# Listas Listas Listas!

**Abstract.** Listas, listas, listas!

## 1 Commitment schemes

**Definition 1.** *A commitment scheme is a tuple of three algorithms* $(\mathsf{K}, \mathsf{Com}, \mathsf{Vrfy})$ *such that:*

– $\mathsf{K}$ *is a randomized algorithm, which on input the security parameter* $1^\lambda$ *outputs a commitment key* $ck$*,*
– $\mathsf{Com}$ *is a randomized algorithm which, on input the commitment key* $ck$ *and a message* $m$ *in the message space* $\mathcal{M}_{ck}$ *outputs a commitment* $c$ *in the commitment space* $\mathcal{C}_{ck}$ *and an opening* $Op$*,*
– $\mathsf{Vrfy}$ *is a deterministic algorithm which, on input the commitment key* $ck$*, a message* $m$ *in the message space* $\mathcal{M}_{ck}$ *and an opening* $Op$*, outputs* $1$ *if* $Op$ *is a valid opening of* $c$ *to the message* $m$ *and* $0$ *otherwise.*

Correctness requires that for any $m \in \mathcal{M}_{ck}$

$$\Pr\left[ck \leftarrow \mathsf{K}(1^\lambda); m \leftarrow \mathcal{M}_{ck}; (c, Op) \leftarrow \mathsf{Com}(ck, m) : \mathsf{Vrfy}(ck, c, m, Op) = 1\right] = 1.$$

**Definition 2.** *A commitment scheme is binding if, for any polynomial-time adversary* $\mathsf{A}$*,*

$$\Pr\left[ck \leftarrow \mathsf{K}(1^\lambda); (c, m, Op, m', Op') \leftarrow \mathsf{A}(ck) : \mathsf{Vrfy}(ck, c, m, Op) = 1 \cap \mathsf{Vrfy}(ck, c, m', Op') = 1\right]$$

*is negligible. It is hiding if, for any polynomial-time adversary* $\mathsf{A}$*,*

$$\left|\Pr\left[\begin{matrix} ck \leftarrow \mathsf{K}(1^\lambda); (m_0, m_1, st) \leftarrow \mathsf{A}(ck); b \leftarrow \{0,1\}; \\ (c, Op) \leftarrow \mathsf{Com}(ck, m_b); b' \leftarrow \mathsf{A}(st, c) \end{matrix} : b' = b\right] - \frac{1}{2}\right|$$

*is negligible.*

In this paper we will be using two definitions of commitments, one is the GS commitment scheme, and the other is a generalization of the Multi-Pedersen commitment, which commits vectors of scalars as a single group element to a vector of two group elements. The advantage of considering such a commitment is that more information about the committed value can be extracted.

**Definition 3.** *The 2-dimensional Multi-Pedersen commitment scheme in the group* $\mathbb{G}_1$ *is specified by the following three algorithms* $\mathsf{MP} = (\mathsf{MP.K}, \mathsf{MP.Com}, \mathsf{MP.Vrfy})$ *such that:*

– $\mathsf{MP.K}$ *is a randomized algorithm, which on input the security parameter* $1^\lambda$ *and a natural number* $n \in \mathbb{N}$*, outputs an asymmetric bilinear group, a group key* $gk$*, and a commitment key* $ck = [\mathbf{G}]_1 = [(\mathbf{g}_1 || \ldots || \mathbf{g}_{n+1})]_1 \in \mathbb{G}_1^{2\times(n+1)}$*, where* $\mathbf{G} \leftarrow \mathbb{Z}_q^{2\times(n+1)}$*.*

- $\mathsf{MP.Com}$ *is a randomized algorithm which, on input a group key $gk$ and a commitment key $ck = [\mathbf{G}]_1$ and a message $\mathbf{m} \in \mathbb{Z}_q^n$ in the message space $\mathcal{M}_{ck} = \mathbb{Z}_q^n$, it samples $r \leftarrow \mathbb{Z}_q$ and outputs a commitment $[\mathbf{c}]_1 := [\mathbf{G}]_1 \left(\begin{smallmatrix} \mathbf{m} \\ r \end{smallmatrix}\right)$ in the commitment space $\mathcal{C}_{ck} = \mathbb{G}^2$ and an opening $Op = r$,*
- $\mathsf{MP.Vrfy}$ *is a deterministic algorithm which, on input the commitment key $ck = [\mathbf{G}]_1$, a commitment $[\mathbf{c}]_1$, a message $\mathbf{m} \in \mathbb{Z}_q^n$ and an opening $Op = r$, outputs 1 if $[\mathbf{c}]_1 = [\mathbf{G}]_1 \left(\begin{smallmatrix} \mathbf{m} \\ r \end{smallmatrix}\right)$ and 0 otherwise.*

**Theorem 1.** $\mathsf{MP}$ *is computationally hiding if* $\mathsf{DDH}$ *holds in $\mathbb{G}_1$ and computationally binding if the Discrete Logarithm Assumption holds in $\mathbb{G}_1$.*

**Definition 4.** *The Groth-Sahai commitment scheme in the group $\mathbb{G}_1$ is specified by the following three algorithms* ($\mathsf{GS.K}, \mathsf{GS.Com}, \mathsf{GS.Vrfy}$) *such that:*

- $\mathsf{GS.K}$ *is a randomized algorithm, which on input the security parameter $1^\lambda$, outputs an asymmetric bilinear group, a group key $gk$, and a commitment key $ck = [\mathbf{U}]_1 \in \mathbb{G}^{2\times 2}$, where $\mathbf{U} \leftarrow \mathbb{Z}_q^{2\times 2}$.*
- $\mathsf{GS.Com}$ *is a randomized algorithm which, on input a group key $gk$, a commitment key $ck = [\mathbf{U}]_1$, and a message $m \in \mathbb{Z}_q$ in the message space $\mathcal{M}_{ck} = \mathbb{Z}_q$, it samples $r \leftarrow \mathbb{Z}_q$ and outputs a commitment $[\mathbf{c}]_1 := [\mathbf{U}]_1 \left(\begin{smallmatrix} m \\ r \end{smallmatrix}\right)$ in the commitment space $\mathcal{C}_{ck} = \mathbb{G}^2$ and an opening $Op = r$,*
- $\mathsf{MP.Vrfy}$ *is a deterministic algorithm which, on input the commitment key $ck = [\mathbf{U}]_1$, a commitment $[\mathbf{c}]_1$, a message $m \in \mathbb{Z}_q$ and an opening $Op = r$, outputs 1 if $[\mathbf{c}]_1 = [\mathbf{U}]_1 \left(\begin{smallmatrix} m \\ r \end{smallmatrix}\right)$ and 0 otherwise.*

**Theorem 2.** $\mathsf{GS.Com}$ *is perfectly binding and computationally hiding if the* $\mathsf{DDH}$ *Assumption holds in $\mathbb{G}_1$.*

## 2 QA-NIZK For Linear Spaces

Our construction uses as building blocks.

## 3 QA-NIZK For Bit-Strings, Revisited

**$\mathsf{K}_1(\Gamma, [\mathbf{G}]_1, \mathbf{H})$:** Pick $\mathbf{T} \leftarrow \mathbb{Z}_q^{2\times 2}$ andi for each $(i,j) \in \mathcal{I}_{n,1}$ define matrices

$$([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) := ([\mathbf{g}_i]_1 \mathbf{h}_j^\top + [\mathbf{T}]_1, -[\mathbf{T}]_2).$$

Let $\Phi$ be the proof system for Sum in Subspace (Sect. **??**) and $\Psi$ be an instance of the proof system for Equal Commitment Opening (Sect. **??**).
Let $\mathsf{crs}_\Phi \leftarrow \Phi.\mathsf{K}_1(\Gamma, \{[\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2\}_{(i,j)\in\mathcal{I}_{n,1}})$.[1] and let $\mathsf{crs}_\Psi \leftarrow \Psi.\mathsf{K}_1(\Gamma, [\mathbf{G}]_1, [\mathbf{H}]_2, n)$.
The common reference string is given by:

$$\mathsf{crs} := \left([\mathbf{G}]_1, [\mathbf{H}]_2, \{[\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2\}_{(i,j)\in\mathcal{I}_{n,1}}, \mathsf{crs}_\Phi, \mathsf{crs}_\Psi\right).$$

[1] We identify matrices in $\hat{\mathbb{G}}^{2\times 2}$ (resp. in $\check{\mathbb{H}}^{2\times 2}$) with vectors in $\hat{\mathbb{G}}^4$ (resp. in $\check{\mathbb{H}}^4$).

$\mathsf{P}(\mathsf{crs}, [\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$**:** Pick $w_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and then:

1. Define
$$[\mathbf{d}]_2 := \mathsf{MP.Com}_{[\mathbf{H}]_2}(\mathbf{b}; w_h) = [\mathbf{H}]_2 \left( \begin{smallmatrix} \mathbf{b} \\ w_h \end{smallmatrix} \right).$$
2. Compute
$$\begin{aligned}([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2) := \sum_{i\in[n]} \sum_{j\in[n]} b_i(b_i - 1)([\mathbf{C}_{i,j}]_1, [\mathbf{D}_{i,j}]_2) + w_g w_h([\mathbf{C}_{n+1,n+1}]_1, [\mathbf{D}_{n+1,n+1}]_2) \\ \sum_{i\in[n]} b_i w_h([\mathbf{C}_{i,n+1}]_1, [\mathbf{D}_{i,n+1}]_2) + w_g(b_i - 1)([\mathbf{C}_{n+1,i}]_1, [\mathbf{D}_{n+1,i}]_2).\end{aligned}$$
3. Compute a proof $([\boldsymbol{\rho}_1]_1, [\boldsymbol{\sigma}_1]_2)$ that $\mathbf{\Theta} + \check{\mathbf{\Pi}}$ is in the span of $\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j}\}_{(i,j)\in\mathcal{I}_{n,1}}$. and a proof $([\boldsymbol{\rho}_2]_1, [\boldsymbol{\sigma}_2]_2)$ that $([\mathbf{c}]_1, [\mathbf{d}]_2)$ open to the same value, using $\mathbf{b}, w_g$, and $w_h$.

$\mathsf{V}(\mathsf{crs}, [\mathbf{c}]_1, [\mathbf{d}]_2, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \{([\boldsymbol{\rho}_i]_1, [\boldsymbol{\sigma}_i]_2)\}_{i\in[2]})$**:**

1. Check if
$$e([\mathbf{c}]_1, [\mathbf{d}]_2^\top - \sum_{j\in[n]} [\mathbf{h}_j]_2^\top) = e([\mathbf{\Theta}]_1, [\mathbf{I}_{2\times 2}])e([\mathbf{I}_{2\times 2}]_1, [\mathbf{\Pi}]_2). \qquad (1)$$
2. Verify that $([\boldsymbol{\rho}_1]_1, [\boldsymbol{\sigma}_1]_2), ([\boldsymbol{\rho}_2]_1, [\boldsymbol{\sigma}_2]_2)$ are valid proofs for $([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2)$ and $([\mathbf{c}]_1, [\mathbf{d}]_2)$ using $\mathsf{crs}_\Phi$ and $\mathsf{crs}_\Psi$ respectively.

If any of these checks fails, the verifier outputs 0, else it outputs 1.

The simulators $\mathsf{S}_1$ and $\mathsf{S}_2$ are defined as follows.

$\mathsf{S}_1(\mathit{\Gamma}, [\mathbf{G}]_1, \mathbf{H})$**:** It generates and outputs the CRS in the same way as $\mathsf{K}_1$, but additionally it also outputs the simulation trapdoor
$$\tau = (\mathbf{H}, \tau_\Phi, \tau_\Psi),$$
where $\tau_\Phi$ and $\tau_\Psi$ are, respectively, $\Phi$'s and $\Psi$'s simulation trapdoors.

$\mathsf{S}_2(\mathsf{crs}, [\mathbf{c}]_1, (\mathbf{H}, \tau_\Phi, \tau_\Psi))$**:** Given the matrix $\mathbf{H}$ of discrete logarithms of $[\mathbf{H}]_2$, $\tau_\Phi$ and $\tau_\Psi$ which are, respectively, $\Phi$'s and $\Psi$'s simulation trapdoors, this algorithm samples $\overline{w}_h \leftarrow \mathbb{Z}_q$, $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and defines $\mathbf{d} := \overline{w}_h \mathbf{h}_{n+1}$. Then it sets:
$$[\mathbf{\Theta}]_1 := [\mathbf{c}]_1 \left( \mathbf{d} - \sum_{i\in[n]} \mathbf{h}_i \right)^\top + [\mathbf{R}]_1, \qquad [\mathbf{\Pi}]_2 := -[\mathbf{R}]_2.$$
Finally, it simulates proofs $([\boldsymbol{\rho}_i]_1, [\boldsymbol{\sigma}_i]_2)$ for $i \in \{1, 2\}$ using $\tau_\Phi$ and $\tau_\Psi$.

**Theorem 3.** *Algorithms* $(\mathsf{K}, \mathsf{P}, \mathsf{V}, \mathsf{S}_2)$ *satisfy that*

*a) Perfect Completeness: If* $[\mathbf{c}]_1 = [\mathbf{G}]_1 \left( \begin{smallmatrix} \mathbf{b} \\ w_g \end{smallmatrix} \right)$, $\mathbf{b} \in \{0,1\}^n$, *and* $\mathsf{proof} \leftarrow \mathsf{P}(\mathsf{crs}, [\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$, *then* $\mathsf{V}(\mathsf{crs}, [\mathbf{c}], \mathsf{proof}) = 1$.

*b)* *1-coordinate Soundness: If* $\mathbf{g}_{n+1} \neq \mathbf{0}$*,* $\mathbf{h}_{n+1} \neq \mathbf{0}$*, and there exists an index* $i^*$ *such that* $\mathbf{g}_{i^*} \notin \mathsf{Span}(\{\mathbf{g}_i : i \neq i^*\})$ *and* $\mathbf{h}_{i^*} \notin \mathsf{Span}(\{\mathbf{h}_i : i \neq i^*\})$*, then:*

$$\Pr\left[\begin{array}{l}\mathsf{crs} \leftarrow \mathsf{K}(\mathit{\Gamma}, [\mathbf{G}]_1, [\mathbf{H}]_2); \\ ([\mathbf{c}]_1, \mathsf{proof}) \leftarrow \mathsf{A}(\mathsf{crs}, \mathbf{H})\end{array} : \begin{array}{l}\exists b_{i^*} \in \mathbb{Z}_q, \mathbf{w} \in \mathbb{Z}_q^n \ s.t. \ b_{i^*} \notin \{0,1\} \wedge \\ \hat{\mathbf{c}} = b_{i^*}\hat{\mathbf{g}}_{i^*} + \sum_{j \in [n+1], j \neq i^*} w_j \hat{\mathbf{g}}_j \wedge \mathsf{V}(\mathsf{crs}, [\mathbf{c}]_1, \mathsf{proof}) = 1\end{array}\right] \leq negl(\lambda).$$

*Note that soundeness is guaranteed even when* $\mathsf{A}$ *receives the discrete lograrithms of* $[\mathbf{H}]_2$*.*

*c)* *Perfect Zero-Knowledge: If* $\mathbf{rank}(\mathbf{H}) = 1$ *and* $\mathbf{h}_{n+1} \neq \mathbf{0}$*, then for every PPT adversary* $\mathsf{A}$*.*

$$\begin{aligned}&\Pr[\mathsf{crs} \leftarrow \mathsf{K}_1(\mathit{\Gamma}, [\mathbf{G}]_1, \mathbf{H}) : \mathsf{A}^{\mathsf{P}(\mathsf{crs},\cdot,\cdot)}(\mathit{\Gamma}, \mathsf{crs}) = 1] = \\ &\Pr[(\mathsf{crs}, \tau) \leftarrow \mathsf{S}_1(\mathit{\Gamma}, [\mathbf{G}]_1, \mathbf{H}) : \mathsf{A}^{\mathsf{S}(\mathsf{crs},\tau,\cdot,\cdot)}(\mathit{\Gamma}, \mathsf{crs}) = 1]\end{aligned}$$

*where*

- $\mathsf{P}(\mathsf{crs}, \cdot, \cdot)$ *emulates the actual prover. It takes input* $([\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$ *and outputs a proof* $\mathsf{proof} \leftarrow \mathsf{P}(\mathsf{crs}, [\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$*, if* $[\mathbf{c}]_1 = [\mathbf{G}]_1 \binom{\mathbf{b}}{w_g}$ *for some* $\mathbf{b} \in \{0,1\}^n$ *and* $w_g \in \mathbb{Z}_q$*. Otherwise, it outputs* $\perp$*.*
- $\mathsf{S}(\mathsf{crs}, \tau, \cdot, \cdot)$ *is an oracle that takes input* $([\mathbf{c}]_1, \langle \mathbf{b}, w_g \rangle)$*. It outputs a simulated proof* $\mathsf{proof} \leftarrow \mathsf{S}_2(\mathsf{crs}, \tau, [\mathbf{c}]_1)$*, if* $[\mathbf{c}]_1 = [\mathbf{G}]_1 \binom{\mathbf{b}}{w_g}$ *for some* $\mathbf{b} \in \{0,1\}^n$ *and* $w_g \in \mathbb{Z}_q$*. Otherwise, it outputs* $\perp$*.*

*Proof.* **Perfect Completeness:** Note that, by definition of $\mathbf{C}_{i,j}$ and $\mathbf{D}_{i,j}$, $e([\mathbf{C}_{i,j}]_1, [\mathbf{I}_{2\times 2}]_2) \cdot e([\mathbf{I}_{2\times 2}]_1, [\mathbf{D}_{i,j}]_2) = e([\mathbf{g}_i]_1, [\mathbf{h}_j]_2^\top)$. Since $b_i(b_i - 1) = 0$ for each $i \in [n]$,

$$\begin{aligned}&e\left([\mathbf{c}]_1, [\mathbf{d}]_2^\top - \sum_{i\in[n]} [\mathbf{h}_i]_2^\top\right) \\ &= \prod_{i\in[n]} \left( e([\mathbf{g}_i]_1, [\mathbf{h}_{n+1}]_2^\top)^{b_i w_h} \cdot e([\mathbf{g}_{n+1}]_1, [\mathbf{h}_i]_2^\top)^{w_g(b_i-1)} \cdot \prod_{j\in[n]} e([\mathbf{g}_i]_1, [\mathbf{h}_j]_2^\top)^{b_i(b_j-1)} \right) \\ &\quad \cdot e([\mathbf{g}_{n+1}]_1, [\mathbf{h}_{n+1}]_2^\top)^{w_g w_h} \\ &= e\left( \sum_{i\in[n]} \left( b_i w_h [\mathbf{g}_i]_1 \mathbf{h}_{n+1}^\top + w_g(b_i - 1)[\mathbf{g}_{n+1}]_1 \mathbf{h}_i^\top + \sum_{\substack{j\in[n] \\ j\neq i}} b_i(b_i - 1)[\mathbf{g}_i]_1 \mathbf{h}_j^\top \right), [\mathbf{I}_{2\times 2}]_2 \right) \\ &\quad \cdot e(w_g w_h [\mathbf{g}_{n+1}]_1 \mathbf{h}_{n+1}^\top, [\mathbf{I}_{2\times 2}]_2) \cdot e([\mathbf{R}]_1, [\mathbf{I}_{2\times 2}]_2)/e([\mathbf{I}_{2\times 2}]_1, [\mathbf{R}]_2) \\ &= e([\mathbf{\Theta}]_1, [\mathbf{I}_{2\times 2}]_2) \cdot e([\mathbf{I}_{2\times 2}]_1, [\mathbf{\Pi}]_2).\end{aligned}$$

Finally, the rest of the proof follows from completeness of $\mathit{\Phi}$ and $\mathit{\Psi}$.

**1-coordinate Soundness:** Since $\{\mathbf{g}_{i^*}, \mathbf{g}_{n+1}\}$ and $\{\mathbf{h}_{i^*}, \mathbf{h}_{n+1}\}$ are both basis of $\mathbb{Z}_q^2$, we can define $b_{i^*}, \overline{w}_g, \overline{w}_h, \overline{b}_{i^*}$ as the unique coefficients in $\mathbb{Z}_q$ such that $\mathbf{c} = b_{i^*}\mathbf{g}_{i^*} + \overline{w}_g \mathbf{g}_{n+1}$ and $\mathbf{d} = \overline{b}_{i^*}\mathbf{h}_{i^*} + \overline{w}_h \mathbf{h}_{n+1}$.

Additionally, If $\mathsf{A}$ breaks 1-coordinate soudness implies that $b_{i^*} \notin \{0,1\}$, while the verifier accepts the proof $([\mathbf{d}]_2, ([\mathbf{\Theta}]_1, [\mathbf{\Pi}]_2), \{([\boldsymbol{\rho}_i]_1, [\boldsymbol{\sigma}_i]_2)\}_{i\in[2]})$ produced by $\mathsf{A}$. We distinguish two cases:

1) If $b_{i^*} \neq \bar{b}_{i^*}$. Given that $(b_i \mathbf{g}_{i^*}, \bar{b}_{i^*} \mathbf{h}_{i^*})$ is linearly independent from $\{(\mathbf{g}_{i^*}, \mathbf{h}_{i^*}), (\mathbf{g}_{n+1}, \mathbf{h}_{n+1})\}$ whenever $b_{i^*} \neq \bar{b}_{i^*}$, an adversary $\mathsf{P}_2^*$ against $\Phi$ outputs the pair $([\boldsymbol{\rho}_2]_1, [\boldsymbol{\sigma}_2]_2)$ which is a fake proof for $([\mathbf{c}]_1, [\mathbf{d}]_2)$. HAY QUE DECIR QUE NUESTRA PRUEBA DE MEMBERSHIP EN $\mathbb{G}_1^m \times \mathbb{G}_2^n$ AÚN ES VÁLIDA SI EL ADV CONOCE LOS LOGARITMOS DISCRETOS DE $\mathbf{N}$ (QUE ES LO QUE CORRESPONDE A QUE ACÁ CONOZCA $\mathbf{H}$). ESTO DE ALGUNA FORMA TAMBIÉN PASA EN LA PRUEBA DE LOS BITS, PUES EN LA REDUCCIÓN HAY QUE CALCULAR, DADO $[\mathbf{a}]_2$, $[\mathbf{a}_\Delta]_2 = \boldsymbol{\Delta}^\top [\mathbf{a}]_2 \Rightarrow$ CONOCER $\mathbf{G} = \boldsymbol{\Delta}\mathbf{U}$.
2) If $b_{i^*} = \bar{b}_{i^*}$ but $b_{i^*}(\bar{b}_{i^*} - 1) \neq 0$. If we express $\boldsymbol{\Theta} + \boldsymbol{\Pi}$ as a linear combination of $\{\mathbf{g}_i \mathbf{h}_j^\top : i, j \in [n+1]\}$, the coordinate of $\mathbf{g}_{i^*} \mathbf{h}_{i^*}^\top$ is $b_{i^*}(\bar{b}_{i^*} - 1) \neq 0$ and thus $\boldsymbol{\Theta} + \boldsymbol{\Pi} \notin \mathsf{Span}(\{\mathbf{C}_{i,j} + \mathbf{D}_{i,j} : (i,j) \in \mathcal{I}_{n,1}\})$. The adversary $\mathsf{P}_1^*$ against $\Psi$ outputs the pair $([\boldsymbol{\rho}_1]_1, [\boldsymbol{\sigma}_1]_2)$ which is a fake proof for $([\boldsymbol{\Theta}]_1, [\boldsymbol{\Pi}]_2)$. NO SE SI ACÁ PASA LO ANTERIOR.

**Perfect Zero-Knowledge:** First, note that the vector $[\mathbf{d}]_2 \in \mathbb{G}_2^2$ output by the prover and the vector output by $\mathsf{S}_2$ follow exactly the same distribution. This is because the rank of $\mathbf{H}$ is 1 and $\mathbf{h}_{n+1} \neq \mathbf{0}$. In particular, although the simulator $\mathsf{S}_2$ does not know $\mathbf{b} \in \{0,1\}^n$ such that $[\mathbf{c}]_1 = [\mathbf{G}]_1 \binom{\mathbf{b}}{w_g}$, for some $w_g \in \mathbb{Z}_q$, there exists $w_h \in \mathbb{Z}_q$ such that $[\mathbf{d}]_2 = [\mathbf{H}]_2 \binom{\mathbf{b}}{w_h}$.
Since $\mathbf{R}$ is chosen uniformly at random in $\mathbb{Z}_q^{2\times 2}$, the proof $([\boldsymbol{\Theta}]_1, [\boldsymbol{\Pi}]_2)$ is uniformly distributed conditioned on satisfying check 1) of algorithm $\mathsf{V}$. Finally, the rest of the proof follows from Zero-Knowledge of $\Phi$ and $\Psi$.

# 4 Aggregated Proofs of Membership in a List

# 5 Aggregated Proofs of Membership in a List

We wish to prove that $m$ GS commitments to group elements open to some value in a list (or an ordered set) $L := \{\hat{l}_1, \ldots, \hat{l}_n\}$. We note that the values may not be necessarily distinct. More specifically, we wish to prove membership in the language

$$\mathcal{L}_{\hat{\mathbf{U}},L,m} := \{[(\hat{c}_1, \ldots, \hat{c}_m)]_2 \forall i \in [m]\ \exists (\mathbf{r}_i, \hat{x}_i) \in \mathbb{Z}_q^2 \times L \ \text{ s.t. } \hat{c}_i = \mathsf{GS.Com}_{\hat{\mathbf{U}}}(\hat{x}_i; \mathbf{r}_i)\},$$

where the witness for membership in the language are the pairs $(\mathbf{r}_i, \hat{x}_i)$. Below, we provide a proof whose communication is $\Theta(n)$, regardless of $m$.

We note in particular that such a proof also works when $\hat{c}_i$ is an ElGamal ciphertext or the encryption scheme based on the 2-Lin Assumption due to XXX — which are special cases of GS commitments where some randomness is set to 0 — for different instantiations of GS

## 5.1 Intuition

**Observation**. If $(\hat{x}_1, \ldots, \hat{x}_m)$ is a vector of elements in a list $L$ if and only if there exists a matrix $\mathbf{B} = (b_{i,j}) \in \{0,1\}^{m\times n}$, whose rows are denoted by $\mathbf{b}_1, \ldots, \mathbf{b}_m$, such that, $[(x_1, \ldots, x_m)]_1 = [(l_1, \ldots, l_m)]_2 \begin{pmatrix} b_{1,1} & \ldots & b_{1,n} \\ \vdots & & \vdots \\ b_{m,1} & \ldots & b_{m,n} \end{pmatrix} = \sum_{i\in[n]} [l_i]_2 \mathbf{b}_i$. If we define

*Example 1.* If $[(x_1,x_2,x_3,x_4)]_1 = [(l_1,l_3,l_2,l_1)]_1$, then

$$[(x_1,x_2,x_3,x_4)]_1 = [(l_1,l_3,l_2,l_1)]_1 \begin{pmatrix} 1\,0\,0\,1 \\ 0\,0\,1\,0 \\ 0\,1\,0\,0 \end{pmatrix} = [l_1]_1 \begin{pmatrix} 1\,0\,0\,1 \end{pmatrix} + [l_2]_1 \begin{pmatrix} 0\,0\,1\,0 \end{pmatrix} + [l_3]_1 \begin{pmatrix} 0\,1\,0\,0 \end{pmatrix}.$$

**Trivial Approach**. This suggests the following trivial approach. Problem. XX.

$\mathsf{K}_0(1^\lambda)$**:** Return $\Gamma := (q, \hat{\mathbb{G}}, \check{\mathbb{H}}, \mathbb{T}, e, \hat{g}, \check{h}) \leftarrow \mathsf{Gen}_a(1^\lambda)$.

$\mathsf{K}_1(\Gamma, (\hat{\mathbf{U}}, L, m))$**:** Let $\Psi_{\mathsf{bits}}$ the proof system described in XXX and let $\mathsf{crs}_{\mathsf{bits}} = (\hat{\mathbf{G}}, \check{\mathbf{H}}, \mathsf{crs}'_{\mathsf{bits}}) \leftarrow \Psi_{\mathsf{bits}}.\mathsf{K}_1(\Gamma, m)$. For each $i \in [m+1]$ denote by $\check{\mathbf{h}}_i$ the $i$ th column of $\check{\mathbf{H}}$. Let $\Phi$ the proof system for proving membership in linear subspaces of $\hat{\mathbb{G}}^2$ and let $\mathsf{crs}_\Phi \leftarrow \Phi.\mathsf{K}_1(\Gamma, \check{\mathbf{h}}_{m+1}, 2)$. The common reference string is given by $\mathsf{crs} := (\hat{\mathbf{U}}, L, m, \mathsf{crs}_{\mathsf{bits}}, \mathsf{crs}_\Phi)$

$\mathsf{P}(\mathsf{crs}, \hat{\mathbf{C}}, (\hat{\mathbf{R}}, \mathbf{B}))$**:** Denote $\mathbf{b}_i \in \{0,1\}^n$ as the ith row of $\mathbf{B}$.

1. Let $\hat{\boldsymbol{\beta}}_i = \mathsf{Comm}^{\mathsf{MP}}_{\hat{\mathbb{G}},\hat{\mathbf{G}}}(\mathbf{b}_i; w_i)$, $w_i \leftarrow \mathbb{Z}_q$.
2. $\pi_{i,\mathsf{bits}} \leftarrow \mathsf{Bits}.\mathsf{P}(\hat{\boldsymbol{\beta}}_i; w_i)$.
3. Let $\hat{\mathbf{v}} := \sum_{i\in[m]} \hat{\boldsymbol{\beta}}_i - \sum_{j\in[n]} \hat{\mathbf{g}}_i$ and $\pi_{\mathsf{LinSp}} \leftarrow\leftarrow \mathsf{LinSp}.\mathsf{P}(\mathsf{crs}_{\mathsf{LinSp}}, \hat{\mathbf{v}}, \sum_{i\in[n]} w_i)$.
4. Pick $\mathbf{r}_{m+1} \leftarrow \mathbb{Z}_q^2$ and compute $\check{\mathbf{\Pi}} := \sum_{i\in[m+1]} \mathbf{r}_i \check{\mathbf{h}}_i^\top$ and $\hat{\boldsymbol{\theta}} := \sum_{j\in[n]} w_j \iota_1(\hat{l}_j) - \hat{\mathbf{U}}\mathbf{r}_{m+1}$.

$\mathsf{V}(\mathsf{crs}, (\hat{\mathbf{c}}_1, \ldots, \hat{\mathbf{c}}_m), \langle\{(\hat{\boldsymbol{\alpha}}_j, \check{\boldsymbol{\beta}}_j, \pi'_j) : j \in [n]\}, \check{\phi}, \check{\mathbf{\Pi}}, \hat{\boldsymbol{\theta}}\rangle)$ **:**

1. For all $j \in [n]$, check if $\Psi_{\mathsf{bits}}.\mathsf{V}(\mathsf{crs}_{\mathsf{bits}}, (\hat{\boldsymbol{\alpha}}_j, \check{\boldsymbol{\beta}}_j, \pi'_j)) = 1$.
2. Check if $\Phi.\mathsf{V}(\mathsf{crs}_\Phi, \sum_{j\in[n]} \check{\boldsymbol{\beta}}_j - \sum_{i\in[m]} \check{\mathbf{h}}_i, \check{\phi}) = 1$.
3. Check if $\sum_{i\in[m]} \hat{\mathbf{c}}_i \check{\mathbf{h}}_i^\top - \sum_{j\in[n]} \iota_1(\hat{l}_j) \check{\boldsymbol{\beta}}_j^\top = \hat{\mathbf{U}}\check{\mathbf{\Pi}}^\top + \hat{\boldsymbol{\theta}}\check{\mathbf{h}}_{m+1}^\top$

If any of these checks fails, the verifier outputs 0, else it outputs 1.

$\mathsf{S}_1(\Gamma, (\hat{\mathbf{U}}, L, m))$**:** The simulator receives as input a description of an asymmetric bilinear group $\Gamma$ and the triplet $(\hat{\mathbf{U}}, L, m) \in \hat{\mathbb{G}}^{2\times 2} \times 2^{\hat{\mathbb{G}}} \times \mathbb{N}$ sampled according to distribution $\mathcal{D}_\Gamma$. It generates and outputs the CRS in the same way as $\mathsf{K}_1$, but additionally it also outputs the simulation trapdoor

$$\tau = \left(\epsilon_1, \ldots, \epsilon_m, \tau_{\Psi_{\overline{\mathcal{D}}_k,+}}, \tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}, \tau_\Phi\right),$$

where $\tau_{\Psi_{\overline{\mathcal{D}}_k,+}}$, $\tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$, and $\tau_\Phi$ are $\Psi_{\overline{\mathcal{D}}_k,+}$'s, $\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}$'s, and $\Phi$'s simulation trapdoors, respectively, and $\check{\mathbf{h}}_i = \epsilon_i \check{\mathbf{h}}_{m+1}$ for each $i \in [m]$.

$\mathsf{S}_2(\mathsf{crs}, (\hat{\mathbf{c}}_1, \ldots, \hat{\mathbf{c}}_m), \tau)$**:** For each $j \in [n]$ compute $\pi_j \leftarrow \Psi_{\mathsf{bits}}.\mathsf{P}(\mathsf{crs}_{\mathsf{bits}}, \mathbf{0}_{n\times 1})$, that is, pick random $w_{g,j}, w_{h,j} \leftarrow \mathbb{Z}_q$ $\mathbf{R} \leftarrow \mathbb{Z}_q^{2\times 2}$ and define:

$$\begin{aligned} \hat{\boldsymbol{\alpha}}_j &:= w_{g,j}\hat{\mathbf{g}}_{m+1} & \check{\boldsymbol{\beta}}_j &:= w_{h,j}\check{\mathbf{h}}_{m+1} \\ \hat{\mathbf{\Theta}}_{b(\bar{b}-1),j} &:= w_{g,j}w_{h,j}\hat{\mathbf{C}}_{m+1,m+1} + \hat{\mathbf{R}} & \check{\mathbf{\Pi}}_{b(\bar{b}-1),j} &:= w_{g,j}w_{h,j}\check{\mathbf{D}}_{m+1,m+1} - \check{\mathbf{R}}. \end{aligned}$$

Simulate proofs $(\hat{\boldsymbol{\rho}}_X, \check{\boldsymbol{\sigma}}_X)$, for $X \in \{b(\bar{b}-1), b-\bar{b}\}$, and $\check{\phi}$ using $\tau_{\Psi_{\overline{\mathcal{D}}_k,+}}$, $\tau_{\Psi_{\overline{\mathcal{D}}_k,\mathsf{com}}}$, and $\tau_\Phi$. Finally, pick $\bar{\mathbf{r}} \leftarrow \mathbb{Z}_q^2$ and compute proofs

$$\check{\mathbf{\Pi}} := \bar{\mathbf{r}}\check{\mathbf{h}}_{m+1}^\top, \qquad \check{\boldsymbol{\theta}} := \sum_{i\in[m]} \epsilon_i \hat{\mathbf{c}}_i - \sum_{j\in[n]} w_{h,j}\iota_1(\hat{l}_j) - \hat{\mathbf{U}}\bar{\mathbf{r}}.$$

# 6 A Non-Interactive Verifiable Shuffle

This gives the following construction

## 6.1 Detailed Construction