Bayer-Groth mixserver protocol

Anonymous Author(s)

ACM Reference Format:
Anonymous Author(s). 2026. Bayer-Groth mixserver protocol. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 23 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

REFERENCES

[1] Stephanie Bayer and Jens Groth. 2012. Efficient Zero-Knowledge Argument for Correctness of a Shuffle. In *EUROCRYPT (Lecture Notes in Computer Science, Vol. 7237).* Springer, 263–280.
[2] proofwiki.org. 2022. *Inverse of Vandermonde Matrix.* https://proofwiki.org/wiki/Inverse_of_Vandermonde_Matrix

A CRYPTOGRAPHIC DEFINITIONS

From now on, we abbreviate *Probabilistic Polynomial-time Turing Machine* into *PPTM.*

A.1 Commitment schemes

For an infinite countable set $\mathbb{X}$, we define the property $\Phi[\mathbb{X}]$ as follows

$$\Phi[\mathbb{X}] \text{ holds} \overset{\text{def}}{\iff} \begin{cases} \mathbb{X} \overset{\text{def}}{=} \bigcup\limits_{\eta\in\mathbb{N}^*} \mathbb{X}^{(\eta)} \ ; \\ \forall\, \eta \in \mathbb{N}^*,\ \mathsf{Card}(\mathbb{X}^{(\eta)}) < +\infty \quad (\mathbb{X}^{(\eta)} \textit{ is finite}) \ ; \\ \quad \textit{and} \quad \log_2 \mathsf{Card}(\mathbb{X}^{(\eta)}) \geqslant \eta. \end{cases} \tag{Φ}$$

Let $\mathbb{M}$ be an infinite countable set of messages such that $\Phi[\mathbb{M}]$ holds and, for all $\eta \in \mathbb{N}^*$, $\left(\mathbb{M}^{(\eta)}, \otimes\right)$ is an abelian group (let us say multiplicative). Let $\mathbb{KS}[\mathbb{M}]$ be a tuple

$$\mathbb{KS}[\mathbb{M}] \overset{\text{def}}{=} \left\langle \mathbb{P}_{\mathbb{M}}, \mathbb{S}_{\mathbb{M}}, \mathbb{V}_{\mathbb{M}}, \mathsf{Gen}_{\mathbb{M}}, \mathsf{Com}_{\mathbb{M}} \right\rangle$$

where

- For any set $\mathbb{X} \in \left\{\mathbb{P}_{\mathbb{M}}, \mathbb{S}_{\mathbb{M}}, \mathbb{V}_{\mathbb{M}}\right\}$ the property $\Phi[\mathbb{X}]$ holds ;
- The PPTM algorithm $\mathsf{Gen}_{\mathbb{M}} : \mathbb{N}^* \longrightarrow \mathbb{P}_{\mathbb{M}}$ takes as input a security parameter $\eta \in \mathbb{N}^*$ and outputs a commitment key $ck \leftarrow \mathsf{Gen}_{\mathbb{M}}(\eta) \in \mathbb{P}_{\mathbb{M}}^{(\eta)}$;
- The PPTM algorithm $\mathsf{Com}_{\mathbb{M}} : \mathbb{P}_{\mathbb{M}} \times \mathbb{M} \times \mathbb{S}_{\mathbb{M}} \longrightarrow \mathbb{V}_{\mathbb{M}}$ takes as inputs a commitment key $ck \in \mathbb{P}_{\mathbb{M}}$, a message $m \in \mathbb{M}$ and a random value $r \in \mathbb{S}_{\mathbb{M}}$. Then it outputs a commit value $a \leftarrow \mathsf{Com}_{\mathbb{M}}(ck, m\,;\, r) \in \mathbb{V}_{\mathbb{M}}$. Besides, for all security parameter $\eta \in \mathbb{N}^*$, we **must have** $ck \in \mathbb{P}_{\mathbb{M}}^{(\eta)}$, $m \in \mathbb{M}^{(\eta)}$, $r \in \mathbb{S}_{\mathbb{M}}^{(\eta)}$ **and** $a \in \mathbb{V}_{\mathbb{M}}^{(\eta)}$.

Definition A.1 (Perfect hiding).

Definition A.2 (Binding error).

Definition A.3 (Homomorphic commitment scheme). We say that the tuple $\mathbb{KS}[\mathbb{M}]$ is a *homomorphic commitment scheme for the message set* $\mathbb{M}$ when the following properties hold

- For all security parameter $\eta \in \mathbb{N}^*$, the *randomness space* $\left(\mathbb{S}_{\mathbb{M}}^{(\eta)}, \oplus\right)$ is an abelian group (let us say additive) and the *commit value space* $\left(\mathbb{V}_{\mathbb{M}}^{(\eta)}, \odot\right)$ is also an abelian group (let us say multiplicative) ;
- $\mathbb{KS}[\mathbb{M}]$ is *perfectly hiding* ;
- There exists a negligible function $\delta : \mathbb{N}^* \longrightarrow [0,1]$ such that $\mathbb{KS}[\mathbb{M}]$ is *computationally binding* with binding error δ ;
- For all security parameter $\eta \in \mathbb{N}^*$, for all commitment key parameter $ck \in \mathbb{P}_{\mathbb{M}}^{(\eta)}$, the following function $\phi_{ck}^{(\eta)}$ is a *group homorphism*:

$$\begin{array}{rccc} \phi_{ck}^{(\eta)} : & \left(\mathbb{M}^{(\eta)}, \otimes\right) \times \left(\mathbb{S}_{\mathbb{M}}^{(\eta)}, \oplus\right) & \longrightarrow & \left(\mathbb{V}_{\mathbb{M}}^{(\eta)}, \odot\right) \\ & (m, r) & \longmapsto & \mathsf{Com}_{\mathbb{M}^{(\eta)}}(ck, m\,;\, r) \end{array}$$

A.2 *Zero-Knowledge* proofs

In all this subsection, we fix a natural number $\mu \in \mathbb{N}$ and a relation $\mathcal{R} \subseteq \mathcal{PP}_{\mathcal{R}} \times \mathcal{X}_{\mathcal{R}} \times \mathcal{W}_{\mathcal{R}}$. Let $\mathbb{ZK}^{(\mu)}[\mathcal{R}] \overset{\text{def}}{=} (\mathcal{I}, \mathcal{P}, \mathcal{V})$ be a $(2\mu+1)$-move interactive protocol for $\mathcal{R}$.

Definition A.4 (Perfect completeness). The protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is said to be *perfectly complete* when, for all PPTM adversary $\mathcal{A}$, the following property holds:

$$\forall\, \eta \in \mathbb{N}^*,\ \mathbb{P}r_{\rho\in\mathbb{T}_\eta}\left[\ 1 \leftarrow_{\mathcal{G}} \textbf{Completeness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho)\ \right] = 0,$$

where the cryptographic *completeness game* is defined in **Game 1**.

Completeness$^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, (\rho_h, \rho_a))$ – Completeness

$\sigma \leftarrow \mathcal{I}(\eta\,;\, \rho_h)$;
$(x, w) \leftarrow \mathcal{A}(\eta, \sigma\,;\, \rho_a)$;
$\mathrm{tr} \leftarrow \left(\mathcal{P}(w) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}\right)(\eta, \sigma, x\,;\, \rho_h)$;
$b \leftarrow v^{\sigma,x}_{\mathcal{R}}(\mathrm{tr}) \ \wedge\ \neg\left(\varphi_{\mathcal{R}}((\sigma, x, w))\right)$;
returns b ;

Game 1: Cryptographic completeness game for interactive protocols

Definition A.5 (Public coin). The protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is said to be *public coin* when, for all security parameter $\eta \in \mathbb{N}^*$, for all public parameter $\sigma \in \mathcal{PP}_{\mathcal{R}}$, for all public statement $x \in \mathcal{X}_{\mathcal{R}}$, for all witness $w \in \mathcal{W}_{\mathcal{R}}$ and for all PPTM prover $\mathcal{P}^*$ (both honest or dishonest), the following property holds

$$\forall\, i \in [\![1; \mu]\!],\ m_{2i} = \left(c_i \overset{\$}{\leftarrow} \mathsf{Ch}^i_{\mathcal{R}}\right),$$

Conference'17, July 2017, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

where $(m_i)_{i=1}^{2\mu+1} \stackrel{\text{def}}{=} \left(\mathcal{P}^*(w) \rightleftharpoons_{\mathcal{R}}^{(\mu)} \mathcal{V}\right)(\eta, \sigma, x)$ is an interaction of $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ with the **honest** verifier $\mathcal{V}$.

Definition A.6 (Soundness error). Let $\mathcal{A}$ be a PPTM adversary. We define the *soundness error of $\mathcal{V}$ against the adversarial prover $\mathcal{A}$*, noted $\varepsilon_{\mathcal{A}}$, to be the following function

$$\begin{array}{rccl} \varepsilon_{\mathcal{A}} : & \mathbb{N}^* & \longrightarrow & [0,1] \\ & \eta & \longmapsto & \mathbb{P}\mathrm{r}_{\rho \in \mathbb{T}_\eta}\left[\, 1 \leftarrow_{\mathcal{G}} \mathbf{Soundness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, \rho) \,\right], \end{array}$$

where the cryptographic *soundness game* is defined in **Game 2**.

$\mathbf{Soundness}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}]}(\eta, (\rho_h, \rho_a))$ – Soundness

$\sigma \leftarrow \mathcal{I}(\eta\,;\, \rho_h)$;
$x \leftarrow \mathcal{A}(\eta, \sigma\,;\, \rho_a)$;
$\mathrm{tr} \leftarrow \left(\mathcal{A}(\rho_a) \rightleftharpoons_{\mathcal{R}}^{(\mu)} \mathcal{V}(\rho_h)\right)(\eta, \sigma, x)$;
$b \leftarrow v_{\mathcal{R}}^{\sigma,\chi}(\mathrm{tr}) \ \wedge \ x \notin \mathcal{L}_\sigma(\mathcal{R})$;
returns b ;

Game 2: Cryptographic soundness game for interactive protocols

Definition A.7 (Knowledge soundness). The protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is said to be *knowledge sound with knowledge error* $\kappa : \mathbb{N}^* \longrightarrow [0,1]$ when, for all **deterministic** Polynomial-time adversarial prover $\mathcal{P}^*$, there exists a PPTM algorithm $\mathcal{E}_{\mathcal{R}}$, called the *knowledge extractor*, such that, for all PPTM adversary $\mathcal{A}$, and for all security parameter $\eta \in \mathbb{N}^*$, the following lower bound holds:

$$\mathbb{P}\mathrm{r}_{\rho \in \mathbb{T}_\eta}\left[\, 1 \leftarrow_{\mathcal{G}} \mathbf{KnowSound}^{\mathcal{A},\mathcal{P}^*}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}(\eta, \rho) \;\middle|\; \varepsilon_{\mathcal{P}^*} \notin \mathrm{negl}(\eta) \,\right] \geqslant 1 - \kappa(\eta),$$

where the cryptographic *knowledge soundness game* is defined in **Game 3**.

$\mathbf{KnowSound}^{\mathcal{A},\mathcal{P}^*}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}(\eta, (\rho_h, \rho_a))$ – Knowledge soundness

$\sigma \leftarrow \mathcal{I}(\eta\,;\, \rho_h)$;
$(x, \rho^*) \leftarrow \mathcal{A}(\eta, \sigma\,;\, \rho_a)$;
$w \leftarrow \mathcal{E}_{\mathcal{R}}^{\mathcal{P}^*(\rho^*), \mathcal{V}(\rho_h)}(\eta, \sigma, x)$;
$b \leftarrow \varphi_{\mathcal{R}}((\sigma, x, w))$;
returns b ;

Game 3: Cryptographic knowledge soundness game for interactive protocols

Definition A.8 (Perfect Honest-Verifier Zero-Knowledge). The protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is said to be *perfectly Honest-Verifier Zero-Knowledge* when there exists a PPTM algorithm $\mathcal{S}\mathrm{im}_{\mathcal{R}}$, called the *simulator*, such that, for all PPTM adversary $\mathcal{A}$, the following property holds

$$\forall\, \eta \in \mathbb{N}^*,\ \mathbf{Adv}_{\mathbf{HVZK}}\left[\mathcal{A} \;\middle|\; \mathbb{ZK}^{(\mu)}[\mathcal{R}],\, \mathcal{S}\mathrm{im}_{\mathcal{R}}\right](\eta) = 0,$$

where the cryptographic *Honest-Verifier Zero-Knowledge* game is defined in **Game 4** and the *advantage of the adversary $\mathcal{A}$ against the HVZK game* is defined as follows

$$\forall\, \eta \in \mathbb{N}^*,\ \mathbf{Adv}_{\mathbf{HVZK}}\left[\mathcal{A} \;\middle|\; \mathbb{ZK}^{(\mu)}[\mathcal{R}],\, \mathcal{S}\mathrm{im}_{\mathcal{R}}\right](\eta) \stackrel{\text{def}}{=} \left| 2 \cdot \mathbb{P}\mathrm{r}_{\rho \in \mathbb{T}_\eta}\left[\, 1 \leftarrow_{\mathcal{G}} \mathbf{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{E}_{\mathcal{R}}}(\eta, \rho\,;\, \beta) \,\right] - 1 \right|.$$

*Definition A.9 (*Zero-Knowledge *argument of knowledge).* The protocol $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is said to be *a zero-knowledge argument of knowledge for the relation $\mathcal{R}$* when the following properties hold

- $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is *perfectly complete* ;
- $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is *public coin* ;
- There exists a negligible function $\kappa : \mathbb{N}^* \longrightarrow [0,1]$ such that $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is *knowledge sound* with knowledge error κ ;
- $\mathbb{ZK}^{(\mu)}[\mathcal{R}]$ is *perfectly Honest-Verifier Zero-Knowledge*.

B SPECIFICATION AND CRYPTOGRAPHIC PROOFS OF BAYER-GROTH PROTOCOL

B.1 Shuffle argument protocol

We define

$$\mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}} \subseteq \underbrace{\left(\mathbb{G}_{p_\eta}^{n+1} \times \mathcal{PK}_{\mathbb{CS}}\right)}_{\text{Public parameter set}} \times \underbrace{\left(\mathbb{H}_{p_\eta}^{N} \times \mathbb{H}_{p_\eta}^{N}\right)}_{\text{Statement set}} \times \underbrace{\left(\mathfrak{S}_N \times \mathbb{F}_{p_\eta}^{N}\right)}_{\text{Witness set}}$$

to be the *shuffle relation* defined as follows:

$$\left((ck, pk), (\mathbf{c}, \mathbf{c}'), (\pi, \mathbf{r})\right) \in \mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}} \iff \mathbf{c}' = \mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \mathbf{r}) \odot \mathbf{c}_\pi$$

Hence, we define a 13-move shuffle argument protocol $\mathbb{ZK}^{(6)}[\mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}}]$ (**Protocol 1**) following the definition given in [1].

Theorem B.1 (Knowledge soundness of $\mathbb{ZK}^{(6)}[\mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}}]$). *The 13-move shuffle argument protocol $\mathbb{ZK}^{(6)}[\mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}}]$ is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\mathsf{SA}}$ for the Bayer-Groth shuffle argument to be the algorithm defined as follows in **Extractor 2**.

Let $N = nm \in \mathbb{N}^*$ be a natural number. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time (in η) and deterministic adversarial prover. Let $\sigma = (ck, pk) \leftarrow \mathcal{I}_{\mathsf{SA}}(\eta)$ be an honest public parameter for the shuffle relation $\mathcal{R}^{\mathrm{BG}}_{\mathsf{SA}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, \sigma)$ be an adversarial statement where

$$\chi \stackrel{\text{def}}{=} (\mathbf{c}, \mathbf{c}') \in \mathbb{H}_{p_\eta}^{N} \times \mathbb{H}_{p_\eta}^{N}.$$

Then, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\mathsf{SA}}$ on inputs σ and χ with access to oracles $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{SA}}$ and obtains

$$\tau_{\mathsf{SA}} \stackrel{\text{def}}{=} \Bigg(\mathbf{c}_A, \Big(x_l, \mathbf{c}_B^{(l)}, (y_l, z_l), \big(\mathbf{c}_D^{(l)}, \mathbf{c}_{-z}^{(l)}, \beta^{(l)}, C^{(l)}\big), \underbrace{\big(\Gamma^{(l)}, \mathbf{v}^{(l)}\big)}_{\substack{\text{Witness of the} \\ \text{Product Argument}}}, \underbrace{\big(B^{(l)}, \mathbf{t}^{(l)}, \varrho^{(l)}\big)}_{\substack{\text{Witness of the Multi-} \\ \text{Exponentiation Argument}}}\Big)_{l=1}^{N}\Bigg).$$

$\mathbf{HVZK}^{\mathcal{A}}_{\mathbb{ZK}^{(\mu)}[\mathcal{R}],\,\mathcal{S}im_{\mathcal{R}}}\big(\eta,(\rho_h,\rho_a)\,;\,\beta\big)$ – Honest-Verifier Zero-Knowledge

Case $\beta=0$ – *Real world*	**Case** $\beta=1$ – *Simulated world*
$\sigma \leftarrow \mathcal{I}(\eta\,;\,\rho_h)$;	$\sigma \leftarrow \mathcal{I}(\eta\,;\,\rho_h)$;
$(x,w,\rho^*) \leftarrow \mathcal{A}(\eta,\sigma\,;\,\rho_a)$;	$(x,w,\rho^*) \leftarrow \mathcal{A}(\eta,\sigma\,;\,\rho_a)$;
$\mathrm{tr} \leftarrow \Big(\mathcal{P}(w\,;\,\rho_h) \rightleftharpoons^{(\mu)}_{\mathcal{R}} \mathcal{V}(\rho^*)\Big)(\eta,\sigma,x)$;	$\mathrm{tr} \leftarrow \mathcal{S}im_{\mathcal{R}}(\eta,\sigma,x,\rho^*\,;\,\rho_h)$;
$b \leftarrow v^{\sigma,x}_{\mathcal{R}}(\mathrm{tr}) \;\wedge\; \varphi_{\mathcal{R}}\big((\sigma,x,w)\big)$;	$b \leftarrow v^{\sigma,x}_{\mathcal{R}}(\mathrm{tr}) \;\wedge\; \varphi_{\mathcal{R}}\big((\sigma,x,w)\big)$;
$g_\beta \leftarrow \mathcal{A}(\mathrm{tr}\,;\,\rho_a)$;	$g_\beta \leftarrow \mathcal{A}(\mathrm{tr}\,;\,\rho_a)$;
returns $(b \wedge \neg g_\beta)$; // $\neg g_\beta = 1 \iff g_\beta = 0 = \beta$.	**returns** $(b \wedge g_\beta)$; // $g_\beta = 1 = \beta$.

Game 4: Cryptographic *Honest-Verifier Zero-Knowledge* game for interactive protocols

(Step 1) – Obtain[1] the permutation witness π.

(Step1.1) By the *knowledge soundness* of the product argument protocol (see Theorem B.3), we have

$$\forall\, l \in [\![1;N]\!],\ \prod_{j=1}^{m}\prod_{i=1}^{n}\Gamma^{(l)}_{i,j} = \beta^{(l)} \quad \text{and}$$
$$\mathbf{c}^{(l)}_D \odot \mathbf{c}^{(l)}_{-z} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,\Gamma^{(l)}\,;\,\mathbf{v}^{(l)}\big).$$

Because $\mathbf{c}^{(l)}_{-z}\odot\mathbf{c}^{(l)}_{z} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,Z^{(l)}-Z^{(l)}\,;\,\mathbf{0}\big) = \mathbf{1}$ and because $\odot$ is associative, we have

$$\begin{aligned}\mathbf{c}^{(l)}_D &= \mathbf{c}^{(l)}_D \odot \mathbf{c}^{(l)}_{-z} \odot \mathbf{c}^{(l)}_{z}\\ &= \Big(\mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,\Gamma^{(l)}\,;\,\mathbf{v}^{(l)}\big)\Big)\\ &\quad\odot\Big(\mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,Z^{(l)}\,;\,\mathbf{0}\big)\Big)\\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,\Gamma^{(l)}+Z^{(l)}\,;\,\mathbf{v}^{(l)}\big).\end{aligned}$$

Thus, if we define, for all $l\in[\![1;N]\!]$, $i\in[\![1;n]\!]$ and $j\in[\![1;m]\!]$, $d^{(l)}_k = \Gamma^{(l)}_{i,j}+z_l$ where $k=(j-1)n+i$, the pair of vectors $\big(\mathbf{d}^{(l)},\mathbf{v}^{(l)}\big)\in\mathbb{F}^N_{p_\eta}\times\mathbb{F}^m_{p_\eta}$ is an oppening of the commit value $\mathbf{c}^{(l)}_D$.

(Step1.2) Using the definition of $\beta^{(l)}$ given by **Extractor 2** at line 7, previous results obtained in step **(Step1.1)** lead to

$$\prod_{k=1}^{N}\big(d^{(l)}_k - z_l\big) = \prod_{k=1}^{N}\big(y_l k + (x_l)^k - z_l\big),$$

which is a polynomial equation of degree N in z_l. By the *Schwartz-Zippel lemma*, we conclude the following equality of polynomials

$$\prod_{k=1}^{N}\big(d^{(l)}_k - X\big) = \prod_{k=1}^{N}\Big(y_l k + (x_l)^k - X\Big).$$

However, polynomials $\big(d^{(l)}_k - X\big)$ and $\Big(y_l k+(x_l)^k - X\Big)$ are irreductible (degree 1) and the decomposition in irreductible polynomials is unique. Consequently, there exists a permutation $\pi^{(l)}\in\mathfrak{S}_N$ such that

$$\forall\, k\in[\![1;N]\!],\ d^{(l)}_k = y_l\pi^{(l)}(k) + (x_l)^{\pi^{(l)}(k)}.$$

[1] Using line 9 of **Extractor 2**.

At this point, we have obtained an opening of commit value $\mathbf{c}^{(l)}_D$. It is not this commit value we want to open but $\mathbf{c}_A$. Recalls that commit value $\mathbf{c}^{(l)}_D$ is computed this way: $\mathbf{c}^{(l)}_D \overset{\text{def}}{=} (\mathbf{c}_A \uparrow y_l)\odot\mathbf{c}^{(l)}_B$. This is precisely why we also need to call extractor $\mathcal{E}_{\mathsf{MEA}}$ to obtain an opening of $\mathbf{c}^{(l)}_B$.

(Step1.3) By the *knowledge soundness* of the multi-exponentiation argument protocol (see Theorem B.2), we have

$$\forall\, l\in[\![1;N]\!],\ \mathbf{c}^{(l)}_B = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,B^{(l)}\,;\,\mathbf{t}^{(l)}\big) \quad \text{and}$$
$$C^{(l)} = \mathsf{Enc}_{\mathbb{CS}}\big(pk,1\,;\,\varrho^{(l)}\big)\cdot\prod_{k=1}^{N}\big(c'_k\big)^{b^{(l)}_k}$$

where, for $i\in[\![1;n]\!]$ and $j\in[\![1;m]\!]$, $b^{(l)}_{(j-1)n+i}\overset{\text{def}}{=}B^{(l)}_{i,j}$;

i.e. we have an opening for commit value $\mathbf{c}^{(l)}_B$. Then, for all $l\in[\![1;N]\!]$, as $\mathbf{c}^{(l)}_D = (\mathbf{c}_A\uparrow y_l)\odot\mathbf{c}^{(l)}_B$ with $y_l\neq 0$, properties over $\odot$ and $\uparrow$ lead to the following equality

$$\mathbf{c}_A = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck,\left(\frac{d^{(l)}_k - b^{(l)}_k}{y_l}\right)^{N}_{k=1}\,;\,\frac{1}{y_l}\big(\mathbf{v}^{(l)}-\mathbf{t}^{(l)}\big)\right).$$

Hence, for all $l,k\in[\![1;N]\!]$ and $i\in[\![1;m]\!]$, we define $\big(a^{(l)}_k,s^{(l)}_i\big)\in\mathbb{F}^2_{p_\eta}$ such that

$$d^{(l)}_k \overset{\text{def}}{=} y_l a^{(l)}_k + b^{(l)}_k \qquad\text{and}\qquad v^{(l)}_i \overset{\text{def}}{=} y_l s^{(l)}_i + t^{(l)}_i.$$

(Step1.4) Now, let us suppose just for a moment that we have:

$$\exists\, l,l'\in[\![1;N]\!],\ \mathbf{a}^{(l)}\neq\mathbf{a}^{(l')}.$$

But, by the previous point, the following property holds:

$$\begin{aligned}\mathbf{c}_A &= \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,\mathbf{a}^{(l)}\,;\,\overrightarrow{\varsigma}^{(l)}\big)\\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\big(ck,\mathbf{a}^{(l')}\,;\,\overrightarrow{\varsigma}^{(l')}\big).\end{aligned}$$

Thus, as the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$ is *computationally binding*, with overwhelming probability, we conclude a contradiction. Therefore, we have shown that the following property holds:

$$\forall\, l,l'\in[\![1;N]\!],\ \mathbf{a}^{(l)}=\mathbf{a}^{(l')}.$$

We denote this common value $\mathbf{a}\in\mathbb{F}^N_{p_\eta}$ and we have found an opening $\big(\mathbf{a},\overrightarrow{\varsigma}\big)\in\mathbb{F}^N_{p_\eta}\times\mathbb{F}^m_{p_\eta}$ *independent from challenges*

Protocol 1: 13-move *zero-knowledge* protocol $\mathbb{ZK}^{(6)}[\mathcal{R}_{\mathsf{SA}}^{\mathsf{BG}}]$ for the Bayer-Groth proof of shuffle

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

Private Input : A permutation $\pi \in \mathfrak{S}_N$ and a vector of random values $\mathbf{r} \xleftarrow{\$} \mathbb{F}_{p_\eta}^N$ such that $\mathbf{c}' = \mathsf{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\,\mathbf{r}) \odot \mathbf{c}_\pi$.

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{BG}}$ chooses a vector of random values $\overrightarrow{\varsigma} \xleftarrow{\$} \mathbb{F}_{p_\eta}^m$ and set $\mathbf{a} \leftarrow (\pi(i))_{i=1}^N \in \mathbb{F}_{p_\eta}^N$. Then, $\mathcal{P}_{\mathsf{BG}}$ computes the commit value $\mathbf{c}_A \leftarrow \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, \mathbf{a}\,;\,\overrightarrow{\varsigma}) \in \mathbb{G}_{p_\eta}^m$ and sends it to the verifier $\mathcal{V}_{\mathsf{BG}}$.

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

(3) **(Commit message)** $\mathcal{P}_{\mathsf{BG}}$ chooses a vector of random values $\mathbf{t} \xleftarrow{\$} \mathbb{F}_{p_\eta}^m$ and set $\mathbf{b} \leftarrow (x^{\pi(i)})_{i=1}^N \in \mathbb{F}_{p_\eta}^N$. Then, $\mathcal{P}_{\mathsf{BG}}$ computes the commit value $\mathbf{c}_B \leftarrow \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, \mathbf{b}\,;\,\mathbf{t}) \in \mathbb{G}_{p_\eta}^m$ and sends it to $\mathcal{V}_{\mathsf{BG}}$.

(4) **(Challenge message)** $\mathcal{V}_{\mathsf{BG}}$ chooses uniformly at random two challenges $y \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ and $z \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ then sends them back to $\mathcal{P}_{\mathsf{BG}}$.

(5-11) **(Product argument call)** Let $\mathbf{c}_{-z}$ be the commit value defined by $\mathbf{c}_{-z} \leftarrow \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, \underbrace{(-z, \ldots, -z)}_{N = nm \text{ times}}\,;\, \underbrace{\mathbf{0}}_{\in \mathbb{F}_{p_\eta}^m}) \in \mathbb{G}_{p_\eta}^m$. The prover $\mathcal{P}_{\mathsf{BG}}$ computes the commit value $\mathbf{c}_D \leftarrow (\mathbf{c}_A \uparrow y) \odot c_B \in \mathbb{G}_{p_\eta}^m$, the vector $\mathbf{d} \leftarrow y\mathbf{a} + \mathbf{b} \in \mathbb{F}_{p_\eta}^N$ and the vector of random values $\mathbf{v} \leftarrow y\overrightarrow{\varsigma} + \mathbf{t} \in \mathbb{F}_{p_\eta}^m$. Then, both prover $\mathcal{P}_{\mathsf{BG}}$ and verifier $\mathcal{V}_{\mathsf{BG}}$ engage in the 7-move *zero-knowledge* protocol $\mathbb{ZK}^{(3)}[\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}]$ for the relation $\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}$ with public parameter $\sigma_{\mathsf{PA}} = ck$, public statement $x_{\mathsf{PA}} = \left(\mathbf{c}_D \odot \mathbf{c}_{-z}, \prod_{i=1}^N (yi + x^i - z)\right)$, and private statement $w_{\mathsf{PA}} = (\mathbf{d} - \mathbf{z}, \mathbf{v})$. We denote by τ_{PA} the proof transcript obtained at the end of this 7-move protocol.

(11-13) **(Multi-exponentiation argument call)** $\mathcal{P}_{\mathsf{BG}}$ computes $\varrho \leftarrow -\langle \mathbf{r} \mid \mathbf{b} \rangle \in \mathbb{F}_{p_\eta}$ and sets $\mathbf{x} \leftarrow (x^i)_{i=1}^N \in \mathbb{F}_{p_\eta}^N$. Then, both prover $\mathcal{P}_{\mathsf{BG}}$ and verifier $\mathcal{V}_{\mathsf{BG}}$ engage in the Σ-protocol $\Sigma[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}]$ for the relation $\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}$ with public parameter $\sigma_{\mathsf{MEA}} = (ck, pk)$, public statement $x_{\mathsf{MEA}} = (\mathbf{c}', \mathbf{c} \circledast \mathbf{x}, \mathbf{c}_B)$, and private statement $w_{\mathsf{MEA}} = (\mathbf{b}, \mathbf{t}, \varrho)$. We denote by τ_{MEA} the proof transcript obtained at the end of this Σ-protocol.

(14) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{BG}}$ accepts if and only if properties $v_{\mathsf{PA}}^{\sigma_{\mathsf{PA}}, x_{\mathsf{PA}}}(\tau_{\mathsf{PA}})$ and $v_{\mathsf{MEA}}^{\sigma_{\mathsf{MEA}}, x_{\mathsf{MEA}}}(\tau_{\mathsf{MEA}})$ hold.

Extractor 2: Extractor $\mathcal{E}_{\mathsf{SA}}$ for the 13-move *zero-knowledge* protocol $\mathbb{ZK}^{(6)}[\mathcal{R}_{\mathsf{SA}}^{\mathsf{BG}}]$ of the Bayer-Groth shuffle argument

Input : A security parameter $\eta \in \mathbb{N}^*$. A natural number $N = nm \in \mathbb{N}^*$. A public parameter $(ck, pk) \in \mathbb{G}_{p_\eta}^{n+1} \times \mathcal{PK}_{\mathbb{CS}}$ for the Bayer-Groth shuffle relation $\mathcal{R}_{\mathsf{SA}}^{\mathsf{BG}}$. A statement $(\mathbf{c}, \mathbf{c}') \in (\mathbb{H}_{p_\eta}^N)^2$.

Blackbox access to : An adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{SA}}$.

1 **Begin extractor**

2 **calls $\mathcal{P}^*$ to get** $\mathbf{c}_A \in \mathbb{G}_{p_\eta}^m$; // State at the end of this line: $\mathbf{st}_1 \stackrel{\text{def}}{=} [(ck, pk)\,;\,(\mathbf{c}, \mathbf{c}')\,;\,\mathbf{c}_A]$

3 **rewinds $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{SA}}$ at state $\mathbf{st}_1$ for** $l = 1$ **to** N

4 **calls $\mathcal{V}_{\mathsf{SA}}$ to get** $x_l \xleftarrow{\$} \mathbb{F}_{p_\eta}^* \setminus \{x_i\}_{i=1}^{l-1}$;

5 **calls $\mathcal{P}^*$ to get** $\mathbf{c}_B^{(l)} \in \mathbb{G}_{p_\eta}^m$;

6 **calls $\mathcal{V}_{\mathsf{SA}}$ to get** $y_l, z_l \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$;

7 **computes**
$$\begin{cases} \mathbf{c}_D^{(l)} & \leftarrow & (\mathbf{c}_A \uparrow y_l) \odot \mathbf{c}_B^{(l)} \in \mathbb{G}_{p_\eta}^m \\ \mathbf{c}_{-z}^{(l)} & \leftarrow & \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, -Z^{(l)}\,;\,\mathbf{0}) \in \mathbb{G}_{p_\eta}^m \quad \text{where } Z^{(l)} \leftarrow (z_l)_{i=1}^N \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \\ \beta^{(l)} & \leftarrow & \prod_{k=1}^N (y_l k + (x_l)^k - z_l) \in \mathbb{F}_{p_\eta} \\ C^{(l)} & \leftarrow & \prod_{k=1}^N (c_k)^{(x_l)^k} \in \mathbb{H}_{p_\eta} \end{cases} ;$$

8 **calls $\mathcal{E}_{\mathsf{MEA}}$ with oracles $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{SA}}$ on inputs** $\left((ck, pk), \left((\mathbf{c}'_i)_{i=1}^m, C^{(l)}, \mathbf{c}_B^{(l)}\right)\right)$ **to get** $\left(B^{(l)}, \mathbf{t}^{(l)}, \varrho^{(l)}\right) \in \left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m \times \mathbb{F}_{p_\eta}^N\right)$;

9 **calls $\mathcal{E}_{\mathsf{PA}}$ with oracles $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{SA}}$ on inputs** $\left(ck, (\mathbf{c}_D^{(l)} \odot \mathbf{c}_{-z}^{(l)}, \beta^{(l)})\right)$ **to get** $\left(\Gamma^{(l)}, \mathbf{v}^{(l)}\right) \in \left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m\right)$;

10 **returns** $\tau_{\mathsf{SA}} \stackrel{\text{def}}{=} \left(\mathbf{c}_A, \left(x_l, \mathbf{c}_B^{(l)}, (y_l, z_l), \left(\mathbf{c}_D^{(l)}, \mathbf{c}_{-z}^{(l)}, \beta^{(l)}, C^{(l)}\right), \left(\Gamma^{(l)}, \mathbf{v}^{(l)}\right), \left(B^{(l)}, \mathbf{t}^{(l)}, \varrho^{(l)}\right)\right)_{l=1}^N\right)$.

$(x_l)_{l=1}^N$ of the commit value $\mathbf{c}_A$:

$$\mathbf{c}_A = \mathrm{Com}_{\mathrm{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \mathbf{a}\,;\, \overrightarrow{\varsigma}\right).$$

(**Step1**.5) Thanks to step (**Step1**.2), step (**Step1**.3) and step (**Step1**.4), we obtain the following equalities

$$\forall\, l,k \in [\![1;N]\!],\ y_l \pi^{(l)}(k) + (x_l)^{\pi^{(l)}(k)} = y_l a_k + b_k^{(l)}.$$

Actually, these equalities are N polynomial equations of degree 1 in y_l, for each $l \in [\![1;N]\!]$. Thus, by N^2 applications of the *Schwartz-Zippel lemma*, we obtain

$$\forall\, l,k \in [\![1;N]\!],\ a_k = \pi^{(l)}(k) \text{ and } b_k^{(l)} = (x_l)^{\pi^{(l)}(k)}.$$

Consequently, as the sequence $(a_k)_{k=1}^N$ is *independent from challenges* $(x_l)_{l=1}^N$, so it goes for the permutation sequence $\left(\pi^{(l)}\right)_{l=1}^n$, we denote by π this common value. Putting all together, we conclude the following property:

$$\boxed{\begin{array}{l}\exists\, \pi \in \mathfrak{S}_N,\ \exists\, \overrightarrow{\varsigma} \in \mathbb{F}_{p_\eta}^m,\\ \quad \mathbf{c}_A = \mathrm{Com}_{\mathrm{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, (\pi(k))_{k=1}^N\,;\, \overrightarrow{\varsigma}^{(l)}\right).\end{array}}$$

(Step 2) – Construct[2] the vector of random values r.

(**Step2**.1) We have seen in step (**Step1**.3) that the following property holds:

$$\forall\, l \in [\![1;N]\!],\ C^{(l)} = \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho^{(l)}) \cdot \prod_{k=1}^{N} \left(c'_k\right)^{b_k^{(l)}}. \qquad (\Phi)$$

Besides, step (**Step1**.5) gives us the following property:

$$\forall\, k,l \in [\![1;N]\!],\ b_k^{(l)} = (x_l)^{\pi(k)}. \qquad (\Psi)$$

Thus, Eq. (Φ) becomes, by using Eq. (Ψ) and the definition of $C^{(l)}$ given by **Extractor 2** at line 7, the following property:

$$\begin{array}{rl}\forall\, l \in [\![1;N]\!], & \displaystyle\prod_{k=1}^{N} (c_k)^{(x_l)^k} = \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho^{(l)}) \cdot \prod_{k=1}^{N} \left(c'_k\right)^{(x_l)^{\pi(k)}}\\ \textit{i.e.} & \displaystyle\prod_{k=1}^{N} (c_k)^{(x_l)^k} = \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho^{(l)}) \cdot \prod_{k=1}^{N} \left(c'_{\pi^{-1}(k)}\right)^{(x_l)^k}\end{array} \qquad (\Upsilon)$$

(**Step2**.2) Let $X \in \mathrm{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$ be the matrix defined by

$$X \overset{\text{def}}{=} \begin{pmatrix} x_1 & x_2 & \cdots & x_N \\ x_1^2 & x_2^2 & \cdots & x_N^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^N & x_2^N & \cdots & x_N^N \end{pmatrix}.$$

We notice that this matrix X is in fact a Vandermonde matrix of parameters the challenges $(x_l)_{l=1}^N$. Each challenge of the sequence $(x_l)_{l=1}^N$ is generated *independently and uniformly at random* in $\mathbb{F}_{p_\eta}^*$ (challenges are computed by the **honest** verifier $\mathcal{V}_{\mathrm{BG}}$). In particular, with *overwhelming probability*[3], the following property holds:

$$\bigwedge_{l=1}^{N-1} \bigwedge_{p=l+1}^{N} (x_l \neq x_p).$$

Meaning that the Vandermonde matrix X is invertible.

(**Step2**.3) On another hand, we denote, for all $l \in [\![1;N]\!]$, $\mathbf{X}^{(l)}$ the l-th column of the matrix X, we notice that Eq. (Υ) becomes

$$\forall\, i \in [\![1;N]\!],\ \mathbf{c} \circledast \mathbf{X}^{(l)} = \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho^{(l)}) \cdot \left(\mathbf{c}'_{\pi^{-1}} \circledast \mathbf{X}^{(l)}\right).$$

Thus[4], previous equation becomes

$$\mathbf{c} \circledast X = \left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \overrightarrow{\varrho})\right) \odot \left(\mathbf{c}'_{\pi^{-1}} \circledast X\right),$$

where $\overrightarrow{\varrho} \overset{\text{def}}{=} \left(\varrho^{(l)}\right)_{l=1}^N \in \mathbb{F}_{p_\eta}^N$. As

- X is invertible,
- $(\mathbf{c} \circledast X) \circledast X^{-1} = \mathbf{c} \circledast \left(XX^{-1}\right) = \mathbf{c} \circledast I_N$, [5] and
- $\mathbf{c} \circledast I_N = \mathbf{c}$, [6]

we conclude

$$\mathbf{c} = \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \overrightarrow{\varrho})\right) \odot \left(\mathbf{c}'_{\pi^{-1}} \circledast X\right)\right) \circledast X^{-1}$$

Next, because the following property

$$\forall\, n \in \mathbb{N}^*,\ \forall\, \mathbf{x}, \mathbf{y} \in \mathbb{H}_{p_\eta}^n,\ \forall\, M \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta}),\quad (\mathbf{x} \odot \mathbf{y}) \circledast M = (\mathbf{x} \circledast M) \odot (\mathbf{y} \circledast M)$$

[2] Using line 8 of **Extractor 2**.

[3]

Comment [MC1]: Surely we have to use the property transfer under adversarial selection here!

[4] Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x} \in \mathbb{H}_{p_\eta}$ be a ciphertexts vector of dimension n and let $M \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be a square matrix of dimension $n \times n$. We extend the function $\circledast : \mathbb{H}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \longrightarrow \mathbb{H}_{p_\eta}$ for matrix with coefficients in $\mathbb{F}_{p_\eta}$ as follows:

$$\mathbf{x} \circledast M \overset{\text{def}}{=} \left(\mathbf{x} \circledast \mathbf{M}^{(j)}\right)_{j=1}^n \in \mathbb{H}_{p_\eta}^n,$$

where $\mathbf{M}^{(j)}$ is the j-th column of M.

[5] Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x} \in \mathbb{H}_{p_\eta}^n$ be a ciphertexts vector of dimension n and let $A, B \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be two square matrix of dimensions $n \times n$. By definition of $\circledast$, we have

$$\begin{aligned}(\mathbf{x} \circledast A) \circledast B &= \left((\mathbf{x} \circledast A) \circledast \mathbf{B}^{(j)}\right)_{j=1}^n = \left(\prod_{k=1}^n (\mathbf{x} \circledast A)_k^{b_{k,j}}\right)_{j=1}^n\\ &= \left(\prod_{k=1}^n \left(\mathbf{x} \circledast \mathbf{A}^{(k)}\right)^{b_{k,j}}\right)_{j=1}^n = \left(\prod_{k=1}^n \left(\prod_{i=1}^n (x_i)^{a_{i,k}}\right)^{b_{k,j}}\right)_{j=1}^n\\ &= \left(\prod_{k=1}^n \prod_{i=1}^n (x_i)^{a_{i,k}b_{k,j}}\right)_{j=1}^n = \left(\prod_{i=1}^n (x_i)^{\sum_{k=1}^n a_{i,k}b_{k,j}}\right)_{j=1}^n\\ &= \left(\mathbf{x} \circledast (AB)^{(j)}\right)_{j=1}^n = \mathbf{x} \circledast (AB).\end{aligned}$$

□

[6] Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x} \in \mathbb{H}_{p_\eta}^n$ be a ciphertexts vector of dimension n and let $I_n \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be the identity square matrix of dimensions $n \times n$: for all $i, j \in [\![1;n]\!]$, $(I_n)_{i,j} = \delta_{ij}$ the Kroenecker symbol. By definition of $\circledast$, we have

$$\mathbf{x} \circledast I_N = \left(\mathbf{x} \circledast \mathbf{I}_N^{(i)}\right)_{i=1}^N = \left(\prod_{j=1}^n (x_j)^{\delta_{ji}}\right)_{i=1}^N = (x_i)_{i=1}^N = \mathbf{x}.$$

□

holds[7], it leads to

$$\mathbf{c} = \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \overrightarrow{\varrho})\right) \circledast X^{-1}\right) \odot \left(\left(\mathbf{c}'_{\pi^{-1}} \circledast X\right) \circledast X^{-1}\right)$$
$$= \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \overrightarrow{\varrho})\right) \circledast X^{-1}\right) \odot \mathbf{c}'_{\pi^{-1}}.$$

Finally, we use:
(1) the following identity[8]

$$\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \overrightarrow{\varrho})\right) \circledast X^{-1} = \mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{1} \circledast X^{-1}\,;\, (X^{-1})^T \cdot \overrightarrow{\varrho}\right),$$

(2) and the property[9] $\mathbf{1} \circledast X^{-1} = \mathbf{1}$,
to obtain

$$\mathbf{c} = \mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{1}\,;\, \left(X^{-1}\right)^T \cdot \overrightarrow{\varrho}\right) \odot \mathbf{c}'_{\pi^{-1}}. \qquad (\Upsilon')$$

(Step2.4) Now, we apply both sides of the previous identity the function ψ_N defined as follows

$$\begin{array}{rccl} \psi_N : & \mathbb{H}_{p_\eta}^N & \longrightarrow & \mathbb{H}_{p_\eta} \\ & \mathbf{x} & \longmapsto & \mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{1}\,;\, -\left(X^{-1}\right)^T \cdot \overrightarrow{\varrho}\right) \odot \mathbf{x}. \end{array}$$

[7]Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x}, \mathbf{y} \in \mathbb{H}_{p_\eta}^n$ be two ciphertexts vectors of dimension n, and let $M \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be a matrix of dimensions $n \times n$. By definition of $\circledast$ and $\odot$, we have

$$(\mathbf{x} \odot \mathbf{y}) \circledast M = \left((x_i y_i)_{i=1}^n\right) \circledast M = \left(\left((x_i y_i)_{i=1}^n\right) \circledast \mathbf{M}^{(j)}\right)_{j=1}^n$$
$$= \left(\prod_{i=1}^n (x_i y_i)^{m_{i,j}}\right)_{j=1}^n = \left(\left(\prod_{i=1}^n (x_i)^{m_{i,j}}\right) \cdot \left(\prod_{i=1}^n (y_i)^{m_{i,j}}\right)\right)_{j=1}^n$$
$$= \left((\mathbf{x} \circledast \mathbf{M}^{(j)}) \cdot (\mathbf{y} \circledast \mathbf{M}^{(j)})\right)_{j=1}^n = (\mathbf{x} \circledast M) \odot (\mathbf{y} \circledast M). \qquad \square$$

[8]Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x} \in \mathbb{G}_{p_\eta}^n$ and $\mathbf{y} \in \mathbb{F}_{p_\eta}^n$ be two vectors, both of dimension n. Let $M \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be a square matrix of dimensions $n \times n$. By definition of $\circledast$ and because $\mathbb{CS}$ is homomorphic, we have

$$\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{x}\,;\, \mathbf{y})\right) \circledast M = \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{x}\,;\, \mathbf{y})\right) \circledast \mathbf{M}^{(j)}\right)_{j=1}^n$$
$$= \left(\prod_{i=1}^n \left(\mathrm{Enc}_{\mathbb{CS}}(pk, x_i\,;\, y_i)\right)^{m_{i,j}}\right)_{j=1}^n$$
$$= \left(\prod_{i=1}^n \left(\mathrm{Enc}_{\mathbb{CS}}\left(pk, (x_i)^{m_{i,j}}\,;\, y_i m_{i,j}\right)\right)\right)_{j=1}^n$$
$$= \left(\mathrm{Enc}_{\mathbb{CS}}\left(pk, \prod_{i=1}^n (x_i)^{m_{i,j}}\,;\, \sum_{i=1}^n y_i m_{i,j}\right)\right)_{j=1}^n$$
$$= \left(\mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{x} \circledast \mathbf{M}^{(j)}\,;\, (M^T \cdot \mathbf{y})^{(j)}\right)\right)_{j=1}^n$$
$$= \mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{x} \circledast M\,;\, M^T \cdot \mathbf{y}\right). \qquad \square$$

[9]Let $n \in \mathbb{N}^*$ be a natural number. We denote by $\mathbf{1} \in \mathbb{H}_{p_\eta}^n$ the ciphertexts vector of dimension n such that, for all $i \in [\![1; n]\!]$, $\mathbf{1}_i \overset{\text{def}}{=} 1$. Let $M \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be a square matrix of dimensions $n \times n$. By definition of $\circledast$, we have

$$\mathbf{1} \circledast M = \left(\mathbf{1} \circledast M^{(j)}\right)_{j=1}^n = \left(\prod_{i=1}^N 1^{m_{i,j}}\right)_{j=1}^n = \mathbf{1}. \qquad \square$$

Thus, it leads to[10][11]

$$\mathrm{Enc}_{\mathbb{CS}}\left(pk, \mathbf{1}\,;\, -\left(X^{-1}\right)^T \cdot \overrightarrow{\varrho}\right) \odot \mathbf{c} = \mathbf{c}'_{\pi^{-1}}.$$

By an index change[12], we finally obtain the following equation[13]

$$\boxed{\begin{array}{l} \mathbf{c}' = \mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \mathbf{r}) \odot \mathbf{c}_\pi \\ \quad \text{with} \quad \mathbf{r} \overset{\text{def}}{=} -\left(\left(X^{-1}\right)^T \cdot \overrightarrow{\varrho}\right)_\pi \in \mathbb{F}_{p_\eta}^N. \end{array}}$$

Results obtained in step **(Step 1)** and step **(Step 2)**, give us the following result, proving that, with *overwhelming probability*, we have successfully extract a witness $w \overset{\text{def}}{=} (\pi, \mathbf{r}) \in \mathfrak{S}_N \times \mathbb{F}_{p_\eta}^N$ such

[10]Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x}, \mathbf{y} \in \mathbb{G}_{p_\eta}^n$ and $\mathbf{r}, \overrightarrow{\varsigma} \in \mathbb{F}_{p_\eta}^n$ be four vectors, all of dimension n. By definition of $\odot$ and because $\mathbb{CS}$ is homomorphic, we have

$$\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{x}\,;\, \mathbf{r})\right) \odot \left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{y}\,;\, \overrightarrow{\varsigma})\right)$$
$$= \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, x_i\,;\, r_i)\right) \cdot \left(\mathrm{Enc}_{\mathbb{CS}}(pk, y_i\,;\, s_i)\right)\right)_{i=1}^n$$
$$= \left(\mathrm{Enc}_{\mathbb{CS}}\left(pk, x_i \cdot y_i\,;\, r_i + s_i\right)\right)_{i=1}^n$$
$$= \mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{x} \odot \mathbf{y}\,;\, \mathbf{r} + \overrightarrow{\varsigma}). \qquad \square$$

Now, let $\mathbf{m} \in \mathbb{G}_{p_\eta}^n$ be a vector of dimension n. We denote by $\mathbf{0} \in \mathbb{F}_{p_\eta}^n$ the vector of dimension n defined by, for all $i \in [\![1; n]\!]$, $\mathbf{0}_i = 0$. By definition of $\mathrm{Enc}_{\mathbb{CS}}$, we have

$$\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{m}\,;\, \mathbf{0}) = \left(\mathrm{Enc}_{\mathbb{CS}}(pk, m_i\,;\, 0)\right)_{i=1}^n = (1)_{i=1}^n = \mathbf{1}. \qquad \square$$

[11]Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \mathbb{H}_{p_\eta}^n$ be three vectors of dimension n. By definition of $\odot$, we have

$$\mathbf{x} \odot (\mathbf{y} \odot \mathbf{z}) = \mathbf{x} \odot (y_i \cdot z_i)_{i=1}^n = (x_i \cdot y_i \cdot z_i)_{i=1}^n.$$

Thus, by associativity of the internal law $\cdot : \mathbb{H}_{p_\eta} \times \mathbb{H}_{p_\eta} \longrightarrow \mathbb{H}_{p_\eta}$, so it goes for the function $\odot : \mathbb{H}_{p_\eta}^n \times \mathbb{H}_{p_\eta}^n \longrightarrow \mathbb{H}_{p_\eta}^n$.
Besides, as 1 is the neutral element of the group $(\mathbb{H}_{p_\eta}, \cdot)$, so it goes with $\mathbf{1}$ for the group $(\mathbb{H}_{p_\eta}^n, \odot)$.

$\square$

[12]Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x}, \mathbf{y} \in \mathbb{H}_{p_\eta}^n$ be two ciphertexts vectors of dimension n. Let $\sigma \in \mathfrak{S}_n$ be a permutation. Let $\mathbf{z} \in \mathbb{H}_{p_\eta}^n$ be the permuted result of the $\odot$ product of previous vectors: $\mathbf{z}_\sigma \overset{\text{def}}{=} \mathbf{x} \odot \mathbf{y}$. On one hand, we have

$$(\mathbf{z}_\sigma)_{\sigma^{-1}} = \left((z_{\sigma(i)})_{i=1}^n\right)_{\sigma^{-1}} = \left(z_{\sigma^{-1}(\sigma(i))}\right)_{i=1}^n = \mathbf{z}.$$

On another hand, we have

$$(\mathbf{x} \odot \mathbf{y})_\sigma = \left((x_i \cdot y_i)_{i=1}^n\right)_\sigma = \left(x_{\sigma(i)} \cdot y_{\sigma(i)}\right)_{i=1}^n = \mathbf{x}_\sigma \odot \mathbf{y}_\sigma.$$

Now, let $\mathbf{m} \in \mathbb{G}_{p_\eta}^n$ and $\mathbf{r} \in \mathrm{Mat}_n(\mathbb{F}_{p_\eta})$ be two vectors of dimension n. We have

$$\left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{m}\,;\, \mathbf{r})\right)_\sigma = \left(\left(\mathrm{Enc}_{\mathbb{CS}}(pk, m_i\,;\, r_i)\right)_{i=1}^n\right)_\sigma = \left(\mathrm{Enc}_{\mathbb{CS}}(pk, m_{\sigma(i)}\,;\, r_{\sigma(i)})\right)_{i=1}^n$$
$$= \mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{m}_\sigma\,;\, \mathbf{r}_\sigma).$$

Thus, we finally obtain

$$\mathbf{z} = (\mathbf{z}_\sigma)_{\sigma^{-1}} = \left(\mathrm{Enc}_{\mathbb{CS}}(pk, \mathbf{m}_{\sigma^{-1}}\,;\, \mathbf{r}_{\sigma^{-1}})\right) \odot \mathbf{y}_{\sigma^{-1}}. \qquad \square$$

[13]More precisely, with $X^{-1} \overset{\text{def}}{=} (\tilde{x}_{i,j})_{i,j=1}^N \in \mathrm{Mat}_N(\mathbb{F}_{p_\eta})$ given by **the computation of the inverse of the Vandermonde matrix** X (see [2]) with coefficients the sequence of challenges $(x_l)_{l=1}^N$, we have

$$\forall\, j \in [\![1; N]\!],\ r_j \overset{\text{def}}{=} -\sum_{l=1}^N \varrho^{(l)} \cdot \tilde{x}_{l,\pi(j)}.$$

that $(\sigma, \chi, w) \in \mathcal{R}_{\mathsf{SA}}^{\mathsf{BG}}$.

$$\exists\, \pi \in \mathfrak{S}_N,\ \exists\, \mathbf{r} \in \mathbb{F}_{p_\eta}^N,\quad \mathbf{c}' = \mathsf{Enc}_{\mathbb{CS}}(pk, \mathbf{1}\,;\, \mathbf{r}) \odot \mathbf{c}_\pi.$$

Proof step → / **↓ Property**	step (Step1.1)	step (Step1.2)	step (Step1.3)	step (Step1.4)	step (Step1.5)	step (Step2.2)
Knowledge soundness	$N \times \mathcal{E}_{\mathsf{PA}}$		$N \times \mathcal{E}_{\mathsf{MEA}}$			
***Binding* of commitment scheme**				$\times 1$		
Schwartz-Zippel		$\times 1$			$\times N^2$	
Property transfer under adversarial selection						Yes
Extractor uses *rewinding*?	Yes (N witnesses – 2 witnesses each)					

Table 1: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Shuffle Argument protocol

□

B.2 Multi-exponentiation argument protocol

We define

$$\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}} \subseteq \underbrace{\left(\mathbb{G}_{p_\eta}^{n+1} \times \mathcal{PK}_{\mathbb{CS}}\right)}_{\text{Public parameter set}} \times \underbrace{\left((\mathbb{H}_{p_\eta}^{n})^m \times \mathbb{H}_{p_\eta} \times \mathbb{G}_{p_\eta}^{m}\right)}_{\text{Statement set}} \times \underbrace{\left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}), \mathbb{F}_{p_\eta}^{m}, \mathbb{F}_{p_\eta}\right)}_{\text{Witness set}}$$

to be the *multi-exponentiation relation* defined by

$$\left((ck, pk), \left((\mathbf{c}_i')_{i=1}^m, C, \mathbf{c}_B\right), \left(B, \mathbf{t}, \varrho\right)\right) \in \mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}} \overset{\text{def}}{\iff} \begin{cases} \mathbf{c}_B = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, B\,;\, \mathbf{t}) \\ C = \mathsf{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho) \cdot \prod_{i=1}^{m} \mathbf{c}_i' \circledast \mathbf{b}_i \end{cases}$$

Hence, we define a Σ-protocol for the relation of multi-exponentiation $\Sigma\left[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}\right]$ to be the protocol defined as follows in **Protocol 3**.

Theorem B.2 (Knowledge soundness of $\Sigma\left[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}\right]$). *The Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}\right]$ for the multi-exponentiation relation $\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}$ is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\mathsf{MEA}}$ for the Bayer-Groth multi-exponentiation argument to be the algorithm defined as follows in **Extractor 4**.

Let $n, m \in \mathbb{N}^*$ be two natural numbers. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time and deterministic adversarial prover. Let $\sigma = (ck, pk) \leftarrow \mathcal{I}_{\mathsf{MEA}}(\eta)$ be an honest public parameter for the multi-exponentiation relation $\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, \sigma)$ be an adversarial statement where

$$\chi \overset{\text{def}}{=} \left((\mathbf{c}_i')_{i=1}^m, C, \mathbf{c}_B\right) \in \left(\mathbb{H}_{p_\eta}^n\right)^m \times \mathbb{H}_{p_\eta} \times \mathbb{G}_{p_\eta}^m.$$

Then, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\mathsf{MEA}}$ on inputs σ and χ with access to $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{MEA}}$ and obtains $\tau_{\mathsf{MEA}} \overset{\text{def}}{=} \left(\mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}},\, \mathcal{P}^*}}^{\sigma,\, \chi}(x_l)\right)_{l=1}^{2m}$.

Let $l \in [\![1; 2m]\!]$ be an index. We denote by

- $\alpha \overset{\text{def}}{=} \left(c_{B_0}, (c_{F_k})_{k=0}^{2m-1}, (E_k)_{k=0}^{2m-1}\right) \in \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}^{2m} \times \mathbb{H}_{p_\eta}^{2m}$ the first message ; and
- $\mathfrak{d}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}},\, \mathcal{P}^*}(\alpha, \tilde{x}_l) \overset{\text{def}}{=} \left(\mathbf{b}^{(l)}, t^{(l)}, f^{(l)}, \varsigma^{(l)}, \tau^{(l)}\right) \in \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}$ the response message on challenge $\tilde{x}_l$.

This way, we have the following property

$$\forall\, l \in [\![1; 2m]\!],\ \begin{cases} \bullet\ \mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}},\, \mathcal{P}^*}}^{\sigma,\, \chi}(\tilde{x}_l) = \left\langle \left(c_{B_0}, (c_{F_k})_{k=0}^{2m-1}, (E_k)_{k=0}^{2m-1}\right), \tilde{x}_l, \left(\mathbf{b}^{(l)}, t^{(l)}, f^{(l)}, \varsigma^{(l)}, \tau^{(l)}\right)\right\rangle \\ \bullet\ v_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}}^{\sigma,\, \chi}\left(\mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}},\, \mathcal{P}^*}}^{\sigma,\, \chi}(\tilde{x}_l)\right) = 1. \end{cases}$$

By definition of the Bayer-Groth multi-exponentiation argument protocol, as the proof transcripts are valid, for all $l \in [\![1; 2m]\!]$, we have

$$c_{F_m} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, 0\,;\, 0) \quad \text{and} \quad E_m = C \qquad (\mathcal{H}_1)$$

$$c_{B_0} \cdot \left(\mathbf{c}_B \circledast \tilde{\mathbf{x}}^{(l)}\right) = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}(ck, \mathbf{b}^{(l)}\,;\, t^{(l)}) \qquad (\mathcal{H}_2^{(l)})$$

$$c_{F_0} \cdot \prod_{k=1}^{2m-1} c_{F_k}^{(\tilde{x}_l)^k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, f^{(l)}\,;\, \varsigma^{(l)}) \qquad (\mathcal{H}_3^{(l)})$$

$$E_0 \cdot \prod_{k=1}^{2m-1} E_k^{(\tilde{x}_l)^k} = \mathsf{Enc}_{\mathbb{CS}}(pk, g^{f^{(l)}}\,;\, \tau^{(l)}) \cdot \prod_{i=1}^{m} \left(\mathbf{c}_i' \circledast \left((\tilde{x}_l)^{m-i}\mathbf{b}^{(l)}\right)\right) \qquad (\mathcal{H}_4^{(l)})$$

(Step 1) – Get an opening of commit values $(c_{B_k})_{k=0}^m$

(Step1.1) We define the matrix $\tilde{X}_B \in \mathsf{Mat}_{m+1}(\mathbb{F}_{p_\eta})$ by

$$\tilde{X}_B \overset{\text{def}}{=} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \tilde{x}_1 & x_2 & \cdots & \tilde{x}_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_1^m & \tilde{x}_2^m & \cdots & \tilde{x}_{m+1}^m \end{pmatrix}$$

which is an invertible transposed Vandermonde matrix because, with *overwhelming probability*, the following property holds:

$$\bigwedge_{l=1}^{m} \bigwedge_{p=l+1}^{m+1} (\tilde{x}_l \neq \tilde{x}_p).$$

(Step1.2) We define the following quantities

- $B_{\tilde{x}} \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})$ the matrix with n lines and $(m+1)$ columns where columns of $B_{\tilde{x}}$ are given by vectors $\mathbf{b}^{(l)}$ for all $l \in [\![1; m+1]\!]$. More precisely, we have

$$\forall\, i \in [\![1; n]\!],\ \forall\, l \in [\![1; m+1]\!],\ \left(B_{\tilde{x}}\right)_{i,l} \overset{\text{def}}{=} \left(\mathbf{b}^{(l)}\right)_i.$$

Protocol 3: Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}\right]$ for the Bayer-Groth multi-exponentiation argument

Public Input : Two natural numbers $n, m \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{n+1}$ for the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$. A public key $pk \in \mathcal{PK}_{\mathbb{CS}}$ of the cryptosystem $\mathbb{CS}$. A list of ciphertexts vectors $(\mathbf{c}'_i)_{i=1}^m \in (\mathbb{H}_{p_\eta}^n)^m$, a ciphertext $C \in \mathbb{H}_{p_\eta}$ and a commit value $\mathbf{c}_B \in \mathbb{G}_{p_\eta}^m$.

Private Input : A matrix $B = (\mathbf{b}_i)_{i=1}^m \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$, a vector of random values $\mathbf{t} \xleftarrow{\$} \mathbb{F}_{p_\eta}^m$ and a random value $\varrho \xleftarrow{\$} \mathbb{F}_{p_\eta}$ such that $\mathbf{c}_B = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, B\,;\,\mathbf{t})$, and $C = \mathsf{Enc}_{\mathbb{CS}}(pk, 1\,;\,\varrho) \prod_{i=1}^m \mathbf{c}'_i \circledast \mathbf{b}_i$.

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{MEA}}$ chooses a vector of random values $\mathbf{b}_0 \xleftarrow{\$} \mathbb{F}_{p_\eta}^n$, a random value $t_0 \xleftarrow{\$} \mathbb{F}_{p_\eta}$, and, for all $i \in [\![0; 2m-1]\!]$, three random values $f_i, s_i, \tau_i \xleftarrow{\$} \mathbb{F}_{p_\eta}$. Then, the prover sets $f_m, s_m \leftarrow 0 \in \mathbb{F}_{p_\eta}$ and $\tau_m \leftarrow \varrho \in \mathbb{F}_{p_\eta}$. $\mathcal{P}_{\mathsf{MEA}}$ computes $c_{B_0} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}(ck, \mathbf{b}_0\,;\,t_0) \in \mathbb{G}_{p_\eta}$, and, for all $k \in [\![0; 2m-1]\!]$, $c_{F_k} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, f_k\,;\,s_k) \in \mathbb{G}_{p_\eta}$ and $E_k \leftarrow \mathsf{Enc}_{\mathbb{CS}}(pk, g^{f_k}\,;\,\tau_k) \cdot \prod_{i=1}^m \mathbf{c}'_i \circledast \mathbf{b}_{(k-m)+i} \in \mathbb{H}_{p_\eta}$. Finally, $\mathcal{P}_{\mathsf{MEA}}$ sends to $\mathcal{V}_{\mathsf{MEA}}$ values $\left(c_{B_0}, (c_{F_i})_{i=0}^{2m-1}, (E_i)_{i=0}^{2m-1}\right)$.

(2) **(Challenge message)** $\mathcal{V}_{\mathsf{MEA}}$ chooses uniformly at random a challenge $\tilde{x} \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ and sends it to $\mathcal{P}_{\mathsf{MEA}}$.

(3) **(Response message)** Let $\tilde{\mathbf{x}}$ be the vector defined by $\tilde{\mathbf{x}} \leftarrow (\tilde{x}^i)_{i=1}^m \in \mathbb{F}_{p_\eta}^m$. The prover $\mathcal{P}_{\mathsf{MEA}}$ computes values $\mathbf{b} \leftarrow \mathbf{b}_0 + B \cdot \tilde{\mathbf{x}} \in \mathbb{F}_{p_\eta}^n$, $t \leftarrow t_0 + \langle \mathbf{t} \mid \tilde{\mathbf{x}} \rangle \in \mathbb{F}_{p_\eta}$, $f \leftarrow \sum_{k=0}^{2m-1} f_k \tilde{x}^k \in \mathbb{F}_{p_\eta}$, $\varsigma \leftarrow \sum_{k=0}^{2m-1} s_k \tilde{x}^k \in \mathbb{F}_{p_\eta}$, and $\tau \leftarrow \sum_{k=0}^{2m-1} \tau_k \tilde{x}^k \in \mathbb{F}_{p_\eta}$. Then, $\mathcal{P}_{\mathsf{MEA}}$ sends to the verifier values $(\mathbf{b}, t, f, \varsigma, \tau)$.

(4) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{MEA}}$ accepts if and only if the following equations hold

$$c_{F_m} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, 0\,;\,0), \quad E_m = C, \quad c_{B_0}(\mathbf{c}_B \circledast \tilde{\mathbf{x}}) = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}(ck, \mathbf{b}\,;\,t), \quad c_{F_0} \prod_{k=1}^{2m-1} c_{F_k}^{\tilde{x}^k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, f\,;\,\varsigma),$$

$$\text{and} \quad E_0 \prod_{k=1}^{2m-1} E_k^{\tilde{x}^k} = \mathsf{Enc}_{\mathbb{CS}}(pk, g^f\,;\,\tau) \prod_{i=1}^m \mathbf{c}'_i \circledast (\tilde{x}^{m-i}\mathbf{b}).$$

Extractor 4: Extractor $\mathcal{E}_{\mathsf{MEA}}$ for the Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}\right]$ of the Bayer-Groth multi-exponentiation argument

Input : A security parameter $\eta \in \mathbb{N}^*$. Two natural numbers $n, m \in \mathbb{N}^*$. A public parameter $\sigma \stackrel{\text{def}}{=} (ck, pk) \in \mathbb{G}_{p_\eta}^{n+1} \times \mathcal{PK}_{\mathbb{CS}}$ for the Bayer-Groth multi-exponentiation relation $\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}$. A statement $\chi \stackrel{\text{def}}{=} \left((\mathbf{c}'_i)_{i=1}^m, C, \mathbf{c}_B\right) \in \left(\mathbb{H}_{p_\eta}^n\right)^m \times \mathbb{H}_{p_\eta} \times \mathbb{G}_{p_\eta}^m$.

Blackbox access to : A deterministic adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{MEA}}$.

1 **Begin extractor**

2 **calls $\mathcal{P}^*$ to get** $\alpha \stackrel{\text{def}}{=} \left(c_{B_0}, (c_{F_i})_{i=0}^{2m-1}, (E_i)_{i=0}^{2m-1}\right) \in \left(\mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}^{2m} \times \mathbb{H}_{p_\eta}^{2m}\right)$;

3 // State at this point: $\mathbf{st}_1 \stackrel{\text{def}}{=} \left[(ck, pk)\,;\,\left((\mathbf{c}'_i)_{i=1}^m, C, \mathbf{c}_B\right)\,;\,\left(c_{B_0}, (c_{F_i})_{i=0}^{2m-1}, (E_i)_{i=0}^{2m-1}\right)\right]$.

4 **rewinds $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{MEA}}$ at state $\mathbf{st}_1$ and begins with** $l \leftarrow 1 \in \mathbb{N}$

5 **calls $\mathcal{V}_{\mathsf{MEA}}$ to get** $\tilde{x}_l \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$;

6 **calls $\mathcal{P}^*$ to get** $z_l \leftarrow \mathfrak{z}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}, \mathcal{P}^*}(\alpha, \tilde{x}_l) \in \left(\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}\right)$;

7 **if** $v_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}}^{\sigma,\chi}\left(\mathsf{tr}_{\alpha, \mathfrak{z}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{\sigma,\chi}(\tilde{x}_l)\right)$ **and** $\bigwedge_{i=1}^{l-1} \bigwedge_{j=i+1}^{l} (\tilde{x}_i \neq \tilde{x}_j)$ **then** $l \leftarrow l + 1$;

8 **until** $l > 2m$; // i.e. *until $2m$ valid proof transcripts with pairwise distinct challenges are obtained.*

9 **returns** $\tau_{\mathsf{MEA}} \stackrel{def}{=} \left(\mathsf{tr}_{\alpha, \mathfrak{z}_{\mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{\sigma,\chi}(\tilde{x}_l)\right)_{l=1}^{2m}$.

- $\mathbf{t}_{\tilde{x}} \in \mathbb{F}_{p_\eta}^{m+1}$ the vector defined by $\mathbf{t}_{\tilde{x}} \overset{\text{def}}{=} (t^{(l)})_{l=1}^{m+1}$.

By properties of the operator $\circledast$[14], we have

$$\begin{aligned}(c_{B_0},\dots,c_{B_m}) &= (c_{B_0},\dots,c_{B_m}) \circledast (\tilde{X}_B\tilde{X}_B^{-1}) \\ &\qquad \textit{see footnote 6} \\ &= \left((c_{B_0},\dots,c_{B_m}) \circledast \tilde{X}_B\right) \circledast \tilde{X}_B^{-1} \\ &\qquad \textit{see footnote 5} \\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})}\left(ck, B_{\tilde{x}}\,;\,\mathbf{t}_{\tilde{x}}\right) \circledast \tilde{X}_B^{-1} \\ &\textit{by definitions of } B_{\tilde{x}} \textit{ and } \mathbf{t}_{\tilde{x}} \textit{ and by } \left(\textit{Eq. } (\mathcal{H}_2^{(l)})\right)_{l=1}^{m+1} \\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})}\left(ck, B_{\tilde{x}}\tilde{X}_B^{-1}\,;\,\mathbf{t}_{\tilde{x}}\tilde{X}_B^{-1}\right). \\ &\qquad \textit{see footnote 14}\end{aligned}$$

(**Step1**.3) Now, let us suppose just for a moment that we have[15]

$$\exists\, B_{\tilde{x}}(\tilde{X}_B)^{-1}, B_{\tilde{x}'}(\tilde{X}'_B)^{-1} \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta}),\ B_{\tilde{x}}(\tilde{X}_B)^{-1} \neq B_{\tilde{x}'}(\tilde{X}'_B)^{-1}.$$

But, by the previous point, the following property holds

$$\begin{aligned}(c_{B_0},\dots,c_{B_m}) &= \mathsf{Com}_{\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})}\left(ck, B_{\tilde{x}}(\tilde{X}_B)^{-1}\,;\,\mathbf{t}_{\tilde{x}}(\tilde{X}_B)^{-1}\right) \\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})}\left(ck, B_{\tilde{x}'}(\tilde{X}'_B)^{-1}\,;\,\mathbf{t}_{\tilde{x}'}(\tilde{X}'_B)^{-1}\right)\end{aligned}$$

Thus, as the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})]$ is *computationally binding*, with *overwhelming probability*, we conclude a contradiction. Therefore, we have shown that the following property holds

$$\forall\, B_{\tilde{x}}, B_{\tilde{x}'} \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta}),\ \forall\, \tilde{X}_B, \tilde{X}'_B \in \mathsf{Mat}_{m+1}(\mathbb{F}_{p_\eta}),\quad B_{\tilde{x}}(\tilde{X}_B)^{-1} = B_{\tilde{x}'}(\tilde{X}'_B)^{-1}.$$

We denote this common value $\tilde{B} \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})$ with columns $(\mathbf{b}_k)_{k=0}^{2m}$. Thus, we have found an opening $(\tilde{B}, \mathbf{t}) \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m+1}$ *independent from challenges* $(\tilde{x}_l)_{l=1}^{2m}$ of the commit value $\mathbf{c}_B$:

$$\boxed{\forall\, k \in [\![0; m]\!],\ c_{B_k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \mathbf{b}_k\,;\,t_k\right).}$$

[14] Let $n, m \in \mathbb{N}^*$ be two natural numbers. Let $ck \in \mathbb{G}_{p_\eta}^{n+1}$ be a commitment key parameter for the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$. Let $M \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$ be a matrix of dimensions $n \times m$ and let $B \in \mathsf{Mat}_m(\mathbb{F}_{p_\eta})$ be a square matrix of dimensions $m \times m$. Let $\mathbf{r} \in \mathbb{F}_{p_\eta}^m$ be a vector of dimension m. By definition of $\mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}$, we have

$$\begin{aligned}\left(\mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, M\,;\,\mathbf{r}\right)\right) \circledast B &= \left(\mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, M\,;\,\mathbf{r}\right) \circledast \mathbf{B}^{(j)}\right)_{j=1}^{m} \\ &= \left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, M\cdot\mathbf{B}^{(j)}\,;\,\langle \mathbf{r} \mid \mathbf{B}^{(j)}\rangle\right)\right)_{j=1}^{m} \\ &= \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, MB\,;\,\mathbf{r}B\right). \qquad \square\end{aligned}$$

[15] More precisely, we suppose the existence of $B_{\tilde{x}}, B_{\tilde{x}'} \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})$ two matrix of dimensions $n \times (m+1)$ and $\tilde{X}_B, \tilde{X}'_B \in \mathsf{Mat}_{m+1}(\mathbb{F}_{p_\eta})$ two square matrix of dimensions $m+1$ such that we are in one of the two following cases:

- **Case 1:** Their exists a sequence $(\tilde{x}_l)_{l=1}^{m+1}$ of challenges in $\mathbb{F}_{p_\eta}^*$ and *at least* another challenge $\tilde{x}'_{l_0} \in \mathbb{F}_{p_\eta}^*$ with $\tilde{x}'_{l_0} \neq \tilde{x}_{l_0}$ for some $l_0 \in [\![1; m+1]\!]$ such that $\tilde{X}_B \overset{\text{def}}{=} V(\tilde{x}_1,\dots,\tilde{x}_{l_0-1},\tilde{x}_{l_0},\tilde{x}_{l_0+1},\dots,\tilde{x}_{m+1})$ and $\tilde{X}'_B \overset{\text{def}}{=} V(\tilde{x}_1,\dots,\tilde{x}_{l_0-1},\tilde{x}'_{l_0},\tilde{x}_{l_0+1},\dots,\tilde{x}_{m+1})$;
- **Case 2:** Their exists *at least* one column $l_0 \in [\![1; m+1]\!]$ such that $\mathbf{B}_{\tilde{x}}^{(l_0)} \neq \mathbf{B}_{\tilde{x}'}^{(l_0)}$.

(Step 2) – Get an opening of commit values $(c_{F_k})_{k=0}^{2m-1}$

(**Step2**.1) We define the matrix $\tilde{X}_F \in \mathsf{Mat}_{2m}(\mathbb{F}_{p_\eta})$ by

$$\tilde{X}_F \overset{\text{def}}{=} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \tilde{x}_1 & \tilde{x}_2 & \cdots & \tilde{x}_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ \tilde{x}_1^{2m-1} & \tilde{x}_2^{2m-1} & \cdots & \tilde{x}_{2m}^{2m-1} \end{pmatrix},$$

which is again an invertible transposed Vandermonde matrix because $(\tilde{x}_l)_{l=1}^{2m}$ are pairwise distincts, with *overwhelming probability*.

(**Step2**.2) We define the following quantities

$$\mathbf{f}_{\tilde{x}} \overset{\text{def}}{=} (f^{(l)})_{l=1}^{2m} \in \mathbb{F}_{p_\eta}^{2m} \quad \text{and} \quad \overrightarrow{\varsigma}_{\tilde{x}} \overset{\text{def}}{=} (\varsigma^{(l)})_{l=1}^{2m} \in \mathbb{F}_{p_\eta}^{2m}.$$

Thus, we have

$$\begin{aligned}(c_{F_0},\dots,c_{F_{2m-1}}) &= \left((c_{F_0},\dots,c_{F_{2m-1}}) \circledast \tilde{X}_F\right) \circledast \tilde{X}_F^{-1} \\ &= \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, \mathbf{f}_{\tilde{x}}\,;\,\overrightarrow{\varsigma}_{\tilde{x}}\right) \circledast \tilde{X}_F^{-1} \\ &\qquad \textit{by hypothesis } \left(\textit{Eq. } (\mathcal{H}_3^{(l)})\right)_{l=1}^{2m} \\ &= \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, \mathbf{f}_{\tilde{x}}\tilde{X}_F^{-1}\,;\,\overrightarrow{\varsigma}_{\tilde{x}}\tilde{X}_F^{-1}\right).\end{aligned}$$

(**Step2**.3) As seen in step (**Step1**.3), by the *binding* property for the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}]$, we conclude with *overwhelming probability*, the existence of a sequence $((f_k, \varsigma_k))_{k=0}^{2m-1} \in (\mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta})^{2m}$ which is *independent from challenges* $(\tilde{x}_l)_{l=1}^{2m}$ and such that

$$\boxed{\forall\, k \in [\![0; 2m-1]\!],\ c_{F_k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, f_k\,;\,\varsigma_k\right).}$$

(Step 3) – Obtain the computation of values $(E_k)_{k=0}^{2m-1}$

(**Step3**.1) By hypothesis Eq. $(\mathcal{H}_2^{(l)})$, and by definition of vectors $(\mathbf{b}_i)_{i=0}^{m}$ (see step (**Step1**.3)), for all $l \in [\![1; m+1]\!]$, we have

$$\sum_{i=0}^{n} (\tilde{x}_l)^i \mathbf{b}_i = \tilde{B}\cdot\tilde{\mathbf{X}}_B^{(l)} = \left(\tilde{B}\tilde{X}_B\right)^{(l)} = \left(B_{\tilde{x}}\tilde{X}_B^{-1}\tilde{X}_B\right)^{(l)} = \mathbf{B}_{\tilde{x}}^{(l)}.$$

Thus, by definition of $B_{\tilde{x}}$, the following equation holds

$$\forall\, l \in [\![1; m+1]\!], \mathbf{b}^{(l)} = \sum_{i=0}^{m} (x_l)^i \mathbf{b}_i. \qquad (\Phi)$$

(**Step3**.2) Likewise but with hypothesis Eq. $(\mathcal{H}_3^{(l)})$ and definition of vector $\mathbf{f}_{\tilde{x}}$ (see step (**Step2**.3)), the following property holds

$$\forall\, l \in [\![1; 2m]\!],\ f^{(l)} = \sum_{i=0}^{2m-1} (\tilde{x}_l)^k f_k. \qquad (\Psi)$$

(**Step3**.3) For all $l \in [\![1; m+1]\!]$, Eq. (Φ) leads to

$$\begin{aligned}\prod_{i=1}^{m} \mathbf{c}'_i \circledast \left((\tilde{x}_l)^{m-i}\mathbf{b}^{(l)}\right) &= \prod_{i=1}^{m} \mathbf{c}'_i \circledast \left(\sum_{j=0}^{m} (\tilde{x}_l)^{m-i+j}\mathbf{b}^{(j)}\right) \\ &= \prod_{i=1}^{m}\prod_{j=0}^{m} \left(\mathbf{c}'_i \circledast \mathbf{b}^{(j)}\right)^{(\tilde{x}_l)^{m-i+j}} \\ &= \prod_{k=0}^{2m-1} \left(\prod_{\substack{j=0 \\ 1\leqslant m-i+j\leqslant m}}^{m} \left(\mathbf{c}_{m-k+j} \circledast \mathbf{b}^{(j)}\right)\right)^{(x_l)^k}\end{aligned}$$

We define $\mathbf{E} \stackrel{\text{def}}{=} (E_k)_{k=0}^{2m-1} \in \mathbb{H}_{p_\eta}^{2m}$ and, for all $i \in [\![0; 2m-1]\!]$, $\tilde{\mathbf{y}}^{(i)} \in \mathbb{F}_{p_\eta}^{2m}$ the $(i+1)$-th column of the matrix $\tilde{X}_F^{-1}$. Let $i \in [\![0; 2m-1]\!]$. We have[16]

$$\begin{aligned}E_i &= \mathbf{E} \circledast \left(\tilde{X}_F \cdot \tilde{\mathbf{y}}^{(i)}\right) && \text{because } \tilde{X}_F \cdot \tilde{\mathbf{y}}^{(i)} = \mathbf{u}_i \\ &= \prod_{k=0}^{2m-1} E_k^{\left(\tilde{X}_F \cdot \tilde{\mathbf{y}}^{(i)}\right)_k} && \text{by definition of } \circledast\end{aligned}$$

By definition of $\tilde{X}_F$, for all $k \in [\![0; 2m-1]\!]$, we have

$$\left(\tilde{X}_F \cdot \tilde{\mathbf{y}}^{(i)}\right)_k = \sum_{l=1}^{2m} \left(\tilde{X}_F\right)_{k,l} \tilde{y}_l^{(i)} = \sum_{l=1}^{2m} \tilde{x}_l^k \tilde{y}_l^{(i)}.$$

Thus, we can compute E_i as follows

$$\begin{aligned}E_i &= \prod_{k=0}^{2m-1}\prod_{l=1}^{2m} E_k^{\tilde{x}_l^k \tilde{x}_l^{(i)}} = \prod_{l=1}^{2m}\left(\prod_{k=0}^{2m-1} E_l^{\tilde{x}_l^k}\right)^{\tilde{y}_l^{(i)}} \\ &= \prod_{l=1}^{2m}\left(\mathrm{Enc}_{\mathbb{CS}}\left(pk, g^{f^{(l)}}\,;\, \tau^{(l)}\right) \cdot \prod_{i=1}^{m}\left(\mathbf{c}'_i \circledast \left(\tilde{x}_l^{m-i}\mathbf{b}^{(l)}\right)\right)\right)^{\tilde{x}_l^{(i)}} \\ &\qquad \text{by hypothesis } \left(\text{Eq. } (\mathcal{H}_4^{(l)})\right)_{l=1}^{2m} \\ &= \prod_{l=1}^{2m}\left(\begin{array}{l}\mathrm{Enc}_{\mathbb{CS}}\left(pk, g^{f^{(l)}}\,;\, \tau^{(l)}\right) \cdot \\ \quad \prod_{k=0}^{2m-1}\left(\prod_{\substack{j=0 \\ 1\leqslant m-k+j\leqslant m}}^{m}\left(\mathbf{c}'_{m-k+j} \circledast \mathbf{b}^{(j)}\right)\right)^{\tilde{x}_l^k}\end{array}\right)^{\tilde{y}_l^{(i)}} \\ &= \mathrm{Enc}_{\mathbb{CS}}\left(pk, g^{\sum_{l=1}^{2m} f^{(l)}\tilde{y}_l^{(i)}}\,;\, \sum_{l=1}^{2m}\tau^{(l)}\tilde{y}_l^{(i)}\right) \\ &\qquad \cdot \prod_{k=0}^{2m-1}\left(\prod_{\substack{j=0 \\ 1\leqslant m-k+j\leqslant m}}^{m}\left(\mathbf{c}'_{m-k+j} \circledast \mathbf{b}^{(j)}\right)\right) \\ &\qquad \text{because } \mathbb{CS} \text{ is homomorphic}\end{aligned}$$

[16] Let $n \in \mathbb{N}^*$ be a natural number. Let $\mathbf{x} \in \mathbb{H}_{p_\eta}^n$ be a ciphertexts vector of dimension n. Let $i \in [\![1; n]\!]$. By definition of $\circledast$, we have

$$\mathbf{x} \circledast \mathbf{u}_i = \prod_{j=1}^{n} x_j^{\delta_{ji}} = x_i. \qquad \square$$

It follows

$$E_i = \mathrm{Enc}_{\mathbb{CS}}\left(pk, g^{f_i}\,;\, \tau_i\right) \cdot \prod_{k=0}^{2m-1}\left(\prod_{\substack{j=0 \\ 1\leqslant m-k+j\leqslant m}}^{m}\left(\mathbf{c}'_{m-k+j} \circledast \mathbf{a}^{(j)}\right)\right)^{\delta_{ki}},$$

because, for all $k \in [\![0; 2m-1]\!]$, the following properties hold

- $f_k \stackrel{\text{def}}{=} \left(\mathbf{f}_{\tilde{x}}\tilde{X}_F^{-1}\right)_k = \sum_{l=1}^{2m} f^{(l)}\tilde{y}_l^{(k)}$;
- $\forall\, j \in [\![0; 2m-1]\!]$, $\sum_{l=1}^{2m} \tilde{x}_l^k \tilde{y}_k^{(j)} = \left(\tilde{X}_F^{-1}\tilde{\mathbf{y}}^{(j)}\right)_k = \delta_{kj}$;
- We define t_k to be $\tau_k \stackrel{\text{def}}{=} \sum_{l=1}^{2m} \tau^{(l)}\tilde{y}_l^{(k)} \in \mathbb{F}_{p_\eta}$.

Consequently, we conclude the following property

$$\boxed{\begin{array}{l}\forall\, k \in [\![0; 2m-1]\!],\ E_k = \mathrm{Enc}_{\mathbb{CS}}\left(pk, g^{f_k}\,;\, \tau_k\right)\prod_{i=1}^{m}\left(\mathbf{c}'_i \circledast \mathbf{b}_{k-m+i}\right) \\ \qquad \text{where } f_k = \sum_{l=1}^{2m} f^{(l)}\tilde{y}_l^{(k)} \text{ and } \tau_k = \sum_{l=1}^{2m}\tau^{(l)}\tilde{y}_l^{(k)}.\end{array}}$$

(Step 4) – Obtain the computation of value C

By hypothesis Eq. $(\mathcal{H}_1)$, we have $c_{F_m} = \mathrm{Com}_{\mathbb{F}_{p_\eta}}(ck, 0\,;\, 0)$ and $E_m = C$. As the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}]$ is *computationally binding*, with overwhelming probability, we have $f_m = 0$. This leads to

$$C = E_m = \mathrm{Enc}_{\mathbb{CS}}\left(pk, g^0\,;\, t_m\right)\prod_{i=1}^{m}\left(\mathbf{c}'_i \circledast \mathbf{b}_i\right).$$

Results obtained in steps **(Step 1)** to **(Step 4)** give us the following result, proving that, with *overwhelming probability*, we have successfully extract a witness $w \stackrel{\text{def}}{=} (B, \mathbf{t}, \varrho) \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m \times \mathbb{F}_{p_\eta}$ such that $(\sigma, \chi, w) \in \mathcal{R}_{\mathsf{MEA}}^{\mathsf{BG}}$.

$$\boxed{\begin{array}{l}\exists\, B \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}),\ \exists\, \mathbf{t} \in \mathbb{F}_{p_\eta}^m,\ \exists\, \varrho \in \mathbb{F}_{p_\eta}, \\ \qquad \left\{\begin{array}{l}\mathbf{c}_B = \mathrm{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, B\,;\, \mathbf{t}) \\ C = \mathrm{Enc}_{\mathbb{CS}}(pk, 1\,;\, \varrho)\cdot\prod_{i=1}^{m}\left(\mathbf{c}'_i \circledast \mathbf{b}_i\right)\end{array}\right. \\ \qquad \text{where } \mathbf{B}^{(j)} \stackrel{\text{def}}{=} \mathbf{b}^{(j)}, \text{ for all } j \in [\![1; m]\!].\end{array}}$$

Proof step → / ↓ Property	step (Step1.1)	step (Step1.3)	step (Step2.1)	step (Step2.3)
***Binding* of commitment scheme**		× 1		× 1
Property transfer under adversarial selection	Yes		Yes	
Extractor uses *rewinding*?	Yes ($2m$ valid proof transcripts)			

Table 2: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Multi-Exponentiation Argument protocol

□

B.3 Product argument protocol

We define

$$\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}} \subseteq \underbrace{\mathbb{G}_{p_\eta}^{n+1}}_{\text{Public parameter set}} \times \underbrace{\left(\mathbb{G}_{p_\eta}^{m} \times \mathbb{F}_{p_\eta}\right)}_{\text{Statement set}} \times \underbrace{\left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m}\right)}_{\text{Witness set}}$$

to be the *product relation* defined by

$$\left(ck, (\mathbf{c}_\Gamma, \beta), (\Gamma, \mathbf{v})\right) \in \mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}} \overset{\text{def}}{\iff} \begin{cases} \mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma\,;\, \mathbf{v}\right) \\ \prod_{i=1}^{n}\prod_{j=1}^{m} \Gamma_{i,j} = \beta \end{cases}$$

Hence, we define a 7-move product argument protocol to be the protocol defined as follows in **Protocol 5**.

Theorem B.3 (Knowledge soundness of $\mathbb{ZK}^{(3)}[\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}]$). *The 7-move* zero-knowledge *protocol* $\mathbb{ZK}^{(3)}[\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}]$ *is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\mathsf{PA}}$ for the Bayer-Groth product argument to be the algorithm defined as follows in **Extractor 6**.

Let $n, m \in \mathbb{N}^*$ be two natural numbers. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time and deterministic adversarial prover. Let $ck \leftarrow \mathcal{I}_{\mathsf{PA}}(\eta)$ be an honest public parameter for the product argument relation $\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, ck)$ be an adversarial statement where

$$\chi \overset{\text{def}}{=} (\mathbf{c}_\Gamma, \beta) \in \mathbb{G}_{p_\eta}^{m} \times \mathbb{F}_{p_\eta}.$$

Then, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\mathsf{PA}}$ on inputs ck and χ with access to $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{PA}}$ and obtains

$$\tau_{\mathsf{PA}} \overset{\text{def}}{=} \Big(c_\beta, \underbrace{(\Gamma, \mathbf{v}, \overrightarrow{\beta}^{(1)}, \xi_\delta)}_{\substack{\text{Witness of the Hadamard} \\ \text{Product Argument}}}, \underbrace{(\overrightarrow{\beta}^{(2)}, \xi_2)}_{\substack{\text{Witness of the Single} \\ \text{Value Product Argument}}}\Big).$$

(Step 1) By the *knowledge soundness* of the Hadamard product argument protocol (see Theorem B.5), we have, with overwhelming probability in η, the following equations

$$\mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma\,;\, \mathbf{v}\right) \qquad (\mathcal{H}_{\mathsf{HPA}}^{(1)})$$

$$c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}^{(1)}\,;\, \xi_\delta\right) \qquad (\mathcal{H}_{\mathsf{HPA}}^{(2)})$$

$$\overrightarrow{\beta}^{(1)} = \bigodot_{j=1}^{m} \Gamma^{(j)} \qquad (\mathcal{H}_{\mathsf{HPA}}^{(3)})$$

(Step 2) Besides, by the *knowledge soundness* of the Single value product argument protocol (see Theorem B.4), we have, with overwhelming probability in η, the following equations

$$c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}^{(2)}\,;\, \xi_2\right) \qquad (\mathcal{H}_{\mathsf{SVPA}}^{(1)})$$

$$\beta = \prod_{i=1}^{n} \beta_i^{(2)} \qquad (\mathcal{H}_{\mathsf{SVPA}}^{(2)})$$

(Step 3) By equations Eq. $(\mathcal{H}_{\mathsf{HPA}}^{(2)})$ and Eq. $(\mathcal{H}_{\mathsf{SVPA}}^{(1)})$, we have

$$c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}^{(1)}\,;\, \xi_\delta\right) = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}^{(2)}\,;\, \xi_2\right).$$

Thus, because the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^{n}]$ is *computationally binding*, we conclude with overwhelming probability in η that $\overrightarrow{\beta}^{(1)} = \overrightarrow{\beta}^{(2)}$. We denote this common value $\overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^{n}$.

Results obtained in steps **(Step 1)** to **(Step 3)** give us the following result[17], proving that, with *overwhelming probability*, we have successfully extract a witness $w \overset{\text{def}}{=} (\Gamma, \mathbf{v}) \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m}$ such that $(\sigma, \chi, w) \in \mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}$.

$$\exists\, \Gamma \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}),\ \exists\, \mathbf{v} \in \mathbb{F}_{p_\eta}^{m},\ \begin{cases} \mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma\,;\, \mathbf{v}\right) \\ \beta = \prod_{i=1}^{n}\prod_{j=1}^{m} \Gamma_{i,j} \end{cases}$$

[17] More precisely, on one hand we have

$$\begin{aligned} \beta &= \prod_{i=1}^{n} \beta_i && \text{by step } \textbf{(Step 3)} \text{ and Eq. } (\mathcal{H}_{\mathsf{SVPA}}^{(2)}) \\ &= \prod_{i=1}^{n} \left(\bigodot_{j=1}^{m} \Gamma^{(j)}\right)_i && \text{by step } \textbf{(Step 3)} \text{ and Eq. } (\mathcal{H}_{\mathsf{HPA}}^{(3)}) \\ &= \prod_{i=1}^{n}\prod_{j=1}^{m} \Gamma_{i,j}. && \text{by definition of operator } \odot \end{aligned}$$

And on another hand, Eq. $(\mathcal{H}_{\mathsf{HPA}}^{(1)})$ gives us

$$\mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma\,;\, \mathbf{v}\right).$$

Protocol 5: 7-move *zero-knowledge* protocol $\mathbb{ZK}^{(3)}[\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}]$ for the Bayer-Groth product argument

Public Input : Two natural numbers $n, m \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{n+1}$ for the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$. A commit value $\mathbf{c}_\Gamma \in \mathbb{G}_{p_\eta}^{m}$, and a value $\beta \in \mathbb{F}_{p_\eta}$.

Private Input : A matrix $A \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$, and a vector of random values $\mathbf{v} \xleftarrow{\$} \mathbb{F}_{p_\eta}^{m}$ such that $\mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, \Gamma\,; \mathbf{v})$ and $\prod_{i=1}^{n}\prod_{j=1}^{m}\Gamma_{i,j} = \beta$.

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{PA}}$ chooses uniformly at random a value $\xi \xleftarrow{\$} \mathbb{F}_{p_\eta}$ and computes the commit value $c_b \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \left(\prod_{j=1}^{m}\Gamma_{i,j}\right)_{i=1}^{n}\,; \xi\right) \in \mathbb{G}_{p_\eta}$. Then, $\mathcal{P}_{\mathsf{PA}}$ sends this commit value c_β to the verifier $\mathcal{V}_{\mathsf{PA}}$.

(1-5) **(Hadamard product argument call)** Both prover $\mathcal{P}_{\mathsf{PA}}$ and verifier $\mathcal{V}_{\mathsf{PA}}$ engage in the 5-move *zero-knowledge* protocol $\mathbb{ZK}^{(2)}[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}]$ for the relation $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$ with public parameter $\sigma_{\mathsf{HPA}} \stackrel{\text{def}}{=} ck$, public statement $\chi_{\mathsf{HPA}} \stackrel{\text{def}}{=} (\mathbf{c}_\Gamma, c_\beta)$, and private statement $w_{\mathsf{HPA}} \stackrel{\text{def}}{=} \left(\Gamma, \mathbf{v}\bigodot_{j=1}^{m}\mathbf{\Gamma}^{(j)}, \xi\right)$. We denote by τ_{HPA} the proof transcript obtained at the end of this 5-move protocol.

(5-7) **(Single value product argument call)** Both prover $\mathcal{P}_{\mathsf{PA}}$ and verifier $\mathcal{V}_{\mathsf{PA}}$ engage in the Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$ for the relation $\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}$ with public parameter $\sigma_{\mathsf{SVPA}} \stackrel{\text{def}}{=} ck$, public statement $\chi_{\mathsf{SVPA}} \stackrel{\text{def}}{=} (c_\beta, \beta)$, and private statement $w_{\mathsf{SVPA}} \stackrel{\text{def}}{=} \left(\bigodot_{j=1}^{m}\mathbf{\Gamma}^{(j)}, \xi\right)$. We denote by τ_{SVPA} the proof transcript obtained at the end of this Σ-protocol.

(8) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{PA}}$ accepts if and only if the following property holds $\left(v_{\mathsf{HPA}}^{\sigma_{\mathsf{HPA}},\,\chi_{\mathsf{HPA}}}(\tau_{\mathsf{HPA}}) \wedge v_{\mathsf{SVPA}}^{\sigma_{\mathsf{SVPA}},\,\chi_{\mathsf{SVPA}}}(\tau_{\mathsf{SVPA}})\right)$.

Extractor 6: Extractor $\mathcal{E}_{\mathsf{PA}}$ for the 7-move *zero-knowledge* protocol $\mathbb{ZK}^{(3)}[\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}]$ of the Bayer-Groth product argument

Input : A security parameter $\eta \in \mathbb{N}^*$. Two natural numbers $n, m \in \mathbb{N}^*$. A public parameter $\sigma \stackrel{\text{def}}{=} ck \in \mathbb{G}_{p_\eta}^{n+1}$ for the Bayer-Groth product relation $\mathcal{R}_{\mathsf{PA}}^{\mathsf{BG}}$. A statement $\chi \stackrel{\text{def}}{=} (\mathbf{c}_\Gamma, \beta) \in \mathbb{G}_{p_\eta}^{m} \times \mathbb{F}_{p_\eta}$.

Blackbox access to : A deterministic adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{PA}}$.

1 **Begin extractor**

2 **calls** $\mathcal{P}^*$ **to get** $c_\beta \in \mathbb{G}_{p_\eta}$;

3 **calls** $\mathcal{E}_{\mathsf{HPA}}$ **with oracles** $\mathcal{P}^*$ **and** $\mathcal{V}_{\mathsf{PA}}$ **on inputs** $\left(\sigma, (\mathbf{c}_\Gamma, c_\beta)\right)$ **to get** $\left(\Gamma, \mathbf{v}, \overrightarrow{\beta}^{(1)}, \xi_\delta\right) \in \left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m} \times \mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta}\right)$;

4 **calls** $\mathcal{E}_{\mathsf{SVPA}}$ **with oracles** $\mathcal{P}^*$ **and** $\mathcal{V}_{PA}$ **on inputs** $\left(\sigma, (c_\beta, \beta)\right)$ **to get** $\left(\overrightarrow{\beta}^{(2)}, \xi_2\right) \in \left(\mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta}\right)$;

5 **returns** $\tau_{\mathsf{PA}} \stackrel{def}{=} \left(c_\beta, \left(\Gamma, \mathbf{v}, \overrightarrow{\beta}^{(1)}, \xi_\delta\right), \left(\overrightarrow{\beta}^{(2)}, \xi_2\right)\right)$.

Proof step → / **↓ Property**	step **(Step 1)**	step **(Step 2)**	step **(Step 3)**
Knowledge Soundness	$1\times \mathcal{E}_{\mathsf{HPA}}$	$1\times \mathcal{E}_{\mathsf{SVPA}}$	
***Binding* of commitment scheme**			$\times 1$
Extractor uses *rewinding*?	No		

Table 3: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Product Argument protocol

□

B.4 Single value product argument protocol

We define

$$\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}} \subseteq \underbrace{\mathbb{G}_{p_\eta}^{n+1}}_{\text{Public parameter set}} \times \underbrace{(\mathbb{G}_{p_\eta} \times \mathbb{F}_{p_\eta})}_{\text{Statement set}} \times \underbrace{(\mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta})}_{\text{Witness set}}$$

Protocol 7: Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$ for the Bayer-Groth single value product argument

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 scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^n]$. A commit value $c_\beta \in \mathbb{G}_{p_\eta}$ and a value $\beta \in \mathbb{F}_{p_\eta}$.

Private Input : A vector $\overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^n$ and a random value $\xi \xleftarrow{\$} \mathbb{F}_{p_\eta}$ such that $c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \overrightarrow{\beta}\,;\, \xi\right)$, and $\beta = \prod_{i=1}^{n} \beta_i$.

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{SVPA}}$ computes, for all $j \in [\![1; n]\!]$, $\tilde{\beta}^{(j)} \leftarrow \prod_{i=1}^{j} \beta_i \in \mathbb{F}_{p_\eta}^n$. Then, he chooses uniformly at random values $\Delta_1, \ldots, \Delta_n \xleftarrow{\$} \mathbb{F}_{p_\eta}$, $\delta_2, \ldots, \delta_{n-1} \xleftarrow{\$} \mathbb{F}_{p_\eta}$, and $\xi_\delta, \xi_\Lambda, \xi_\Delta \xleftarrow{\$} \mathbb{F}_{p_\eta}$. Next, $\mathcal{P}_{\mathsf{SVPA}}$ sets $\delta_1 \leftarrow \Delta_1 \in \mathbb{F}_{p_\eta}$ and $\delta_n \leftarrow 0 \in \mathbb{F}_{p_\eta}$ then computes

$$c_\Delta \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \mathbf{\Delta}\,;\, \xi_\Delta\right) \in \mathbb{G}_{p_\eta}, \quad c_\delta \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \left(-\delta_i \Delta_{i+1}\right)_{i=1}^{n-1}\,;\, \xi_\delta\right) \in \mathbb{G}_{p_\eta}, \quad \text{and}$$

$$c_\Lambda \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \left(\delta_i - \beta_i \delta_{i-1} - \tilde{\beta}_{i-1}\Delta_i\right)_{i=2}^{n}\,;\, \xi_\Lambda\right) \in \mathbb{G}_{p_\eta}$$

Finally, $\mathcal{P}_{\mathsf{SVPA}}$ sends to $\mathcal{V}_{\mathsf{SVPA}}$ values $\left(c_\Delta, c_\delta, c_\Lambda\right)$.

(2) **(Challenge message)** The verifier $\mathcal{V}_{\mathsf{SVPA}}$ chooses uniformly at random a challenge $\hat{x} \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ and sends it to $\mathcal{P}_{\mathsf{SVPA}}$.

(3) **(Response message)** The prover $\mathcal{P}_{\mathsf{SVPA}}$ computes values $\hat{\xi} \leftarrow \hat{x}\xi + \xi_\Delta \in \mathbb{F}_{p_\eta}$, $\hat{\zeta} \leftarrow \hat{x}\xi_\Lambda + \xi_\delta \in \mathbb{F}_{p_\eta}$, and, for all $i \in [\![1; n]\!]$, $\hat{\beta}_i \leftarrow \hat{x}\beta_i + \Delta_i \in \mathbb{F}_{p_\eta}$ and $\hat{\delta}_i \leftarrow \hat{x}\tilde{\beta}_i + \delta_i \in \mathbb{F}_{p_\eta}$. Then, $\mathcal{P}_{\mathsf{SVPA}}$ sends values $\left(\left(\hat{\beta}_i\right)_{i=1}^{n}, \left(\hat{\delta}_i\right)_{i=1}^{n}, \hat{\xi}, \hat{\zeta}\right)$ to $\mathcal{V}_{\mathsf{SVPA}}$.

(4) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{SVPA}}$ accepts if and only if the following equations hold

$$c_\beta^{\hat{x}} c_\Delta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i\right)_{i=1}^{n}, \hat{\xi}\right), \qquad c_\Lambda^{\hat{x}} c_\delta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \left(\hat{x}\hat{\delta}_i - \hat{\delta}_{i-1}\hat{\beta}_i\right)_{i=2}^{n}, \hat{\zeta}\right), \qquad \hat{\delta}_1 = \hat{\beta}_1, \qquad \text{and} \qquad \hat{\delta}_n = \hat{x}\beta.$$

Extractor 8: Extractor $\mathcal{E}_{\mathsf{SVPA}}$ for the Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$ of the Bayer-Groth single value product argument

Input : A security parameter $\eta \in \mathbb{N}^*$. A natural number $n \in \mathbb{N}^*$. A public parameter $\sigma \overset{\text{def}}{=} ck \in \mathbb{G}_{p_\eta}^{n+1}$ for the Bayer-Groth single value product relation $\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}$. A statement $\chi \overset{\text{def}}{=} (c_\beta, \beta) \in \mathbb{G}_{p_\eta} \times \mathbb{F}_{p_\eta}$.

Blackbox access to : A deterministic adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{SVPA}}$.

Begin extractor

- **calls** $\mathcal{P}^*$ **to get** $\alpha \overset{\text{def}}{=} (c_\Delta, c_\delta, c_\Lambda) \in \left(\mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}\right)$; // State at this point: $\mathbf{st}_1 \overset{\text{def}}{=} \left[ck\,;\, (c_\beta, \beta)\,;\, (c_\Delta, c_\delta, c_\Lambda)\right]$.
- **rewinds** $\mathcal{P}^*$ **and** $\mathcal{V}_{\mathsf{SVPA}}$ **at state** $\mathbf{st}_1$ **and begins with** $l \leftarrow 1 \in \mathbb{N}$
  - **calls** $\mathcal{V}_{\mathsf{SVPA}}$ **to get** $\hat{x}_l \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$;
  - **calls** $\mathcal{P}^*$ **to get** $\mathfrak{d}_{\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}, \mathcal{P}^*}(\alpha, \hat{x}_l) \in \left(\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}\right)$;
  - **if** $v_{\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}}^{ck, \chi}\left(\mathsf{tr}_{\alpha, \mathfrak{d}_{\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{ck, \chi}(\hat{x}_l)\right)$ **and** $\bigwedge_{i=1}^{l-1}(\hat{x}_i \neq \hat{x}_l)$ **then** $l \leftarrow l + 1$;
- **until** $l > 2$;
- **returns** $\tau_{\mathsf{SVPA}} \overset{\text{def}}{=} \left(\mathsf{tr}_{\alpha, \mathfrak{d}_{\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{ck, \chi}(\hat{x}_1),\ \mathsf{tr}_{\alpha, \mathfrak{d}_{\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{ck, \chi}(\hat{x}_2)\right)$.

to be the *single value product relation* defined by

$$\left(ck, (c_\beta, \beta), \left(\overrightarrow{\beta}, \xi\right)\right) \in \mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}} \overset{\text{def}}{\iff} \begin{cases} c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \overrightarrow{\beta}\,;\, \xi\right) \\ \beta = \prod_{i=1}^{n} \beta_i \end{cases}$$

Hence, we define a Σ-protocol for the relation of single value product $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$ to be the protocol defined as follows in **Protocol 7**.

Theorem B.4 (Knowledge soundness of $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$). *The Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}\right]$ for the single value product relation $\mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}$ is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\mathsf{SVPA}}$ for the Bayer-Groth single value product argument to be the algorithm defined as follows in **Extractor 8**.

Let $n \in \mathbb{N}^*$ be a natural number. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time and deterministic adversarial prover. Let $\sigma = ck \leftarrow \mathcal{I}_{\mathsf{SVPA}}(\eta)$ be an honest public parameter for the single value product relation $\mathcal{R}^{\mathsf{BG}}_{\mathsf{SVPA}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, ck)$ be an adversarial statement where

$$\chi \overset{\text{def}}{=} (c_\beta, \beta) \in \mathbb{G}_{p_\eta} \times \mathbb{F}_{p_\eta}.$$

Next, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\mathsf{SVPA}}$ on inputs ck and χ with access to $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{SVPA}}$ and obtains a pair of valid proof transcripts τ_{SVPA} where

$$\tau_{\mathsf{SVPA}} \overset{\text{def}}{=} \left(\mathsf{tr}^{ck,\,\chi}_{\alpha,\,\mathfrak{z}_{\mathcal{R}^{\mathsf{BG}}_{\mathsf{SVPA}},\,\mathcal{P}^*}}(\hat{x}_1),\ \mathsf{tr}^{ck,\,\chi}_{\alpha,\,\mathfrak{z}_{\mathcal{R}^{\mathsf{BG}}_{\mathsf{SVPA}},\,\mathcal{P}^*}}(\hat{x}_2)\right).$$

We denote by

- $\alpha \overset{\text{def}}{=} (c_\Delta, c_\delta, c_\Lambda) \in \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}$ the first message ; and
- for $l \in \{1, 2\}$, the response message on challenge $\hat{x}_l$ is

$$\mathfrak{z}_{\mathcal{R}^{\mathsf{BG}}_{\mathsf{SVPA}},\,\mathcal{P}^*}(\alpha, \hat{x}_l) \overset{\text{def}}{=} \left((\hat{\beta}_i^{(l)})_{i=1}^n, (\hat{\delta}_i^{(l)})_{i=1}^n, \hat{\xi}^{(l)}, \hat{\zeta}^{(l)}\right) \in \left(\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}\right).$$

By definition of the Bayer-Groth single value product argument protocol, as the proof transcripts in τ_{SVPA} are valid, for $l \in \{1, 2\}$, we have

$$c_\beta^{\hat{x}_l} c_\Delta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(l)}\right)_{i=1}^n ; \hat{\xi}^{(l)}\right) \qquad (\mathcal{H}_1^{(l)})$$

$$c_\Lambda^{\hat{x}_l} c_\delta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \left(\hat{x}_l\hat{\delta}_i^{(l)} - \hat{\delta}_{i-1}^{(l)}\hat{\beta}_i^{(l)}\right)_{i=2}^n ; \hat{\zeta}^{(l)}\right) \qquad (\mathcal{H}_2^{(l)})$$

$$\hat{\delta}_1^{(l)} = \hat{\beta}_1^{(l)} \quad \text{and} \quad \hat{\delta}_n^{(l)} = \hat{x}_l\beta \qquad (\mathcal{H}_3^{(l)})$$

(Step 1) – Get an opening of commit value c_β.

(**Step1**.1) Hypothesis Eq. $(\mathcal{H}_1^{(l)})$ and homomorphism of $\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}$ lead to

$$c_\beta^{\hat{x}_1 - \hat{x}_2} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(1)} - \hat{\beta}_i^{(2)}\right)_{i=1}^n ; \hat{\xi}^{(1)} - \hat{\xi}^{(2)}\right).$$

Because $\hat{x}_1 \neq \hat{x}_2$, we have

$$c_\beta = \left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(1)} - \hat{\beta}_i^{(2)}\right)_{i=1}^n ; \hat{\xi}^{(1)} - \hat{\xi}^{(2)}\right)\right)^{\frac{1}{\hat{x}_1 - \hat{x}_2}}$$
$$= \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{\beta}_i^{(1)} - \hat{\beta}_i^{(2)}\right)_{i=1}^n ; \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{\xi}^{(1)} - \hat{\xi}^{(2)}\right)\right).$$

(**Step1**.2) Therefore, the pair $\left((\beta_i)_{i=1}^n, r\right) \in \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$ is an opening of c_β with

$$\forall\, i \in [\![1; n]\!],\quad \beta_i \overset{\text{def}}{=} \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{\beta}_i^{(1)} - \hat{\beta}_i^{(2)}\right)$$
$$\text{and} \quad \xi \overset{\text{def}}{=} \frac{1}{\hat{x}_1, \hat{x}_2}\left(\hat{\xi}^{(1)} - \hat{\xi}^{(2)}\right),$$

which is *independent* of challenges $\hat{x}_1$ and $\hat{x}_2$ because the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^n]$ is *computationally binding*.

(Step 2) – Get an opening of commit value c_Δ.

(**Step2**.1) We have,

- $c_\Delta = c_\beta^{-\hat{x}_1}\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(1)}\right)_{i=1}^n ; \hat{\xi}^{(1)}\right)$ by hypothesis Eq. $(\mathcal{H}_1^{(l)})$ applied to $l = 1$; and
- by step **(Step 1)**, $c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, (\beta_i)_{i=1}^n ; \xi\right)$.

This leads to

$$c_\Delta = \left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, (\beta_i)_{i=1}^n ; \xi\right)\right)^{-\hat{x}_1} \cdot \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(1)}\right)_{i=1}^n ; \hat{\xi}^{(1)}\right)$$
$$= \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{\beta}_i^{(1)} - \hat{x}_1\beta_i\right)_{i=1}^n, \hat{\xi}^{(1)} - \hat{x}_1\xi\right).$$

(**Step2**.2) Therefore, the pair $\left((\Delta_i)_{i=1}^n, \xi_\Delta\right) \in \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$ is an opening of c_Δ with

$$\boxed{\forall\, i \in [\![1; n]\!],\ \Delta_i \overset{\text{def}}{=} \hat{\beta}_i^{(1)} - \hat{x}_1\beta_i \quad \text{and} \quad \xi_\Delta \overset{\text{def}}{=} \hat{\xi}^{(1)} - \hat{x}_1\xi,}$$

which is *independent* of challenge $\hat{x}_1$ because the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^n]$ is *computationally binding*.

(Step 3) – Get an opening of commit value c_Λ.

(**Step3**.1) By hypothesis Eq. $(\mathcal{H}_2^{(l)})$ and because $\hat{x}_1 \neq \hat{x}_2$, we have

$$c_\Lambda = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{x}_1\hat{\delta}_i^{(1)} - \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)} - \hat{x}_2\hat{\delta}_i^{(2)} + \hat{\delta}_{i-1}^{(2)}\hat{\beta}_i^{(2)}\right)_{i=2}^n ; \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{\xi}^{(1)} - \hat{\xi}^{(2)}\right)\right).$$

(**Step3**.2) Thus, $\left((\lambda_i)_{i=2}^n, \xi_\Lambda\right) \in \mathbb{F}_{p_\eta}^{n-1} \times \mathbb{F}_{p_\eta}$ is an opening – *independent* of challenges $\hat{x}_1$ and $\hat{x}_2$ by the *binding property* for the commiment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^{n-1}]$ – of c_Λ with

$$\boxed{\forall\, i \in [\![2; n]\!],\quad \lambda_i \overset{\text{def}}{=} \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{x}_1\hat{\delta}_i^{(1)} - \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)} - \hat{x}_2\hat{\delta}_i^{(2)} + \hat{\delta}_{i-1}^{(2)}\hat{\beta}_i^{(2)}\right)$$
$$\text{and} \quad \xi_\Lambda \overset{\text{def}}{=} \frac{1}{\hat{x}_1 - \hat{x}_2}\left(\hat{\zeta}^{(1)} - \hat{\zeta}^{(2)}\right).}$$

(Step 4) – Get an opening of commit value c_δ.

(**Step4**.1) We have,

- $c_\delta = c_\Lambda^{-\hat{x}_1}\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \left(\hat{x}_1\hat{\delta}_i^{(1)} - \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)}\right)_{i=2}^n ; \hat{\zeta}^{(1)}\right)$ by hypothesis Eq. $(\mathcal{H}_2^{(l)})$ applied to $l = 1$; and
- by step **(Step 3)**, $c_\Lambda = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, (\lambda_i)_{i=2}^n ; \xi_\Lambda\right)$.

This leads to

$$c_\delta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n-1}}\left(ck, \left(\hat{x}_1\hat{\delta}_i^{(1)} - \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)} - \hat{x}_1\lambda_i\right)_{i=2}^n ; \hat{\zeta}^{(1)} - \hat{x}_1\xi_\Lambda\right).$$

(**Step4**.2) Thus, $\left((\gamma_i)_{i=2}^n, \xi_\delta\right) \in \mathbb{F}_{p_\eta}^{n-1} \times \mathbb{F}_{p_\eta}$ is an opening – *independent* of challenge $\hat{x}_1$ by the *binding property* for the commitment scheme $\mathbb{KS}[\mathbb{F}_{p_\eta}^{n-1}]$ – of c_δ with

$$\boxed{\forall\, i \in [\![2; n]\!],\quad \gamma_i \overset{\text{def}}{=} \hat{x}_1\hat{\delta}_i^{(1)} - \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)} - \hat{x}_1\lambda_i$$
$$\text{and} \quad \xi_\delta \overset{\text{def}}{=} \hat{\zeta}^{(1)} - \hat{x}_1\xi_\Lambda.}$$

(Step 5) – It remains to verify equation $\beta = \prod_{i=1}^{n} \beta_i$.

(**Step5**.1) By step **(Step 4)** and because sequences $(\lambda_i)_{i=2}^n$ and $(\gamma_i)_{i=2}^n$ are independent of challenge $\hat{x}_1$, we have:

$$\forall\, i \in [\![2;n]\!],\ \hat{x}_1\hat{\delta}_i^{(1)} = \hat{\delta}_{i-1}^{(1)}\hat{\beta}_i^{(1)} + p_1^{(i)}(\hat{x}_1) \qquad (*)$$

where $p_1^{(i)}$ is a polynomial of degree 1 in variable $\hat{x}_1$[18].

(**Step5**.2) Now, let us prove the following property $\mathcal{P}(j)$ for $j \in [\![1;n]\!]$ by induction:

$$\hat{x}_1^{j-1}\hat{\delta}_j^{(1)} = \prod_{i=1}^{j}\hat{\beta}_i^{(1)} + p_{j-1}^{(j)}(\hat{x}_1) \quad \text{where } p_{j-1}^{(j)} \text{ is a polynomial of degree at most } j-1 \text{ in variable } \hat{x}_1. \qquad (\mathcal{P}(j))$$

- **Initialisation ($j = 1$):** By hypothesis Eq. $(\mathcal{H}_3^{(l)})$, we have $\hat{\delta}_1^{(1)} = \hat{\beta}_1^{(1)}$. Thus, we have $\hat{x}_1^{1-1}\hat{\delta}_1 = \prod_{i=1}^{1}\hat{\beta}_i + 0$ with $p_0^{(1)} \stackrel{\text{def}}{=} 0$ a polynomial of degree at most 0. Consequently, $\mathcal{P}(1)$ holds.
- **Heredity (let $j \in [\![2;n]\!]$):** We suppose $\mathcal{P}(j-1)$. By Eq. $(*)$, we have $\hat{x}_1\hat{\delta}_j^{(1)} = \hat{\delta}_{j-1}^{(1)}\hat{\beta}_j^{(1)} + p_1^{(j)}(\hat{x}_1)$ with $p_1^{(j)}$ of degree at most 1. Thus, we have

$$\begin{aligned}\hat{x}_1^{j-1}\hat{\delta}_j^{(1)} &= \hat{x}_1^{j-2}\hat{\delta}_{j-1}^{(1)}\hat{\beta}_j^{(1)} + \hat{x}_1^{j-2}p_1^{(j)}(\hat{x}_1)\\ &= \left(\prod_{i=1}^{j-1}\hat{\beta}_i^{(1)}\right)\cdot\hat{\beta}_j^{(1)} + \hat{\beta}_j^{(1)}p_{j-2}^{(j-1)}(\hat{x}_1) + \hat{x}_1^{j-2}p_1^{(j)}(x)\end{aligned}$$

because $\mathcal{P}(j-1)$ holds

$$= \prod_{i=1}^{j}\hat{\beta}_i^{(1)} + \Big(\overbrace{\hat{\beta}_j^{(1)}p_{j-2}^{(j-1)}(\hat{x}_1)}^{\deg \leqslant j-2} + \overbrace{\hat{x}_1^{j-2}p_1^{(j)}(\hat{x}_1)}^{\deg \leqslant j-1}\Big).$$

$$\deg \leqslant \max\big(j-2, j-1\big) = j-1$$

Consequently, we have

$$\hat{x}_1^{j-1}\hat{\delta}_j^{(1)} = \prod_{i=1}^{j}\hat{\beta}_i^{(1)} + p_{j-1}^{(j)}(\hat{x}_1)$$

where $p_{j-1}^{(j)}$ is a polynomial of degree at most $j-1$ in $\hat{x}_1$.

Thus, by induction, for all $j \in [\![1;n]\!]$, the property $\mathcal{P}(j)$ holds. In particular, because $\hat{x}_1\beta = \hat{\delta}_n^{(1)}$ (hypothesis Eq. $(\mathcal{H}_3^{(l)})$), for $j = n$, we have

$$\hat{x}_1^n\beta = \hat{x}_1^{n-1}\hat{\delta}_n^{(1)} = \prod_{i=1}^{n}\hat{\beta}_i + \underbrace{p_{n-1}^{(n)}(\hat{x}_1)}_{\text{of degree} \leqslant n-1}. \qquad (i)$$

(**Step5**.3) On another hand, by the opening of c_Δ (see step **(Step 2)**), we have

$$\forall\, i \in [\![1;n]\!],\ \Delta_i = \hat{\beta}_i^{(1)} - \hat{x}_1\beta_i, \qquad (ii)$$

where sequences $(\Delta_i)_{i=1}^n$ and $\left(\hat{\beta}_i^{(1)}\right)_{i=1}^n$ are independent of challenge $\hat{x}_1$.

Thus, by Eq. (i) and Eq. (ii), previous property leads to

$$\hat{x}_1^n\beta = \prod_{i=1}^{n}\left(\hat{x}_1\beta_i + \Delta_i\right) + p_{n-1}^{(n)}(\hat{x}_1).$$

Besides, there exists a polynomial $\Theta \in \mathbb{F}_{p_\eta}[X]$ such that

$$\prod_{i=1}^{n}\left(\hat{x}_1\beta_i + \Delta_i\right) = \hat{x}_1^n\prod_{i=1}^{n}\beta_i + \Theta(\hat{x}_1)$$

and Θ is of degree at most $n-1$ by construction.

(**Step5**.4) Consequently, the two results obtained in step (**Step5**.3) lead to

$$\left(\prod_{i=1}^{n}\beta_i - \beta\right)\hat{x}_1^n + \underbrace{p_{n-1}^{(n)}(\hat{x}_1) + \Theta(\hat{x}_1)}_{\text{of degree at most } n-1} = 0.$$

By the *Schwartz-Zippel* lemma, we conclude with overwhelming probability the following result

$$\boxed{\beta = \prod_{i=1}^{n}\beta_i.}$$

Results obtained in steps **(Step 1)** to **(Step 5)**, give us the following result, proving that, with *overwhelming probability*, we have successfully extract a witness $w \stackrel{\text{def}}{=} (\overrightarrow{\beta}, \xi) \in \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$ such that $(\sigma, \chi, w) \in \mathcal{R}_{\mathsf{SVPA}}^{\mathsf{BG}}$.

$$\boxed{\exists\, \overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^n,\ \exists\, \xi \in \mathbb{F}_{p_\eta},\ \begin{cases} c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \overrightarrow{\beta}\,;\, \xi\right) \\ \beta = \prod_{i=1}^{n}\beta_i \end{cases}}$$

Proof step → / **↓ Property**	step **(Step 1)**	step **(Step 2)**	step **(Step 3)**	step **(Step 4)**	step **(Step5.4)**
***Binding* of commitment scheme**	× 1	× 1	× 1	× 1	
Schwartz-Zippel					× 1
Extractor uses *rewinding*?	Yes (2 witnesses)				

Table 4: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Single Value Product Argument protocol

Comment [MC2]: Verify if we need property transfer under adversarial selection here

□

[18] More precisely, polynomial $p_1^{(i)}$ is defined as follows:

$$\forall\, i \in [\![2;n]\!],\ p_1^{(i)}(X) \stackrel{\text{def}}{=} \gamma_i + \lambda_i X,$$

where γ_i and λ_i are some constant values regarding X.

B.5 Hadamard product argument protocol

We define

$$\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}} \subseteq \underbrace{\mathbb{G}_{p_\eta}^{n+1}}_{\text{Public parameter set}} \times \underbrace{\left(\mathbb{G}_{p_\eta}^{m} \times \mathbb{G}_{p_\eta}\right)}_{\text{Statement set}} \times \underbrace{\left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m} \times \mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta}\right)}_{\text{Witness set}}$$

to be the *Hadamard product relation* defined by

$$\left(ck, (\mathbf{c}_\Gamma, c_\beta), \left(\left(\mathbf{\Gamma}^{(j)}\right)_{j=1}^{m}, \mathbf{v}, \overrightarrow{\beta}, \xi\right)\right) \in \mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$$

$$\overset{\text{def}}{\iff} \begin{cases} \mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \left(\mathbf{\Gamma}^{(j)}\right)_{j=1}^{m}; \mathbf{v}\right) \\ c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}; \xi\right) \\ \overrightarrow{\beta} = \bigodot_{j=1}^{m} \mathbf{\Gamma}^{(j)} \end{cases}$$

Hence, we define a 5-move *zero-knowledge* protocol for the Hadamard product argument $\mathbb{ZK}^{(2)}[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}]$ to be the protocol defined as follows in **Protocol 9**.

Theorem B.5 (Knowledge soundness of $\mathbb{ZK}^{(2)}[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}]$). *The 5-move* zero-knowledge *protocol* $\mathbb{ZK}^{(2)}[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}]$ *for the Hadamard product relation* $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$ *is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\mathsf{HPA}}$ for the Bayer-Groth Hadamard product argument to be the algorithm defined as follows in **Extractor 10**[19].

Let $n, m \in \mathbb{N}^*$ be two natural numbers. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time and deterministic adversarial prover. Let $\sigma = ck \leftarrow \mathcal{I}_{\mathsf{HPA}}(\eta)$ be an honest public parameter for the Hadamard product relation $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, ck)$ be an adversarial statement where

$$\chi \overset{\text{def}}{=} (c_\Gamma, c_\beta) \in \mathbb{G}_{p_\eta}^{m} \times \mathbb{G}_{p_\eta}.$$

Next, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\mathsf{HPA}}$ on inputs ck and χ with access to $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{HPA}}$ and obtains a witness candidate w_{out} **– in particular, $\mathcal{E}_{\mathsf{HPA}}$ has not aborted –** where

$$w_{\text{out}} \overset{\text{def}}{=} \left(\Gamma, \mathbf{v}, \Xi^{(m)}, \varsigma_m\right).$$

The only thing it remains to prove is to verify if we have indeed a witness for $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$ with public parameter σ and adversarial statement χ, *i.e.* we have to show the following property:

$$\left(ck, (\mathbf{c}_\Gamma, \mathbf{c}_\beta), w_{\text{out}}\right) \in \mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}.$$

[19]

Comment [MC3]: Funny fact:
– **Warning –** **Extractor 10** at line 3 leads to some probability of failure. It depends whether $\mathcal{P}^*$ gives a suitable commit vector value $\mathbf{c}_\Gamma$ or not.
– **Proposed fix –** A possible fix to this issue is to rewind $\mathcal{P}^*$ until we have a suitable commit vector value $\mathbf{c}_\Gamma$.

More precisely, by definition of the relation $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$, we have to prove the three following properties

$$\mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma; \mathbf{v}\right), \tag{O_1}$$

$$c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \Xi^{(m)}; \varsigma_m\right), \tag{O_2}$$

$$\Xi^{(m)} = \bigodot_{j=1}^{m} \mathbf{\Gamma}^{(j)} \tag{O_3}$$

(Step 1) – Preliminaries – Zero Argument consequences.

(Step1.1) By the *knowledge soundness* of the zero argument protocol (see Theorem B.6), we obtain

- $\mathbf{c}_{\tilde{\Gamma}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \left(\tilde{\mathbf{\Gamma}}^{(j)}\right)_{j=1}^{m}; \overrightarrow{\mu}\right)$;
- $\mathbf{c}_{\tilde{\Upsilon}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \left(\tilde{\mathbf{\Upsilon}}^{(j)}\right)_{j=1}^{m}; \overrightarrow{\nu}\right)$; and
- $0 = \sum_{j=1}^{m} \tilde{\mathbf{\Gamma}}^{(j)} \star_v \tilde{\mathbf{Y}}^{(j-1)}$.

Using definitions given by the extractor $\mathcal{E}_{\mathsf{HPA}}$ (see **Extractor 10**), these hypothesis become:

($\mathcal{H}_1$) For all $j \in [\![1; m-1]\!]$,

$$c_{\Gamma_{j+1}} = c_{\tilde{\Gamma}_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\mathbf{\Gamma}}^{(j)}; \mu_j\right) \quad \textit{see line 5}$$

$$= \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \mathbf{\Gamma}^{(j+1)}; v_{j+1}\right) \quad \textit{see line 9}$$

and, for the special case $j = m$, we have

$$c_{-1} = c_{\tilde{\Gamma}_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\mathbf{\Gamma}}^{(m)}; \mu_m\right) \quad \textit{see line 5}$$

($\mathcal{H}_2$) For all $j \in [\![0; m-2]\!]$,

$$c_{\Upsilon_{j+1}}^{u^{j+1}} = c_{\tilde{\Upsilon}_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\mathbf{\Upsilon}}^{(j)}; \nu_j\right) \quad \textit{see line 5}$$

$$= \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, u^{j+1}\Xi^{(j+1)}; u^{j+1}\varsigma_{j+1}\right) \quad \textit{see line 8}$$

and, for the special case $j = m-1$, we have

$$c_{\tilde{\Upsilon}_{m-1}} = \prod_{j=1}^{m-1} c_{\Upsilon_{j+1}}^{u^j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\mathbf{\Upsilon}}^{(m-1)}; \nu_{m-1}\right) \quad \textit{see line 5}$$

$$= \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \sum_{j=1}^{m-1} u^j \Xi^{(j+1)}; \sum_{j=1}^{m-1} u^j \varsigma_{j+1}\right) \quad \textit{see line 8}$$

($\mathcal{H}_3$) The following equation holds:

$$0 = \sum_{j=1}^{m} \tilde{\mathbf{\Gamma}}^{(j)} \star_v \tilde{\mathbf{Y}}^{(j-1)}$$

$$= \sum_{j=1}^{m-1} \mathbf{\Gamma}^{(j+1)} \star_v \left(u^j \Xi^{(j)}\right) + \tilde{\mathbf{\Gamma}}^{(m)} \star_v \tilde{\mathbf{Y}}^{(m-1)} \quad \textit{see lines 8 and 9}$$

(Step1.2) Notice that, thanks to the *rewinding* lemma, with *overwhelming probability*, extractor $\mathcal{E}_{\mathsf{HPA}}$ does not abort.

(Step 2) – Let us show equation Eq. (O_1).

(Step2.1) Using Hypo. ($\mathcal{H}_1$), we already have

$$\boxed{\forall\, j \in [\![2; m]\!],\ c_{\Gamma_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \mathbf{\Gamma}^{(j)}; v_j\right).}$$

Protocol 9: 5-move *zero-knowledge* protocol $\mathbb{ZK}^{(2)}\left[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}\right]$ for the Bayer-Groth Hadamard product argument

Public Input : Two natural numbers $n, m \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{n+1}$ for the commitment scheme $\mathbb{KS}\left[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})\right]$. Two commit values $\mathbf{c}_\Gamma \in \mathbb{G}_{p_\eta}^m$ and $c_\beta \in \mathbb{G}_{p_\eta}$.

Private Input : A matrix $\Gamma = \left(\mathbf{\Gamma}^{(j)}\right)_{j=1}^m \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$, a vector of random values $\mathbf{v} \xleftarrow{\$} \mathbb{F}_{p_\eta}^m$, a vector $\overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^n$, and a random value $\xi \xleftarrow{\$} \mathbb{F}_{p_\eta}$, such that

$$\mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \Gamma\,;\, \mathbf{v}\right),\ c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \overrightarrow{\beta}\,;\, \xi\right), \text{ and } \overrightarrow{\beta} = \bigodot_{j=1}^m \mathbf{\Gamma}^{(j)}.$$

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{HPA}}$ defines, for all $j \in [\![1; m-1]\!]$, $\mathbf{Y}^{(j)} \leftarrow \bigodot_{k=1}^{j} \mathbf{\Gamma}^{(k)} \in \mathbb{F}_{p_\eta}^n$ and $\mathbf{Y}^{(m)} \leftarrow \overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^n$. Next, the prover generates random values $\varsigma_2, \ldots, \varsigma_{m-1} \xleftarrow{\$} \mathbb{F}_{p_\eta}$ and computes commit values $c_{\Upsilon_j} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \mathbf{Y}_j\,;\, \varsigma_j\right) \in \mathbb{G}_{p_\eta}$ for all $j \in [\![2; m-1]\!]$. Then, $\mathcal{P}_{\mathsf{HPA}}$ defines $\varsigma_1 \leftarrow v_1 \in \mathbb{F}_{p_\eta}$ and $\varsigma_m \leftarrow \xi \in \mathbb{F}_{p_\eta}$ and then sets $c_{\Upsilon_1} \leftarrow c_{\Gamma_1} \in \mathbb{G}_{p_\eta}$ and $c_{\Upsilon_m} \leftarrow c_\beta \in \mathbb{G}_{p_\eta}$. Finally, the prover $\mathcal{P}_{\mathsf{HPA}}$ sends to the verifier $\mathcal{V}_{\mathsf{HPA}}$ the commit value $\mathbf{c}_\Upsilon$.

(2) **(Challenge message)** The verifier $\mathcal{V}_{\mathsf{HPA}}$ generates two challenges $u, v \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ and sends them to the prover.

(3-5) **(Zero argument call)** For all $i \in [\![1; m-1]\!]$, let $c_{\tilde{\Upsilon}_i}$ the value defined by $c_{\tilde{\Upsilon}_i} \leftarrow c_{\Upsilon_i}^{u^i} \in \mathbb{G}_{p_\eta}$, let $c_{\tilde{\Upsilon}}$ be the value defined by $c_{\tilde{\Upsilon}} \leftarrow \prod_{i=1}^{m-1} c_{\Upsilon_{i+1}}^{u^i} \in \mathbb{G}_{p_\eta}$, and let c_{-1} the commit value $c_{-1} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, -\mathbf{1}\,;\, 0\right) \in \mathbb{G}_{p_\eta}$. Let $\star_v : \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \longrightarrow \mathbb{F}_{p_\eta}$ be the bilinear application defined by, for two vectors $\mathbf{a} = (a_i)_{i=1}^n \in \mathbb{F}_{p_\eta}^n$ and $\mathbf{b} = (b_i)_{i=1}^n \in \mathbb{F}_{p_\eta}^n$, $\mathbf{a} \star_v \mathbf{b} \overset{\text{def}}{=} \sum_{i=1}^n a_i b_i v^i$. Then, both prover $\mathcal{P}_{\mathsf{HPA}}$ and verifier $\mathcal{V}_{\mathsf{HPA}}$ engage in the Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}\right]$ for the relation $\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}$ with public parameter $\sigma_{\mathsf{ZA}} \overset{\text{def}}{=} ck$, public statement $x_{\mathsf{ZA}} \overset{\text{def}}{=} \left((c_{\Gamma_2}, \ldots, c_{\Gamma_m}, c_{-1}), (c_{\tilde{\Upsilon}_1}, \ldots, c_{\tilde{\Upsilon}_{m-1}}, c_{\tilde{\Upsilon}})\right)$, and private statement $w_{\mathsf{ZA}} \overset{\text{def}}{=} \left(\left(\mathbf{\Gamma}^{(2)}, \ldots, \mathbf{\Gamma}^{(m)}, -\mathbf{1}\right), (v_2, \ldots, v_m, 0), \left(u\mathbf{Y}_1, \ldots, u^{m-1}\mathbf{Y}^{(m-1)}, \sum_{j=1}^{m-1} u^j \mathbf{Y}^{(j+1)}\right), \left(u\varsigma_1, \ldots, u^{m-1}\varsigma_{m-1}, \sum_{j=1}^{m-1} u^j \varsigma_{j+1}\right)\right)$. We denote by τ_{ZA} the proof transcript obtained at the end of this Σ-protocol.

(6) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{ZA}}$ checks if $c_{\Upsilon_1} = c_{\Gamma_1}$ and $c_{\Upsilon_m} = c_\beta$. Then, $\mathcal{V}_{\mathsf{ZA}}$ accepts if and only if $v_{\mathsf{ZA}}^{\sigma_{\mathsf{ZA}}, x_{\mathsf{ZA}}}\left(\tau_{\mathsf{ZA}}\right)$ holds.

Extractor 10: Extractor $\mathcal{E}_{\mathsf{HPA}}$ for the 5-move *zero-knowledge* protocol $\mathbb{ZK}^{(2)}\left[\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}\right]$ of the Bayer-Groth Hadamard product argument

Input : A security parameter $\eta \in \mathbb{N}^*$. Two natural numbers $n, m \in \mathbb{N}^*$. A public parameter $\sigma \overset{\text{def}}{=} ck \in \mathbb{G}_{p_\eta}^{n+1}$ for the Bayer-Groth Hadamard product relation $\mathcal{R}_{\mathsf{HPA}}^{\mathsf{BG}}$. A statement $\chi \overset{\text{def}}{=} (\mathbf{c}_\Gamma, c_\beta) \in \mathbb{G}_{p_\eta}^m \times \mathbb{G}_{p_\eta}$.

Blackbox access to : A deterministic adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{HPA}}$.

1 **Begin extractor**

2 **calls $\mathcal{P}^*$ to get** $\mathbf{c}_\Upsilon \overset{\text{def}}{=} \left(c_{\Upsilon_i}\right)_{i=1}^m \in \mathbb{G}_{p_\eta}^m$;

3 **if** $c_{\Upsilon_1} \neq c_{\Gamma_1}$ **or** $c_{\Upsilon_m} \neq c_\beta$ **then abort**;

4 **calls $\mathcal{V}_{\mathsf{HPA}}$ to get** $(u, v) \xleftarrow{\$} \mathbb{F}_{p_\eta}^* \times \mathbb{F}_{p_\eta}^*$;

5 **computes**
$$\begin{cases} \mathbf{c}_{\tilde{\Gamma}} \leftarrow \left(c_{\tilde{\Gamma}_i}\right)_{i=1}^m \in \mathbb{G}_{p_\eta}^m & \text{where, for all } i \in [\![1; m]\!],\ c_{\tilde{\Gamma}_i} \leftarrow \begin{cases} c_{\Gamma_{i+1}} & \textbf{if } i < m \\ c_{-1} \overset{\text{def}}{=} \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, -\mathbf{1}\,;\, 0\right) & \textbf{otherwise, i.e. } i = m. \end{cases} \\ \mathbf{c}_{\tilde{\Upsilon}} \leftarrow \left(c_{\tilde{\Upsilon}_i}\right)_{i=0}^{m-1} \in \mathbb{G}_{p_\eta}^m & \text{where, for all } i \in [\![0; m-1]\!],\ c_{\tilde{\Upsilon}_i} \leftarrow \begin{cases} c_{\Upsilon_{i+1}}^{u^{i+1}} & \textbf{if } i < m-1 \\ \prod_{j=1}^{m-1} c_{\Upsilon_{j+1}}^{u^j} & \textbf{otherwise, i.e. } i = m-1. \end{cases} \end{cases} ;$$

6 **sets** $\star_v : \begin{array}{ccc} \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n & \longrightarrow & \mathbb{F}_{p_\eta} \\ \left((a_i)_{i=1}^n, (b_i)_{i=1}^n\right) & \longmapsto & \sum_{i=1}^n a_i b_i v^i \end{array}$;

7 **calls $\mathcal{E}_{\mathsf{ZA}}$ with oracles $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{HPA}}$ on inputs** $\left(ck, \star_v\right), \left(\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}}\right)$ **to get** $\left(\left(\tilde{\mathbf{\Gamma}}^{(j)}\right)_{j=1}^m, \overrightarrow{\mu}, \left(\tilde{\mathbf{Y}}^{(j)}\right)_{j=0}^{m-1}, \overrightarrow{\nu}\right) \in \left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m \times \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m\right)$;

8 **computes**
$$\begin{cases} \Xi \leftarrow \left(\Xi^{(j)}\right)_{j=1}^m \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) & \text{where, for all } j \in [\![1; m]\!],\ \Xi^{(j)} \leftarrow \begin{cases} u^{-j}\tilde{\mathbf{Y}}^{(j-1)} & \textbf{if } j < m \\ u^{1-m}\left(\tilde{\mathbf{Y}}^{(m-1)} - \sum_{j=1}^{m-2} u^j \Xi^{(j+1)}\right) & \textbf{otherwise, i.e. } j = m \end{cases} \\ \overrightarrow{\varsigma} \leftarrow \left(\varsigma_j\right)_{j=1}^m \in \mathbb{F}_{p_\eta}^m & \text{where, for all } j \in [\![1; m]\!],\ \varsigma_j \leftarrow \begin{cases} u^{-j} v_{j-1} & \textbf{if } j < m \\ u^{1-m}\left(v_{m-1} - \sum_{j=1}^{m-2} u^j \varsigma_{j+1}\right) & \textbf{otherwise, i.e. } j = m. \end{cases} \end{cases} ;$$

9 **computes**
$$\begin{cases} \Gamma \leftarrow \left(\mathbf{\Gamma}^{(j)}\right)_{j=1}^m \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) & \text{where, for all } j \in [\![1; m]\!],\ \mathbf{\Gamma}^{(j)} \leftarrow \begin{cases} \tilde{\mathbf{\Gamma}}^{(j-1)} & \textbf{if } j > 1 \\ \Xi^{(1)} & \textbf{otherwise, i.e. } j = 1 \end{cases} \\ \mathbf{v} \leftarrow \left(v_j\right)_{j=1}^m \in \mathbb{F}_{p_\eta}^m & \text{where, for all } j \in [\![1; m]\!],\ v_j \leftarrow \begin{cases} \mu_{j-1} & \textbf{si } j > 1 \\ \varsigma_1 & \textbf{otherwise, i.e. } j = 1. \end{cases} \end{cases} ;$$

10 **returns** $\left(\Gamma, \mathbf{v}, \Xi^{(m)}, \varsigma_m\right)$.

(**Step2**.2) Next, by definition given in line 9, we have

$$\mathbf{\Gamma}^{(1)} \stackrel{\text{def}}{=} \Xi^{(1)} \quad \text{and} \quad v_1 \stackrel{\text{def}}{=} \varsigma_1.$$

By definition given in line 8, we have

$$\Xi^{(1)} \stackrel{\text{def}}{=} u^{-1}\tilde{\mathbf{Y}}^{(0)} \quad \text{and} \quad \varsigma_1 \stackrel{\text{def}}{=} u^{-1}v_0.$$

Then, Hypo. ($\mathcal{H}_2$) leads to

$$c_{\Upsilon_1}^{u} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\mathbf{Y}}^{(0)}\,;\, v_0\right) = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, u\Xi^{(1)}\,;\, u\varsigma_1\right)$$

It follows, because $\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}$ is homomorphic and because $u \neq 0$, the following equations

$$c_{\Upsilon_1}^{u} = \left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(1)}\,;\, \varsigma_1\right)\right)^u$$

$$\textit{i.e.} \quad c_{\Upsilon_1} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(1)}\,;\, \varsigma_1\right) = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \mathbf{\Gamma}^{(1)}\,;\, v_1\right).$$

(**Step2**.3) Because $\mathcal{E}_{\mathsf{HPA}}$ has not aborted, the if-condition in line 3 does not hold. In particular, we have $c_{\Upsilon_1} = c_{\Gamma_1}$. This finally leads to

$$\boxed{c_{\Gamma_1} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \mathbf{\Gamma}^{(1)}\,;\, v_1\right).}$$

(Step 3) – Let us show equation Eq. (O_2).

(**Step3**.1) Using Hypo. ($\mathcal{H}_2$), we have

$$\prod_{j=1}^{m-1} c_{\Upsilon_{j+1}}^{u^j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \sum_{j=1}^{m-1} u^j\Xi^{(j+1)}\,;\, \sum_{j=1}^{m-1} u^j\varsigma_{j+1}\right)$$

$$= \prod_{j=1}^{m-1}\left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(j+1)}\,;\, \varsigma_{j+1}\right)\right)^{u^j}$$

(**Step3**.2) By application of the function $\log_g : \mathbb{G}_{p_\eta} \longrightarrow \mathbb{F}_{p_\eta}$, the previous equation becomes

$$\sum_{j=1}^{m-1} u^j \log_g c_{\Upsilon_{j+1}} = \sum_{j=1}^{m-1} u^j \log_g\left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(j+1)}\,;\, \varsigma_{j+1}\right)\right),$$

which is a polynomial equation of degree at most $m-1$ in challenge u. Thus, by the *Schwartz-Zippel* lemma, we conclude with overwhelming probability the following property

$$\forall\, j \in [\![1; m-1]\!],\ \log_g c_{\Upsilon_{j+1}} = \log_g\left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(j+1)}\,;\, \varsigma_{j+1}\right)\right).$$

The *injectivity* of function $\log_g$ leads to

$$\forall\, j \in [\![2; m]\!],\ c_{\Upsilon_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(j)}\,;\, \varsigma_j\right).$$

(**Step3**.3) In the particular case of $j = m$, we have

$$c_{\Upsilon_m} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(m)}\,;\, \varsigma_m\right).$$

And, because $\mathcal{E}_{\mathsf{HPA}}$ has not aborted, line 3 leads to $c_{\Upsilon_m} = c_\beta$. Consequently, we finally obtain the following equation

$$\boxed{c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \Xi^{(m)}\,;\, \varsigma_m\right).}$$

(Step 4) – Let us finally show equation Eq. (O_3).

(**Step4**.1) Using Hypo. ($\mathcal{H}_3$) and because $\star_v$ is bilinear (see line 7), we have

$$0 = \sum_{j=1}^{m-1} u^j\left(\mathbf{\Gamma}^{(j+1)} \star_v \Xi^{(j)}\right) + \tilde{\mathbf{\Gamma}}^{(m)} \star_v \tilde{\mathbf{Y}}^{(m-1)}. \tag{∇}$$

(**Step4**.2) Next, Hypo. ($\mathcal{H}_1$) leads to

$$\mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, -\mathbf{1}\,;\, 0\right) = c_{-1} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\mathbf{\Gamma}}^{(m)}\,;\, \mu_m\right).$$

Thus, because $\mathbb{KS}[\mathbb{F}_{p_\eta}^n]$ is *computationally binding*, with overwhelming probability, the equation above leads to $\tilde{\mathbf{\Gamma}}^{(m)} = -\mathbf{1}$. Moreover, by definition of $\tilde{\mathbf{Y}}^{(m-1)}$ given in line 8, we have

$$\tilde{\mathbf{Y}}^{(m-1)} = \sum_{j=1}^{m-1} u^j\Xi^{(j+1)}.$$

(**Step4**.3) Therefore, by the two results obtained in previous step (**Step4**.2) and because $\star_v$ is bilinear, equation Eq. (∇) becomes

$$0 = \sum_{j=1}^{m-1}\left(\mathbf{\Gamma}^{(j+1)} \star_v \Xi^{(j)} - \mathbf{1} \star_v \Xi^{(j+1)}\right)u^j, \tag{∇'}$$

which is a polynomial equation in challenge u. Thus, by the *Schwartz-Zippel* lemma, with overwhelming probability, this previous equation Eq. (∇') leads to

$$\forall\, j \in [\![1; m-1]\!],\ \mathbf{1} \star_v \Xi^{(j+1)} = \mathbf{\Gamma}^{(j+1)} \star_v \Xi^{(j)}. \tag{Ψ}$$

(**Step4**.4) By definition of the bilinear map $\star_v$ given in line 7, previous property Eq. (Ψ) becomes

$$\forall\, j \in [\![1; m-1]\!],\ \sum_{i=1}^{n} \Xi_{i,j+1}v^i = \sum_{i=1}^{n} \Gamma_{i,j+1}\Xi_{i,j}v^i,$$

which are $m-1$ polynomial equations in challenge v. Thus, by the *Schwartz-Zippel* lemma, with overwhelming probability, and then by definition of operator $\odot$, these equations above become

$$\forall\, j \in [\![1; m-1]\!],\ \Xi^{(j+1)} = \mathbf{\Gamma}^{(j+1)} \odot \Xi^{(j)}.$$

(**Step4**.5) By immediate induction, this leads to

$$\Xi^{(m)} = \left(\bigodot_{j=2}^{m} \mathbf{\Gamma}^{(j)}\right) \odot \Xi^{(1)}.$$

Consequently, by definition of $\mathbf{\Gamma}^{(1)}$ given in line 9, we finally obtain

$$\boxed{\Xi^{(m)} = \bigodot_{j=1}^{m} \mathbf{\Gamma}^{(j)}.}$$

Results obtained in steps **(Step 2)** to **(Step 4)**, give us the following result, proving that, with *overwhelming probability*, we have successfully extract a witness

$$w_{\text{out}} \stackrel{\text{def}}{=} \left(\Gamma, \mathbf{v}, \Xi^{(m)}, \varsigma_m\right) \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m \times \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$$

such that $(ck, \chi, w_{\text{out}}) \in \mathcal{R}_{\text{HPA}}^{\text{BG}}$.

$$\exists\, \Gamma \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}),\ \exists\, \mathbf{v} \in \mathbb{F}_{p_\eta}^{m},\ \exists\, \overrightarrow{\beta} \in \mathbb{F}_{p_\eta}^{n},\ \exists\, \xi \in \mathbb{F}_{p_\eta},$$
$$\begin{cases} \mathbf{c}_\Gamma = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}(ck, \Gamma\,;\, \mathbf{v}) \\ c_\beta = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \overrightarrow{\beta}\,;\, \xi\right) \\ \overrightarrow{\beta} = \bigodot_{j=1}^{m} \Gamma^{(j)} \end{cases}$$

Proof step → / ↓ Property	step (Step 1.1)	step (Step 3.2)	step (Step 4.2)	step (Step 4.3)	step (Step 4.4)
Knowledge soundness	$1\times$ $\mathcal{E}_{\text{ZA}}$				
Binding of commitment scheme			$\times 1$		
Schwartz-Zippel		$\times 1$		$\times 1$	$\times$ $(m-1)$
Extractor uses *rewinding*?	Yes (to obtain a suitable commit vector value $\mathbf{c}_\Upsilon$)				

Table 5: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Hadamard Product Argument protocol

□

B.6 Zero argument protocol

We define

$$\mathcal{R}_{\text{ZA}}^{\text{BG}} \subseteq \underbrace{\left(\mathbb{G}_{p_\eta}^{n+1} \times \left(\mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta}^{n} \longrightarrow \mathbb{F}_{p_\eta}\right)\right)}_{\text{Public parameter set}} \times \underbrace{\left(\mathbb{G}_{p_\eta}^{m} \times \mathbb{G}_{p_\eta}^{m}\right)}_{\text{Statement set}}$$
$$\times \underbrace{\left(\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m} \times \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^{m}\right)}_{\text{Witness set}}$$

to be the *zero argument relation* defined by

$$\left((ck, \star), \left(\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}}\right), \left(\left(\tilde{\Gamma}^{(j)}\right)_{j=1}^{m}, \overrightarrow{\mu}, \left(\tilde{\Upsilon}^{(j)}\right)_{j=0}^{m-1}, \overrightarrow{\nu}\right)\right) \in \mathcal{R}_{\text{ZA}}^{\text{BG}}$$
$$\overset{\text{def}}{\iff} \begin{cases} \mathbf{c}_{\tilde{\Gamma}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \left(\tilde{\Gamma}^{(j)}\right)_{j=1}^{m}\,;\, \overrightarrow{\mu}\right) \\ \mathbf{c}_{\tilde{\Upsilon}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \left(\tilde{\Upsilon}^{(j)}\right)_{j=0}^{m-1}\,;\, \overrightarrow{\nu}\right) \\ 0 = \sum_{j=1}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\Upsilon}^{(j-1)}. \end{cases}$$

Hence, we define a Σ-protocol for the zero argument relation $\Sigma\left[\mathcal{R}_{\text{ZA}}^{\text{BG}}\right]$ to be the protocol defined as follows in **Protocol 11**.

Theorem B.6 (Knowledge soundness of $\Sigma\left[\mathcal{R}_{\text{ZA}}^{\text{BG}}\right]$). *The Σ-protocol $\Sigma\left[\mathcal{R}_{\text{ZA}}^{\text{BG}}\right]$ for the Bayer-Groth zero relation $\mathcal{R}_{\text{ZA}}^{\text{BG}}$ is* knowledge sound.

Proof. We define the extractor $\mathcal{E}_{\text{ZA}}$ for the Bayer-Groth zero argument to be the algorithm defined as follows in **Extractor 12**.

Let $n, m \in \mathbb{N}^*$ be two natural numbers. Let $\eta \in \mathbb{N}^*$ be a security parameter. Let $\mathcal{P}^*$ be a polynomial-time and deterministic adversarial prover. Let $(ck, \star) \leftarrow \mathcal{I}_{\text{ZA}}(\eta)$ ve an honest public parameter for the zero argument relation $\mathcal{R}_{\text{ZA}}^{\text{BG}}$. Let $\mathcal{A}$ be a probabilistic and polynomial-time adversary. Let $\chi \leftarrow \mathcal{A}(\eta, \sigma)$ be an adversarial statement where

$$\chi \overset{\text{def}}{=} \left(\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}}\right) \in \mathbb{G}_{p_\eta}^{m} \times \mathbb{G}_{p_\eta}^{m}.$$

Then, the adversary $\mathcal{A}$ calls the extractor $\mathcal{E}_{\text{ZA}}$ on inputs σ and χ with access to $\mathcal{P}^*$ and $\mathcal{V}_{\text{ZA}}$ and obtains a sequence of valid proof transcripts $\tau_{\text{ZA}} \overset{\text{def}}{=} \left(\mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\text{ZA}}^{\text{BG}},\, \mathcal{P}^*}(\omega_l)}^{\sigma,\, \chi}\right)_{l=1}^{2m+1}$. Let $l \in [\![1; 2m+1]\!]$ be an index. We denote by

- $\alpha \overset{\text{def}}{=} \left(c_{\tilde{\Gamma}_0}, c_{\tilde{\Upsilon}_m}, \mathbf{c}_\Psi\right) \in \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}^{2m+1}$ the first message ; and
- $\mathfrak{d}_{\mathcal{R}_{\text{ZA}}^{\text{BG}},\, \mathcal{P}^*}(\alpha, \omega_l) \overset{\text{def}}{=} \left(\tilde{\Gamma}_\omega^{(l)}, \mu_\omega^{(l)}, \tilde{\Upsilon}_\omega^{(l)}, \nu_\omega^{(l)}, \varsigma_\omega^{(l)}\right) \in \mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}^{n} \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}$ the response message on challenge ω_l.

This way, we have the following property

$$\forall\, l \in [\![1; 2m+1]\!], \begin{cases} \bullet\ \mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\text{ZA}}^{\text{BG}},\, \mathcal{P}^*}}^{\sigma,\, \chi}(\omega_l) = \left\langle \left(c_{\tilde{\Gamma}_0}, c_{\tilde{\Upsilon}_m}, \mathbf{c}_\Psi\right), \omega_l, \left(\tilde{\Gamma}_\omega^{(l)}, \mu_\omega^{(l)}, \tilde{\Upsilon}_\omega^{(l)}, \nu_\omega^{(l)}, \varsigma_\omega^{(l)}\right)\right\rangle \\ \bullet\ v_{\mathcal{R}_{\text{ZA}}^{\text{BG}}}^{\sigma,\, \chi}\left(\mathsf{tr}_{\alpha,\, \mathfrak{d}_{\mathcal{R}_{\text{ZA}}^{\text{BG}},\, \mathcal{P}^*}}^{\sigma,\, \chi}(\omega_l)\right) = 1. \end{cases}$$

By definition of the Bayer-Groth zero argument protocol, as the proof transcripts are valid, for all $l \in [\![1; 2m+1]\!]$, we have

$$c_{\Psi_{m+1}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, 0\,;\, 0), \tag{$\mathcal{H}_1$}$$
$$\prod_{i=0}^{m} c_{\tilde{\Gamma}_i}^{\omega_l^i} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\Gamma}_\omega^{(l)}\,;\, \mu_\omega^{(l)}\right), \tag{$\mathcal{H}_2^{(l)}$}$$
$$\prod_{i=0}^{m} c_{\tilde{\Upsilon}_i}^{\omega_l^{m-i}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^{n}}\left(ck, \tilde{\Upsilon}_\omega^{(l)}\,;\, \nu_\omega^{(l)}\right), \tag{$\mathcal{H}_3^{(l)}$}$$
$$\prod_{k=0}^{2m} c_{\Psi_k}^{\omega_l^k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, \tilde{\Gamma}_\omega^{(l)} \star \tilde{\Upsilon}_\omega^{(l)}\,;\, \varsigma_\omega^{(l)}\right). \tag{$\mathcal{H}_4^{(l)}$}$$

(Step 1) – Preliminaries – Vandermonde matrix of challenges sequence $(\omega_l)_{l=1}^{2m+1}$.
Let $\Omega_{\text{all}} \in \mathsf{Mat}_{2m+1}(\mathbb{F}_{p_\eta})$ and $\Omega_{\text{part}} \in \mathsf{Mat}_{m+1}(\mathbb{F}_{p_\eta})$ be two matrix defined as follows

$$\Omega_{\text{all}} \overset{\text{def}}{=} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega_1 & \omega_2 & \cdots & \omega_{2m+1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{2m} & \omega_2^{2m} & \cdots & \omega_{2m+1}^{2m} \end{pmatrix}$$

and

$$\Omega_{\text{part}} \overset{\text{def}}{=} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \omega_1 & \omega_2 & \cdots & \omega_{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1^{m} & \omega_2^{m} & \cdots & \omega_{m+1}^{m} \end{pmatrix}$$

Protocol 11: Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}\right]$ for the Bayer-Groth zero argument

Public Input : Two natural numbers $n, m \in \mathbb{N}^*$. A security parameter $\eta \in \mathbb{N}^*$. A commitment key $ck = (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{n+1}$ for the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$. A bilinear map $\star : \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \longrightarrow \mathbb{F}_{p_\eta}$. Two commit values $\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}} \in \mathbb{G}_{p_\eta}^m$.

Private Input : Two matrix $\tilde{\Gamma} = \left(\tilde{\Gamma}^{(j)}\right)_{j=1}^{m} \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$ and $\tilde{\Upsilon} = \left(\tilde{\Upsilon}^{(j)}\right)_{j=0}^{m-1} \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})$, and two vectors of random values $\overrightarrow{\mu}, \overrightarrow{\nu} \xleftarrow{\$} \mathbb{F}_{p_\eta}^m$ such that $\mathbf{c}_{\tilde{\Gamma}} \overset{\text{def}}{=} \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \tilde{\Gamma}\,;\, \overrightarrow{\mu}\right)$, $\mathbf{c}_{\tilde{\Upsilon}} \overset{\text{def}}{=} \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \tilde{\Upsilon}\,;\, \overrightarrow{\nu}\right)$, and $0 = \sum_{j=1}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\Upsilon}^{(j-1)}$.

Begin protocol

(1) **(Commit message)** The prover $\mathcal{P}_{\mathsf{ZA}}$ generates two random vectors $\tilde{\Gamma}^{(0)}, \tilde{\Upsilon}^{(m)} \xleftarrow{\$} \mathbb{F}_{p_\eta}^n$ and two random values $\mu_0, \nu_m \xleftarrow{\$} \mathbb{F}_{p_\eta}$. Then, the prover computes values $c_{\tilde{\Gamma}_0} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\Gamma}^{(0)}\,;\, \mu_0\right) \in \mathbb{G}_{p_\eta}$, $c_{\tilde{\Upsilon}_m} \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\Upsilon}^{(m)}\,;\, \nu_m\right) \in \mathbb{G}_{p_\eta}$, and, for all $k \in [\![0; 2m]\!]$, $\Psi_k \leftarrow \sum_{j=0}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\Upsilon}^{(m-k+j)} \in \mathbb{F}_{p_\eta}$. Next, $\mathcal{P}_{\mathsf{ZA}}$ generates a vector of random values $\overrightarrow{\varsigma} = (\varsigma_i)_{i=0}^{2m} \xleftarrow{\$} \mathbb{F}_{p_\eta}^{2m+1}$, sets $\varsigma_{m+1} \leftarrow 0 \in \mathbb{F}_{p_\eta}$, and computes commit value $\mathbf{c}_\Psi \leftarrow \mathsf{Com}_{\mathbb{F}_{p_\eta}^{2m+1}}\left(ck, \Psi\,;\, \overrightarrow{\varsigma}\right) \in \mathbb{G}_{p_\eta}^{2m+1}$. Finally, the prover $\mathcal{P}_{\mathsf{ZA}}$ sends commit values $\left(c_{\tilde{\Gamma}_0}, c_{\tilde{\Upsilon}_m}, \mathbf{c}_\Psi\right)$ to the verifier $\mathcal{V}_{\mathsf{ZA}}$.

(2) **(Challenge message)** The verifier $\mathcal{V}_{\mathsf{ZA}}$ generates a challenge $\omega \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$ and sends it to the prover $\mathcal{P}_{\mathsf{ZA}}$.

(3) **(Response message)** The prover $\mathcal{P}_{\mathsf{ZA}}$ computes values $\tilde{\Gamma} \leftarrow \sum_{j=0}^{m} \omega^j \tilde{\Gamma}^{(j)} \in \mathbb{F}_{p_\eta}^n$, $\mu \leftarrow \sum_{i=0}^{m} \omega^i \mu_i \in \mathbb{F}_{p_\eta}$, $\tilde{\Upsilon} \leftarrow \sum_{j=0}^{m} \omega^{m-j} \tilde{\Upsilon}^{(j)} \in \mathbb{F}_{p_\eta}^n$, $\nu \leftarrow \sum_{i=0}^{m} \omega^{m-i} \nu_i \in \mathbb{F}_{p_\eta}$, and $\varsigma \leftarrow \sum_{k=0}^{2m} \omega^k \varsigma_k \in \mathbb{F}_{p_\eta}$. Then, $\mathcal{P}_{\mathsf{ZA}}$ sends those values $\left(\tilde{\Gamma}, \mu, \tilde{\Upsilon}, \nu, \varsigma\right)$ to the verifier.

(4) **(Conclusion's bit)** The verifier $\mathcal{V}_{\mathsf{ZA}}$ accepts if and only if the following equations hold

$$c_{\Psi_{m+1}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, 0\,;\, 0\right), \quad \prod_{i=0}^{m} c_{\tilde{\Gamma}_i}^{\omega^i} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\Gamma}\,;\, \mu\right), \quad \prod_{i=0}^{m} c_{\tilde{\Upsilon}_i}^{\omega^{m-i}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\Upsilon}\,;\, \nu\right),$$

$$\text{and} \quad \prod_{k=0}^{2m} c_{\Psi_k}^{\omega^k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, \tilde{\Gamma} \star \tilde{\Upsilon}\,;\, \varsigma\right).$$

Extractor 12: Extractor $\mathcal{E}_{\mathsf{ZA}}$ for the Σ-protocol $\Sigma\left[\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}\right]$ of the Bayer-Groth zero argument

Input : A security parameter $\eta \in \mathbb{N}^*$. Two natural numbers $n, m \in \mathbb{N}^*$. A public parameter $\sigma \overset{\text{def}}{=} (ck, \star)$ for the Bayer-Groth zero argument relation $\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}$ with a bilinear map $\star : \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}^n \longrightarrow \mathbb{F}_{p_\eta}$ and a commitment key $ck \in (g, \mathbf{g}) \in \mathbb{G}_{p_\eta}^{n+1}$ for the commiment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})]$. A statement $\chi \overset{\text{def}}{=} \left(\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}}\right) \in \mathbb{G}_{p_\eta}^m \times \mathbb{G}_{p_\eta}^m$.

Blackbox access to : A deterministic adversarial prover $\mathcal{P}^*$ and an honest verifier $\mathcal{V}_{\mathsf{ZA}}$.

1 **Begin extractor**

2 **calls $\mathcal{P}^*$ to get** $\alpha \overset{\text{def}}{=} \left(c_{\tilde{\Gamma}_0}, c_{\tilde{\Upsilon}_m}, \mathbf{c}_\Psi\right) \in \left(\mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta} \times \mathbb{G}_{p_\eta}^{2m+1}\right)$; // State at this point: $\mathbf{st}_1 \overset{\text{def}}{=} \left[(ck, \star), \left(\mathbf{c}_{\tilde{\Gamma}}, \mathbf{c}_{\tilde{\Upsilon}}\right), \left(c_{\tilde{\Gamma}_0}, c_{\tilde{\Upsilon}_m}, \mathbf{c}_\Psi\right)\right]$.

3 **rewinds $\mathcal{P}^*$ and $\mathcal{V}_{\mathsf{ZA}}$ at state $\mathbf{st}_1$ and begins with** $l \leftarrow 1 \in \mathbb{N}$

4 **calls $\mathcal{V}_{\mathsf{ZA}}$ to get** $\omega_l \xleftarrow{\$} \mathbb{F}_{p_\eta}^*$;

5 **calls $\mathcal{P}^*$ to get** $z_l \leftarrow \mathfrak{d}_{\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}, \mathcal{P}^*}\left(\alpha, \omega_l\right) \in \left(\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}\right)$;

6 **if** $v_{\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}}^{ck, \chi}\left(\mathsf{tr}_{\alpha, \mathfrak{d}_{\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{ck, \chi}(\omega_l)\right)$ **and** $\bigwedge_{i=1}^{l-1} \bigwedge_{j=i+1}^{l} (\omega_i \neq \omega_j)$ **then** $l \leftarrow l + 1$;

7 **until** $l > 2m + 1$;

8 **returns** $\tau_{\mathsf{ZA}} \overset{\text{def}}{=} \left(\mathsf{tr}_{\alpha, \mathfrak{d}_{\mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}, \mathcal{P}^*}}^{\sigma, \chi}(\omega_l)\right)_{l=1}^{2m+1}$.

Ω_{all} and Ω_{part} are both transposed Vandermonde matrix with parameters the challenges sequence $(\omega_l)_{l=1}^{2m+1}$, which is a sequence of pairwise distincts values with overwhelming probability in η. Thus, Ω_{all} and Ω_{part} are invertible matrix.

(Step 2) – Get an opening of commit value $\mathbf{c}_\Psi$.

(**Step2**.1) We denote by $\mathbf{\Psi}_\omega \in \mathbb{F}_{p_\eta}^{2m+1}$ and $\overrightarrow{\varsigma}_\omega \in \mathbb{F}_{p_\eta}^{2m+1}$ the two vectors defined by

$$\mathbf{\Psi}_\omega \stackrel{\text{def}}{=} \left(\tilde{\Gamma}_\omega^{(l)} \star \tilde{\Upsilon}_\omega^{(l)}\right)_{l=1}^{2m+1}, \quad \text{and} \quad \overrightarrow{\varsigma}_\omega \stackrel{\text{def}}{=} \left(\varsigma_\omega^{(l)}\right)_{l=1}^{2m+1}. \qquad (\nabla)$$

Thus, we have

$$\begin{aligned}
\mathbf{c}_\Psi &= \left(\mathbf{c}_\Psi \circledast \Omega_{\mathsf{all}}\right) \circledast \Omega_{\mathsf{all}}^{-1} && \text{see footnotes 5 and 6}\\
&= \left(\mathsf{Com}_{\mathbb{F}_{p_\eta}^{2m+1}}\left(ck, \mathbf{\Psi}_\omega ; \overrightarrow{\varsigma}_\omega\right)\right) \circledast \Omega_{\mathsf{all}}^{-1} && \text{see Eq. } (\nabla) \text{ and Hypo. } \mathcal{H}_1\\
&= \mathsf{Com}_{\mathbb{F}_{p_\eta}^{2m+1}}\left(ck, \mathbf{\Psi}_\omega \cdot \Omega_{\mathsf{all}}^{-1} ; \overrightarrow{\varsigma}_\omega \cdot \Omega_{\mathsf{all}}^{-1}\right) && \text{see footnote 14}
\end{aligned}$$

(**Step2**.2) Next, by the *binding property* of $\mathbb{KS}[\mathbb{F}_{p_\eta}^{2m+1}]$, with overwhelming probability, there exists a sequence $\left((\Psi_k, \varsigma_k)\right)_{k=0}^{2m}$ of elements in $\mathbb{F}_{p_\eta} \times \mathbb{F}_{p_\eta}$ *independent of the sequence of challenges* $(\omega_l)_{l=1}^{2m+1}$ and such that the following property holds

$$\begin{array}{|l|}\hline \forall\, k \in [\![0; 2m]\!],\ c_{\Psi_k} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}\left(ck, \Psi_k ; \varsigma_k\right);\\ \quad \text{where } \Psi_k \stackrel{\text{def}}{=} \left(\mathbf{\Psi}_\omega \cdot \Omega_{\mathsf{all}}^{-1}\right)_k \text{ and } \varsigma_k \stackrel{\text{def}}{=} \left(\overrightarrow{\varsigma}_\omega \cdot \Omega_{\mathsf{all}}^{-1}\right)_k \\ \hline \end{array}$$

(Step 3) – Get an opening of commit value $\mathbf{c}_{\tilde{\Gamma}}$.

We denote by $\tilde{\Gamma}_\omega \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})$ the matrix and $\overrightarrow{\mu}_\omega \in \mathbb{F}_{p_\eta}^{m+1}$ the vector defined as follows

$$\tilde{\Gamma}_\omega \stackrel{\text{def}}{=} \left(\tilde{\Gamma}_\omega^{(l)}\right)_{l=1}^{m+1}, \quad \text{and} \quad \overrightarrow{\mu}_\omega \stackrel{\text{def}}{=} \left(\mu_\omega^{(l)}\right)_{l=1}^{m+1}.$$

Thus, similarly to the previous step **(Step 2)** but with matrix Ω_{part} instead of matrix Ω_{all} and with *binding property* on the commitment scheme $\mathbb{KS}[\mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})]$ instead of $\mathbb{KS}[\mathbb{F}_{p_\eta}^{2m+1}]$, extractor $\mathcal{E}_{\mathsf{ZA}}$ obtains an opening of $\mathbf{c}_{\tilde{\Gamma}}$. Thus, there exists a sequence $\left(\left(\tilde{\mathbf{\Gamma}}^{(j)}, \mu_j\right)\right)_{j=0}^{m}$ of elements in $\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$ *independent of the challenges sequence* $(\omega_l)_{l=1}^{2m+1}$ such that

$$\begin{array}{|l|}\hline \forall\, j \in [\![0; m]\!],\ c_{\tilde{\Gamma}_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\mathbf{\Gamma}}^{(j)} ; \mu_j\right)\\ \quad \text{where } \tilde{\mathbf{\Gamma}}^{(j)} \stackrel{\text{def}}{=} \left(\tilde{\Gamma}_\omega \Omega_{\mathsf{part}}^{-1}\right)^{(j+1)} \text{ and } \mu_j \stackrel{\text{def}}{=} \left(\overrightarrow{\mu}_\omega \cdot \Omega_{\mathsf{part}}^{-1}\right)_j \\ \hline \end{array}$$

(Step 4) – Get an opening of commit value $\mathbf{c}_{\tilde{\Upsilon}}$.

For all $l \in [\![1; 2m+1]\!]$, we rewrite Hypo. $\mathcal{H}_3^{(l)}$ as follows:

$$\prod_{j=0}^{m} c_{\tilde{\Upsilon}_{m-j}}^{\omega_l^j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\mathbf{\Upsilon}}_\omega^{(l)} ; \nu_\omega^{(l)}\right).$$

Let $\mathbf{c}'_{\tilde{\Upsilon}} \in \mathbb{F}_{p_\eta}^{m+1}$ be the vector defined by, for all $j \in [\![0; m]\!]$, $c'_{\tilde{\Upsilon}_j} \stackrel{\text{def}}{=} c_{\tilde{\Upsilon}_{m-j}}$. We denote by $\tilde{\Upsilon}_\omega \in \mathsf{Mat}_{n\times(m+1)}(\mathbb{F}_{p_\eta})$ the matrix and $\overrightarrow{\nu}_\omega \in \mathbb{F}_{p_\eta}^{m+1}$ the vector defined as follows

$$\tilde{\Upsilon}_\omega \stackrel{\text{def}}{=} \left(\tilde{\mathbf{\Upsilon}}_\omega^{(l)}\right)_{l=1}^{m+1}, \quad \text{and} \quad \overrightarrow{\nu}_\omega \stackrel{\text{def}}{=} \left(\nu_\omega^{(l)}\right)_{l=1}^{m+1}.$$

Thus, similarly to previous points with commit vector $\mathbf{c}'_{\tilde{\Upsilon}}$, Vandermonde matrix Ω_{part}, and by the *binding property* of $\mathbb{KS}[\mathbb{F}_{p_\eta}^{m+1}]$, $\mathcal{E}_{\mathsf{ZA}}$ obtains an opening of $\mathbf{c}'_{\tilde{\Upsilon}}$, and then of $\mathbf{c}_{\tilde{\Upsilon}}$. Therefore, there exists a sequence $\left(\left(\tilde{\mathbf{\Upsilon}}^{(j)}, \nu_j\right)\right)_{j=0}^{m}$ of elements in $\mathbb{F}_{p_\eta}^n \times \mathbb{F}_{p_\eta}$ *independent of the challenges sequence* $(\omega_l)_{l=1}^{2m+1}$ such that

$$\begin{array}{|l|}\hline \forall\, j \in [\![0; m]\!],\ c_{\tilde{\Upsilon}_j} = \mathsf{Com}_{\mathbb{F}_{p_\eta}^n}\left(ck, \tilde{\mathbf{\Upsilon}}^{(j)} ; \nu_j\right)\\ \quad \text{where } \tilde{\mathbf{\Upsilon}}^{(j)} \stackrel{\text{def}}{=} \left(\tilde{\Upsilon}_\omega \Omega_{\mathsf{part}}^{-1}\right)^{(m+1-j)} \text{ and}\\ \quad \nu_j \stackrel{\text{def}}{=} \left(\overrightarrow{\nu}_\omega \cdot \Omega_{\mathsf{part}}^{-1}\right)_{m+1-j} \\ \hline \end{array}$$

(Step 5) – It remains to prove the following equation:

$$0 = \sum_{j=1}^{m} \tilde{\mathbf{\Gamma}}^{(j)} \star \tilde{\mathbf{\Upsilon}}^{(j-1)}.$$

(**Step5**.1) For all $l \in [\![1; m+1]\!]$ and $i \in [\![1; n]\!]$, we have

$$\begin{aligned}
\left(\sum_{j=0}^{m} \omega_l^j \tilde{\mathbf{\Gamma}}^{(j)}\right)_i &= \left(\sum_{j=0}^{m} \omega_l^j \left(\tilde{\Gamma}_\omega \Omega_{\mathsf{part}}^{-1}\right)^{(j+1)}\right)_i && \text{by step (Step 3)}\\
&= \left(\sum_{j=1}^{m+1} \left(\Omega_{\mathsf{part}}\right)_{j,l} \left(\tilde{\Gamma}_\omega \Omega_{\mathsf{part}}^{-1}\right)^{(j)}\right)_i && \text{see definition of } \Omega_{\mathsf{part}} \text{ in step (Step 1)}\\
&= \sum_{j=1}^{m+1} \left(\Omega_{\mathsf{part}}\right)_{j,l} \left(\tilde{\Gamma}_\omega \Omega_{\mathsf{part}}^{-1}\right)_{i,j}\\
&= \left(\left(\tilde{\Gamma}_\omega \Omega_{\mathsf{part}}^{-1}\right)\Omega_{\mathsf{part}}\right)_{i,l} = \left(\tilde{\Gamma}_\omega\right)_{i,l} = \left(\tilde{\mathbf{\Gamma}}_\omega^{(l)}\right)_i.
\end{aligned}$$

Consequently, we have the following property

$$\forall\, l \in [\![1; m+1]\!],\ \tilde{\mathbf{\Gamma}}_\omega^{(l)} = \sum_{j=0}^{m} \omega_l^j \tilde{\mathbf{\Gamma}}^{(j)}.$$

(**Step5**.2) Similarly, for all $l \in [\![1; m+1]\!]$, we have

$$\sum_{j=0}^{m} \omega_l^{m-j} \tilde{\mathbf{\Upsilon}}^{(j)} = \sum_{j=0}^{m} \left(\Omega_{\mathsf{part}}\right)_{m+1-j,l} \left(\tilde{\Upsilon}_\omega \Omega_{\mathsf{part}}^{-1}\right)^{(m+1-j)} = \tilde{\mathbf{\Upsilon}}_\omega^{(l)}.$$

by step **(Step 4)**

(**Step5**.3) As in steps (**Step5**.1) and (**Step5**.2) but with full Vandermonde matrix Ω_{all} instead of Ω_{part}, step **(Step 2)** leads to

$$\forall\, l \in [\![1; 2m+1]\!],\ \tilde{\mathbf{\Gamma}}^{(l)} \star \tilde{\mathbf{\Upsilon}}^{(l)} = \sum_{k=0}^{2m} \omega_l^k \Psi_k.$$

(**Step5**.4) Hence, from equations obtained in steps (**Step5**.1) to (**Step5**.3), and using Hypo. $\mathcal{H}_1$, we conclude, for all $l \in [\![1; m+1]\!]$, the following equation:

$$\sum_{k=0}^{2m} \omega_l^k \Psi_k = \left(\sum_{i=0}^{m} \omega_l^i \tilde{\Gamma}^{(i)}\right) \star \left(\sum_{j=0}^{m} \omega_l^{m-j} \tilde{\mathbf{Y}}^{(j)}\right).$$

(**Step5**.5) By the previous step and because $\star$ is a bilinear map, for all $l \in [\![1; m+1]\!]$, we have

$$\left(\sum_{i=0}^{m} \omega_l^i \tilde{\Gamma}^{(i)}\right) \star \left(\sum_{j=0}^{m} \omega_l^{m-j} \tilde{\mathbf{Y}}^{(j)}\right) = \sum_{i=0}^{m}\sum_{j=0}^{m} \omega_l^{i+m-j} \tilde{\Gamma}^{(i)} \star \tilde{\mathbf{Y}}^{(j)}$$

$$= \sum_{k=0}^{m} \left(\sum_{\substack{j=0 \\ 0 \leqslant j+m-k \leqslant m}}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\mathbf{Y}}^{(j+m-k)} \right) \omega_l^k,$$

where "$k \leftarrow i + m - j$"

which is a polynomial equation of degree at most $2m$ in the challenges sub-sequence $(\omega_l)_{l=1}^{m+1}$. Thus, by the *Schwartz-Zippel* lemma, with overwhelming probability, equation obtained in the previous step leads to

$$\forall\, k \in [\![0; 2m]\!],\ \Psi_k = \sum_{\substack{j=0 \\ 0 \leqslant j+m-k \leqslant m}}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\mathbf{Y}}^{(j+m-k)}$$

(**Step5**.6) In the particular case of $k = m+1$, property obtained in previous step (**Step5**.5) leads to

$$\Psi_{m+1} = \sum_{j=1}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\mathbf{Y}}^{(j-1)}.$$

But, we have

- $c_{\Psi_{m+1}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, 0\,;\, 0)$ by Hypo. $\mathcal{H}_1$; and
- $c_{\Psi_{m+1}} = \mathsf{Com}_{\mathbb{F}_{p_\eta}}(ck, \Psi_{m+1}\,;\, \varsigma_{m+1})$ by definition of Ψ_{m+1} – see step **(Step 2)**.

Therefore, the *binding property* of $\mathbb{KS}[\mathbb{F}_{p_\eta}]$ leads to $\Psi_{m+1} = 0$ with overwhelming probability. Consequently, the following equality holds:

$$\boxed{0 = \sum_{j=1}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\mathbf{Y}}^{(j-1)}.}$$

Results obtained in steps **(Step 2)** to **(Step 5)**, give us the following result, proving that, with *overwhelming probability*, we have successfully extract a witness $w \overset{\text{def}}{=} \left(\tilde{\Gamma}, \overrightarrow{\mu}, \tilde{\Upsilon}, \overrightarrow{\nu}\right) \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m \times \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}) \times \mathbb{F}_{p_\eta}^m$ such that $(ck, \chi, w) \in \mathcal{R}_{\mathsf{ZA}}^{\mathsf{BG}}$.

$$\boxed{\begin{array}{l} \exists\, \tilde{\Gamma} \overset{\text{def}}{=} \left(\tilde{\Gamma}^{(j)}\right)_{j=1}^{m} \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}),\ \exists\, \overrightarrow{\mu} \in \mathbb{F}_{p_\eta}^m, \\ \exists\, \tilde{\Upsilon} \overset{\text{def}}{=} \left(\tilde{\mathbf{Y}}^{(j)}\right)_{j=0}^{m} \in \mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta}),\ \exists\, \overrightarrow{\nu} \in \mathbb{F}_{p_\eta}^m \\ \quad \begin{cases} \mathbf{c}_{\tilde{\Gamma}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \tilde{\Gamma}\,;\, \overrightarrow{\mu}\right) \\ \mathbf{c}_{\tilde{\Upsilon}} = \mathsf{Com}_{\mathsf{Mat}_{n\times m}(\mathbb{F}_{p_\eta})}\left(ck, \tilde{\Upsilon}\,;\, \overrightarrow{\nu}\right) \\ 0 = \sum\limits_{j=1}^{m} \tilde{\Gamma}^{(j)} \star \tilde{\mathbf{Y}}^{(j-1)} \end{cases} \end{array}}$$

Proof step → / **↓ Property**	step **(Step 1)**	step **(Step2.2)**	step **(Step 3)**	step **(Step 4)**	step **(Step5.5)**	step **(Step5.6)**
***Binding* of commitment scheme**		× 1	× 1	× 1		× 1
Schwartz-Zippel					× 1	
Property transfer under adversarial selection	Yes					
Extractor uses *rewinding*?	Yes ()					

Table 6: Assessment of cryptographic or probabilistic properties used to prove *Knowledge Soundness* of Zero Argument protocol

□

Zero-Knowledge protocol	Uses *Rewinding*?	Needs *Schwartz-Zippel*?	Needs *Binding* property?	Uses *Knowledge Soundness*?	Uses property transfer under adversarial selection
Single value product argument (SVPA)	**Yes:** 2 valid proof transcripts	**Yes:** $\times$ 1	**Yes:** $\times$ 4	**No**	**No**
Zero argument (ZA)	**Yes:** $2m + 1$ valid proof transcripts	**Yes:** $\times$ 1	**Yes:** $\times$ 4	**No**	**Yes:** 1 $\times$ pairwise distincts challenges
Hadamard product argument (HPA)	**Yes:** 1 suitable commit vector value	**Yes:** $\times$ $(m + 1)$	**Yes:** $\times$ 1	**Yes:** $1 \times \mathcal{E}_{\mathsf{ZA}}$	**No**
Product argument (PA)	**No**	**No**	**Yes:** $\times$ 1	**Yes:** $1 \times \mathcal{E}_{\mathsf{SVPA}}$ and $1 \times \mathcal{E}_{\mathsf{HPA}}$	**No**
Multi-exponentiation argument (MEA)	**Yes:** $2m$ valid proof transcripts	**No**	**Yes:** $\times$ 2	**No**	**Yes:** 2 $\times$ pairwise distincts challenges
Shuffle argument (SA)	**Yes:** N times for a total of $2N$ witnesses	**Yes:** $\times$ $(N^2 + 1)$	**Yes:** $\times$ 1	**Yes:** $N \times \mathcal{E}_{\mathsf{PA}}$ and $N \times \mathcal{E}_{\mathsf{MEA}}$	**Yes:** 1 $\times$ pairwise distincts challenges

Table 7: Quick overview of arguments needed to prove knowledge soundness