$[\![\Psi^{\mathbf{n}, t_0}_{\mathsf{fresh}}(\mathbf{u}, t)]\!]^{\eta, \rho}_{\mathbb{M} : \mathcal{E}} = 1 \stackrel{\mathrm{def}}{\Longrightarrow} \forall\, \phi \in \Phi^{\mathbf{n}, t_0}_{\mathsf{fresh}}(\mathcal{ST}_{\mathcal{E}}(\mathbf{u}, t_0)),\ [\![\phi]\!]^{\eta, \rho}_{\mathbb{M} : \mathcal{E}} = 1.$$

- **(Good use of secret keys)** Let $sk : \tau_0 \to \mathbf{skey}$ be a name which generates secret key terms. Let $t_0 : \tau_0$ be a term. Informally, the secret key term $sk\ t_0 : \mathbf{skey}$ is said to be *well-used* when the adversary only has access to the corresponding public key and the decryption oracle. More precisely, the secret key $sk\ t_0$ may only appear in terms $\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0)$ or $\mathbf{dec}_{\mathbb{CS}}\ (sk\ t_0)\ c$. Then, we define the *set $\mathcal{ST}^{\textit{skey}}_{\mathcal{E}, sk, t_0}(u)$ of generalised subterms for secret keys* for a term u recursively as the classic definition of

$$
\begin{array}{rcll}
\mathcal{ST}_{\mathcal{E}}(x) & \overset{\text{def}}{=} & \{(\varepsilon, \top, x)\} & \text{when } (x : \tau) \in \mathcal{E} \text{ or } x \notin \mathcal{E} \\
\mathcal{ST}_{\mathcal{E}}(x) & \overset{\text{def}}{=} & \mathcal{ST}_{\mathcal{E}}(t) & \text{when } (x : \tau = t) \in \mathcal{E} \\
\mathcal{ST}_{\mathcal{E}}(t\ t') & \overset{\text{def}}{=} & \begin{cases} \mathcal{ST}_{\mathcal{E}}(t_0\{y \mapsto t'\}) \\ \{(\varepsilon, \top, (t\ t'))\} \cup \mathcal{ST}_{\mathcal{E}}(t) \cup \mathcal{ST}_{\mathcal{E}}(t') \end{cases} & \begin{array}{r} \text{when } t = x \text{ and } (x : \tau = \lambda y.\ t_0) \in \mathcal{E} \\ \text{otherwise} \end{array} \\
\mathcal{ST}_{\mathcal{E}}(\lambda(x : \tau).\ t) & \overset{\text{def}}{=} & \{(\varepsilon, \top, \lambda(x : \tau).\ t)\} \cup (x : \tau).\mathcal{ST}_{\mathcal{E}}(t) & \text{where } x \text{ is taken fresh} \\
\mathcal{ST}_{\mathcal{E}}(\textbf{if } \phi \textbf{ then } t_1 \textbf{ else } t_0) & \overset{\text{def}}{=} & \{(\varepsilon, \top, \textbf{if } \phi \textbf{ then } t_1 \textbf{ else } t_0)\} \cup \mathcal{ST}_{\mathcal{E}}(\phi) & \\
 & & \cup[\phi]\mathcal{ST}_{\mathcal{E}}(t_1) \cup [\neg\, \phi]\mathcal{ST}_{\mathcal{E}}(t_0) & \\
\mathcal{ST}_{\mathcal{E}}((u_i)_{i=1}^n) & \overset{\text{def}}{=} & \displaystyle\bigcup_{i=1}^{n} \mathcal{ST}_{\mathcal{E}}(u_i) &
\end{array}
$$

Fig. 14. Generalised subterms

$\mathcal{ST}_{\mathcal{E}}(u)$ with the two following exceptions when u is a function application

$$
\begin{aligned}
&\mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(\mathtt{pk}_{\mathbb{CS}}\ (sk\ t)) \\
&\quad \overset{\text{def}}{=} \quad \{(\varepsilon, \top, \mathtt{pk}_{\mathbb{CS}}\ (sk\ t)), (\varepsilon, \top, \mathtt{pk}_{\mathbb{CS}})\} \cup\ \mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(t) \\
&\qquad\quad \cup[t \neq t_0]\mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(sk\ t), \text{ and} \\
&\mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(\mathbf{dec}_{\mathbb{CS}}\ (sk\ t)\ u) \\
&\quad \overset{\text{def}}{=} \quad \{(\varepsilon, \top, \mathbf{dec}_{\mathbb{CS}}\ (sk\ t)\ u), (\varepsilon, \top, \mathbf{dec}_{\mathbb{CS}})\} \\
&\qquad\quad \cup\ \mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(t) \cup \mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(u) \\
&\qquad\quad \cup[t \neq t_0]\mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(sk\ t).
\end{aligned}
$$

Hence, for any sequence of terms $\mathbf{u}$, we denote by $\Psi^{sk,t_0}_{\mathsf{skey}}(\mathbf{u}, t)$: **bool** to be any *well-typed* **bool** formula in $\mathcal{E}$ implying the *good use* of the secret key term $sk\ t_0$. Formally, for all model $\mathbb{M} : \mathcal{E}$ for the environment $\mathcal{E}$, all security parameter $\eta \in \mathbb{N}^*$, and all random tape $\rho \in \mathbb{T}$, we have

$$
\begin{aligned}
&[\![\Psi^{sk,t_0}_{\mathsf{skey}}(\mathbf{u}, t)]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1 \overset{\text{def}}{\Longrightarrow} \\
&\qquad \forall\, (\overrightarrow{\alpha}, \psi, sk\ t') \in \mathcal{ST}^{\mathsf{skey}}_{\mathcal{E},sk,t_0}(\mathbf{u}, t), \\
&\qquad\qquad [\![\forall\, \overrightarrow{\alpha}.\, \psi \to t' \neq t_0]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1.
\end{aligned}
$$

- **(Good use of commitment key parameters)** Let $ck : \tau_0 \to$ **comkey** be a name which generates commitment key parameter terms. Let $n : \tau_0$ be a term. Informally, the commitment key parameter term $ck\ n$: **comkey** is said to be *well-used* when the adversary only has access to the commit oracle. More precisely, the commitment key parameter term $ck\ n$ may only appear in the term **com** $(ck\ n)\ m\ r$. To do so, we define the *set* $\mathcal{ST}^{\mathsf{comkey}}_{\mathcal{E},ck,n}(u)$ *of generalised subterms for commitment key parameters* for a term u recursively as the classic definition of $\mathcal{ST}_{\mathcal{E}}(u)$ with the following exception

$$
\begin{aligned}
&\mathcal{ST}^{\mathsf{comkey}}_{\mathcal{E},ck,n}(\mathbf{com}\ (ck\ n')\ m\ r) \overset{\text{def}}{=} \\
&\{(\varepsilon, \top, m), (\varepsilon, \top, r), (\varepsilon, \top, n')\} \cup [n' \neq n]\mathcal{ST}^{\mathsf{comkey}}_{\mathcal{E},ck,n}(ck\ n').
\end{aligned}
$$

Hence, for any sequence of terms $\mathbf{u}$, we denote by $\Psi^{ck,n}_{\mathsf{comkey}}(\mathbf{u}, t)$: **bool** to be any *well-typed* **bool** formula in $\mathcal{E}$ implying the *good use* of the commitment key parameter $ck\ n$. Formally, for all model $\mathbb{M} : \mathcal{E}$ for the environment $\mathcal{E}$, all security parameter $\eta \in \mathbb{N}^*$, and all random tape $\rho \in \mathbb{T}$, we have

$$
\begin{aligned}
&[\![\Psi^{ck,n}_{\mathsf{comkey}}(\mathbf{u}, t)]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1 \overset{\text{def}}{\Longrightarrow} \\
&\qquad \forall\, (\overrightarrow{\alpha}, \psi, ck\ n_0) \in \mathcal{ST}^{\mathsf{comkey}}_{\mathcal{E},ck,n}(\mathbf{u}, t), \\
&\qquad\qquad [\![\forall\, \overrightarrow{\alpha}.\ \psi \to n_0 \neq n]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1.
\end{aligned}
$$

APPENDIX D
PROOF SYSTEM

Global and local judgements about logical reasoning (and in particular proofs of soundness for these rules) can be mostly found in [12], or in [30] for concrete security variants. More precisely, the rule G.$\sim$:FRESH comes from [30] in the case where the term ε of the concrete security version of the rule is a negligible function. Besides, the rule G.$\tilde{\neg}$:CHARAC is a new rule we add in our case, which is immediately sound by the semantics of the predicate **non-negl**/1. All other rules come from the paper [12]. Nevertheless, we remind several useful rules used in this paper in Fig. 15.

A. *Soundness of* ***low-bound*** *rules*

In this subsection, we prove the soundness of rules about **low-bound** predicate. Let $\mathcal{E}$ be an environment and Θ be a context of global formulas. Let g : **real** with $\mathcal{E}; \Theta \vdash$ **non-negl**$(g)\ \tilde{\wedge}\ $**det**$(g)$ be a non-negligible parameter. Let $\phi : \tau_1 \to \cdots \to \tau_n \to$ **bool** be a formula with n parameters.

- (G.LB:ELIM) We proceed by contraposition, *i.e.* we suppose $\mathcal{E}; \Theta \vdash \tilde{\neg}\ [\phi\ \mathbf{r} \to \psi\ \mathbf{r}]$. Hence, by classical logic operations, we have $\mathcal{E}; \Theta \vdash \tilde{\neg}\ [\neg\ (\phi\ \mathbf{r} \wedge \neg\ (\psi\ \mathbf{r}))]$. Therefore, by characterization of non-negligibility, we conclude by the rule G.$\tilde{\neg}$:CHARAC the existency of a non-negligible parameter g : **real** such that $\mathcal{E}'; \Theta' \vdash {}_g[(\phi \wedge \neg\ \psi)\ \mathbf{r}]$ where $\mathcal{E}' \overset{\text{def}}{=} \mathcal{E} \cup \{(g : \mathbf{real})\}$ and $\Theta' \overset{\text{def}}{=} \Theta,\ $**non-negl**$(g)$. Actually, without loss of generality, we suppose that parameter g is deterministic, *i.e.* we add

Global judgements: equivalence rules

G.$\sim$:Refl
$$\frac{}{\mathcal{E};\Theta\vdash \mathbf{u},t\sim\mathbf{u},t}$$

G.$\sim$:CS
$$\frac{\mathcal{E};\Theta\vdash \mathbf{u}_l,b_l,s_l\sim\mathbf{u}_r,b_r,s_r\qquad \mathcal{E};\Theta\vdash \mathbf{u}_l,b_l,t_l\sim\mathbf{u}_r,b_r,s_r}{\mathcal{E};\Theta\vdash \mathbf{u}_l,\textbf{if } b_l \textbf{ then } s_l \textbf{ else } t_l\sim\mathbf{u}_r,\textbf{if } b_r \textbf{ then } s_r \textbf{ else } t_r}$$

G.$\sim$:FA
$$\frac{\mathcal{E};\Theta\vdash \mathbf{u}_l,t_l\sim\mathbf{u}_r,t_r\qquad \mathcal{E};\Theta\vdash \textbf{adv}(f)}{\mathcal{E};\Theta\vdash \mathbf{u}_l,f\ t_l\sim\mathbf{u}_r,f\ t_r}$$

G.$\sim$:Dup
$$\frac{\mathcal{E};\Theta\vdash \mathbf{u}_l,t_l\sim\mathbf{u}_r,t_r}{\mathcal{E};\Theta\vdash \mathbf{u}_l,t_l,t_l\sim\mathbf{u}_r,t_r,t_r}$$

G.$\sim$:Fresh
$$\frac{\mathcal{E};\Theta\vdash [\Psi^{\mathbf{n},t}_{\mathsf{fresh}}(\mathbf{u},C(\mathbf{n}_{\mathsf{fresh}}\ ()),t)]}{\mathcal{E};\Theta\vdash \mathbf{u},C(\mathbf{n}\ t)\sim\mathbf{u},C(\mathbf{n}_{\mathsf{fresh}}\ ())}$$

G.$\sim$:Simpl
$$\frac{\mathcal{E};\Theta\vdash \mathbf{u}_l\sim\mathbf{u}_r}{\mathcal{E};\Theta\vdash \mathbf{u}_l,\mathbf{n}_{\mathsf{fresh}}\ ()\sim\mathbf{u}_r,\mathbf{n}_{\mathsf{fresh}}\ ()}$$

G.$\sim$:Trans
$$\frac{\mathcal{E};\Theta\vdash \mathbf{u}\sim\mathbf{v}\qquad \mathcal{E};\Theta\vdash \mathbf{v}\sim\mathbf{w}}{\mathcal{E};\Theta\vdash \mathbf{u}\sim\mathbf{w}}$$

Other rules

L.ByGlob
$$\frac{\mathcal{E};\Theta\vdash[\phi]}{\mathcal{E};\Theta;\Gamma\vdash\phi}$$

G.ByLoc
$$\frac{\mathcal{E};\Theta;\varnothing\vdash\phi}{\mathcal{E};\Theta\vdash[\phi]}$$

L.Rewrite
$$\frac{\mathcal{E};\Theta;\Gamma\vdash\phi[s]\qquad \mathcal{E};\Theta;\Gamma\vdash s=t}{\mathcal{E};\Theta;\Gamma\vdash\phi[t]}$$

G.Rewrite
$$\frac{\mathcal{E};\Theta\vdash F[\phi]\qquad \mathcal{E};\Theta\vdash[\phi\leftrightarrow\psi]}{\mathcal{E};\Theta\vdash F[\psi]}$$

G.R-$\tilde{\exists}$
$$\frac{\mathcal{E};\Theta\vdash F\left\{x\longmapsto t\right\}\qquad \mathcal{E}\vdash(t:\tau)}{\mathcal{E};\Theta\vdash\tilde{\exists}\,(x:\tau).\ F}$$

G.$\tilde{\neg}$:Charac
$$\frac{}{\mathcal{E};\Theta\vdash\tilde{\neg}\,[\neg\,\phi]\ \tilde{\leftrightarrow}\ \tilde{\exists}\,(g:\textbf{real}).\ \textbf{non-negl}(g)\ \tilde{\wedge}\ {}_{g}[\phi]}$$

Fig. 15. Structural local and global rules in the CCSA logic

the property $\textbf{det}(g)$ to the context Θ'. Then, by the introduction rule G.LB:Intro of the predicate **low-bound**, we conclude $\mathcal{E}';\Theta'\vdash{}_{g/2}[\textbf{low-bound}\ (g/2)\ (\phi\wedge\neg\,\psi)]$. As parameter g is deterministic and by the rule G.LB:Out, we conclude

$$\mathcal{E}';\Theta'\vdash{}_{g^2/4}[\textbf{low-bound}\ (g/2)\ (\phi\wedge\neg\,\psi)\wedge(\phi\wedge\neg\,\psi)\ \mathbf{r}].$$

Therefore, as we have $\mathcal{E}';\Theta'\vdash{}_{1}[(\phi\wedge\neg\,\psi)\ \mathbf{r}\to\phi\ \mathbf{r}]$, we conclude by the global transitivity rule G.LB:Trans the following property

$$\mathcal{E}';\Theta'\vdash{}_{g^2/4}[\textbf{low-bound}\ (g/2)\ \phi\wedge(\phi\wedge\neg\,\psi)\ \mathbf{r}].$$

However, by logical operations, we have

$$\begin{aligned}&\textbf{low-bound}\ (g/2)\ \phi\wedge(\phi\wedge\neg\,\psi)\ \mathbf{r}\\ &\quad=\ \textbf{low-bound}\ (g/2)\ \phi\wedge\neg\,(\neg\,\phi\vee\psi)\ \mathbf{r}\\ &\quad=\ \textbf{low-bound}\ (g/2)\ \phi\wedge\neg\,(\phi\ \mathbf{r}\to\psi\ \mathbf{r})\\ &\quad=\ \neg\,(\neg\,\textbf{low-bound}\ (g/2)\ \phi\vee(\phi\ \mathbf{r}\to\psi\ \mathbf{r}))\\ &\quad=\ \neg\,(\textbf{low-bound}\ (g/2)\ \phi\to\phi\ \mathbf{r}\to\psi\ \mathbf{r})\end{aligned}$$

Besides, as $\mathcal{E}';\Theta'\vdash\textbf{non-negl}(g)$, we have $\mathcal{E}';\Theta'\vdash\textbf{non-negl}(g^2/4)$ (the same holds for **det** predicate) by operations on non-negligible real terms. Hence, by the rule G.R-$\tilde{\exists}$, we conclude the following property

$$\begin{aligned}\mathcal{E}';\Theta'\vdash\tilde{\exists}\,(h_g:\textbf{real}).\ \textbf{non-negl}(h_g)\ \tilde{\wedge}\ \textbf{det}(h_g)\ \tilde{\wedge}\\ {}_{h_g}[\neg\,(\textbf{low-bound}\ (g/2)\ \phi\to\phi\ \mathbf{r}\to\psi\ \mathbf{r})].\end{aligned}$$

By characterization of non-negligibility, we conclude by the rule G.$\tilde{\neg}$:Charac the property

$$\mathcal{E}';\Theta'\vdash\tilde{\neg}\,[\textbf{low-bound}\ (g/2)\ \phi\to\phi\ \mathbf{r}\to\psi\ \mathbf{r}].$$

Finally, as $\mathcal{E}'\vdash(g:\textbf{real})$ and by the rule G.R-$\tilde{\exists}$, we conclude

$$\begin{aligned}\mathcal{E};\Theta\vdash\tilde{\exists}\,(g':\textbf{real}).\ \textbf{non-negl}(g')\ \tilde{\wedge}\ \textbf{det}(g')\\ \tilde{\to}\ \tilde{\neg}\,[\textbf{low-bound}\ g'\ \phi\to\phi\ \mathbf{r}\to\psi\ \mathbf{r}]\end{aligned}$$

Which achieves the proof of soundness of the rule G.LB:Elim by contraposition.

- (G.LB:Intro) We suppose the property $\mathcal{E};\Theta\vdash{}_{g}[\phi\ r_1\ \ldots\ r_n]$, *i.e.* by definition of the predicate ${}_{g}[\phi]$ semantics, we suppose the following property

$$\forall\,\eta\in\mathbb{N}^*,\mathrm{Pr}_{\rho\in\mathbb{T}}\Big[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \Big]\geqslant\mathbb{E}_{\rho\in\mathbb{T}}\big([\![g]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\big).\qquad(*)$$

We have to prove the following property

$$\forall\,\eta\in\mathbb{N}^*,\mathrm{Pr}_{\rho\in\mathbb{T}}\Big[\ [\![\textbf{low-bound}\ (g/2)\ \phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \Big]\geqslant\mathbb{E}_{\rho\in\mathbb{T}}\big([\![g/2]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\big).$$

Let $\eta\in\mathbb{N}^*$. By definition of the predicate **low-bound** semantics, we have

$$\mathrm{Pr}_{\rho\in\mathbb{T}}\Big[\ [\![\textbf{low-bound}\ (g/2)\ \phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \Big]=$$
$$\mathrm{Pr}_{\rho\in\mathbb{T}}\left[\begin{array}{l}\mathrm{Pr}_{r_i\in[\![\tau_i]\!]^{\eta}_{\mathbb{M}},i\in[\![1;n]\!]}\Big[\ [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}(r_1,\ldots,r_n)\ \Big]\\ \quad\geqslant\ \mathbb{E}_{\rho'\in\mathbb{T}}\big([\![g/2]\!]^{\eta,\rho'}_{\mathbb{M}:\mathcal{E}}\big)\end{array}\right].$$

Moreover, by semantics of real terms, we have $[\![g/2]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}=\frac{1}{2}[\![g]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}$. Therefore, by linearity of the function $\mathbb{E}_{\rho}\big(X(\rho)\big)$, we have

$$\mathbb{E}_{\rho\in\mathbb{T}}\big([\![g/2]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\big)=\frac{1}{2}\mathbb{E}_{\rho\in\mathbb{T}}\big([\![g]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\big).$$

We denote by p_ϕ the function defined by

$$p_\phi(\eta,\rho)\overset{\text{def}}{=}\mathrm{Pr}_{r_i\in[\![\tau_i]\!]^{\eta}_{\mathbb{M}},i\in[\![1;n]\!]}\Big[\ [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}(r_1,\ldots,r_n)\ \Big].$$

and we denote by e_g the function defined by

$$e_g(\eta)\overset{\text{def}}{=}\mathbb{E}_{\rho\in\mathbb{T}}\big([\![g]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\big).$$

Consequently, we have to prove the following property

$$\mathrm{Pr}_{\rho\in\mathbb{T}}\Big[\ p_\phi(\eta,\rho)\geqslant\frac{1}{2}e_g(\eta)\ \Big]\geqslant\frac{1}{2}e_g(\eta).$$

Rules for low-bound predicate

G.LB:Elim
$$\frac{\mathcal{E}; \Theta \vdash \tilde{\forall} g : \textbf{real}.\ \textbf{non-negl}(g) \mathrel{\tilde{\wedge}} \textbf{det}(g) \mathrel{\tilde{\rightarrow}} [\textbf{low-bound}\ g\ \phi \to \phi\ \mathbf{r} \to \psi\ \mathbf{r}]}{\mathcal{E}; \Theta \vdash [\phi\ \mathbf{r} \to \psi\ \mathbf{r}]}$$

G.LB:Intro
$$\frac{\mathcal{E}; \Theta \vdash_{g} [\phi\ r_1\ \ldots\ r_n]}{\mathcal{E}; \Theta \vdash_{g/2} [\textbf{low-bound}\ (g/2)\ \phi]}$$

G.LB:Out
$$\frac{\mathcal{E}; \Theta \vdash \textbf{det}(h) \qquad \mathcal{E}; \Theta \vdash_{g} [\textbf{low-bound}\ h\ \phi]}{\mathcal{E}; \Theta \vdash_{g \cdot h} [(\textbf{low-bound}\ h\ \phi) \wedge (\phi\ r_1\ \ldots\ r_n)]}$$

L.LB:Trans
$$\frac{\begin{array}{c}\mathcal{E}; \Theta \vdash \textbf{non-negl}(g) \\ \mathcal{E}; \Theta \vdash_{1} [(\phi\ r_1\ \ldots\ r_n) \to (\psi\ r_1\ \ldots\ r_n)]\end{array}}{\mathcal{E}; \Theta; \varnothing \vdash \textbf{low-bound}\ g\ \phi \to \textbf{low-bound}\ g\ \psi}$$

G.LB:Trans
$$\frac{\begin{array}{c}\mathcal{E}; \Theta \vdash_{1} [(\phi\ r_1\ \ldots\ r_n) \to (\psi\ r_1\ \ldots\ r_n)] \\ \mathcal{E}; \Theta \vdash_{g} [(\textbf{low-bound}\ h\ \phi) \wedge \chi]\end{array}}{\mathcal{E}; \Theta \vdash_{g} [(\textbf{low-bound}\ h\ \psi) \wedge \chi]}$$

Probabilistic rule

G.Sel
$$\frac{\begin{array}{c}\mathcal{E}; \Theta \vdash \textbf{det}(k) \mathrel{\tilde{\wedge}} \textbf{pbound}(k) \qquad \mathcal{E}; \Theta \vdash [\phi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)] \\ \mathcal{E}; \Theta \vdash [\forall\,(t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s\ \to\ (\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \ldots, \mathbf{r}_s\ k\}]\end{array}}{\mathcal{E}; \Theta \vdash [n \leqslant k \to \phi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]}$$

Predicates correctness rules

L.Eqm:Charac
$$\frac{\mathcal{E}; \Theta; \Gamma \vdash \textbf{perm}_N\ \pi \qquad \mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} (\langle \mathbf{x} \mid \mathbf{i} \rangle = \langle \mathbf{x} \mid \pi \cdot \mathbf{i} \rangle)}{\mathcal{E}; \Theta; \Gamma \vdash \textbf{eqm}_N\ \mathbf{x}\ \mathbf{y}}$$

L.Wf:Valid
$$\frac{\mathcal{E}; \Theta; \Gamma \vdash \textbf{valid}\ (\texttt{pk}_{\mathbb{CS}}\ sk)\ c\ v}{\mathcal{E}; \Theta; \Gamma \vdash \textbf{wf\_ctxt}\ sk\ c}$$

L.π:Inj
$$\frac{\mathcal{E}; \Theta; \Gamma \vdash \textbf{perm}_N\ \pi}{\mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} \bigvee_{j=1}^{N} (\pi \cdot \mathbf{i} = \mathbf{j})}$$

L.DecList
$$\frac{}{\mathcal{E}; \Theta; \Gamma \vdash \langle \textbf{dec-list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{x} \mid \mathbf{i} \rangle = \textbf{dec}_{\mathbb{CS}}\ sk\ \langle \mathbf{x} \mid \mathbf{i} \rangle}$$

L.$\circledast$:CanoVec
$$\frac{}{\mathcal{E}; \Theta; \Gamma \vdash \mathbf{x} \circledast \mathbf{i} = \langle \mathbf{x} \mid \mathbf{i} \rangle}$$

L.$\circledast$:Com
$$\frac{}{\mathcal{E}; \Theta; \Gamma \vdash (\textbf{com-mat}\ ck\ M\ \mathbf{s}) \circledast \mathbf{x} = \textbf{com-vec}\ ck\ (M \cdot \mathbf{x})\ \langle \mathbf{s} \mid \mathbf{x} \rangle}$$

L.Shuffle
$$\frac{}{\mathcal{E}; \Theta; \Gamma \vdash \mathbf{c}' = \textbf{shuffle}_{\phi_{\mathbb{CS}}}\ pk\ \mathbf{c}\ \pi\ (\mathbf{r}\ j) \leftrightarrow \bigwedge_{i=1}^{N} (\mathbf{c}' \circledast (\pi \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ pk\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ j \mid \mathbf{i} \rangle)}$$

Algebraic rules For the rule L.Open, terms M and $\mathbf{s}$ are defined by $(M, \mathbf{s}) \overset{\text{def}}{=} \textbf{solve}\ \mathbf{a}\ (\mathbf{e}_i)_{i=1}^{N}\ (\mathbf{e}'_i, k_i)_{i=1}^{N}$.

L.π:Charac
$$\frac{\begin{array}{c}\mathcal{E}; \Theta; \Gamma \vdash M \cdot \mathbf{1} = \mathbf{1} \\ \mathcal{E}; \Theta; \Gamma \vdash \textbf{prod}_N\ (M \cdot X) - \textbf{prod}_N\ X = \mathbf{0}\end{array}}{\mathcal{E}; \Theta; \Gamma \vdash \textbf{perm}_N\ M}$$

L.Open
$$\frac{\begin{array}{c}\mathcal{E}; \Theta; \Gamma \vdash \textbf{basis}_N\ (\mathbf{e}_i)_{i=1}^{N} \\ \mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} (\mathbf{a} \circledast \mathbf{e}_i = \textbf{com-vec}\ ck\ \mathbf{e}'_i\ k_i)\end{array}}{\mathcal{E}; \Theta; \Gamma \vdash \mathbf{a} = \textbf{com-mat}\ ck\ M\ \mathbf{s}}$$

L.Basis
$$\frac{\begin{array}{c}\mathcal{E} \vdash x_1, \ldots x_n : \textbf{nat} \qquad \mathcal{E} \vdash \mathbf{e}_s : \textbf{nat} \to \tau \\ \mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{1 \leqslant i < j \leqslant n} x_i \neq x_j\end{array}}{\mathcal{E}; \Theta; \Gamma \vdash \textbf{basis}_n\ (\mathbf{e}_s\ x_i)_{i=1}^{n}}$$

L.Sz
$$\frac{\mathcal{E}; \Theta; \Gamma \vdash \Psi^{\mathbf{x}, t_0}_{\mathsf{fresh}}(P) \qquad \mathcal{E}; \Theta; \Gamma \vdash P(\mathbf{x}\ t_0) = 0}{\mathcal{E}; \Theta; \Gamma \vdash P = \mathbf{0}}$$

Fig. 16. CCSA rules sheet

We have, by definition of $p_\phi(\eta, \rho)$,

$$\mathrm{Pr}_{\rho \in \mathbb{T}} \left[\, [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta, \rho}_{\mathbb{M}:\mathcal{E}} \, \right] = \int_{\rho \in \mathbb{T}} p_\phi(\eta, \rho)\, d\rho$$

Hence, the idea is to split the space of random tapes $\mathbb{T}$ whether or not $p_\phi(\eta, \rho)$ is greater than $\frac{1}{2} e_g(\eta)$. To do so, we denote by $\mathbb{T}_{\text{inf}}$, respectively $\mathbb{T}_{\text{sup}}$, the set of random tapes defined by

$$\mathbb{T}_{\text{sup}} \overset{\text{def}}{=} \left\{ \rho \in \mathbb{T} \ \middle|\ p_\phi(\eta, \rho) \geqslant \tfrac{1}{2} e_g(\eta) \right\}$$
$$\mathbb{T}_{\text{inf}} \overset{\text{def}}{=} \left\{ \rho \in \mathbb{T} \ \middle|\ p_\phi(\eta, \rho) < \tfrac{1}{2} e_g(\eta) \right\}.$$

As $\mathbb{T} = \mathbb{T}_{\text{inf}} \sqcup \mathbb{T}_{\text{sup}}$ (these two subsets form a partition

Cryptographic rules: commitment schemes

G.COM:HIDE

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, m_1, m_2) \qquad \mathcal{E};\Theta \vdash [\Psi^{r,i}_{\mathsf{fresh}}(\mathbf{u}, m_1, m_2) \wedge \Psi^{ck,n}_{\mathsf{comkey}}(\mathbf{u}, m_1, m_2)]}{\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{com}\ (ck\ n)\ m_1\ (r\ i) \sim \mathbf{u}, \mathbf{com}\ (ck\ n)\ m_2\ (r\ i)}$$

L.COM:BIND

$$\frac{\begin{array}{c}\mathcal{E};\Theta \vdash \mathbf{adv}(m_1, m_2, r_1, r_2) \qquad \mathcal{E};\Theta;\Gamma \vdash \Psi^{ck,n}_{\mathsf{comkey}}(m_1, m_2) \\ \mathcal{E};\Theta;\Gamma \vdash \mathbf{com}\ (ck\ n)\ m_1\ r_1 = \mathbf{com}\ (ck\ n)\ m_2\ r_2\end{array}}{\mathcal{E};\Theta;\Gamma \vdash m_1 = m_2}$$

Cryptographic rules: Σ-protocols For the rule L.Σ-P:SPSOUND, for $i \in \{1, 2\}$, the term notation $\mathfrak{p}^{(i)}_{\mathcal{R}}(c_i)$ is an alias for $\mathfrak{p}^{(i)}_{\mathcal{R}}(c_i) \stackrel{\text{def}}{=} \langle \alpha, c_i, z(c_i) \rangle$.

L.Σ-P:SPSOUND

$$\frac{\begin{array}{c}\mathcal{E};\Theta \vdash \mathbf{adv}(x, \mathfrak{p}^{(1)}_{\mathcal{R}}(c_1), \mathfrak{p}^{(2)}_{\mathcal{R}}(c_2)) \qquad \mathcal{E};\Theta;\Gamma \vdash c_1 \neq c_2 \\ \mathcal{E};\Theta;\Gamma \vdash \displaystyle\bigwedge_{i \in \{1,2\}} \mathbf{zkp\text{-}verif}_{\mathcal{R}}\ (\sigma\ s)\ x\ \mathfrak{p}^{(i)}_{\mathcal{R}}(c_i)\end{array}}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{zkp\text{-}rel}_{\mathcal{R}}\ (\sigma\ s)\ x\ (\mathbf{zkp\text{-}extract}_{\mathcal{R}}\ (\sigma\ s)\ x\ \mathfrak{p}^{(1)}_{\mathcal{R}}(c_1)\ \mathfrak{p}^{(2)}_{\mathcal{R}}(c_2))}$$

G.Σ-P:HVZK

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, x, w) \qquad \mathcal{E};\Theta \vdash [\Psi^{r,i}_{\mathsf{fresh}}(\mathbf{u}, x, w)]}{\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{zkp\text{-}prove}_{\mathcal{R}}\ (\sigma\ s)\ x\ w\ (r\ i) \sim \mathbf{u}, \mathbf{zkp\text{-}sim}_{\mathcal{R}}\ (\sigma\ s)\ x\ (r\ i)}$$

Cryptographic rules: *shuffle-friendly* maps

L.SFM:CORRECT

$$\frac{\begin{array}{c}\mathcal{E};\Theta;\Gamma \vdash \mathbf{wf\_ctxt}\ sk\ c \\ \mathcal{E};\Theta;\Gamma \vdash \exists\, v.\ c' = \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ c\ v\end{array}}{\mathcal{E};\Theta;\Gamma \vdash \mathbf{dec}_{\mathbb{CS}}\ sk\ c = \mathbf{dec}_{\mathbb{CS}}\ sk\ c'}$$

L.SFM:CHARAC

$$\frac{\begin{array}{c}\mathcal{E};\Theta;\Gamma \vdash \mathbf{perm}_N\ \pi \qquad \mathcal{E};\Theta;\Gamma \vdash \Psi^{\mathbf{e},t}_{\mathsf{fresh}}(\mathbf{c}, \mathbf{c}', \pi) \\ \mathcal{E};\Theta;\Gamma \vdash \exists\, v.\ \mathbf{c}' \circledast (\pi \cdot (\mathbf{e}\ t)) = \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ pk\ (\mathbf{c} \circledast (\mathbf{e}\ t))\ v\end{array}}{\mathcal{E}, (\mathbf{x} : \mathbf{msg});\Theta;\Gamma \vdash \exists\ v_{\mathbf{x}}.\ \mathbf{c}' \circledast (\pi \cdot \mathbf{x}) = \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ pk\ (\mathbf{c} \circledast \mathbf{x})\ v_{\mathbf{x}}}$$

G.SFM:INDCCA

$$\frac{\mathcal{E};\Theta \vdash \mathbf{adv}(\mathbf{u}, c, v) \qquad \mathcal{E};\Theta \vdash [\Psi^{sk,t_0}_{\mathsf{skey}}(\mathbf{u}, c, v) \wedge \Psi^{r,i}_{\mathsf{fresh}}(\mathbf{u}, c, v)]}{\begin{array}{l}\mathcal{E};\Theta \vdash \mathbf{u}, \mathbf{if\ valid}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ v\ \mathbf{then\ shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ (r\ i) \\ \qquad \sim\ \mathbf{u}, \mathbf{if\ valid}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ c\ v\ \mathbf{then\ shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ t_0))\ (\mathbf{0}\ (\mathbf{len}\ c))\ (r\ i)\end{array}}$$

Fig. 17. Added axiom rules for algebraic properties and cryptographic security properties

of the random tape space $\mathbb{T}$), we conclude

$$\mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] = \int_{\rho \in \mathbb{T}_{\mathrm{inf}}} p_\phi(\eta, \rho)\, d\rho + \int_{\rho \in \mathbb{T}_{\mathrm{sup}}} p_\phi(\eta, \rho)\, d\rho$$

Besides, on the set $\mathbb{T}_{\mathrm{inf}}$, we have by definition of this subset $p_\phi(\eta, \rho) \leqslant \frac{1}{2} e_g(\eta)$. As for the set $\mathbb{T}_{\mathrm{sup}}$, because $p_\phi(\eta, \rho)$ is a probability, we have $p_\phi(\eta, \rho) \leqslant 1$. Therefore, we have

$$\begin{aligned}\mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] &\leqslant \int_{\rho \in \mathbb{T}_{\mathrm{inf}}} \left(\tfrac{1}{2} e_g(\eta)\right) d\rho + \int_{\rho \in \mathbb{T}_{\mathrm{sup}}} d\rho \\ &= \frac{1}{2} e_g(\eta) \int_{\rho \in \mathbb{T}_{\mathrm{inf}}} d\rho + \int_{\rho \in \mathbb{T}_{\mathrm{sup}}} d\rho\end{aligned}$$

Now, by property on probabilities, we have

$$\int_{\rho \in \mathbb{T}_{\mathrm{inf}}} d\rho \leqslant \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ p_\phi(\eta, \rho) \leqslant \frac{1}{2} e_g(\eta)\ \right] \leqslant 1$$

and

$$\int_{\rho \in \mathbb{T}_{\mathrm{sup}}} d\rho \leqslant \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ p_\phi(\eta, \rho) \geqslant \frac{1}{2} e_g(\eta)\ \right]$$

Moreover, by hypothesis Eq. $(*)$, we conclude

$$\begin{aligned}e_g(\eta) &\leqslant \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] \\ &\leqslant \frac{1}{2} e_g(\eta) + \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ p_\phi(\eta, \rho) \geqslant \frac{1}{2} e_g(\eta)\ \right]\end{aligned}$$

Therefore, we have the following probability

$$\forall\, \eta \in \mathbb{N}^*, \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ p_\phi(\eta, \rho) \geqslant \frac{1}{2} e_g(\eta)\ \right] \geqslant \frac{1}{2} e_g(\eta)$$

which achieves the soundness proof of the rule G.LB:INTRO.

- (G.LB:OUT) We suppose the property $\mathcal{E};\Theta \vdash {}_g[\mathbf{low\text{-}bound}\ h\ \phi]$ where the parameter h verifies $\mathcal{E};\Theta \vdash \mathbf{non\text{-}negl}(h)\ \tilde{\wedge}\ \mathbf{det}(h)$. By definition of ${}_g[\phi]$ semantics, this leads to the following property

$$\forall\, \eta \in \mathbb{N}^*, \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\mathbf{low\text{-}bound}\ h\ \phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] \geqslant \mathbb{E}_{\rho \in \mathbb{T}}\left([\![g]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\right). \quad (\mathcal{H})$$

Let $\eta \in \mathbb{N}^*$ be a security parameter. By definition of $\wedge$ semantics, we have

$$\begin{aligned}\mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![(\mathbf{low\text{-}bound}\ h\ \phi) \wedge (\phi\ r_1\ \ldots\ r_n)]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] &= \\ \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\mathbf{low\text{-}bound}\ h\ \phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] & \\ \cdot \mathrm{Pr}_{\rho \in \mathbb{T}}\left[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \middle|\ [\![\mathbf{low\text{-}bound}\ h\ \phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}\ \right] &\end{aligned}$$

Besides, by definition of **low-bound** semantics, we have $\mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\left[\ [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}(r_1, \ldots, r_n)\ \right] \geqslant \mathbb{E}_{\rho'}\left([\![h]\!]^{\eta,\rho'}_{\mathbb{M}:\mathcal{E}}\right)$.

Moreover, for all $\rho \in \mathbb{T}$, we have the following lower bound

$$\begin{aligned}\mathrm{Pr}_{\rho' \in \mathbb{T}}\left[\ [\![\phi\ r_1\ \ldots\ r_n]\!]^{\eta,\rho'}_{\mathbb{M}:\mathcal{E}}\ \right] & \\ \geqslant \mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\left[\ [\![\phi]\!]^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}(r_1, \ldots, r_n)\ \right]. &\end{aligned}$$

Protocol 4: 9-move *zero-knowledge* protocol $\mathbb{ZK}^{(4)}[\mathcal{R}^{\mathsf{TW}}_{\phi_{\mathbb{CS}}}]$ for the Terelius-Wikström commitment-consistent proof of shuffle using a *shuffle-friendly map* $\phi_{\mathbb{CS}}$

Public Input : A natural number $N \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{N+1}$ for the commitment schemes $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ and $\mathbb{KS}[\mathsf{Mat}_N(\mathbb{F}(p_\eta))]$. A public key $pk \in \mathcal{PK}_{\mathbb{CS}}$ of the cryptosystem $\mathbb{CS}$. A list of ciphertexts $\mathbf{c} = (c_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$.

Begin protocol

[Offline phase]:

1) **(Commitment message)** The prover $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ chooses a random permutation matrix $\pi \xleftarrow{\$} \Pi_N(\mathbb{F}(p_\eta))$ and a vector of random values $\mathbf{s} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$. Then, $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ computes the commitment value $\mathbf{a} = \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, \pi\,;\,\mathbf{s})$ and hands it to the verifier $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$.

2) **(Challenge message)** $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ chooses uniformly at random a vector challenge $\mathbf{e}_{\mathsf{off}} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ and sends it to $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$.

(3-5) **(Rest of the *offline* phase)** Both prover $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ and verifier $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ engage in the Σ-protocol $\Sigma_{\mathsf{off}}(\mathbf{e}_{\mathsf{off}})$ for the relation $\mathcal{R}^{\mathsf{off}}$ with public parameter $\sigma_{\mathsf{off}} = \big(ck, \mathbf{e}_{\mathsf{off}}\big)$, public statement $x_{\mathsf{off}} = \mathbf{a}$, and private statement $w_{\mathsf{off}} = \big(\pi, \mathbf{s}\big)$. Hence, we obtain the proof transcript $\tau_{\mathsf{off}}\big(\sigma_{\mathsf{off}}, x_{\mathsf{off}}, w_{\mathsf{off}}\big) = \langle \alpha_{\mathsf{off}}, \gamma_{\mathsf{off}}, z_{\mathsf{off}} \rangle$.

[Online phase]:

5) **(Commitment message)** The prover $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ chooses a vector random values $\mathbf{r} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$. Then, $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ computes the list of ciphertexts $\mathbf{c}' = (c'_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$ defined by the following equation
$$\forall\, i \in [\![1; N]\!],\; c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i).$$
Finally, $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ sends the freshly computed list of ciphertexts $\mathbf{c}'$ along with the response message of the *offline* phase z_{off}.

6) **(Challenge message)** $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ chooses uniformly at random a vector challenge $\mathbf{e}_{\mathsf{on}} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ and sends it to $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$.

(7-9) **(Rest of the *online* phase)** Both prover $\mathcal{P}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ and verifier $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ engage in the Σ-protocol $\Sigma_{\mathsf{on}}^{(\phi_{\mathbb{CS}})}(\mathbf{e}_{\mathsf{on}})$ for the relation $\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}$ with public parameter $\sigma_{\mathsf{on}} = \big(ck, pk, \mathbf{e}_{\mathsf{on}}\big)$, public statement $x_{\mathsf{on}} = \big(\mathbf{a}, \mathbf{c}, \mathbf{c}'\big)$, and private statement $w_{\mathsf{on}} = \big(\pi, \mathbf{s}, \mathbf{r}\big)$. Hence, we obtain the proof transcript $\tau\big(\sigma_{\mathsf{on}}, x_{\mathsf{on}}, w_{\mathsf{on}}\big) = \langle \alpha_{\mathsf{on}}, \gamma_{\mathsf{on}}, z_{\mathsf{on}} \rangle$.

[Conclusion]:

10) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{TW}}^{(\phi_{\mathbb{CS}})}$ accepts if and only if the following equations hold
$$v_{\mathsf{off}}^{(ck, \mathbf{e}_{\mathsf{off}}),\, \mathbf{a}}\big(\langle \alpha_{\mathsf{off}}, \gamma_{\mathsf{off}}, z_{\mathsf{off}} \rangle\big) = 1,$$
$$\text{and} \quad v_{\mathsf{on}}^{(ck, pk, \mathbf{e}_{\mathsf{on}}),\, (\mathbf{a}, \mathbf{c}, \mathbf{c}')}\big(\langle \alpha_{\mathsf{on}}, \gamma_{\mathsf{on}}, z_{\mathsf{on}} \rangle\big) = 1.$$

End

Therefore, by the two previous equations, we have the following lower bound
$$\mathrm{Pr}_{\rho \in \mathbb{T}}\Big[\; [\![\phi\; r_1\; \ldots\; r_n]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \;\Big|\; [\![\textbf{low-bound}\; h\; \phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \;\Big] \geqslant \mathbb{E}_{\rho \in \mathbb{T}}\big([\![h]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$

Consequently, by hypothesis Eq. ($\mathcal{H}$) and by the previous equation, we have
$$\mathrm{Pr}_{\rho \in \mathbb{T}}\Big[\; [\![(\textbf{low-bound}\; h\; \phi) \wedge (\phi\; r_1\; \ldots\; r_n)]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \;\Big] \geqslant \mathbb{E}_{\rho \in \mathbb{T}}\big([\![g]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big) \cdot \mathbb{E}_{\rho \in \mathbb{T}}\big([\![h]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big)$$

As $\mathcal{E}; \Theta \vdash \textbf{det}(h)$ holds, we have $\mathbb{E}_{\rho \in \mathbb{T}}\big([\![h]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big) = h$ (here we blend h with its deterministic semantics). Therefore, we conclude the following lower bound by properties on expected value
$$\mathrm{Pr}_{\rho \in \mathbb{T}}\Big[\; [\![(\textbf{low-bound}\; h\; \phi) \wedge (\phi\; r_1\; \ldots\; r_n)]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \;\Big] \geqslant \mathbb{E}_{\rho \in \mathbb{T}}\big([\![g \cdot h]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big)$$

which achieve proof of soundness for G.LB:Out.

- (L.LB:Trans) Let $\eta \in \mathbb{N}^*$ be a security parameter and $\rho \in \mathbb{T}$ be a random tape. We suppose $[\![\textbf{low-bound}\; g\; \phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$. By definition of **low-bound** semantics, we have the following inequality
$$\mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\Big[\; [\![\phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r_1, \ldots, r_n) \;\Big] \geqslant \mathbb{E}_{\rho' \in \mathbb{T}}\big([\![g]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$
However, by hypothesis $\mathcal{E}; \Theta \vdash {}_1[(\phi\; r_1\; \ldots\; r_n) \to (\psi\; r_1\; \ldots\; r_n)]$, we conclude the following inequality
$$\mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\Big[\; [\![\phi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r_1, \ldots, r_n) \;\Big] \leqslant \mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\Big[\; [\![\psi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r_1, \ldots, r_n) \;\Big].$$
Therefore, the two previous inequalities leads to the following property
$$\mathrm{Pr}_{r_i \in [\![\tau_i]\!]^{\eta}_{\mathbb{M}}, i \in [\![1;n]\!]}\Big[\; [\![\psi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r_1, \ldots, r_n) \;\Big] \geqslant \mathbb{E}_{\rho' \in \mathbb{T}}\big([\![g]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$
Said otherwise, for all security parameter $\eta \in \mathbb{N}^*$ and for all random tape $\rho \in \mathbb{T}$, we conclude $[\![\textbf{low-bound}\; g\; \psi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$, and achieves this way the proof.
- (G.LB:Trans) Let h : **real** with $\mathcal{E}; \Theta \vdash \textbf{non-negl}(h)$ be another non-negligible parameter. Let $\psi : \tau_1 \to \cdots \to \tau_n \to$ **bool** be a formula with n parameters. Let $\chi : \tau \to$ **bool** be a formula. By definition of ${}_g[\phi]$ semantics, we have to prove
$$\forall\, \eta \in \mathbb{N}^*, \mathrm{Pr}_{\rho \in \mathbb{T}}\Big[\; [\![(\textbf{low-bound}\; h\; \psi) \wedge \chi]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \;\Big] \geqslant \mathbb{E}_{\rho \in \mathbb{T}}\big([\![h]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$
Let $\eta \in \mathbb{N}^*$ be a security parameter. Because we have as hypothesis $\mathcal{E}; \Theta \vdash {}_1[(\phi\; r_1\; \ldots\; r_n) \to (\psi\; r_1\; \ldots\; r_n)]$, we

conclude by the rule L.LB:Trans the following property $\mathcal{E};\Theta;\varnothing \vdash \big(\textbf{low-bound}\ h\ \phi\wedge\chi\big) \to \big(\textbf{low-bound}\ h\ \psi\wedge\chi\big)$. Therefore, we have the following inequality

$$\Pr_{\rho\in\mathbb{T}}\Big[\ [\![(\textbf{low-bound}\ h\ \phi)\wedge\chi]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big] \leqslant \Pr_{\rho\in\mathbb{T}}\Big[\ [\![(\textbf{low-bound}\ h\ \psi)\wedge\chi]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big].$$

Then, by the hypothesis $\mathcal{E};\Theta \vdash_{g} [(\textbf{low-bound}\ h\ \phi)\wedge\chi]$, we conclude the property we want.

B. Soundness of property transfer under adversarial selection

Let $k:\textbf{nat}$ be a polynomial bounded and deterministic natural term. As k is deterministic, that is the semantics of k does not depend on the random tape ρ (*i.e.* for all random tapes $\rho,\rho'\in\mathbb{T}$ and for all security parameter $\eta\in\mathbb{N}^*$, we have $[\![k]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = [\![k]\!]^{\eta\,,\,\rho'}_{\mathbb{M}\,:\,\mathcal{E}}$). Therefore, we denote by k the function $k:\eta\longmapsto[\![k]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$ and because $\textbf{pbound}(k)$ holds, the related function k is polynomially bounded. Let $\mathbf{r}_s:\textbf{nat}\to\tau$ be a random source term of *uniformly distributed* random terms of type τ. Let $n\in\mathbb{N}^*$ be a natural number and $\phi:\tau\to\cdots\to\tau\to\textbf{bool}$ be a formula of n parameters of the same type τ. Let $\textbf{select}^{(n)}_{\text{rand}}:\textbf{nat}\to(\textbf{nat}\to\tau)\to\textbf{set}_n(\tau)$ be an adversarial selection function of n distinct terms of type τ given by a random source term. Let $\eta\in\mathbb{N}^*$ be a security parameter. We suppose that we are in the case where $k(\eta)\geqslant n$. By definition of the type $\textbf{set}_n(\tau)$, we have $\mathrm{Card}([\![\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}) = n$. Then, by hypothesis $\mathcal{E};\Theta\vdash[\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s\subseteq\{\mathbf{r}_s\ 1,\ldots,\mathbf{r}_s\ k\}]$, we conclude, without loss of generality, the existency of n distinct natural terms $t_1,\ldots,t_n:\textbf{nat}$, such that $1\leqslant t_1<\cdots<t_n\leqslant k$ and $\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s=\{\mathbf{r}_s\ t_i\}_{i=1}^{n}$. Therefore, we have

$$\begin{aligned}\Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big] &= \Pr_{\rho\in\mathbb{T}}\Big[\ \exists\,1\leqslant j_1<\cdots<j_n\leqslant k(\eta),\\ &\qquad [\![\neg\ \phi\ (\mathbf{r}_s\ j_1)\ \ldots\ (\mathbf{r}_s\ j_n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big]\end{aligned}$$

By property on probabilities, we have the following upper bound

$$\begin{aligned}&\Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big]\\ &\leqslant \sum_{\{j_i\}_{i=1}^{n}\,\subseteq\,[\![1;k(\eta)]\!]} \Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\mathbf{r}_s\ j_1)\ \ldots\ (\mathbf{r}_s\ j_n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big].\end{aligned}$$

But as $\mathbf{r}_s$ is a random source term of *uniformly distributed* random terms of type τ, we have

$$\begin{aligned}&\forall\,\{j_i\}_{i=1}^{n}\ \subseteq\ [\![1;k(\eta)]\!],\\ &\quad \Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\mathbf{r}_s\ j_1)\ \ldots\ (\mathbf{r}_s\ j_n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big]\\ &\qquad = \Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big].\end{aligned}$$

Besides, we have

$$\mathrm{Card}(\{j_i\}_{i=1}^{n}\ \subseteq\ [\![1;k(\eta)]\!]) = \binom{k(\eta)}{n} \leqslant k(\eta)^n.$$

Therefore, we conclude the following upper bound

$$\begin{aligned}&\Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big]\\ &\leqslant \underbrace{k(\eta)^n}_{\text{polynomial in }\eta}\ \cdot \underbrace{\Pr_{\rho\in\mathbb{T}}\Big[\ [\![\neg\ \phi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big]}_{\text{negligible in }\eta}.\end{aligned}$$

By hypothesis $\mathcal{E};\Theta\vdash[\phi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)]$, we conclude the property we want, *i.e.* we obtain the following property

$$\mathcal{E};\Theta\vdash[n\leqslant k\to\phi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)].$$

C. Soundness of algebraic rules

- (L.π:Charac) This rule is a model of the following proposition:

  Proposition 3 (Characterization of permutation matrix). *Let $M\in\mathsf{Mat}_N(\mathbb{F}(p_\eta))$ be a matrix. Let $\mathbf{e}\xleftarrow{\$}\mathbb{F}(p_\eta)^N$ be a vector of N independent variables and chosen uniformly at random. We suppose that the two following equations, denoted by (i) and (ii) hold, for M and $\mathbf{e}$.*

  $$(i)\quad M\cdot\mathbf{1}=\mathbf{1}\quad\textit{and}\quad(ii)\quad\textstyle\prod_{i=1}^{N}\big(M\cdot\mathbf{e}\big)_i=\prod_{i=1}^{N}e_i.$$

  Then we conclude that M is a permutation matrix with probability at least equal to $1-\frac{N}{p_\eta^N}$.

  A proof of this proposition can be found in [5].

- (L.Open) Soundness of this rule come quite straightforwardly from the following lemma:

  Lemma 1. *Let $\mathbf{a}=(a_i)_{i=1}^{N}\in\mathbb{G}_{p_\eta}^{N}$ be a vector. Suppose there exists a set $\mathcal{W}=\{\mathbf{e}_i\}_{i=1}^{N}$ of N linearly independent vectors of $\mathbb{F}(p_\eta)^N$ such that*

  $$\begin{aligned}&\forall\,i\in[\![1;N]\!],\exists\,\mathbf{e}'_i\in\mathbb{F}(p_\eta)^N,\exists\,k_i\in\mathbb{F}(p_\eta),\\ &\qquad\mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck,\mathbf{e}'_{\mathbf{i}}\,;\,k_i)=\mathbf{a}\circledast\mathbf{e}_{\mathbf{i}}.\end{aligned}$$

  Then $\mathbf{a}$ is a commitment message to a matrix $M_{\mathcal{W}}\in\mathsf{Mat}_N(\mathbb{F}(p_\eta))$ using the vector of random values $\mathbf{s}_{\mathcal{W}}\in\mathbb{F}(p_\eta)^N$, i.e. *we have* $\mathbf{a}=\mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck,M_{\mathcal{W}}\,;\,\mathbf{s}_{\mathcal{W}})$*. Besides, these opening $(M_{\mathcal{W}},\mathbf{s}_{\mathcal{W}})$ can be obtained in polynomial time.*

  Proof. Let $\mathbf{a}=(a_i)_{i=1}^{N}\in\mathbb{G}_{p_\eta}^{N}$ be a vector of values in the group $\mathbb{G}_{p_\eta}$. Let $\mathcal{W}=\{\mathbf{e}_i\}_{i=1}^{N}$ a set of N linearly independent vectors of $\mathbb{F}(p_\eta)^N$ such that

  $$\begin{aligned}&\forall\,i\in[\![1;N]\!],\exists\,\mathbf{e}'_i\in\mathbb{F}(p_\eta)^N,\exists\,k_i\in\mathbb{F}(p_\eta),\\ &\qquad\mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck,\mathbf{e}'_i\,;\,k_i)=\mathbf{a}\circledast\mathbf{e}_i.\quad(*)\end{aligned}$$

  As the vectors of the set $\mathcal{W}=\{\mathbf{e}_i\}_{i=1}^{N}$ are linearly independent, and because $\dim(\mathbb{F}(p_\eta)^N)=N$, the family $\mathcal{B}_{\mathcal{W}}=\big(\mathbf{e}_1,\ldots,\mathbf{e}_N\big)$ is a basis of $\mathbb{F}(p_\eta)^N$. Hence, for all $j\in[\![1;N]\!]$, there exists a set of scalar values $\{\lambda_i^{(j)}\}_{i=1}^{N}\in\mathbb{F}(p_\eta)^N$ such that $\sum_{i=1}^{N}\lambda_i^{(j)}\mathbf{e}_i=\mathbf{u}_j$ where $\mathbf{u}_j$ is the j-th standard vector of $\mathbb{F}(p_\eta)^N$. In fact, such set of scalar values can be obtain in polynomial time by

Gaussian elimination. Let $j \in [\![1;N]\!]$. By basic properties on $\circledast$, we have

$$a_j = \mathbf{a} \circledast \left(\sum_{i=1}^{N} \lambda_i^{(j)} \mathbf{e}_i\right) = \prod_{i=1}^{N} \left(\mathbf{a} \circledast \mathbf{e}_i\right)^{\lambda_i^{(j)}}.$$

By the equation Eq. $(*)$, we have, for all $i \in [\![1;N]\!]$, $\mathbf{a} \circledast \mathbf{e}_i = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'_i\,;\, k_i)$. Thus,

$$a_j = \prod_{i=1}^{N} \left(\mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'_i\,;\, k_i)\right)^{\lambda_i^{(j)}}$$

By definition of the commitment algorithm $\mathrm{Com}_{\mathbb{F}(p_\eta)^N}$, we have $\mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, \mathbf{e}'_i\,;\, k_i) = g^{k_i} \prod_{l=1}^{N} g_l^{(\mathbf{e}'_i)_l}$. Consequently,

$$\begin{aligned} a_j &= \prod_{i=1}^{N} \left(g^{\lambda_i^{(j)} k_i} \prod_{l=1}^{N} g_l^{\lambda_i^{(j)} (\mathbf{e}'_i)_l} \right) \\ &= g^{\sum_{i=1}^{N} \lambda_i^{(j)} k_i} \prod_{l=1}^{N} g_l^{\sum_{i=1}^{N} \lambda_i^{(j)} (\mathbf{e}'_i)_l} \end{aligned}$$

Finally, we have, for all $j \in [\![1;N]\!]$,

$$a_j = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}\left(ck, \sum_{i=1}^{N} \lambda_i^{(j)} \mathbf{e}'_i\,;\, \sum_{i=1}^{N} \lambda_i^{(j)} k_i\right).$$

Consequently, we conclude that $\mathbf{a}$ is indeed a commitment message produced by the commitment algorithm $\mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}$, *i.e.* $\mathbf{a} = \mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, M_{\mathcal{W}}\,;\, \mathbf{s}_{\mathcal{W}})$ where $M_{\mathcal{W}} \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))$ and $\mathbf{s}_{\mathcal{W}} \in \mathbb{F}(p_\eta)^N$ are defined as follows.

$$\boxed{M_{\mathcal{W}} = \left(\sum_{j=1}^{N} \lambda_j^{(l)} \mathbf{e}'_j\right)_{l=1}^{N} \quad \text{and} \quad \mathbf{s}_{\mathcal{W}} = \left(\sum_{j=1}^{N} \lambda_j^{(l)} k_j\right)_{l=1}^{N}}$$

□

- (L.Basis) Let $n \in \mathbb{N}^*$ be a non-null natural number. Let $(\mathbf{e}_i)_{i=1}^{n-1}$ be a free family of vector in $\mathbb{F}(p_\eta)^n$. Let $\mathbb{H}$ be the linear span of vectors set $(\mathbf{e}_i)_{i=1}^{n-1}$. Hence, $\mathbb{H}$ defines an hyperplane of $\mathbb{F}(p_\eta)^n$. Therefore, the probability to choose a new vector $\mathbf{e}$ uniformly and independently from vectors family $(\mathbf{e}_i)_{i=1}^{n-1}$ such that $\mathbf{e} \in \mathbb{H}$ is at most equal to $\frac{1}{p_\eta}$:

$$\Pr_{\mathbf{e} \xleftarrow{\$} \mathbb{F}(p_\eta)^n} \Big[\, \mathbf{e} \in \mathbb{H} \,\Big] \leqslant \frac{1}{p_\eta}.$$

Which achieve proof of soundness of the rule L.Basis.

- (L.π:Charac) This rule is a model of the following lemma:

Lemma 2 (Schwartz-Zippel)**.** *Let $f_d \in \mathbb{F}(p_\eta)[X_1, \ldots, X_N]$ be a non-zero multivariate polynomial of total degree $d \in \mathbb{N}$ over $\mathbb{F}(p_\eta)$. Let $\mathbf{e} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ be a vector chosen uniformly at random in the vector space $\mathbb{F}(p_\eta)^N$. Then* $\Pr_{\mathbf{e} \in \mathbb{F}(p_\eta)^N} \Big[\, f_d(\mathbf{e}) = 0 \,\Big] \leqslant \frac{d}{p_\eta^N}$.

A proof of this lemma can be found in [23] and [24].

- (L.$\circledast$:Com) Soundness of this rule come from the following proposition:

Proposition 4. *For $ck = (g, \mathbf{g}) \leftarrow \mathrm{Gen}(1^\eta, N)$ be a commitment key, for all matrix $M \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))$ and for all vectors $\mathbf{x}, \mathbf{s} \in \mathbb{F}(p_\eta)^N$, we have the following identity.*

$$\begin{aligned} &\mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, M\,;\, \mathbf{s}) \circledast \mathbf{x} = \\ &\qquad\qquad \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, M \cdot x\,;\, \langle \mathbf{s} \mid \mathbf{x} \rangle) \end{aligned}$$

Proof. Let $ck = (g, g_1, \ldots, g_N) \leftarrow \mathrm{Gen}(1^\eta, N)$ be a commitment key. Let $M \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))$ be a matrix and let $\mathbf{x}, \mathbf{s} \in \mathbb{F}(p_\eta)^N$ be two vectors. Then, by definitions of both commitment schemes and of operator $\circledast$, we have

$$\begin{aligned} &\mathrm{Com}_{\mathsf{Mat}_N(\mathbb{F}(p_\eta))}(ck, M\,;\, \mathbf{s}) \circledast \mathbf{x} \\ &\quad = \prod_{i=1}^{N} g^{s_i x_i} \prod_{j=1}^{N} g_j^{m_{j,i} x_i} \\ &\quad = g^{\sum_{i=1}^{N} s_i x_i} \prod_{j=1}^{N} g_j^{\sum_{i=1}^{N} m_{j,i} x_i} \\ &\quad = \mathrm{Com}_{\mathbb{F}(p_\eta)^N}(ck, M \cdot \mathbf{x}\,;\, \langle \mathbf{s} \mid \mathbf{x} \rangle). \end{aligned}$$

□

D. Soundness of cryptographic rules

In this subsection, we briefly give some flavour of key arguments to prove soundness of the cryptographic rules. More details for these kind of proofs can be found in [12].

- (G.Com:Hide) Soundness of this rule comes from the *hiding* security property, and more precisely from the *hiding* game Game 5 of the commitment scheme defined consistently with the semantics of the function symbol $\mathbf{com}/3$. Notice that in this game, commitment key parameter ck is honestly computed, meaning that the adversary can only uses this parameter. This is why we have the global hypothesis $\mathcal{E}; \Theta \vdash [\Psi_{\mathsf{comkey}}^{ck,n}(\mathbf{u}, m_1, m_2)]$. Besides the random value $r \xleftarrow{\$} \mathbb{F}(p_\eta)$ is chosen uniformly at random and independently from all other computations of the game, r is then *fresh*. Thus, we have to suppose the global hypothesis $\mathcal{E}; \Theta \vdash [\Psi_{\mathsf{fresh}}^{r,i}(\mathbf{u}, m_1, m_2)]$. All other terms (in $\mathbf{u}$, and message terms m_1 and m_2) are computed by the adversary.
- (L.Com:Bind) Based on the *binding* game Game 6, only the commitment key parameter ck is not computed by the adversary. Thus, we suppose the local property $\mathcal{E}; \Theta; \Gamma \vdash \Psi_{\mathsf{comkey}}^{ck,n}(m_1, m_2, r_1, r_2)$. Which gives us the soundness of this rule.
- (L.Σ-P:SpSound) For this property, we only have two accepted proof transcripts $\mathfrak{p}_{\mathcal{R}}^{(i)}(c_i) \overset{\text{def}}{=} \langle \alpha, c_i, z(c_i) \rangle$ regardless the way these proofs are generated. Only requirements are to have the same commitment message α and two different challenges $c_1 \neq c_2$. Besides, these transcripts prove that any statement x belongs to the

language $\mathcal{L}_\sigma(\mathcal{R})$ of the relation $\mathcal{R}$. Besides, the existency of the function symbol **zkp-extract**$_\mathcal{R}/4$ in the CCSA logic and the soundness of the rule follows from the *special-soundness* security property Game 10 for the Σ-protocol given by semantics of function symbols (**zkp-prove**$_\mathcal{R}/4$, **zkp-verif**$_\mathcal{R}/3$).

- (G.Σ-P:HVZK) By definition of the *Honest-Verifier Zero-Knowledge* game given in G.Σ-P:HVZK, even if the adversary can force the witness-statement pair (x, w) and the challenge c used by honest prover and verifier, they cannot distinguish between an honestly computed proof transcript, using the witness w, from a simulated one, which does not uses w. Moreover, the existency of the simulator function symbol **zkp-sim**$_\mathcal{R}/3$ and the soundness of the rule follows from the *Honest-Verifier Zero-Knowledge* security property.
- (L.SFM:CORRECT and G.SFM:INDCCA) As soundness of these two rules are strongly dependent from the definition of the *shuffle-friendly* map considered, these rules have to be proved as soon as such map is defined.
- (L.SFM:CHARAC) Soundness of this rule follows from the following lemma giving a criterion of correct shuffle.

Lemma 3 (Characterization of correct shuffle)**.** *Let $\phi_{\mathbb{CS}}$ be a* shuffle-friendly *map for a cryptosystem $\mathbb{CS}$. Let $\mathbf{c} = (c_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$ and $\mathbf{c}' = (c'_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$ be two lists of ciphertexts. Let $\pi \in \mathfrak{S}_N$ be a permutation of length N. Let $pk \in \mathcal{PK}_{\mathbb{CS}}$ be a public-key for the cryptosystem $\mathbb{CS}$. We denote by $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} \subseteq \mathbb{F}(p_\eta)^N$ the following set*

$$\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} = \left\{ \mathbf{e} \in \mathbb{F}(p_\eta)^N \;\middle|\; \begin{array}{r} \exists\, v \in \mathbb{F}(p_\eta), \mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{e}\big) \\ = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}\,;\, v) \end{array} \right\}$$

Then, we have an equivalence between the following properties.

(i) There exists a vector of random values $\mathbf{r} = (r_i)_{i=1}^N \in \mathbb{F}(p_\eta)^N$ such that we have:

$$\forall\, i \in [\![1; N]\!], c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i).$$

(ii) $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} = \mathbb{F}(p_\eta)^N$.

(iii) $\mathrm{Card}(\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}) > p_\eta^{N-1}$.

(iv) $\Pr_{\mathbf{e} \xleftarrow{\$} \mathbb{F}(p_\eta)^N}\Big[\, \mathbf{e} \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} \,\Big] > \dfrac{1}{p_\eta}$.

Proof. Let $\phi_{\mathbb{CS}}$ be a *shuffle-friendly* map for a cryptosystem $\mathbb{CS}$. Let $\mathbf{c} = (c_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$ and $\mathbf{c}' = (c'_i)_{i=1}^N \in \mathcal{C}_{\mathbb{CS}}^N$ be two lists of ciphertexts. Let $\pi \in \mathfrak{S}_N$ be a permutation of length N. Let $pk \in \mathcal{PK}_{\mathbb{CS}}$ be a public-key for the cryptosystem $\mathbb{CS}$.

- $(i) \implies (ii)$ *Suppose there exists a vector of random values $\mathbf{r} = (r_i)_{i=1}^N \in \mathbb{F}(p_\eta)^N$ such that: $\forall\, i \in [\![1; N]\!], c'_{\pi(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i)$.* We want to prove the following inclusion: $\mathbb{F}(p_\eta)^N \subseteq \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$. Let $\mathbf{e} \in \mathbb{F}(p_\eta)^N$ be a vector. Let $M_\pi \in \mathsf{Mat}_N(\mathbb{F}(p_\eta))$ be the permutation matrix representing the permutation π. We set $\mathbf{e}' = M_\pi \cdot \mathbf{e}$. By definition of $\mathbf{e}'$, we have, for all $i \in [\![1; N]\!]$,

$$e'_i = \big(M_\pi \cdot \mathbf{e}\big)_i = \sum_{j=1}^N m_{i,j}^{(\pi)} e_j = \sum_{j=1}^N \delta_{i\pi(j)} e_j = e_{\pi^{-1}(i)}.$$

Hence, we have

$$\begin{aligned}
\mathbf{c}' \circledast \mathbf{e}' &= \prod_{i=1}^N (c'_i)^{e_{\pi^{-1}(i)}} \\
&= \prod_{i=1}^N \big(\phi_{\mathbb{CS}}(pk, c_{\pi^{-1}(i)}\,;\, r_{\pi^{-1}(i)})\big)^{e_{\pi^{-1}(i)}} \\
&\quad \text{(by the hypothesis } (i)) \\
&= \phi_{\mathbb{CS}}\left(pk, \prod_{i=1}^N c_{\pi^{-1}(i)}^{e_{\pi^{-1}(i)}}\,;\, \sum_{i=1}^N e_{\pi^{-1}(i)} r_{\pi^{-1}(i)}\right) \\
&\quad \text{(because } \phi_{\mathbb{CS}} \text{ is an homomorphism)} \\
&= \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}\,;\, \langle \mathbf{e} \mid \mathbf{r} \rangle).
\end{aligned}$$

Thus, we have $\mathbf{e} \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$, *i.e.* we have proved (ii).

- $(ii) \implies (i)$ Actually, we proceed by contraposition. Hence, we suppose the existence of $i_0 \in [\![1; N]\!]$ such that we have the following property

$$\forall\, v \in \mathbb{F}(p_\eta), c'_{\pi(i_0)} \neq \phi_{\mathbb{CS}}(pk, c_{i_0}\,;\, v).$$

We show that $\mathbf{u}_{i_0} \notin \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$. Let $v \in \mathbb{F}(p_\eta)$. Hence, we have.

$$\begin{aligned}
\mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{u}_{i_0}\big) = c'_{\pi(i_0)} &\neq \phi_{\mathbb{CS}}(pk, c_{i_0}\,;\, v) \\
&\quad \text{(by definition of } \neg\,(i)) \\
&= \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{u}_{i_0}\,;\, v)
\end{aligned}$$

Consequently, we have $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} \subsetneq \mathbb{F}(p_\eta)^N$.

- $(ii) \iff (iii)$ In fact, we prove that $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$ is a subgroup of $\big(\mathbb{F}(p_\eta)^N, +\big)$. Let $\mathbf{e}_1, \mathbf{e}_2 \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$. By definition of $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$, there exists $v_1, v_2 \in \mathbb{F}(p_\eta)$ such that

$$\left\{ \begin{array}{l} \mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{e}_1\big) = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}_1\,;\, v_1) \\ \mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{e}_2\big) = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}_2\,;\, v_2) \end{array} \right.$$

Then, we have

$$\begin{aligned}
&\mathbf{c}' \circledast \big(M_\pi \cdot (\mathbf{e}_1 - \mathbf{e}_2)\big) \\
&\quad = \mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{e}_1\big) \cdot \Big(\mathbf{c}' \circledast \big(M_\pi \cdot \mathbf{e}_2\big)\Big)^{-1} \\
&\quad = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}_1\,;\, v_1) \cdot \Big(\phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast \mathbf{e}_2\,;\, v_2)\Big)^{-1} \\
&\quad \text{(because } \mathbf{e}_1 \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi} \text{ and } \mathbf{e}_2 \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}) \\
&\quad = \phi_{\mathbb{CS}}(pk, \mathbf{c} \circledast (\mathbf{e}_1 - \mathbf{e}_2)\,;\, v_1 - v_2) \\
&\quad \text{(by a basic property of } \phi_{\mathbb{CS}})
\end{aligned}$$

Consequently, we have $\mathbf{e}_1 - \mathbf{e}_2 \in \mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$. Thus, $\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}$ is a subgroup of $\big(\mathbb{F}(p_\eta)^N, +\big)$. However, by the Lagrange's theorem, the cardinal $\mathrm{Card}(\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi})$ divides the cardinal $\mathrm{Card}(\mathbb{F}(p_\eta)^N) = p_\eta^N$. Therefore, we have $(ii) \iff (iii)$.

- $\underline{(iii) \iff (iv)}$ As the vector $\mathbf{e} \xleftarrow{\$} \mathbb{F}(p_\eta)^N$ is *chosen uniformly at random*, we have

$$\Pr_{\mathbf{e}\xleftarrow{\$}\mathbb{F}(p_\eta)^N}\left[\,\mathbf{e}\in\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi}\,\right] = \frac{\mathrm{Card}(\mathbb{H}_{\mathbf{c},\mathbf{c}',\pi})}{p_\eta^N}.$$

  Consequently, we have $(iii) \iff (iv)$.

□

Hence, to obtain soundness of the L.SFM:CHARAC rule, as we have the hypothesis $\mathcal{E};\Theta;\Gamma \vdash \Psi^{\mathbf{e},t}_{\mathsf{fresh}}(\mathbf{c},\mathbf{c}',\pi)$, we can use the equivalence $(ii) \iff (iv)$.

Notice that all these rules hold regardless whether the cryptographic property considered is *perfect* or *computational*.

Appendix E
Rewinding algorithms

The procedure of witness extraction for the Σ-protocol $\Sigma_{\mathcal{R}}$ is given by Algorithm 5.

Algorithm 5: Witness extraction procedure using the rewinding technique

```
Input  : A security parameter $\eta \in \mathbb{N}^*$. An adversary $\mathcal{A}$.
         A $\Sigma$-protocol $\Sigma_{\mathcal{R}} = (\mathcal{S}, \mathcal{P}, \mathcal{V})$ for a computable
         binary relation $\mathcal{R}$. An extractor $\mathcal{E}_{\mathcal{R}}$ for $\Sigma_{\mathcal{R}}$. A
         public parameter $\sigma$ for the relation $\mathcal{R}$. A
         statement $x_\eta \in \mathcal{L}_{\mathcal{R}}(\sigma)$ of bit-size polynomial in
         the security parameter $\eta$, i.e. $|x_\eta| = \eta^{O(1)}$.
Output : A witness $w \in \mathcal{W}_{\mathcal{R}}$ such that $(\sigma, x_\eta, w) \in \mathcal{R}$.
let extract-sigp$_{\mathcal{R}}$ $\sigma$ $x_\eta$ =
    The adversary $\mathcal{A}$ begins by computing some
      commitment message for the statement $x_\eta$ which
      updates their state and sends it to the verifier:
      $(\mathtt{st}^{(1)}_{\mathcal{A}}, \alpha) \leftarrow \mathcal{A}(\sigma, x_\eta)$ ;
    repeat
        The verifier $\mathcal{V}$ chooses a first challenge
          $c_1 \leftarrow \mathcal{V}(\sigma, x_\eta, \alpha)$ ;
        $\mathcal{A}$ produces a response for this challenge, which
          also updates their state:
          $(\mathtt{st}^{(2)}_{\mathcal{A}}, z_1(c_1)) \leftarrow \mathcal{A}(\sigma, x_\eta, \alpha, c_1 \ ;\ \mathtt{st}^{(1)}_{\mathcal{A}})$ ;
        Then, we rewind $\mathcal{A}$ to their previous state $\mathtt{st}^{(1)}_{\mathcal{A}}$ ;
        One more time, $\mathcal{V}$ chooses a second challenge
          $c_2 \leftarrow \mathcal{V}(\sigma, x_\eta, \alpha)$ and $\mathcal{A}$ produces another
          response for this challenge:
          $(\mathtt{st}^{(2')}_{\mathcal{A}}, z_2(c_2)) \leftarrow \mathcal{A}(\sigma, x_\eta, \alpha, c_2 \ ;\ \mathtt{st}^{(1)}_{\mathcal{A}})$ ;
        Finally, the verifier $\mathcal{V}$ check whether or not the
          two produced proofs are valid
          $b_i \leftarrow \mathcal{V}(\sigma, x_\eta, \langle \alpha, c_i, z_i(c_i) \rangle)$ ;
    until both Boolean $b_1$ and $b_2$ are true ($b_1 = b_2 = 1$)
      and the challenges are different ($c_1 \neq c_2$).;
    Finally, at this point, we finally extract the witness
      from the two proof transcripts $\mathfrak{p}^{(i)}_{\mathcal{R}}(c_i) \overset{\mathrm{def}}{=} \langle \alpha, c_i, z_i(c_i) \rangle$:
    return $w \leftarrow \mathcal{E}_{\mathcal{R}}(\sigma, x_\eta, \mathfrak{p}^{(1)}_{\mathcal{R}}(c_1), \mathfrak{p}^{(2)}_{\mathcal{R}}(c_2))$
```

The procedure given in Algorithm 6 defines an adversarial selection function $\mathbf{select}^{(n)}_{\mathrm{rand}} : \mathbf{nat} \to (\mathbf{nat} \to \tau) \to \mathbf{set}_n(\tau)$.

Algorithm 6: Adversarial selection function for rewinding

```
Input  : A natural number $k \in \mathbb{N}^*$ and a source of
         uniformly distributed and independent random
         values $\mathbf{r}_s : \mathbb{N}^* \longrightarrow X$. (implicit inputs) A natural
         number $n \in \mathbb{N}^*$ such that $n \leqslant k$ and a formula
         $\phi_{\eta,\rho} : X \longrightarrow \{0,1\}$ evaluable in polynomial
         time.
Output : $n$ random values $(\mathbf{r}_s(i_j))_{j=1}^{n} \subseteq X^n$ with
         $1 \leqslant i_1 < \ldots < i_n \leqslant k$.
let select$^{(n)}_{rand}$ $k$ $\mathbf{r}_s$ =
    $t \leftarrow 1$ ; $l \leftarrow 1$ ; $\mathbb{L} \leftarrow [\,]$ ;
    while $(l \leqslant n \ \wedge\ t \leqslant k)$ do
        $i_l \xleftarrow{\$} [\![1;k]\!] \setminus \{i_j\}_{j=1}^{l-1}$ ;
        if $\phi_{\eta,\rho}(\mathbf{r}_s(i_l))$ then
            $\mathbb{L} \leftarrow \mathbf{r}_s(i_l) :: \mathbb{L}$ ;
            $l \leftarrow l + 1$ ;
        $t \leftarrow t + 1$ ;
    end
    return $\mathbb{L}$
```

Appendix F
Full version of security properties proof

Before giving security properties proofs, a disclaimer. In this section, we present pen-and-paper proofs of security properties. Therefore, to ease readability, we won't precise when we use CCSA rules about logical reasoning, *i.e.* when we use the following rules: G.$\sim$:TRANS, G.BYLOC, and G.REWRITE. Moreover, when $b : \mathbf{bool}$ is a Boolean term and $t : \tau$ is a term of any type, the term **if** b **then** t is a macro for **if** b **then** t **else** $()$. Meaning that, in the case where b is false, no term is output, even if this term is deep in another term. Besides, in the case where $b_c, b_t : \mathbf{bool}$ are Boolean terms, the term **if** b_c **then** b_t is a macro for **if** b_c **then** b_t **else** $\bot$. In the case of application of the function application rule G.$\sim$:FA, we precise only the main relevant function symbols on which we apply the rule, but the rule may be applied to other function symbols like n-tuple ones. Finally, if we want to implement this proof in the Squirrel prover, we may want to adapt some rules to match exactly the structure of the goals. For example, in the case of the *honest-verifier zero-knowledge* rule G.Σ-P:HVZK, we put proof transcript and the simulated transcript term under an if condition.

A. Proof of permutation secrecy

Lemma 4. *Let $\mathcal{E}$ be an environment, let Θ be a context of global formulas and let Γ be a context of local formulas. Let $i \in [\![1;n]\!]$ be an index. We have an equivalence between this two following different properties*

$$\begin{aligned}
&\mathcal{E};\Theta;\Gamma \vdash \langle \mathbf{c}'_\sigma \mid (\sigma\cdot\mathbf{i})\rangle \\
&\qquad = \textbf{\textit{shuf-map}}_{\phi_{\mathsf{CS}}}\,(\mathtt{pk}_{\mathsf{CS}}\,(sk\ k))\,\langle \mathbf{c} \mid \mathbf{i}\rangle\,\langle \mathbf{r}\ l \mid \mathbf{i}\rangle \\
&\leftrightarrow \langle \mathbf{c}'_\sigma \mid \mathbf{i}\rangle = \textbf{\textit{shuf-map}}_{\phi_{\mathsf{CS}}}\,(\mathtt{pk}_{\mathsf{CS}}\,(sk\ k))\,\langle \mathbf{c} \mid (\sigma^{-1}\cdot\mathbf{i})\rangle \\
&\qquad\qquad\qquad\qquad \langle \mathbf{r}\ l \mid (\sigma^{-1}\cdot\mathbf{i})\rangle
\end{aligned}$$

Proof. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\rho \in \mathbb{T}$ be a random tape. Let $pk = [\![\mathrm{pk}_{\mathbb{CS}}\ (sk\ k)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \in \mathcal{PK}_{\mathbb{CS}}$, $(c_i)_{i=1}^n = [\![\mathbf{c}]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \in \mathcal{C}^N_{\mathbb{CS}}$, $(c'_i)_{i=1}^n = [\![\mathbf{c}'_\sigma]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \in \mathcal{C}^N_{\mathbb{CS}}$, $\sigma = [\![\sigma]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$, and $(r_i)_{i=1}^n = [\![\mathbf{r}\ l]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \in (\mathcal{R}_{\mathbb{CS}})^N$. Besides, by definition of the scalar product CCSA function and of the term $\mathbf{j}$, for $j \in [\![1;n]\!]$, we have:

$$\forall\, j \in [\![1;n]\!], \forall\, \mathbf{x} : \mathbf{vect}_n, [\![\langle \mathbf{x} \mid \mathbf{j} \rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = x_j$$
$$\text{where } (x_i)_{i=1}^n = [\![\mathbf{x}]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}.$$

Let $i \in [\![1;n]\!]$ be an index. Hence, the following equations holds

$$\begin{array}{ll}
[\![\langle \mathbf{c}'_\sigma \mid (\sigma \cdot \mathbf{i})\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = c'_{\sigma(i)} & [\![\langle \mathbf{c}'_\sigma \mid \mathbf{i}\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = c'_i \\
[\![\langle \mathbf{c} \mid \mathbf{i}\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = c_i & [\![\langle \mathbf{c} \mid (\sigma^{-1} \cdot \mathbf{i})\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = c_{\sigma^{-1}(i)} \\
[\![\langle \mathbf{r}\ l \mid \mathbf{i}\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = r_i & [\![\langle \mathbf{r}\ l \mid (\sigma^{-1} \cdot \mathbf{i})\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = r_{\sigma^{-1}(i)}.
\end{array}$$

However, as we have the following equation

$$c'_{\sigma(i)} = \phi_{\mathbb{CS}}(pk, c_i\,;\, r_i) \iff c'_i = \phi_{\mathbb{CS}}(pk, c_{\sigma^{-1}(i)}\,;\, r_{\sigma^{-1}(i)}),$$

which achieves this way the proof. □

Lemma 5. *Let $\mathcal{E}$ be an environment and let Θ be a context of global formulas. We suppose the following global judgement*

$$\mathcal{E}; \Theta \vdash [\Psi^{\mathbf{r},l}_{\mathit{fresh}}(\mathbf{u}, l)] \qquad (\mathcal{H})$$

Then, the following property holds for all $i \in [\![1;n]\!]$

$$\mathcal{E}; \Theta \vdash \mathbf{u}, \langle \mathbf{r}\ l \mid \mathbf{i}\rangle \sim \mathbf{u}, \mathbf{r}_{\mathit{fresh}}\ ().$$

Proof. Actually, we will only give key elements of this proof, a full detailed version of the proof can be found in [12] with the proof of soundness of the freshness rule G.$\sim$:FRESH. Let $\mathcal{E}$ be an environment and let Θ be a context of global formulas. Let $i \in [\![1;n]\!]$ be an index. By property Eq. ($\mathcal{H}$), we have in particular the property $[\Psi^{\mathbf{r},l}_{\mathsf{fresh}}(l)]$. Hence, conclude the following property, for all security parameter $\eta \in \mathbb{N}^*$

$$\Big[[\![\langle \mathbf{r}\ l \mid \mathbf{i}\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \mid \rho \in \mathbb{T}\Big] = \Big[[\![\mathbf{r}_{\mathsf{fresh}}\ ()]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \mid \rho \in \mathbb{T}\Big].$$

Besides, by Eq. ($\mathcal{H}$), we have $[\Psi^{\mathbf{r},l}_{\mathsf{fresh}}(\mathbf{u})]$, meaning that, for all security parameter $\eta \in \mathbb{N}^*$, the three following distributions are independent

$$\Big[[\![\mathbf{u}]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \mid \rho \in \mathbb{T}\Big], \quad \Big[[\![\langle \mathbf{r}\ l \mid \mathbf{i}\rangle]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \mid \rho \in \mathbb{T}\Big],$$
$$\Big[[\![\mathbf{r}_{\mathsf{fresh}}\ ()]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \mid \rho \in \mathbb{T}\Big].$$

Therefore, the following property holds

$$\mathcal{E}; \Theta \vdash \mathbf{u}, \langle \mathbf{r}\ l \mid \mathbf{i}\rangle \sim \mathbf{u}, \mathbf{r}_{\mathsf{fresh}}\ ().$$

□

Theorem 1 (Permutation secrecy property)**.** *Let $\mathit{frame}_{\mathit{init}}$ the initial knowledge of the adversary and let Θ_{init} be the initial global context of formulas defined by*

$$\mathit{frame}_{\mathit{init}} \overset{\mathit{def}}{=} (ck\ n), (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k)), \pi, \mathit{id}, \mathbf{c}, v \quad \textit{and}$$
$$\Theta_{\mathit{init}} \overset{\mathit{def}}{=} [\Psi^{ck,n}_{\mathit{comkey}}(\mathit{frame}_{\mathit{init}})], [\Psi^{sk,k}_{\mathit{skey}}(\mathit{frame}_{\mathit{init}})]$$

Then, the Terelius-Wikström shuffle protocol achieves the permutation secrecy property, i.e. *the following property holds*

$$\mathcal{E}; \Theta_{\mathit{init}} \vdash \mathit{frame}_{\mathit{init}}, \boldsymbol{\mathit{mix}}_{\phi_{\mathbb{CS}}}\ \pi\ (ck\ n)\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c}, v)$$
$$\sim \mathit{frame}_{\mathit{init}}, \boldsymbol{\mathit{mix}}_{\phi_{\mathbb{CS}}}\ \mathit{id}\ (ck\ n)\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c}, v)$$

Proof. We denote by terms $\mathbf{a}_\sigma$, $\mathbf{c}'_\sigma$, $\mathfrak{p}_{\mathsf{off}}(\sigma)$ and $\mathfrak{p}_{\mathsf{on}}(\sigma)$ the following terms

$$\begin{aligned}
\mathbf{a}_\sigma &\overset{\mathrm{def}}{=} \textbf{com-mat}\ (ck\ n)\ \sigma\ (\mathbf{s}\ i) \\
\mathbf{c}'_\sigma &\overset{\mathrm{def}}{=} \textbf{shuffle}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ \sigma\ (\mathbf{r}\ l) \\
\mathfrak{p}_{\mathsf{off}}(\sigma) &\overset{\mathrm{def}}{=} \textbf{zkp-prove}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_{\mathsf{off}}\ t_1)\ \mathbf{a}_\sigma\ w_{\mathsf{off}}(\sigma)\ (r_{\mathsf{off}}\ j) \\
\mathfrak{p}_{\mathsf{on}}(\sigma) &\overset{\mathrm{def}}{=} \textbf{zkp-prove}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ (ck\ n, \mathrm{pk}_{\mathbb{CS}}\ (sk\ k), \mathbf{e}_{\mathsf{on}}\ t_2) \\
&\qquad (\mathbf{a}_\pi, \mathbf{c}, \mathbf{c}'_\pi)\ w_{\mathsf{on}}(\sigma)\ (r_{\mathsf{on}}\ p).
\end{aligned}$$

Let $\mathsf{frame}_{\mathsf{end}}(\sigma)$ the frame at the very end of the protocol execution defined by

$$\mathsf{frame}_{\mathsf{end}}(\sigma) \overset{\mathrm{def}}{=} \mathsf{frame}_{\mathsf{init}}, \mathbf{a}_\sigma, (\mathbf{e}_{\mathsf{off}}\ t_1), (r_{\mathsf{off}}\ j), \mathfrak{p}_{\mathsf{off}}(\sigma),$$
$$\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \big(\mathbf{c}'_\sigma, (\mathbf{e}_{\mathsf{on}}\ t_2), (r_{\mathsf{on}}\ p), \mathfrak{p}_{\mathsf{on}}(\sigma)\big)$$

By unfolding the definition of the mix predicate $\mathbf{mix}_{\phi_{\mathbb{CS}}}$, one has to prove the following indistinguishability

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_{\mathsf{end}}(\pi) \sim \mathsf{frame}_{\mathsf{end}}(\mathrm{id}).$$

Notice that **if** b **then** $\langle t_1, t_2, t_3\rangle$ is a macro for $\langle$**if** b **then** t_1, **if** b **then** t_2, **if** b **then** $t_3\rangle$. Hence, by the case study rule for the indistinguishability predicate G.$\sim$:CS, and by the elimination rule of duplicates G.$\sim$:DUP, we have to prove the following property

$$\begin{aligned}
\mathcal{E}; \Theta_{\mathsf{init}} \vdash{}& (ck\ n), \mathrm{pk}_{\mathbb{CS}}\ (sk\ k), (\mathbf{c}, v), \mathbf{a}_\pi, (\mathbf{e}_{\mathsf{off}}\ t_1), \mathfrak{p}_{\mathsf{off}}(\pi), \\
&\big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \mathbf{c}'_\pi\big), \\
&(\textbf{valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v), (\mathbf{e}_{\mathsf{on}}\ t_2), (\mathfrak{p}_{\mathsf{on}}(\pi)) \\
\sim{}& (ck\ n), \mathrm{pk}_{\mathbb{CS}}\ (sk\ k), (\mathbf{c}, v), \mathbf{a}_{\mathrm{id}}, (\mathbf{e}_{\mathsf{off}}\ t_1), \mathfrak{p}_{\mathsf{off}}(\mathrm{id}), \\
&\big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \mathbf{c}'_{\mathrm{id}}\big), \\
&(\textbf{valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v), (\mathbf{e}_{\mathsf{on}}\ t_2), (\mathfrak{p}_{\mathsf{on}}(\mathrm{id}))
\end{aligned}$$
$$.$$

Let $\mathsf{frame}_0(\sigma)$ be the sequence of terms such that

$$\mathsf{frame}_{\mathsf{end}}(\sigma) \overset{\mathrm{def}}{=} \mathsf{frame}_0(\sigma), \mathfrak{p}_{\mathsf{on}}(\sigma).$$

By the rule G.Σ-P:HVZK applied to the *online* relation $\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}$, we have the following indistinguishability

$$\begin{aligned}
\mathcal{E}; \Theta_{\mathsf{init}} \vdash{}& \mathsf{frame}_0(\sigma), \mathfrak{p}_{\mathsf{on}}(\sigma) \\
\sim{}& \mathsf{frame}_0(\sigma), \textbf{zkp-sim}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ (ck\ n, \mathrm{pk}_{\mathbb{CS}}\ (sk\ k), \mathbf{e}_{\mathsf{on}}\ t_2) \\
&\qquad (\mathbf{a}_\sigma, \mathbf{c}, \mathbf{c}'_\sigma)\ (r_{\mathsf{on}}\ p).
\end{aligned}$$

Hence, by the function application rule G.$\sim$:FA applied to the function $\textbf{zkp-sim}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}/3$, and by the duplicates elimination rule G.$\sim$:DUP, we have to prove the following property

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_0(\pi) \sim \mathsf{frame}_0(\mathrm{id})$$

Let $\mathsf{frame}_1(\sigma)$ be the sequence of terms such that

$$\mathsf{frame}_0(\sigma) \overset{\text{def}}{=} \mathsf{frame}_1(\sigma), \big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\ \mathbf{c}'_\sigma\big),$$
$$(\textbf{valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v), (\mathbf{e}_{\mathsf{on}}\ t_2).$$

By the freshness rule G.∼:FRESH applied to the term $\mathbf{e}_{\mathsf{on}}\ t_2$, by simplification of fresh name rule G.∼:SIMPL, by the function application rule G.∼:FA applied to the function $\textbf{valid}_N/3$, by the elimination rule of duplicates G.∼:DUP, and by definition of the ciphertexts list term $\mathbf{c}'_\sigma$, we have to prove the following property

$$\begin{aligned}\mathcal{E}; \Theta_{\mathsf{init}} \vdash{}& \mathsf{frame}_1(\pi), \textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\\ &\textbf{then shuffle}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ \pi\ (\mathbf{r}\ l)\\ \sim{}& \mathsf{frame}_1(\mathrm{id}), \textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\\ &\textbf{then shuffle}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ \mathrm{id}\ (\mathbf{r}\ l). \qquad (*)\end{aligned}$$

However, by the characterization rule of the $\textbf{shuffle}_{\phi_{\mathbb{CS}}}$ predicate L.SHUFFLE, we have

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash [\mathbf{c}'_\sigma = \textbf{shuffle}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ \sigma\ (\mathbf{r}\ l) \leftrightarrow$$
$$\bigwedge_{i=1}^{N} (\mathbf{c}'_\sigma \circledast (\sigma \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)].$$

Therefore, the goal given by Eq. $(*)$ becomes the following

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_1(\pi), \textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$\bigwedge_{i=1}^{N} (\mathbf{c}'_\pi \circledast (\pi \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)$$
$$\sim \mathsf{frame}_1(\mathrm{id}), \textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$\bigwedge_{i=1}^{N} (\mathbf{c}'_{\mathsf{id}} \circledast \mathbf{i} = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)$$

We denote by $b : \textbf{bool}$ the Boolean term defined by

$$b \overset{\text{def}}{=} \textbf{valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v.$$

For $\sigma \in \{\pi, \mathrm{id}\}$ and $i \in [\![1; N]\!]$, we denote by $\psi_{\sigma,i} : \textbf{bool}$ the following Boolean term

$$\psi_{\sigma,i} \overset{\text{def}}{=} \Big(\mathbf{c}'_\sigma \circledast (\sigma \cdot \mathbf{i}) =$$
$$\textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle\Big).$$

Hence, by operations on Boolean terms and properties over the function **if** _ **then** _/2, we have

$$\begin{aligned}\textbf{if}\ b\ \textbf{then} \bigwedge_{i=1}^{N} \psi_{\sigma,i} = b \wedge \bigwedge_{i=1}^{N} \psi_{\sigma,i} &= \bigwedge_{i=1}^{N} (b \wedge \psi_{\sigma,i})\\ &= \bigwedge_{i=1}^{N} (\textbf{if}\ b\ \textbf{then}\ \psi_{\sigma,i})\end{aligned}$$

Besides, as we have, for all sequence of N Boolean terms $(b_i : \textbf{bool})_{i=1}^{N}$

$$\bigwedge_{i=1}^{N} b_i = \textbf{if}\ b_1\ \textbf{then}\ (\textbf{if}\ b_2\ \textbf{then}\ (\textbf{if}\ \ldots\ \textbf{then}\ (\textbf{if}\ b_N\ \textbf{then}\ \top)))$$

then, by N applications of the case study rule G.∼:CS[3], the goal given by Eq. $(*)$ becomes the following

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_1(\pi), \Big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$(\mathbf{c}'_\pi \circledast (\pi \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\Big)_{i=1}^{N}$$
$$\sim \mathsf{frame}_1(\mathrm{id}), \Big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$(\mathbf{c}'_{\mathsf{id}} \circledast \mathbf{i} = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\Big)_{i=1}^{N}$$

Let $i \in [\![1; N]\!]$ be an index. We denote by $\mathsf{frame}_{\neq i}(\sigma)$ the following frame

$$\mathsf{frame}_{\neq i}(\sigma) \overset{\text{def}}{=} \Big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$(\mathbf{c}'_\sigma \circledast (\sigma \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{j})\ \langle \mathbf{r}\ l \mid \mathbf{j}\rangle)\Big)_{j \in [\![1;N]\!] \setminus \{i\}}$$

By the characterization rule for canonical vectors L.⊛:CANOVEC, we want to prove the following property

$$\begin{aligned}\mathcal{E}; \Theta_{\mathsf{init}} \vdash{}& \mathsf{frame}_1(\pi), \mathsf{frame}_{\neq i}(\pi),\\ &\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ &(\langle \mathbf{c}'_\pi \mid (\pi \cdot \mathbf{i})\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \mathbf{i}\rangle\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\\ \sim{}& \mathsf{frame}_1(\mathrm{id}), \mathsf{frame}_{\neq i}(\mathrm{id}),\\ &\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ &(\langle \mathbf{c}'_{\mathsf{id}} \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \mathbf{i}\rangle\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle) \qquad (*_i)\end{aligned}$$

However, by Lemma 4, the i-th goal Eq. $(*_i)$ becomes the following

$$\begin{aligned}\mathcal{E}; \Theta_{\mathsf{init}} \vdash{}& \mathsf{frame}_1(\pi), \mathsf{frame}_{\neq i}(\pi),\\ &\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ &(\langle \mathbf{c}'_\pi \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid (\pi^{-1} \cdot \mathbf{i})\rangle\ \langle \mathbf{r}\ l \mid (\pi^{-1} \cdot \mathbf{i})\rangle)\\ \sim{}& \mathsf{frame}_1(\mathrm{id}), \mathsf{frame}_{\neq i}(\mathrm{id}),\\ &\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ &(\langle \mathbf{c}'_{\mathsf{id}} \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \mathbf{i}\rangle\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\end{aligned}$$

Let $\mathbf{r}_{\mathsf{fresh}} : \textbf{unit} \to \textbf{rand}$ be a name such that $\mathbf{r}_{\mathsf{fresh}}$ does not appear in $\mathcal{E}$, and $\mathsf{frame}_1(\sigma)$ for $\sigma \in \{\pi, \mathrm{id}\}$. Therefore, by

[3] Actually, for all $j \in [\![1; N]\!]$, we have to prove the goal

$$\mathcal{E}; \Theta_{\mathsf{init}} \vdash \mathsf{frame}_1(\pi), \Big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$(\mathbf{c}'_\pi \circledast (\pi \cdot \mathbf{i}) = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\Big)_{i=1}^{j}$$
$$\sim \mathsf{frame}_1(\mathrm{id}), \Big(\textbf{if valid}_N\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}$$
$$(\mathbf{c}'_{\mathsf{id}} \circledast \mathbf{i} = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{c} \circledast \mathbf{i})\ \langle \mathbf{r}\ l \mid \mathbf{i}\rangle)\Big)_{i=1}^{j}$$

which are all subsumed by the case where $j = N$.

the Lemma 5, and by the case study rule G.$\sim$:CS, the goal property Eq. $(*_i)$ becomes the following

$$\begin{aligned}\mathcal{E};\Theta_{\mathsf{init}} \vdash\ & \mathsf{frame}_1(\pi), \mathsf{frame}_{\neq i}(\pi),\\ & \textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ & (\langle \mathbf{c}'_\pi \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid (\pi^{-1}\cdot\mathbf{i})\rangle\ (\mathbf{r}_{\mathsf{fresh}}\ ()))\\ & \sim \mathsf{frame}_1(\mathrm{id}), \mathsf{frame}_{\neq i}(\mathrm{id}),\\ & \textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ & (\langle \mathbf{c}'_{\mathrm{id}} \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \mathbf{i}\rangle\ (\mathbf{r}_{\mathsf{fresh}}\ ()))\end{aligned}$$

However, by definition of the predicate $\textbf{valid}_N$, we have the following property

$$\textbf{valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v \to \bigwedge_{j=1}^{N}\bigwedge_{k=1}^{N}(\textbf{len}\ \langle \mathbf{c} \mid \mathbf{j}\rangle = \textbf{len}\ \langle \mathbf{c} \mid \mathbf{k}\rangle).$$

We denote this common value by the term $m : \textbf{nat}$, *i.e.* m is such that

$$\forall j \in [\![1;N]\!], m = \textbf{len}\ \langle \mathbf{c} \mid \mathbf{j}\rangle.$$

Besides, by definition of the predicate $\textbf{valid}_N$, we have the following property

$$\textbf{valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v \to \textbf{valid}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \pi^{-1}\cdot\mathbf{i}\rangle\ v.$$

Therefore, by the indistinguishability of $\phi_{\mathbb{CS}}$ output rule G.SFM:INDCCA, the goal property Eq. $(*_i)$ becomes the following

$$\begin{aligned}\mathcal{E};\Theta_{\mathsf{init}} \vdash\ & \mathsf{frame}_1(\pi), \mathsf{frame}_{\neq i}(\pi),\\ & \textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ & (\langle \mathbf{c}'_\pi \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ (\mathbf{0}\ m)\ (\mathbf{r}_{\mathsf{fresh}}\ ()))\\ & \sim \mathsf{frame}_1(\mathrm{id}), \mathsf{frame}_{\neq i}(\mathrm{id}),\\ & \textbf{if valid}_N\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \mathbf{c}\ v\ \textbf{then}\\ & (\langle \mathbf{c}'_{\mathrm{id}} \mid \mathbf{i}\rangle = \textbf{shuf-map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ (sk\ k))\ \langle \mathbf{c} \mid \mathbf{i}\rangle\ (\mathbf{r}_{\mathsf{fresh}}\ ()))\end{aligned}$$

Hence, by the function application rule G.$\sim$:FA for the indistinguishability predicate $\sim$ applied to functions $=/2$, $\textbf{valid}_N/3$ and $\textbf{shuf-map}_{\phi_{\mathbb{CS}}}/3$, by the case study rule G.$\sim$:CS, by simplification of fresh names G.$\sim$:SIMPL, and by the duplicates elimination rule G.$\sim$:DUP, we have to prove the following property

$$\mathcal{E};\Theta_{\mathsf{init}} \vdash \mathsf{frame}_1(\pi) \sim \mathsf{frame}_1(\mathrm{id}).$$

By definition of the frame $\mathsf{frame}_1(\sigma)$, we have to prove the following property

$$\begin{aligned}\mathcal{E};\Theta_{\mathsf{init}} \vdash\ & \mathsf{frame}_{\mathsf{init}}, \mathbf{a}_\pi, (e_{\mathsf{off}}\ t_1), \mathfrak{p}_{\mathsf{off}}(\pi)\\ & \sim \mathsf{frame}_{\mathsf{init}}, \mathbf{a}_{\mathrm{id}}, (e_{\mathsf{off}}\ t_1), \mathfrak{p}_{\mathsf{off}}(\mathrm{id}).\end{aligned}$$

By the rule G.Σ-P:HVZK applied to the *offline* relation $\mathcal{R}^{\mathsf{off}}$, by the function application rule G.$\sim$:FA applied to the function $\textbf{zkp-sim}_{\mathcal{R}^{\mathsf{off}}}/3$, by the duplicates elimination rule G.$\sim$:DUP, by the freshness rule G.$\sim$:FRESH applied to terms $r_{\mathsf{off}}\ j$ and $\mathbf{e}_{\mathsf{off}}\ t_1$, by simplification of fresh names G.$\sim$:SIMPL, and by definition of the term $\mathbf{a}_\sigma$, we have to prove the following property

$$\begin{aligned}\mathcal{E};\Theta_{\mathsf{init}} \vdash\ & \mathsf{frame}_{\mathsf{init}}, \textbf{com-mat}\ (ck\ n)\ \pi\ (\mathbf{s}\ i)\\ & \sim \mathsf{frame}_{\mathsf{init}}, \textbf{com-mat}\ (ck\ n)\ \mathrm{id}\ (\mathbf{s}\ i).\end{aligned}$$

By the *hiding* property for the commitment predicate **com-mat**, we conclude the proof by applying the corresponding rule G.COM:HIDE. □

B. Rewinding axiom proof

To prove the rewinding CCSA axiom, we need the Chernoff bound, which we recall here:

Lemma 6 (Chernoff bound)**.** *Let $X_1, \dots, X_n : \mathbb{N} \longrightarrow \{0,1\}$ be n independent and identically distributed random variables,* i.e. *there exists a number $p \in [0,1]$ such that, for all $i \in [\![1;n]\!]$,* $\Pr[X_i = 1] = p$. *Then we have*

$$\forall\, \delta \in]0,1[, \Pr\Big[\sum_{i=1}^{n} X_i \leqslant (1-\delta)np\Big] \leqslant \exp\Big(-\frac{\delta^2}{2}np\Big).$$

Let $n \in \mathbb{N}$, with $n \geqslant 2$, be a natural number. In what follows, we fix a source of random values $\mathbf{r}_s : \textbf{nat} \to \tau$, *i.e.* semantics of $\mathbf{r}_s$ is given by

$$\forall\, \eta \in \mathbb{N}^*, \forall\, \rho \in \mathbb{T}, \forall\,(i : \textbf{nat}), [\![\mathbf{r}_s\ i]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \xleftarrow{\$} [\![\tau]\!]^{\eta}_{\mathbb{M}}.$$

Besides, we consider the function symbol $\textbf{select}^{(n)}_{\text{rand}} : \textbf{nat} \to (\textbf{nat} \to \tau) \to \textbf{set}_n(\tau)$ with semantics given by Algorithm 6.

Axiom 2 (Rewinding)**.** *For all polynomial-time property $\phi \overset{def}{=} \lambda x.\,(\phi\ \ x)\ :\ \tau\ \to$ **bool** [ptime], for all non-negligible parameter g : **real** with **non-negl**(g), the following rule to catch the rewinding argument is sound*

$$\begin{aligned}\mathcal{E};\Theta \vdash\ & \tilde{\exists}\,\textbf{\textit{select}}^{(n)}_{\textit{rand}}.\ \tilde{\exists}\,k_g : \textbf{\textit{nat}}.\ \textbf{\textit{det}}(k_g)\ \tilde{\wedge}\ \textbf{\textit{pbound}}(k_g)\ \tilde{\to}\\ & [\textbf{\textit{low-bound}}\ g\ \phi\ \to\ \forall\,(t : \textbf{\textit{nat}}).\ (\mathbf{r}_s\ t \in \textbf{\textit{select}}^{(n)}_{\textit{rand}}\ k_g\ \mathbf{r}_s)\ \to\\ & \phi\ (\mathbf{r}_s\ t)]\ \tilde{\wedge}\ [\forall\,(t : \textbf{\textit{nat}}).\ (\mathbf{r}_s\ t) \in \textbf{\textit{select}}^{(n)}_{\textit{rand}}\ k_g\ \mathbf{r}_s\ \to\\ & (\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \dots, \mathbf{r}_s\ k_g\}]\end{aligned}$$

Next, we use the same notation between the natural number $i \in \mathbb{N}$ and its corresponding term i : **nat**. Besides, notice that in the rewinding axiom, the natural number $k_g \in \mathbb{N}$ depends only on the non-negligible real parameter g : **real**.

Proof. Let g : **real** with $\mathcal{E};\Theta \vdash$ **non-negl**(g) be a non-negligible parameter. Let $\eta \in \mathbb{N}^*$ be a security parameter and let $\rho \in \mathbb{T}$ be a random tape. Let $Y_{\eta,\rho} : \mathbb{N} \longrightarrow \{0,1\}$ be the following random variable

$$\forall\, i \in \mathbb{N}, Y_{\eta,\rho}(i) \overset{\text{def}}{=} [\![\phi\ (\mathbf{r}_s\ i)]\!]^{\eta\,;\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \in \{0,1\}$$

Let $k(\eta) \in \mathbb{N}$ be a natural number. We consider the family of random variables $\big(Y^{\eta,\rho}_j\big)_{j=1}^{k(\eta)}$ such that we have

$$\forall\, j \in [\![1;k(\eta)]\!],\ Y^{\eta,\rho}_j = 1 \overset{\text{def}}{\Longleftrightarrow} Y_{\eta,\rho}(i_j) = 1,\ i_j \xleftarrow{\$} [\![1;k(\eta)]\!].$$

As $\mathbf{r}_s$ is a source of *uniformly distributed and independent* random variables, the random variables $Y^{\eta,\rho}_j$, for all $j \in [\![1;n]\!]$, are *mutually independent*. Besides, we suppose that we are in the case where $\llbracket \textbf{low-bound}\ g\ \phi \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} = 1$, meaning that we have the following lower bound

$$p_Y(\eta, \rho) \overset{\text{def}}{=} \Pr_{r \in \llbracket \tau \rrbracket^{\eta}_{\mathbb{M}}} \Big[\ \llbracket \phi \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}(r) = 1\ \Big] \geqslant \mathbb{E}_{\rho' \in \mathbb{T}}\big(\llbracket g \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\big).$$

We want to prove that the function $\eta \longmapsto \Pr_{\rho \in \mathbb{T}}\Big[\ \sum_{j=1}^{k} Y_j^{\eta,\rho} \geqslant n\ \Big]$ is overwhelming. In fact, we show that, for all security parameter $\eta \in \mathbb{N}^*$, $\Pr_{\rho \in \mathbb{T}}\Big[\ \sum_{j=1}^{k} Y_j^{\eta,\rho} < n\ \Big] \leqslant \frac{1}{2^\eta}$, which is equivalent to the property we want to show. To prove this property, we use the Chernoff bound which states the following property

$$\begin{aligned}\forall\, \delta \in]0,1[, \Pr_{\rho \in \mathbb{T}}\Big[\ \sum_{j=1}^{k} Y_j^{\eta,\rho} \leqslant (1-\delta) k p_Y(\eta,\rho)\ \Big]& \\ \leqslant \exp\left(-\frac{\delta^2}{2} k p_Y(\eta,\rho)\right).&\end{aligned}$$

Therefore, to obtain the property we want, we have to find a pair $(\delta(\eta), k(\eta)) \in\,]0,1[\, \times \mathbb{N}^*$ such that

$$\begin{aligned}&(1-\delta(\eta))k(\eta)p_Y(\eta,\rho) < n \\ \text{and}\quad &\exp\left(-\frac{\delta(\eta)^2}{2} k(\eta) p_Y(\eta,\rho)\right) \leqslant \frac{1}{2^\eta}\end{aligned} \qquad (\mathcal{I})$$

By monotonic increasing of the logarithm function, the second equation becomes

$$\frac{\delta(\eta)^2}{2} k(\eta) p_Y(\eta,\rho) \geqslant \eta \ln 2.$$

In fact, the system of inequalities Eq. ($\mathcal{I}$) can be solved by solving the following system of equations where we have to find a pair $(\delta(\eta), x(\eta)) \in\,]0,1[\, \times \mathbb{R}^+$ such that

$$(1-\delta(\eta))x(\eta)p_Y(\eta,\rho) = n \qquad (1)$$

$$\text{and}\quad \frac{\delta(\eta)^2}{2} x(\eta) p_Y(\eta,\rho) = \eta \ln 2. \qquad (2)$$

Indeed, if we have found a solution $(\delta(\eta), x(\eta))$ of the second system of equations, the pair $(\delta(\eta), \lceil x(\eta) \rceil)$ is a solution of the first system Eq. ($\mathcal{I}$). The second equation Eq. (2) leads to

$$x(\eta) = \frac{2\eta \ln 2}{\delta(\eta)^2 p_Y(\eta,\rho)}. \qquad (*)$$

Hence, by equations Eq. ($*$) and Eq. (1) leads to the following quadratic equation

$$n\delta(\eta)^2 + (2\eta \ln 2)\delta(\eta) - 2\eta \ln 2 = 0. \qquad (E_\delta)$$

The solutions of this quadratic equation are given by

$$\delta_{\pm}(\eta) \overset{\text{def}}{=} \frac{-2\eta \ln 2 \pm \sqrt{\Delta}}{2n}$$

where $\Delta = (2\eta \ln 2)^2 + 8n\eta \ln 2 > 0$. Moreover, we have $\delta_-(\eta) < 0$ and $\delta_+(\eta) > 0$. Besides, we have

$$\begin{aligned}\delta_+(\eta) < 1 &\iff \sqrt{1 + \frac{2n}{\eta \ln 2}} < \frac{n}{\eta \ln 2} + 1 \\ &\iff 1 + \frac{2n}{\eta \ln 2} < \left(\frac{n}{\eta \ln 2} + 1\right)^2 \\ &\iff \left(\frac{n}{\eta \ln 2}\right)^2 > 0.\end{aligned}$$

Therefore, only the solution $\delta_+(\eta)$ interest us and the partnered solution $x(\eta)$ is given by

$$x(\eta) = \frac{2n^2}{\eta p_Y(\eta,\rho) \ln 2}\left(1 - \sqrt{1 + \frac{2n}{\eta \ln 2}}\right)^{-2}.$$

Therefore, we denote by $f_n : \mathbb{N}^* \longrightarrow \mathbb{R}_+^*$ such that

$$\forall\, \eta \in \mathbb{N}^*, x(\eta) \overset{\text{def}}{=} \frac{f_n(\eta)}{p_Y(\eta,\rho)}.$$

To conclude, we have to study the asymptotic behavior of the function f_n, to show this function is at least polynomial bounded in the security parameter η. By series expansion, we have the following results.

$$\begin{aligned}\forall\, \eta \in \mathbb{N}^*, f_n(\eta) &= \frac{n^2}{\eta \ln 2}\left(1 - \sqrt{1 + \frac{2n}{\eta \ln 2}} + \frac{n}{\eta \ln 2}\right)^{-1} \\ &= \frac{n^2}{\eta \ln 2}\left(2\left(\frac{n}{2 \ln 2}\right)^2 \frac{1}{\eta^2} + o_{\eta \to +\infty}\left(\tfrac{1}{\eta^2}\right)\right)^{-1} \\ &= 2(\ln 2)\eta\left(1 + o_{\eta \to +\infty}(1)\right).\end{aligned}$$

Therefore, the asymptotic analysis of function f_n gives us the following result

$$\boxed{f_n(\eta) \sim_{\eta \to +\infty} 2(\ln 2)\eta}. \qquad (\Theta)$$

Moreover, by hypothesis on $p_Y(\eta,\rho)$ given by the hypothesis **low-bound** $g\ \phi$, we have $x(\eta) \leqslant \frac{f_n(\eta)}{\mathbb{E}_{\rho \in \mathbb{T}}\left(\llbracket g \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\right)}$. Therefore, if we denote by $k(\eta) \in \mathbb{N}^*$ the quantity

$$\boxed{k(\eta) = \left\lceil \frac{f_n(\eta)}{\mathbb{E}_{\rho}\left(\llbracket g \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\right)} \right\rceil},$$

we conclude, as g is a non-negligible parameter and because of result Eq. (Θ) that k is polynomial in the security parameter η.

Consequently, we have proved that if k : **nat** is the natural term for whose semantics is given by

$$\begin{aligned}&\forall\, \eta \in \mathbb{N}^*, \forall\, \rho \in \mathbb{T}, \\ &\llbracket k \rrbracket^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}} \overset{\text{def}}{=} \left\lceil \frac{1}{\mathbb{E}_{\rho'}\left(\llbracket g \rrbracket^{\eta\,,\,\rho'}_{\mathbb{M}\,:\,\mathcal{E}}\right)} \frac{2n^2}{\eta \ln 2}\left(1 - \sqrt{1 + \frac{2n}{\eta \ln 2}}\right)^{-2} \right\rceil\end{aligned}$$

then k is polynomial in the security parameter η and is deterministic. Let $\psi : \underbrace{\tau \to \ldots \to \tau}_{n \text{ times}} \to \textbf{bool}$ be a property defined by

$$\forall (x_1, \ldots, x_n : \tau).\ \psi\ x_1\ \ldots\ x_n \overset{\text{def}}{=} \bigwedge_{i=1}^{n} (\phi\ x_i).$$

Moreover, we denote by Φ and $\mathcal{H}$ the functions in $\mathbb{N}^* \times \mathbb{T} \longrightarrow \{0, 1\}$ respectively defined by

$$\Phi(\eta, \rho) \overset{\text{def}}{=} [\![\forall (t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s\ \ \to\ \ \phi\ (\mathbf{r}_s\ t)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}$$
$$\text{and}\quad \mathcal{H}(\eta, \rho) \overset{\text{def}}{=} [\![\textbf{low-bound}\ g\ \phi]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}.$$

Hence, by what precedes, we have shown the following result

$$\forall \eta \in \mathbb{N}^*, \Pr_{\rho \in \mathbb{T}} \Big[\ [\![\psi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big|\ \mathcal{H}(\eta, \rho)\ \Big]$$
$$\geqslant 1 - \frac{1}{2^\eta}.$$

Thus, we have shown the following global judgement

$$\mathcal{E}; \Theta \vdash [\textbf{low-bound}\ g\ \phi \to \psi\ (\mathbf{r}_s\ 1)\ \ldots\ (\mathbf{r}_s\ n)].$$

Consequently, by using the property transfer under adversarial selection function G.SEL, we conclude

$$\mathcal{E}; \Theta \vdash [\textbf{low-bound}\ g\ \phi \to \psi\ (\textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s)].$$

Thus, by definition of ψ, we have shown the following result

$$\forall \eta \in \mathbb{N}^*, \Pr_{\rho \in \mathbb{T}} \Big[\ \Phi(\eta, \rho)\ \Big|\ \mathcal{H}(\eta, \rho)\ \Big] \geqslant 1 - \frac{1}{2^\eta}.$$

And finally, by definition of the function $\textbf{select}^{(n)}_{\text{rand}}$ given in Algorithm 6, we have, for all natural number term $t : \textbf{nat}$, if $(\mathbf{r}_s\ t) \in \textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s$ then $(\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ i\}_{i=1}^{k}$ and then we conclude

$$\forall \eta \in \mathbb{N}^*, \Pr_{\rho \in \mathbb{T}} \Big[\ [\![\forall (t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(n)}_{\text{rand}}\ k\ \mathbf{r}_s \to$$
$$(\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \ldots, \mathbf{r}_s\ k\}]\!]^{\eta\,,\,\rho}_{\mathbb{M}\,:\,\mathcal{E}}\ \Big] = 1.$$

Consequently, those results achieves the proof of the rewinding CCSA axiom. □

C. Verifiability proof

Let $\mathsf{frame}_{\mathsf{verif}}$ be a trace of the Terelius-Wikström shuffle protocol defined by

$$\mathsf{frame}_{\mathsf{verif}} \overset{\text{def}}{=} (ck\ n), \mathbf{a}, (\mathbf{e}_{\mathsf{off}}\ t_1), \alpha_{\mathsf{off}}, (r_{\mathsf{off}}\ l), z_{\mathsf{off}},$$
$$\langle sk, \mathbf{c}, \mathbf{c}' \rangle, (\mathbf{e}_{\mathsf{on}}\ t_2), \alpha_{\mathsf{on}}, (r_{\mathsf{on}}\ p), z_{\mathsf{on}}.$$

and such that

$$\begin{array}{lll} & \textbf{zkp-verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_{\mathsf{off}}\ t_1)\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, (r_{\mathsf{off}}\ l), z_{\mathsf{off}} \rangle & \\ \wedge & \textbf{zkp-verif}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}} & (ck\ n, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_{\mathsf{on}}\ t_2) \\ & & (\mathbf{a}, \mathbf{c}, \mathbf{c}')\ \langle \alpha_{\mathsf{on}}, (r_{\mathsf{on}}\ p), z_{\mathsf{on}} \rangle \\ \wedge & \textbf{wf\_ctxt}_N\ sk\ \mathbf{c}. & \end{array}$$

1) Extraction of the committed matrix: To be able to rebuild the committed matrix, we have to extract N witnesses $(\mathbf{e}'_i, k_i)_{i=1}^{N}$ for the relations of correct commitment $\mathcal{R}^{\mathsf{com}}(\mathbf{e}_i)$, where $(\mathbf{e}_i)_{i=1}^{N}$ is a free family of $\mathbb{F}(p_\eta)^N$. Consequently, there is two steps of rewinding, one on the vectors $\mathbf{e}_i$, for $i \in [\![1; N]\!]$ and the other one is when we obtain a candidate vector $\mathbf{e}_i$, we have to rewind the challenge $r \in \mathbb{F}(p_\eta)$ to be able to use the *special-soundness* axiom. Therefore, in that case, we have to use two times the predicate **low-bound**, one states there is enough random vectors to rewind and the second one states that for a chosen vector, there is enough random challengs to rewind. Hence, if we denote by ψ_{off} the formula

$$\psi_{\mathsf{off}} \overset{\text{def}}{=} \lambda \mathbf{e}.\ \lambda r.\ \textbf{zkp-verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, r, z_{\mathsf{off}}(r) \rangle,$$

we have to suppose the following property

$$\textbf{low-bound}\ g\ (\lambda \mathbf{e}.\ \textbf{low-bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e}))$$

for two parameters g, g' : **real** with $\textbf{non-negl}(g)$ and $\textbf{non-negl}(g')$.

Lemma 7. *Let $\mathcal{E}$ be an environment, let Θ be a context of global formulas and let Γ be a context of local formulas. We denote by ψ_{off} the formula*

$$\psi_{\mathsf{off}} \overset{\text{def}}{=} \lambda \mathbf{e}.\ \lambda r.\ \textbf{\textit{zkp-verif}}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, r, z_{\mathsf{off}}(r) \rangle.$$

We suppose

$$\mathcal{E}; \Theta; \Gamma \vdash \textbf{\textit{low-bound}}\ g\ (\lambda \mathbf{e}.\ \textbf{\textit{low-bound}}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e})), \quad (\mathcal{H}_{\mathbf{e},r})$$

with

$$\mathcal{E}; \Theta \vdash \textbf{\textit{non-negl}}(g)\ \tilde{\wedge}\ \textbf{\textit{det}}(g)$$
$$\text{and}\ \ \mathcal{E}; \Theta \vdash \textbf{\textit{non-negl}}(g)\ \tilde{\wedge}\ \textbf{\textit{det}}(g)$$

*Then, the property $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{a} = \textbf{\textit{com-mat}}\ (ck\ n)\ M\ \mathbf{s}$ holds, where there exists a name $\mathbf{e}_s$: **nat** $\to$ **msg** and N terms $t_1, \ldots, t_N$: **nat** pairwise distincts such that there exists a name $\mathbf{r}_s$: **nat** $\to$ **msg** and 2 terms $r_{i,1}, r_{i,2}$: **nat** with $r_{i,1} \neq r_{i,2}$ such that if we denote, for all $i \in [\![1; N]\!]$, $\mathbf{e}'_i \overset{\text{def}}{=} \pi_2\ w_{\mathsf{off}}(i)$ and $k_i \overset{\text{def}}{=} \pi_3\ w_{\mathsf{off}}(i)$ with*

$$w_{\mathsf{off}}(i) \overset{\text{def}}{=} \textbf{\textit{zkp-extract}}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_s\ t_i)\ \mathbf{a}$$
$$\langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_{i,1}, z_{\mathsf{off}}(\mathbf{r}_s\ r_{i,1}) \rangle\ \langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_{i,2}, z_{\mathsf{off}}(\mathbf{r}_s\ r_{i,2}) \rangle$$

then terms M and $\mathbf{s}$ are defined by $M \overset{\text{def}}{=} \pi_1\ u$ and $\mathbf{s} \overset{\text{def}}{=} \pi_2\ u$ where $u \overset{\text{def}}{=} \textbf{\textit{solve}}\ \mathbf{a}\ (\mathbf{e}_s\ t_i)_{i=1}^{N}\ (\mathbf{e}'_i, k_i)_{i=1}^{N}$.

Proof. Firstly, we have to obtain N vectors such that the adversary produces at least two different proof transcripts but for the same commitment message to be able to apply the *special-soundness* axiom. Let $\mathbf{e}_s$: **nat** $\to$ $\textbf{vect}_N$ be an uniform source of random vectors with semantics defined by the honest verifier of the Terelius-Wikström shuffle protocol. Then, we apply the rewinding axiom (Axiom 1) to the formula $\psi \overset{\text{def}}{=} \lambda \mathbf{e}.\ \textbf{low-bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e})$. Hence, there exists a

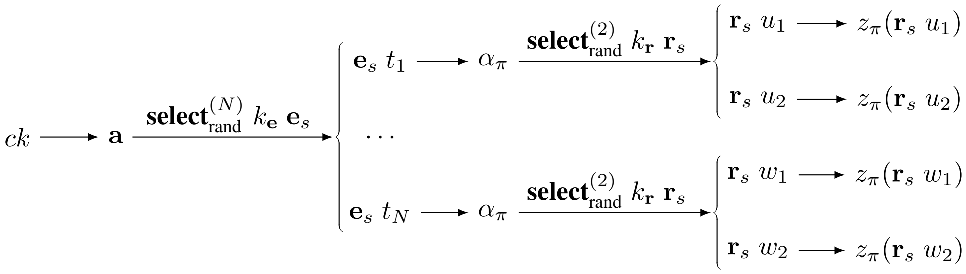
ck
$\mathbf{a}$
$\mathbf{select}^{(N)}_{\text{rand}}\ k_{\mathbf{e}}\ \mathbf{e}_s$
$\mathbf{e}_s\ t_1$
α_π
$\mathbf{select}^{(2)}_{\text{rand}}\ k_{\mathbf{r}}\ \mathbf{r}_s$
$\mathbf{r}_s\ u_1$
$z_\pi(\mathbf{r}_s\ u_1)$
$\mathbf{r}_s\ u_2$
$z_\pi(\mathbf{r}_s\ u_2)$
$\dots$
$\mathbf{e}_s\ t_N$
α_π
$\mathbf{select}^{(2)}_{\text{rand}}\ k_{\mathbf{r}}\ \mathbf{r}_s$
$\mathbf{r}_s\ w_1$
$z_\pi(\mathbf{r}_s\ w_1)$
$\mathbf{r}_s\ w_2$
$z_\pi(\mathbf{r}_s\ w_2)$

Fig. 18. Skeleton of committed matrix extraction proof

polynomial bounded and deterministic term $k_{\mathbf{e}} : \mathbf{nat}$ such that $N \leqslant k_{\mathbf{e}}$ and the following property holds

$$\begin{aligned}&\mathcal{E};\Theta \vdash [\textbf{low-bound}\ g\ \psi \rightarrow\\ &\quad \forall (t : \mathbf{nat}).\ (\mathbf{e}_s\ t) \in \mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s\ \rightarrow\ \psi\ (\mathbf{e}_s\ t)]\\ &\qquad \tilde{\wedge}\ [\forall (t : \mathbf{nat}).\ (\mathbf{r}_s\ t) \in \mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s\ \rightarrow\\ &\qquad\qquad\qquad (\mathbf{r}_s\ t) \in \{\mathbf{e}_s\ 1, \dots, \mathbf{e}_s\ k_{\mathbf{e}}\}]\end{aligned}$$

Therefore, by hypothesis Eq. ($\mathcal{H}_{\mathbf{e},r}$), we conclude

$$\mathcal{E};\Theta;\Gamma \vdash \forall (t : \mathbf{nat}).\ (\mathbf{e}_s\ t) \in \mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s\ \rightarrow\ \psi\ (\mathbf{e}_s\ t).$$

On another hand, we have the following global formula by the rule L.BASIS

$$\mathcal{E};\Theta \vdash [\mathbf{basis}_N\ (\mathbf{e}_s\ i)_{i=1}^{N}].$$

Therefore, by the second conclusion of the rewinding axiom and by the transfer of properties by adversarial selection rule G.SEL, we have

$$\mathcal{E};\Theta \vdash [N \leqslant k_{\mathbf{e}} \rightarrow \mathbf{basis}_N\ (\mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s)] \qquad (\beta)$$

Moreover, by the second conclusion of the rewinding axiom, and because $\text{Card}(\llbracket \mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s \rrbracket^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}) = N$ by definition of the semantics of the type $\mathbf{set}_N(\mathbf{msg})$, we conclude the existence of N pairwise distinct terms $t_1, \dots, t_N : \mathbf{nat}$ such that $1 \leqslant t_1 < \dots < t_N \leqslant k_{\mathbf{e}}$ (without loss of generality for the order of terms t_i) and $\mathbf{select}^{(N)}_{\text{vect}}\ k_{\mathbf{e}}\ \mathbf{e}_s = \{\mathbf{e}_s\ t_i\}_{i=1}^{N}$. Therefore, for all $i \in \llbracket 1; N \rrbracket$, we have

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{low-bound}\ g'\ (\psi_{\mathsf{off}}\ (\mathbf{e}_s\ t_i)) \qquad (\mathcal{H}_r)$$

Now we have obtain those N vectors, we apply the rewinding axiom for each vector to obtain two different proof transcripts but for the same commitment message in the goal of extract a witness by the *special-soundness* property. Let $i \in \llbracket 1; N \rrbracket$. Let $\mathbf{r}_s : \mathbf{nat} \rightarrow \mathbf{chall}_{\mathcal{R}^{\mathsf{off}}}$ be an uniform source of random values with semantics given by the honest verifier of the offline relation $\mathcal{V}_{\mathcal{R}^{\mathsf{off}}}$. By the rewinding axiom (Axiom 1) applied to the formula $\psi_{\mathsf{off}}\ (\mathbf{e}_s\ t_i)$ the existency of a polynomial bounded and deterministic term $k_r : \mathbf{nat}$ such that $2 \leqslant k_r$ and the following property holds

$$\begin{aligned}&\mathcal{E};\Theta \vdash [\textbf{low-bound}\ g'\ (\psi_\pi\ (\mathbf{e}_s\ t_i)) \rightarrow\\ &\forall (t : \mathbf{nat}).\ (\mathbf{r}_s\ t) \in \mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\ \rightarrow\ \psi_{\mathsf{off}}\ (\mathbf{e}_s\ t_i)\ (\mathbf{r}_s\ t)]\\ &\qquad \tilde{\wedge}\ [\forall (t : \mathbf{nat}).\ (\mathbf{r}_s\ t) \in \mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\ \rightarrow\\ &\qquad\qquad\qquad (\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \dots, \mathbf{r}_s\ k_r\}]\end{aligned}$$

Therefore, by hypothesis Eq. ($\mathcal{H}_r$), we conclude

$$\begin{aligned}&\mathcal{E};\Theta;\Gamma \vdash \forall (t : \mathbf{nat}).\ (\mathbf{r}_s\ t) \in \mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\\ &\qquad\qquad\qquad \rightarrow\ \psi_{\mathsf{off}}\ (\mathbf{e}_s\ t_i)\ (\mathbf{r}_s\ t).\end{aligned}$$

By the second conclusion of the rewinding axiom, and because $\text{Card}(\llbracket \mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s \rrbracket^{\eta,\rho}_{\mathbb{M}:\mathcal{E}}) = 2$, we conclude the existency of 2 distinct terms $r_{i,1}, r_{i,2} : \mathbf{nat}$ with, without loss of generality, $1 \leqslant r_{i,1} < r_{i,2} \leqslant k_r$ and $\mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s = \{\mathbf{r}_s\ r_{i,1}, \mathbf{r}_s\ r_{i,2}\}$. Therefore, for all $i \in \llbracket 1; N \rrbracket$ and for all $j \in \{1,2\}$, we have

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{zkp-verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_s\ t_i)\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_{i,j}, z_{\mathsf{off}}(\mathbf{r}_s\ r_{i,j})\rangle$$

By the *special-soundness* property L.Σ-P:SPSOUND applied to the relation for the offline phase $\mathcal{R}^{\mathsf{off}}$, we conclude the existency of an extractor function $\textbf{zkp-extract}_{\mathcal{R}^{\mathsf{off}}}$ such that

$$\begin{aligned}&\mathcal{E};\Theta;\Gamma \vdash \textbf{zkp-rel}_{\mathcal{R}^{\mathsf{off}}}\ \sigma_{\mathsf{off}}(i)\ \mathbf{a}\\ &\qquad\qquad (\textbf{zkp-extract}_{\mathcal{R}^{\mathsf{off}}}\ \sigma_{\mathsf{off}}(i)\ \mathbf{a}\ \mathfrak{p}_{\mathsf{off}}(i,1)\ \mathfrak{p}_{\mathsf{off}}(i,2))\end{aligned}$$

where, for all $i \in \llbracket 1; N \rrbracket$ and $j \in \{1,2\}$, $\sigma_{\mathsf{off}}(i) \overset{\text{def}}{=} (ck\ n, \mathbf{e}_s\ t_i)$ and $\mathfrak{p}_{\mathsf{off}}(i,j) \overset{\text{def}}{=} \langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_{i,j}, z_{\mathsf{off}}(\mathbf{r}_s\ r_{i,j})\rangle$. Hence, for all $i \in \llbracket 1; N \rrbracket$, we denote by $w_{\mathsf{off}}(i)$ the witness given by

$$w_{\mathsf{off}}(i) \overset{\text{def}}{=} \textbf{zkp-extract}_{\mathcal{R}^{\mathsf{off}}}\ \sigma_{\mathsf{off}}(i)\ \mathbf{a}\ \mathfrak{p}_{\mathsf{off}}(i,1)\ \mathfrak{p}_{\mathsf{off}}(i,2).$$

Besides, let $\mathbf{e}'_i$ and k_i be the terms defined by $\mathbf{e}'_i \overset{\text{def}}{=} \pi_2\ w_{\mathsf{off}}(i)$ and $k_i \overset{\text{def}}{=} \pi_3\ w_{\mathsf{off}}(i)$. Therefore, by definition of the predicate $\textbf{zkp-rel}_{\mathcal{R}^{\mathsf{off}}}$, we have in particular

$$\mathcal{E};\Theta;\Gamma \vdash \bigwedge_{i=1}^{N} \mathbf{a} \circledast (\mathbf{e}_s\ t_i) = \textbf{com-vec}\ (ck\ n)\ \mathbf{e}'_i\ k_i. \qquad (*)$$

Hence, by properties Eq. (β), Eq. ($*$) and by the commitment opening rule L.OPEN, we conclude

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \textbf{com-mat}\ (ck\ n)\ M\ \mathbf{s}$$

where $v\overset{\text{def}}{=}\textbf{solve}\ \ \mathbf{a}\ \ (\mathbf{e}_s\ \ t_i)_{i=1}^N\ \ (\mathbf{e}'_i, k_i)_{i=1}^N$, $M\overset{\text{def}}{=}\pi_1\ \ v$, and $\mathbf{s}\overset{\text{def}}{=}\pi_2\ v$. □

2) M represents a permutation:

Lemma 8. *Let $\mathcal{E}$ be an environment, let Θ be a context of global formulas and let Γ be a context of local formulas. We denote by ψ the function $\psi\overset{\textit{def}}{=}\lambda r.\ \textbf{\textit{zkp-verif}}_{\mathcal{R}^{\mathsf{off}}}\ \ (ck\ \ n, \mathbf{e}_{\mathsf{off}}\ \ t_1)\ \ \mathbf{a}\ \ \langle \alpha_{\mathsf{off}}, r, z_{\mathsf{off}}(r)\rangle$. We suppose*

$$\mathcal{E};\Theta \vdash \textbf{\textit{non-negl}}(g)\ \tilde{\wedge}\ \textbf{\textit{det}}(g) \qquad (\mathcal{H}_g)$$

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{\textit{low-bound}}\ g\ \psi, \qquad (\mathcal{H}_1)$$

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \textbf{\textit{com-mat}}\ (ck\ n)\ M\ \mathbf{s}, \qquad (\mathcal{H}_2)$$

Then, we conclude $\mathcal{E};\Theta;\Gamma \vdash \textbf{\textit{perm}}_N\ M$.

Proof. Let $\mathbf{r}_s\ :\ \textbf{nat}\ \rightarrow\ \textbf{chall}_{\mathcal{R}^{\mathsf{off}}}$ be an uniform source of random values with semantics given by the honest verifier of the offline relation $\mathcal{R}^{\mathsf{off}}$. By the rewinding axiom (Axiom 1) applied to the formula ψ, there exists a polynomial bounded and deterministic term $k_r\ :\ \textbf{nat}$ such that $2\ \leqslant\ k_r$ and the following property holds

$$\begin{aligned}\mathcal{E};\Theta \vdash [&\textbf{low-bound}\ g\ \psi \rightarrow \\ &\forall\,(t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\ \rightarrow\ \psi\ (\mathbf{r}_s\ t)] \\ &\tilde{\wedge}\ [\forall\,(t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\ \rightarrow \\ &\qquad (\mathbf{r}_s\ t) \in \{\mathbf{r}_s\ 1, \dots, \mathbf{r}_s\ k_r\}]\end{aligned}$$

Therefore, by hypothesis Eq. $(\mathcal{H}_1)$, we conclude

$$\mathcal{E};\Theta;\Gamma \vdash \forall\,(t : \textbf{nat}).\ (\mathbf{r}_s\ t) \in \textbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s\ \rightarrow\ \psi\ (\mathbf{r}_s\ t).$$

Hence, there exists 2 distinct terms $r_1, r_2 : \textbf{nat}$ with, without loss of generality, $1 \leqslant r_1 < r_2 \leqslant k_r$ and $\textbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s = \{r_1, r_2\}$. Therefore, we have

$$\begin{aligned}\mathcal{E};\Theta;\Gamma \vdash \bigwedge_{j\in\{1,2\}} &\textbf{zkp-verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_{\mathsf{off}}\ t_1)\ \mathbf{a} \\ &\qquad \langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_j, z_{\mathsf{off}}(\mathbf{r}_s\ r_j)\rangle.\end{aligned}$$

By the *special-soundness* property L.Σ-P:SpSound applied to the offline relation $\mathcal{R}^{\mathsf{off}}$, we conclude the existency of an extractor function $\textbf{zkp-extract}_{\mathcal{R}^{\mathsf{off}}}$ such that

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{zkp-rel}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_{\mathsf{off}}\ t_1)\ \mathbf{a}\ w_{\mathsf{off}}.$$

where w_{off} is the witness term defined by

$$\begin{aligned}w_{\mathsf{off}} \overset{\text{def}}{=} &\textbf{zkp-extract}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e}_{\mathsf{off}}\ t_1)\ \mathbf{a} \\ &\langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_1, z_{\mathsf{off}}(\mathbf{r}_s\ r_1)\rangle\ \langle \alpha_{\mathsf{off}}, \mathbf{r}_s\ r_2, z_{\mathsf{off}}(\mathbf{r}_s\ r_2)\rangle.\end{aligned}$$

Hence, let t, $\mathbf{e}'$ and k be the terms defined respectively by $t\overset{\text{def}}{=}\pi_1\ \ w_{\mathsf{off}}$, $\mathbf{e}'\overset{\text{def}}{=}\pi_2\ \ w_{\mathsf{off}}$ and $k\overset{\text{def}}{=}\pi_3\ \ w_{\mathsf{off}}$. By definition of the offline relation predicate $\textbf{zkp-rel}_{\mathcal{R}^{\mathsf{off}}}$, we have the three following properties

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} \circledast \mathbf{1} = \textbf{com-vec}\ (ck\ n)\ \mathbf{1}\ t \qquad (i)$$

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} \circledast (\mathbf{e}_{\mathsf{off}}\ t_1) = \textbf{com-vec}\ (ck\ n)\ \mathbf{e}'\ k \qquad (ii)$$

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{prod}_N\ \mathbf{e}' = \textbf{prod}_N\ (\mathbf{e}_{\mathsf{off}}\ t_1) \qquad (iii)$$

label=–

- By Eq. (i), and by hypothesis Eq. $(\mathcal{H}_2)$, we have $\mathcal{E};\Theta;\Gamma\ \vdash\ (\textbf{com-mat}\ \ (ck\ \ n)\ \ M\ \ \mathbf{s}) \circledast \mathbf{1} = \textbf{com-vec}\ \ (ck\ \ n)\ \ \mathbf{1}\ \ t$. Next, by action of $\circledast$ on commitments and by transitivity, the rule L.$\circledast$:Com applied to the previous identity leads to $\mathcal{E};\Theta;\Gamma\ \vdash\ \textbf{com-vec}\ (ck\ n)\ (M \cdot \mathbf{1})\ \langle \mathbf{s} \mid \mathbf{1}\rangle = \textbf{com-vec}\ (ck\ n)\ \mathbf{1}\ t$. Finally, as the commitment scheme $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$ is *computationally binding*, we conclude, thanks to the related rule L.Com:Bind, the following equality

  $$\mathcal{E};\Theta;\Gamma \vdash M \cdot \mathbf{1} = \mathbf{1}. \qquad (*_1)$$

- Similarly, using equation Eq. (ii) and by hypothesis Eq. $(\mathcal{H}_2)$, we conclude by the *binding* rule L.Com:Bind the following judgement $\mathcal{E};\Theta;\Gamma\ \vdash\ M \cdot (\mathbf{e}_{\mathsf{off}}\ \ t_1) = \mathbf{e}'$. Hence, by the last equation Eq. (iii), the last identity leads to

  $$\mathcal{E};\Theta;\Gamma \vdash \textbf{prod}_N\ (M \cdot (\mathbf{e}_{\mathsf{off}}\ t_1)) = \textbf{prod}_N\ (\mathbf{e}_{\mathsf{off}}\ t_1).$$

  Let $P_N[M]$ be the polynomial defined by $P_N[M]\overset{\text{def}}{=}\textbf{prod}_N\ \ (M \cdot X) - \textbf{prod}_N\ \ X$. As $(\mathbf{e}_{\mathsf{off}}\ \ t_1)$ is a fresh name, we apply the *Schwartz-Zippel* lemma to the polynomial $P_N[M]$ and conclude by the related rule L.Sz

  $$\mathcal{E};\Theta;\Gamma \vdash \textbf{prod}_N\ (M \cdot X) = \textbf{prod}_N\ X. \qquad (*_\Pi)$$

Consequently, as equations Eq. $(*_1)$ and Eq. $(*_\Pi)$ hold, we conclude by the characterization of permutation matrix that M represents a permutation, *i.e.* by applying the rule L.π:Charac, the following judgement holds $\mathcal{E};\Theta;\Gamma\ \vdash\ \textbf{perm}_N\ M$. Therefore, the vector $\mathbf{a}$ is a commitment message to a permutation matrix, *i.e.* we have

$$\begin{aligned}&\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \textbf{com-mat}\ (ck\ n)\ M\ \mathbf{s} \\ &\qquad\qquad \text{and} \quad \mathcal{E};\Theta;\Gamma \vdash \textbf{perm}_N\ M.\end{aligned}$$

□

3) M has been used to shuffle the input ciphertexts list with the shuffle-friendly *map $\phi_{\mathbb{CS}}$:*

Lemma 9. *Let $\mathcal{E}$ be an environment, let Θ be a context of global formulas and let Γ be a context of local formulas. We denote by ψ_{on} the formula defined by*

$$\begin{aligned}\psi_{on} \overset{\textit{def}}{=} \lambda r.\ \textbf{\textit{zkp-verif}}_{\mathcal{R}^{on}_{\phi_{\mathbb{CS}}}}\ (ck\ n, \text{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_{on}\ t_2)\ (\mathbf{a}, \mathbf{c}, \mathbf{c}') \\ \langle \alpha_{on}, r, z_{on}(r)\rangle\end{aligned}$$

We suppose

$$\mathcal{E};\Theta \vdash \textbf{\textit{non-negl}}(g)\ \tilde{\wedge}\ \textbf{\textit{det}}(g) \qquad (\mathcal{H}_g)$$

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{\textit{low-bound}}\ g\ \psi_{on} \qquad (\mathcal{H}_r)$$

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \textbf{\textit{com-mat}}\ (ck\ n)\ M\ \mathbf{s} \qquad (\mathcal{H}_{\mathbf{a}})$$

$$\mathcal{E};\Theta;\Gamma \vdash \textbf{\textit{perm}}_N\ M \qquad (\mathcal{H}_\pi)$$

Then, we conclude the following property

$$\mathcal{E};\Theta;\Gamma \vdash \bigwedge_{i=1}^{N} \Big(\exists\, v_i.\ \mathbf{c}' \circledast (M \cdot \mathbf{i}) = \\ \boldsymbol{\textit{shuf-map}}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c} \circledast \mathbf{i})\ v_i\Big).$$

Proof. For ease of notation, we denote by σ_{on} the public parameter defined by $\sigma_{\mathsf{on}} \overset{\text{def}}{=} (ck\ \ n, \mathtt{pk}_{\mathbb{CS}}\ \ sk, \mathbf{e}_{\mathsf{on}}\ \ t_2)$ and by x_{on} the statement defined by $x_{\mathsf{on}} \overset{\text{def}}{=} (\mathbf{a}, \mathbf{c}, \mathbf{c}')$. Let $\mathbf{r}_s : \mathbf{nat} \to \mathbf{chall}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}$ be an uniform source of random values defined by the verifier of the online relation $\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}$. By hypothesis Eq. $(\mathcal{H}_r)$ and by the rewinding axiom (Axiom 1) applied to the function ψ_{on}, we conclude the existency of a term $k_r : \mathbf{nat}$ such that $2 \leqslant k_r$ and there exists 2 distinct terms $t_1, t_2 : \mathbf{nat}$ with $1 \leqslant t_1 < t_2 \leqslant k_r$ such that $\mathbf{select}^{(2)}_{\text{chall}}\ k_r\ \mathbf{r}_s = \{\mathbf{r}_s\ t_1, \mathbf{r}_s\ t_2\}$ and

$$\mathcal{E};\Theta;\Gamma \vdash \bigwedge_{j\in\{1,2\}} (\mathbf{zkp\text{-}verif}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ \sigma_{\mathsf{on}}\ x_{\mathsf{on}}\ \langle \alpha_{\mathsf{on}}, \mathbf{r}_s\ t_j, z_{\mathsf{on}}(\mathbf{r}_s\ t_j)\rangle).$$

By the *special-soundness* property L.Σ-P:SpSound applied to the relation for the online phase $\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}$, we conclude the existency of an extractor function $\mathbf{zkp\text{-}extract}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}$ such that

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{zkp\text{-}rel}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ \sigma_{\mathsf{on}}\ x_{\mathsf{on}}\ w_{\mathsf{on}}$$

where w_{on} is the witness term defined by

$$w_{\mathsf{on}} \overset{\text{def}}{=} \mathbf{zkp\text{-}extract}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ \sigma_{\mathsf{on}}\ x_{\mathsf{on}}\ \langle \alpha_{\mathsf{on}}, \mathbf{r}_s\ t_1, z_{\mathsf{on}}(\mathbf{r}_s\ t_1)\rangle \\ \langle \alpha_{\mathsf{on}}, \mathbf{r}_s\ t_2, z_{\mathsf{on}}(\mathbf{r}_s\ t_2)\rangle.$$

Hence, let $\mathbf{e}'$, k and u be the terms defined respectively by $\mathbf{e}' \overset{\text{def}}{=} \pi_1\ w_{\mathsf{on}}$, $k \overset{\text{def}}{=} \pi_2\ w_{\mathsf{on}}$ and $u \overset{\text{def}}{=} \pi_3\ w_{\mathsf{on}}$. By definition of the correct shuffle relation predicate $\mathbf{zkp\text{-}rel}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}$, we have the two following properties

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} \circledast (\mathbf{e}_{\mathsf{on}}\ t_2) = \mathbf{com\text{-}vec}\ (ck\ n)\ \mathbf{e}'\ k \qquad (i)$$

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{c}' \circledast \mathbf{e}' = \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c} \circledast (\mathbf{e}_{\mathsf{on}}\ t_2))\ u \qquad (ii)$$

By the first equation Eq. (i), by the hypothesis Eq. $(\mathcal{H}_{\mathbf{a}})$ and by the *binding* rule L.Com:Bind applied to the commitment scheme $\mathbb{KS}[\mathbb{F}(p_\eta)^N]$, we conclude $\mathcal{E};\Theta;\Gamma \vdash M \cdot (\mathbf{e}_{\mathsf{on}}\ t_2) = \mathbf{e}'$. Therefore, the second equation Eq. (ii) becomes

$$\mathcal{E};\Theta;\Gamma \vdash \mathbf{c}' \circledast (M \cdot \mathbf{e}_\phi) = \\ \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c} \circledast (\mathbf{e}_{\mathsf{on}}\ t_2))\ u$$

Besides, as $\mathbf{e}_{\mathsf{on}}\ \ t_2$ is a fresh name, we have $\mathcal{E};\Theta;\Gamma \vdash \Psi^{\mathbf{e}_{\mathsf{on}},t_2}_{\mathsf{fresh}}(\mathbf{c}, \mathbf{c}', M)$. Moreover, by hypothesis Eq. $(\mathcal{H}_\pi)$, M is a permutation matrix, *i.e.* the following property holds $\mathcal{E};\Theta;\Gamma \vdash \mathbf{perm}_N\ M$. Thus, by characterization of *shuffle-friendly* maps given by the rule L.Sfm:Charac, the following property holds

$$\mathcal{E}, (\mathbf{x} : \mathbf{msg});\Theta;\Gamma \vdash \exists\, v_{\mathbf{x}}.\ \mathbf{c}' \circledast (M \cdot \mathbf{x}) = \\ \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathtt{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c} \circledast \mathbf{x})\ v_{\mathbf{x}}$$

In particular, this property holds for all vectors $\mathbf{i}$ where $i \in [\![1; N]\!]$ and achieve this way the proof. □

4) Proof of the verifiability property under conditions: Now we have obtain the 3 key lemmas to show that we extract a permutation matrix π from the commitment message $\mathbf{a}$ sent by the adversary and show that this matrix π was indeed used to *shuffle* the input ciphertexts list $\mathbf{c}$ to form the output ciphertexts list $\mathbf{c}'$, we present the lemma proving the verifiability property we want but *under* some conditions needed to rewind parts of the protocol trace.

Lemma 10. *Let $\mathcal{E}$ be an environment, let Θ be a context of global formulas and let Γ be a context of local formulas. We denote by $\mathcal{H}$ the function defined by*

$$\mathcal{H} \overset{def}{=} \lambda\mathbf{e}.\ \lambda r.\ \lambda r'.\ \boldsymbol{\textit{zkp-verif}}_{\mathcal{R}^{\mathit{off}}}\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_{\mathit{off}}, r, z_{\mathit{off}}(r)\rangle \\ \wedge\ \ \boldsymbol{\textit{zkp-verif}}_{\mathcal{R}^{\mathit{on}}_{\phi_{\mathbb{CS}}}}\ (ck\ n, \mathtt{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_{\mathit{on}}\ t_2)\quad (\mathbf{a}, \mathbf{c}, \mathbf{c}') \\ \langle \alpha_{\mathit{on}}, r', z_{\mathit{on}}(r')\rangle \\ \wedge\ \ \boldsymbol{\textit{wf\_ctxt}}_N\ sk\ \mathbf{c}.$$

We suppose

$$\mathcal{E};\Theta \vdash \boldsymbol{\textit{non-negl}}(g)\ \tilde{\wedge}\ \boldsymbol{\textit{det}}(g) \qquad (\mathcal{H}_g)$$

$$\mathcal{E};\Theta \vdash \boldsymbol{\textit{non-negl}}(g')\ \tilde{\wedge}\ \boldsymbol{\textit{det}}(g') \qquad (\mathcal{H}_{g'})$$

$$\mathcal{E};\Theta;\Gamma \vdash \boldsymbol{\textit{low-bound}}\ g\ (\lambda\mathbf{e}.\ \boldsymbol{\textit{low-bound}}\ g'\ (\mathcal{H}\ \mathbf{e})) \qquad (\mathcal{H}_1)$$

$$\mathcal{E};\Theta;\Gamma \vdash \boldsymbol{\textit{low-bound}}\ g'\ (\mathcal{H}\ (\mathbf{e}_{\mathit{off}}\ t_1)) \qquad (\mathcal{H}_2)$$

$$\mathcal{E};\Theta;\Gamma \vdash \mathcal{H}\ (\mathbf{e}_{\mathit{off}}\ t_1)\ (r_{\mathit{off}}\ l)\ (r_{\mathit{on}}\ p) \qquad (\mathcal{H}_3)$$

Therefore, we conclude the following property

$$\mathcal{E};\Theta;\Gamma \vdash \boldsymbol{\textit{wf\_ctxt}}_N\ sk\ \mathbf{c}' \\ \wedge\ \boldsymbol{\textit{eqm}}_N\ (\boldsymbol{\textit{dec-list}}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})\ (\boldsymbol{\textit{dec-list}}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}').$$

Proof. Let ψ_{off} be the formula defined by

$$\psi_{\mathsf{off}} \overset{\text{def}}{=} \lambda\mathbf{e}.\ \lambda r.\ \mathbf{zkp\text{-}verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, r, z_{\mathsf{off}}(r)\rangle$$

By definition of ψ_{off} and $\mathcal{H}$, we have the following global judgement

$$\mathcal{E};\Theta \vdash {}_1[\mathcal{H}\ \mathbf{e}\ r\ r' \to \psi_{\mathsf{off}}\ \mathbf{e}\ r]. \qquad (*_\pi)$$

Hence, because $\mathcal{E} \vdash g' : \mathbf{real}$ with $\mathcal{E};\Theta \vdash \mathbf{non\text{-}negl}(g')$, we conclude $\mathcal{E};\Theta;\varnothing \vdash \mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ \mathbf{e}) \to \mathbf{low\text{-}bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e})$ for all vector $\mathbf{e}$. In fact, this last property is true with probability 1, *i.e.* we have $\mathcal{E};\Theta \vdash {}_1[\mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ \mathbf{e}) \to \mathbf{low\text{-}bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e})]$. Therefore, because $\mathcal{E} \vdash g : \mathbf{real}$ and $\mathcal{E};\Theta \vdash \mathbf{non\text{-}negl}(g)$, we conclude

$$\mathcal{E};\Theta;\varnothing \vdash \mathbf{low\text{-}bound}\ g\ (\lambda\mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ \mathbf{e})) \\ \to \mathbf{low\text{-}bound}\ g\ (\lambda\mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e})).$$

Hence, by this last judgement and by hypothesis Eq. $(\mathcal{H}_1)$, we conclude $\mathcal{E};\Theta;\Gamma \vdash \mathbf{low\text{-}bound}\ g\ (\lambda\mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\psi_{\mathsf{off}}\ \mathbf{e}))$. Therefore, by the first key lemma (Lemma 7), we conclude the existency of two terms π and $\mathbf{s}$ such that $\mathcal{E};\Theta;\Gamma \vdash \mathbf{a} = \mathbf{com\text{-}mat}\ (ck\ n)\ \pi\ \mathbf{s}$.

Next, by global property Eq. $(*_\pi)$, because $\mathcal{E} \vdash g' : \mathbf{real}$ and $\mathcal{E};\Theta \vdash \mathbf{non\text{-}negl}(g')$ and by hypothesis Eq. $(\mathcal{H}_2)$, we conclude $\mathcal{E};\Theta;\Gamma \vdash \mathbf{low\text{-}bound}\ g'\ (\psi_{\mathsf{off}}\ (\mathbf{e}_{\mathsf{off}}\ t_1))$. Therefore, by the second key lemma (Lemma 8), the rebuild matrix π previously obtained is a permutation matrix, *i.e.* we have the property $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{perm}_N\ \pi$. Hence the vector $\mathbf{a}$ sends by the adversary can be open to a permutation matrix:

$$\mathcal{E}; \Theta; \Gamma \vdash \mathbf{a} = \mathbf{com\text{-}mat}\ (ck\ n)\ \pi\ \mathbf{s} \quad \text{and} \quad \mathcal{E}; \Theta; \Gamma \vdash \mathbf{perm}_N\ \pi. \tag{Γ}$$

Now, let ψ_{on} be the formula defined by

$$\psi_{\mathsf{on}} \overset{\text{def}}{=} \lambda r'.\ \mathbf{zkp\text{-}verif}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ \sigma_{\mathsf{on}}\ x_{\mathsf{on}}\ \langle \alpha_{\mathsf{on}}, r', z_{\mathsf{on}}(r') \rangle$$

where σ_{on} is the public parameter defined by $\sigma_{\mathsf{on}} \overset{\text{def}}{=} (ck\ \ n, \mathrm{pk}_{\mathbb{CS}}\ \ sk, \mathbf{e}_{\mathsf{on}}\ \ t_2)$ and x_{on} is the statement defined by $x_{\mathsf{on}} \overset{\text{def}}{=} (\mathbf{a}, \mathbf{c}, \mathbf{c}')$. Hence, by definition of ψ_{on} and $\mathcal{H}$, we have the following global judgement

$$\mathcal{E}; \Theta \vdash {}_1[\mathcal{H}\ \mathbf{e}\ r\ r' \rightarrow \psi_{\mathsf{on}}\ r']. \tag{$*_\phi$}$$

Hence, by global property Eq. $(*_\phi)$, because $\mathcal{E} \vdash g' : \mathbf{real}$ and $\mathcal{E}; \Theta \vdash \mathbf{non\text{-}negl}(g')$ and by the second hypothesis Eq. $(\mathcal{H}_2)$, we conclude $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{low\text{-}bound}\ g'\ \psi_{\mathsf{on}}$. Therefore, by this last property and by the conclusion Eq. (Γ), we apply the third key lemma (Lemma 9) and conclude the following property

$$\mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} \Big(\exists v_i.\ \mathbf{c}' \circledast (\pi \cdot \mathbf{i}) = \\ \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ sk)\ (\mathbf{c} \circledast \mathbf{i})\ v_i \Big).$$

By conclusion $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{perm}_N\ \pi$ given by Eq. (Γ) and by the injectivity rule for permutations L.π:INJ, we have, for all $i \in [\![1; N]\!]$, the existency of an index $j_i \in [\![1; N]\!]$ such that the property $\mathcal{E}; \Theta; \Gamma \vdash \pi \cdot \mathbf{i} = \mathbf{j_i}$ holds. Hence, by the action rule of $\circledast$ on canonical vectors applied to $\mathbf{i}$ and $\mathbf{j_i}$, we conclude $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{c} \circledast \mathbf{i} = \langle \mathbf{c} \mid \mathbf{i} \rangle$ and $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{c}' \circledast (\pi \cdot \mathbf{i}) = \mathbf{c}' \circledast \mathbf{j_i} = \langle \mathbf{c}' \mid \mathbf{j_i} \rangle = \langle \mathbf{c}' \mid \pi \cdot \mathbf{i} \rangle$. Then, the equation obtained in the previous step becomes

$$\mathcal{E}; \Theta; \Gamma \vdash \exists v_i.\ \langle \mathbf{c}' \mid \pi \cdot \mathbf{i} \rangle = \\ \mathbf{shuf\text{-}map}_{\phi_{\mathbb{CS}}}\ (\mathrm{pk}_{\mathbb{CS}}\ sk)\ \langle \mathbf{c} \mid \mathbf{i} \rangle\ v_i. \tag{Φ}$$

As the input ciphertexts list $\mathbf{c}$ is *well-formed* for the secret key sk by the third hypothesis Eq. $(\mathcal{H}_3)$, *i.e.* $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{wf\_ctxt}\ sk\ \mathbf{c}$, we have by the characterization of the predicate $\mathbf{wf\_ctxt}$ rule L.WF:VALID, for all $i \in [\![1; N]\!]$, $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{wf\_ctxt}\ \ sk\ \langle \mathbf{c} \mid \mathbf{i} \rangle$. Therefore, by the correctness rule for *shuffle-friendly* maps L.SFM:CORRECT, and by the equation Eq. (Φ), we have

$$\mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} \Big(\mathbf{dec}_{\mathbb{CS}}\ sk\ \langle \mathbf{c}' \mid \pi \cdot \mathbf{i} \rangle = \mathbf{dec}_{\mathbb{CS}}\ sk\ \langle \mathbf{c} \mid \mathbf{i} \rangle \Big).$$

Next, by application of the characterization rule of $\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}$ L.DECLIST and by the rewrite rule, the previous equation becomes $\mathcal{E}; \Theta; \Gamma \vdash \bigwedge_{i=1}^{N} \Big(\langle \mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ \ sk\ \ \mathbf{c}' \mid (\pi \cdot \mathbf{i}) \rangle = \langle \mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ \ sk\ \ \mathbf{c} \mid \mathbf{i} \rangle \Big)$. Finally, using this property and because the property $\mathcal{E}; \Theta; \Gamma \vdash \mathbf{perm}_N\ \pi$ holds, the characterization of multisets equality rule L.EQM:CHARAC leads to

$$\boxed{\mathcal{E}; \Theta; \Gamma \vdash \mathbf{eqm}_N\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}')\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})}$$

□

5) Proof of the verifiability property: Now, we finally prove the verifiability property. We denote by $\mathcal{H}$ and Goal the functions defined by

$$\begin{aligned} \mathcal{H} \overset{\text{def}}{=} & \lambda \mathbf{e}.\ \lambda r.\ \lambda r'.\ \mathbf{zkp\text{-}verif}_{\mathcal{R}^{\mathsf{off}}}\ (ck\ n, \mathbf{e})\ \mathbf{a}\ \langle \alpha_{\mathsf{off}}, r, z_{\mathsf{off}}(r) \rangle \\ \wedge \quad & \mathbf{zkp\text{-}verif}_{\mathcal{R}^{\mathsf{on}}_{\phi_{\mathbb{CS}}}}\ (ck\ n, \mathrm{pk}_{\mathbb{CS}}\ sk, \mathbf{e}_{\mathsf{on}}\ t_2) \quad (\mathbf{a}, \mathbf{c}, \mathbf{c}') \\ & \qquad\qquad\qquad\qquad\qquad\qquad \langle \alpha_{\mathsf{on}}, r', z_{\mathsf{on}}(r') \rangle \\ \wedge \quad & \mathbf{wf\_ctxt}_N\ sk\ \mathbf{c}. \end{aligned}$$

and

$$\begin{aligned} \mathrm{Goal} \overset{\text{def}}{=} & \mathbf{wf\_ctxt}_N\ sk\ \mathbf{c}' \\ & \wedge \mathbf{eqm}_N\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c})\ (\mathbf{dec\text{-}list}^{(N)}_{\mathbb{CS}}\ sk\ \mathbf{c}'). \end{aligned}$$

Hence, the verifiability property consists in proving the following global formula

$$\mathcal{E}; \varnothing \vdash [\mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)\ (r_{\mathsf{off}}\ l)\ (r_{\mathsf{on}}\ p)\ \rightarrow\ \mathrm{Goal}].$$

Therefore, by the elimination rule G.LB:ELIM of predicate **low-bound** applied to the hypothesis function $\mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)$ and to the goal Goal, we have to prove

$$\begin{aligned} \mathcal{E}; \varnothing \vdash \tilde{\forall}(g' : \mathbf{real}).\ & \mathbf{non\text{-}negl}(g')\ \tilde{\wedge}\ \mathbf{det}(g')\ \tilde{\rightarrow} \\ & [\mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)) \rightarrow \\ & \qquad \mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)\ (r_{\mathsf{off}}\ l)\ (r_{\mathsf{on}}\ p)\ \rightarrow\ \mathrm{Goal}]. \end{aligned}$$

Let $g' : \mathbf{real}$ be a non-negligible deterministic parameter such that $\mathbf{non\text{-}negl}(g')$ and $\mathbf{det}(g')$. We define $\Theta_{g'}$ be the following context of global formulas

$$\Theta_{g'} \overset{\text{def}}{=} \mathbf{non\text{-}negl}(g'), \mathbf{det}(g').$$

By another use of the elimination rule G.LB:ELIM of predicate **low-bound** applied to the hypothesis function $\mathcal{H}'_{g'} \overset{\text{def}}{=} \lambda \mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ \mathbf{e})$ and to the goal $\mathrm{Goal}' \overset{\text{def}}{=} \lambda \mathbf{e}.\ \mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)\ (r_{\mathsf{off}}\ l)\ (r_{\mathsf{on}}\ p) \rightarrow \mathrm{Goal}$, we have to prove

$$\begin{aligned} \mathcal{E}, (g' : \mathbf{real}); \Theta_{g'} \vdash \tilde{\forall}(g : \mathbf{real}).\ & \mathbf{non\text{-}negl}(g)\ \tilde{\wedge}\ \mathbf{det}(g)\ \tilde{\rightarrow} \\ & [\mathbf{low\text{-}bound}\ g\ \mathcal{H}'_{g'} \rightarrow \mathcal{H}'_{g'}\ (\mathbf{e}_{\mathsf{off}}\ t_1) \rightarrow \mathrm{Goal}'\ (\mathbf{e}_{\mathsf{off}}\ t_1)]. \end{aligned}$$

Let $g : \mathbf{real}$ be a non-negligible deterministic parameter such that $\mathbf{non\text{-}negl}(g)$ and $\mathbf{det}(g)$. We define Θ_g to be the following global context

$$\Theta_g \overset{\text{def}}{=} \mathbf{non\text{-}negl}(g), \mathbf{det}(g).$$

By putting notations back together, we have to prove the following judgement

$$\begin{aligned} & \mathcal{E}, (g, g' : \mathbf{real}); \Theta_{g'}, \Theta_g \vdash \\ & \quad [\mathbf{low\text{-}bound}\ g\ (\lambda \mathbf{e}.\ \mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ \mathbf{e})) \rightarrow \\ & \qquad \mathbf{low\text{-}bound}\ g'\ (\mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)) \rightarrow \\ & \qquad\quad \mathcal{H}\ (\mathbf{e}_{\mathsf{off}}\ t_1)\ (r_{\mathsf{off}}\ l)\ (r_{\mathsf{on}}\ p) \rightarrow \mathrm{Goal}] \end{aligned}$$

Which is exactly the statement of the last key lemma (Lemma 10). Therefore, this achieves the proof of the verifiability property.