On Sigma Protocols and (packed) Black-Box Secret Sharing Schemes

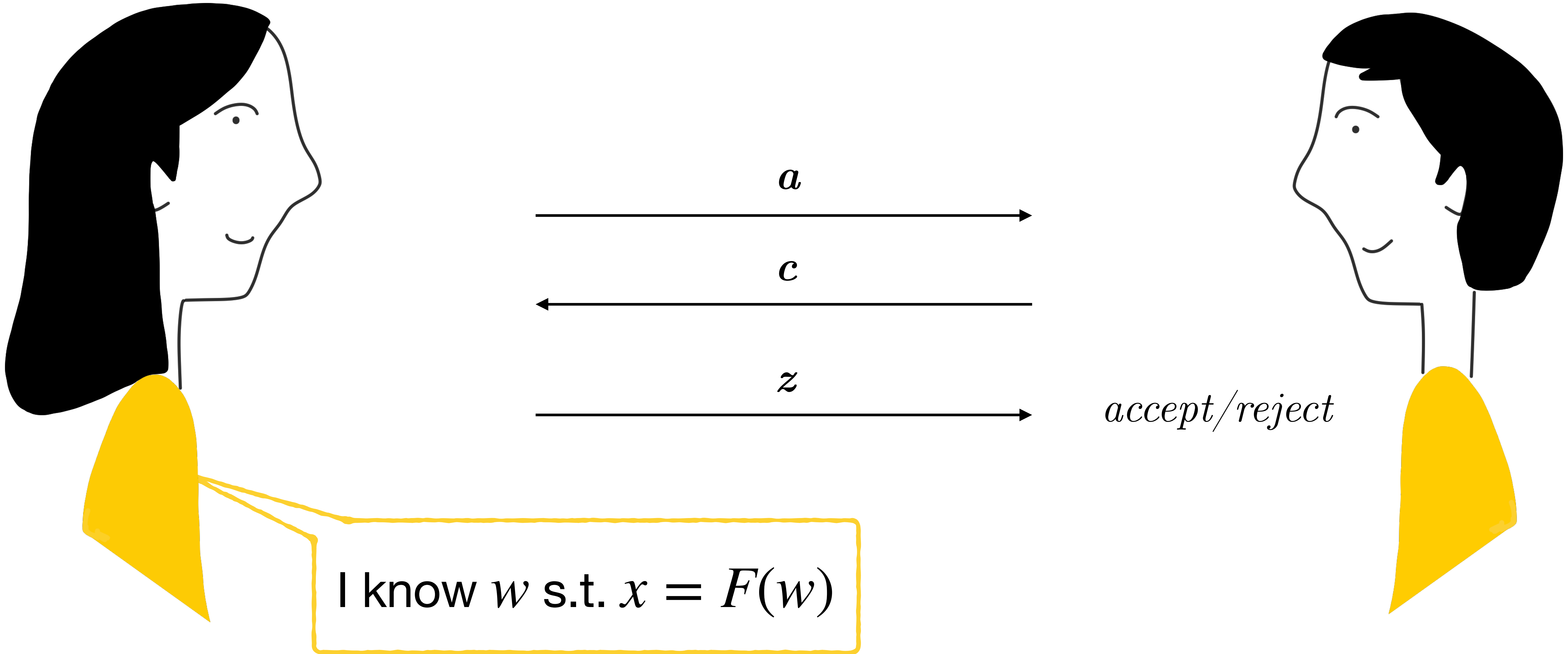
PKC 2024

Claudia Bartoli

Ignacio Cascudo

Σ-protocols

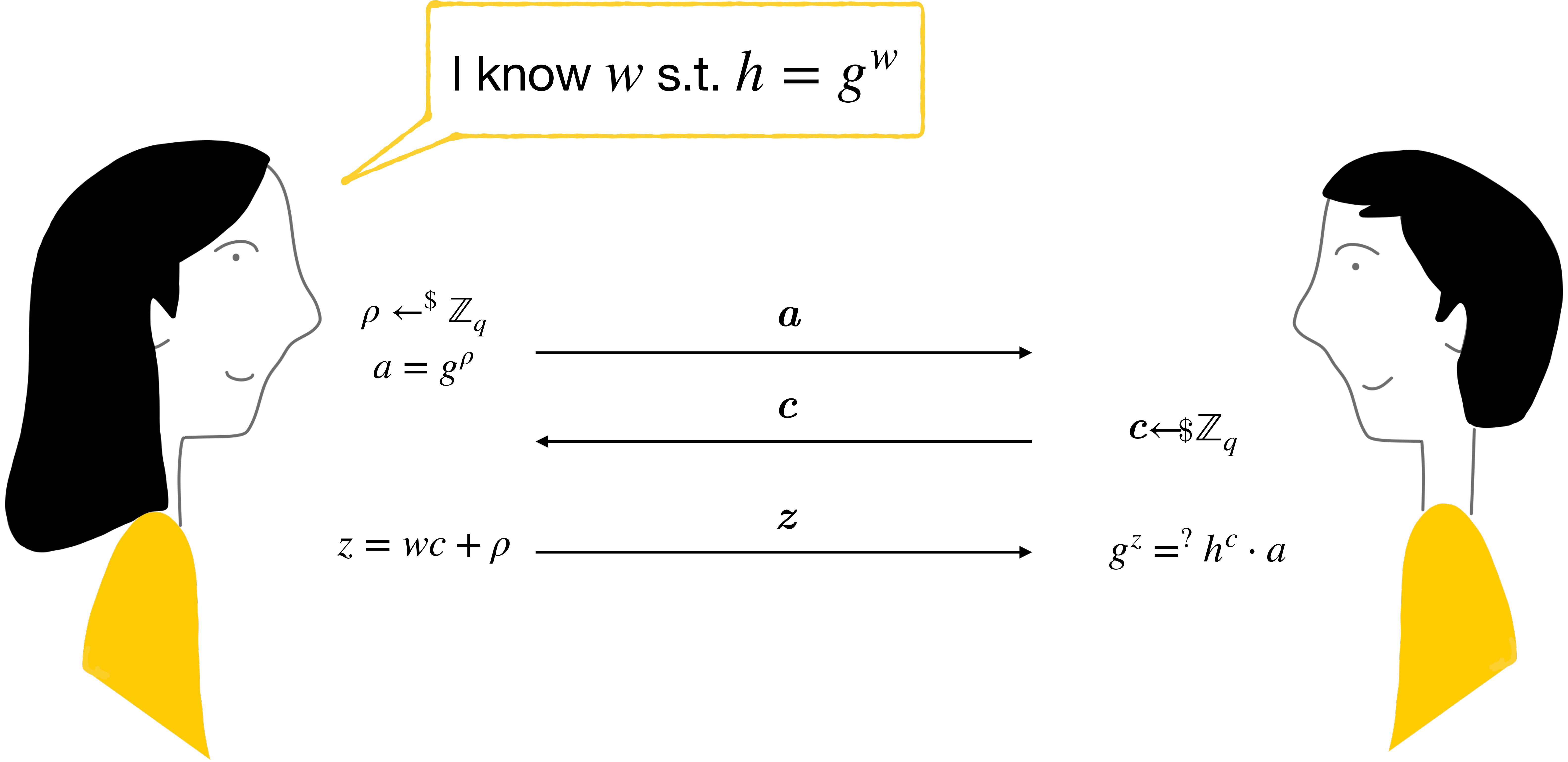
Let W, X be modules over a ring $\mathfrak{R}$, let $F : W \longrightarrow X$ be a module homomorphism and a relation $R := \{(w; x) \in W \times X : F(w) = x\}$.



- **Completeness**
- **κ-Special Soundness**
- **Honest-verifier zero-knowledge (HVZK)**

Schnorr Protocol

Let G_q be a cyclic group, of order q prime, generated by $G_q = < g >$ [Schnorr CRYPTO'89]

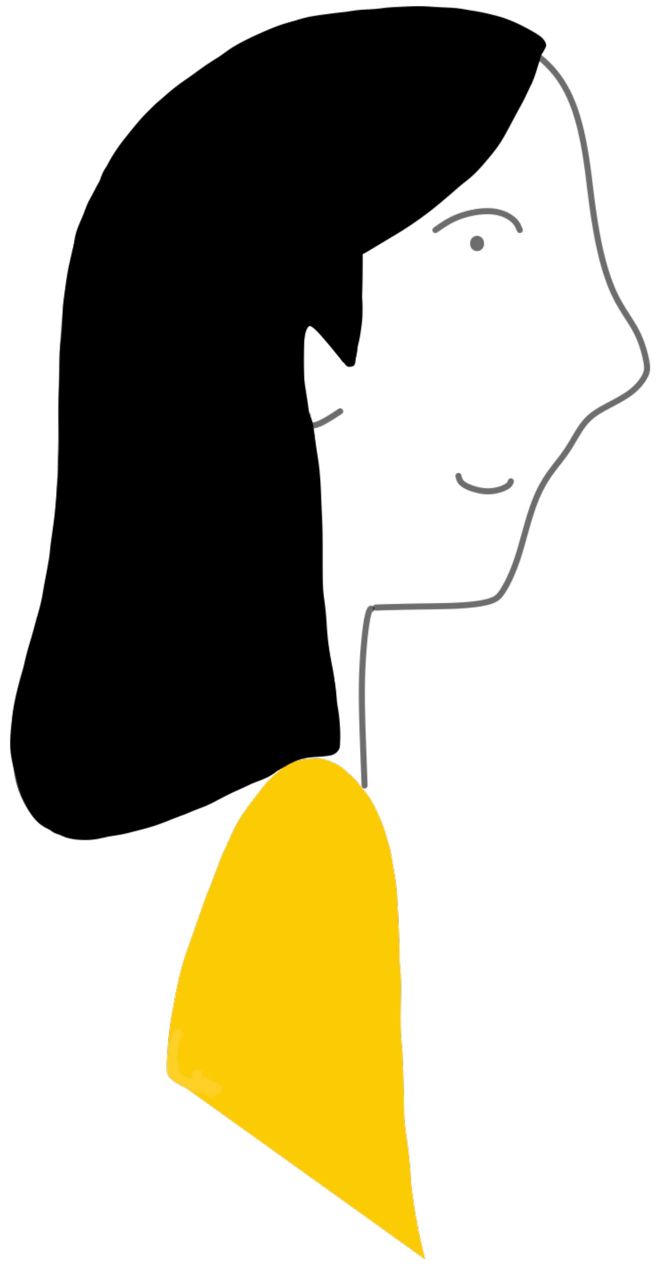


- **Completeness**
- 2**-Special Soundness**
- **Honest-verifier zero-knowledge (HVZK)**

Schnorr Protocol

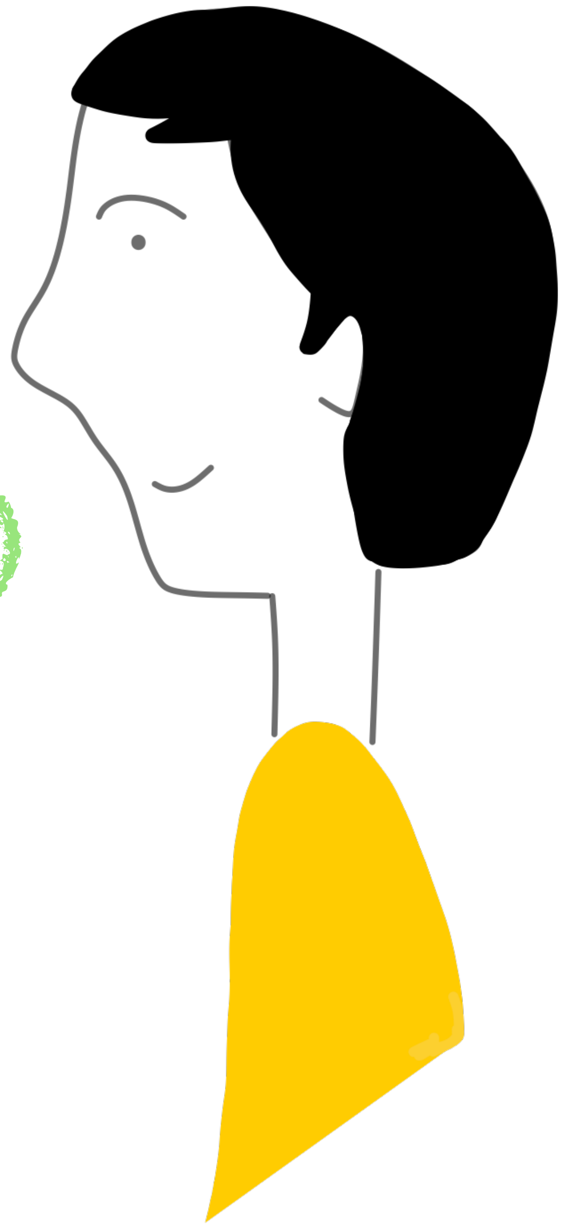
Let G_q be a cyclic group, of order q prime, generated by $G_q = < g >$ [Schnorr CRYPTO'89]

I know w s.t. $h = g^w$



Field with invertible elements

Prover		Verifier
$\rho \leftarrow^{\$} \mathbb{Z}_q$ $a = g^{\rho}$	$\xrightarrow{\boldsymbol{a}}$	
	$\xleftarrow{\boldsymbol{c}}$	$\boldsymbol{c} \leftarrow \$ \mathbb{Z}_q$
$z = wc + \rho$	$\xrightarrow{\boldsymbol{z}}$	$g^z =^? h^c \cdot a$



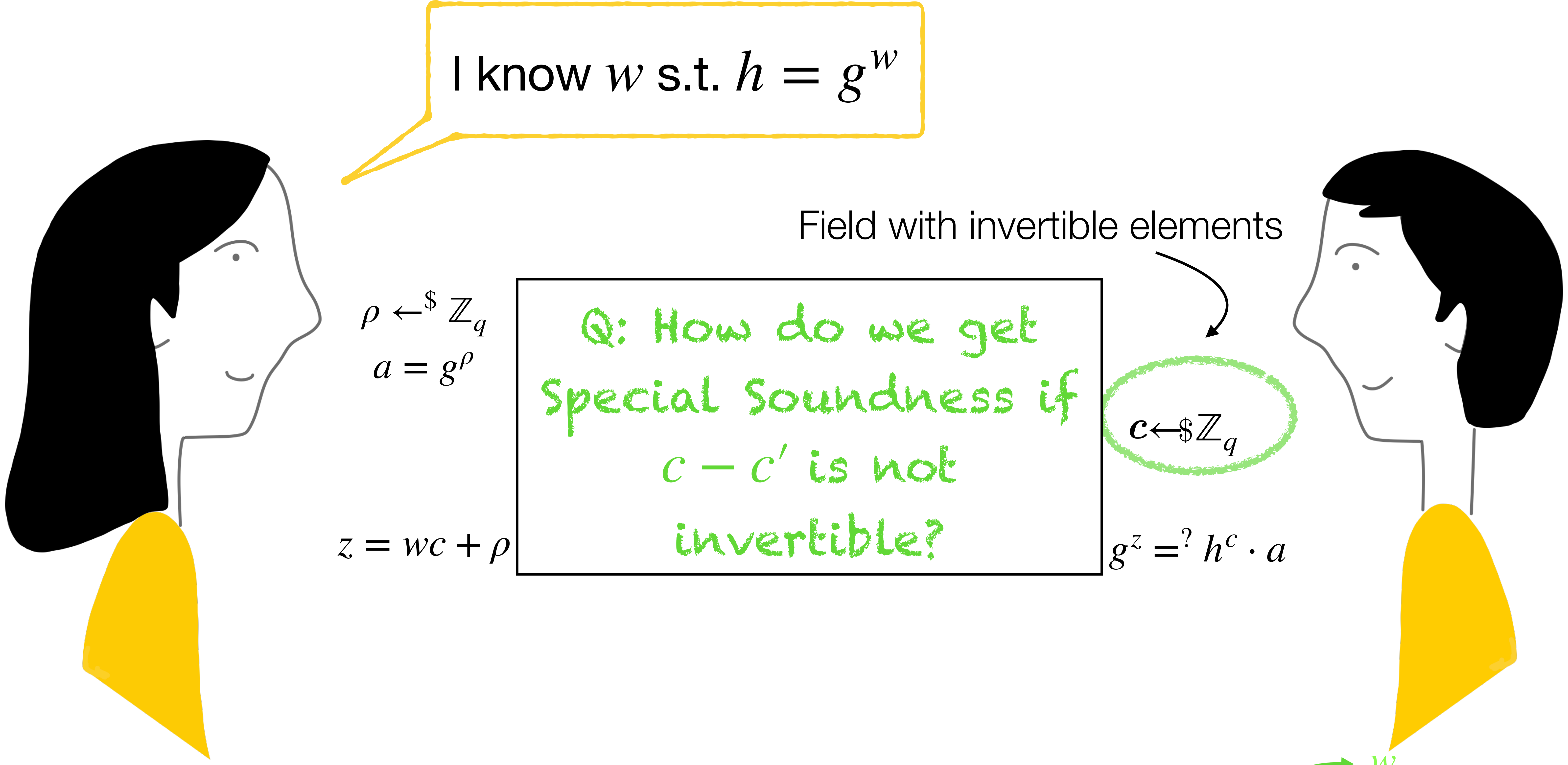
- **Completeness**
- 2**-Special Soundness**
- **Honest-verifier zero-knowledge (HVZK)**

$$\left.\begin{array}{l} (a, c, z) \\ (a, c', z') \end{array}\right\} \begin{array}{l} g^z = h^c \cdot a \\ g^{z'} = h^{c'} \cdot a \end{array} \rightarrow g^{z-z'} = h^{c-c'} \rightarrow g^{\overbrace{\frac{z-z'}{c-c'}}^{w}} = h \rightarrow$$

$c - c'$ must be invertible

Schnorr Protocol

Let G_q be a cyclic group, of order q prime, generated by $G_q = < g >$ [Schnorr CRYPTO'89]



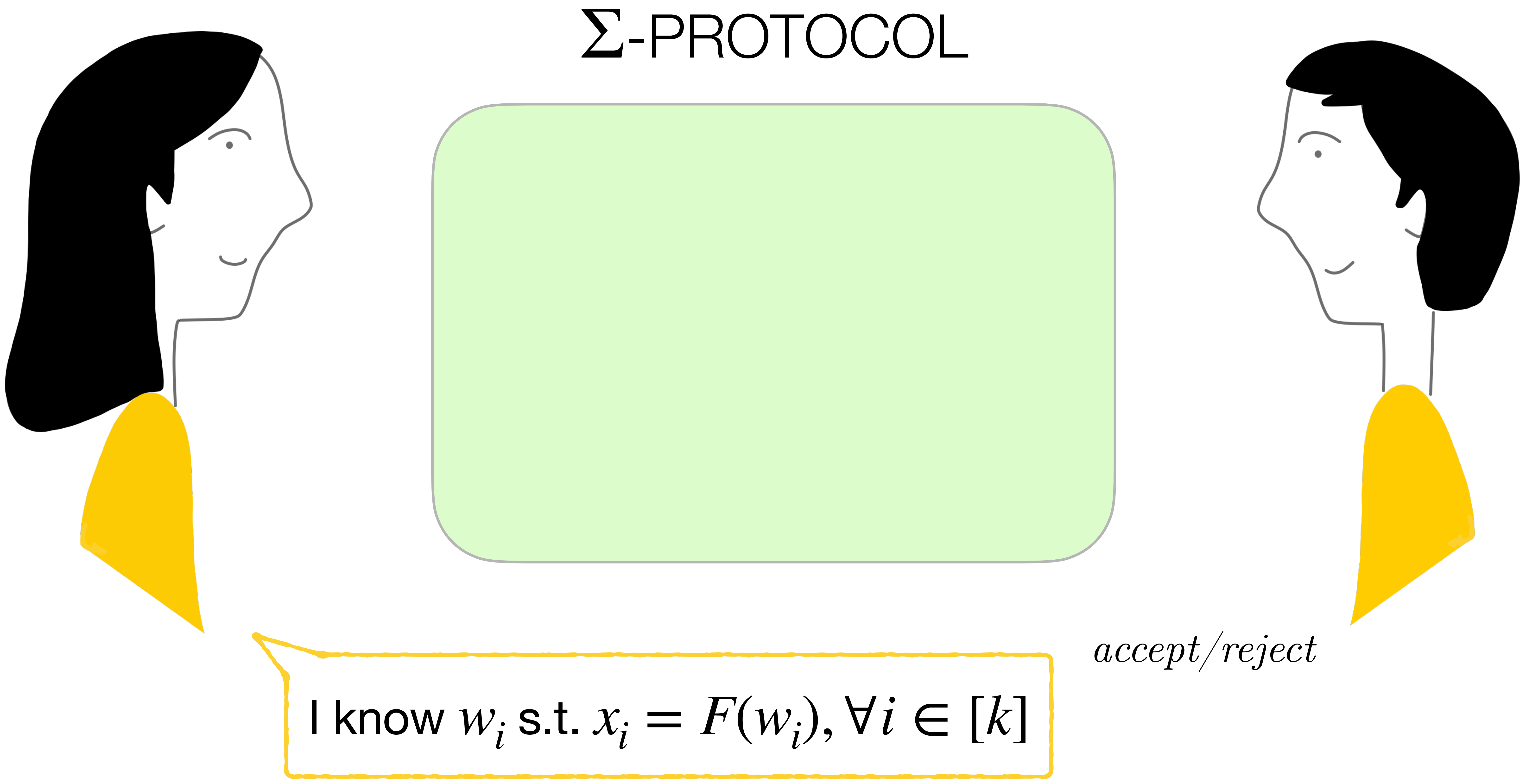
- **Completeness**
- **2-Special Soundness**
- **Honest-verifier zero-knowledge (HVZK)**

$$\left.\begin{matrix}(a, c, z) \\ (a, c', z')\end{matrix}\right\} \begin{matrix} g^z = h^c \cdot a \\ g^{z'} = h^{c'} \cdot a \end{matrix} \rightarrow g^{z-z'} = h^{c-c'} \rightarrow g^{\overset{w}{\frac{z-z'}{c-c'}}} = h \rightarrow$$

$c - c'$ must be invertible

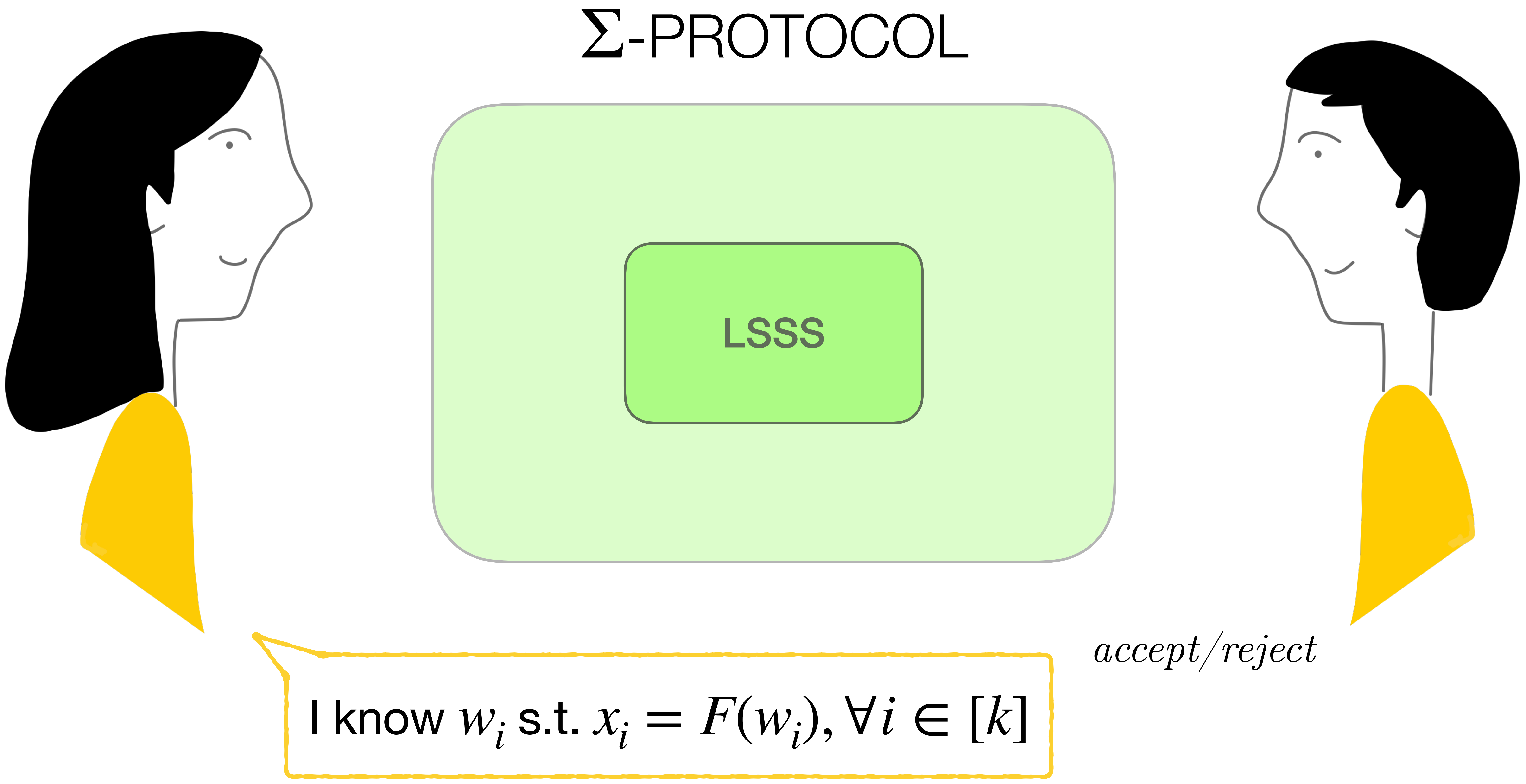
In this work

Efficient Σ-protocol for proving knowledge of k preimages of group homomorphisms **over any abelian group**



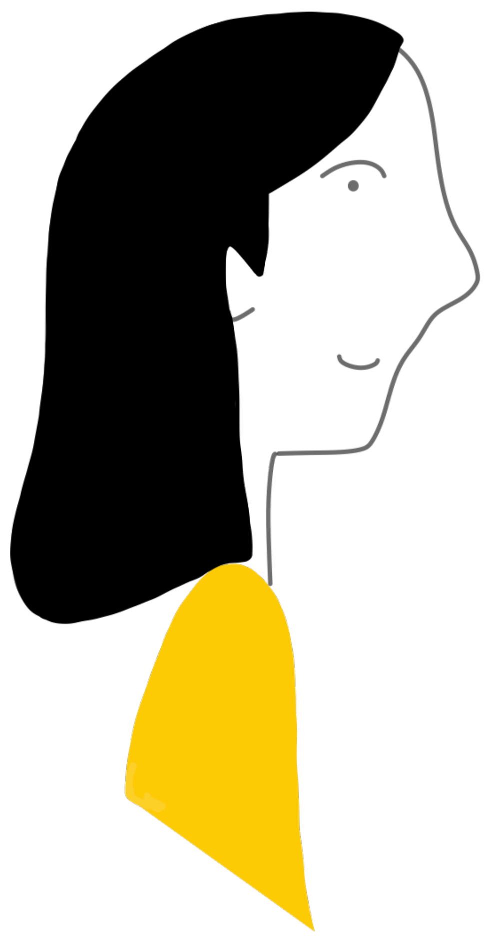
In this work

Efficient Σ-protocol for proving knowledge of k preimages of group homomorphisms **over any abelian group**



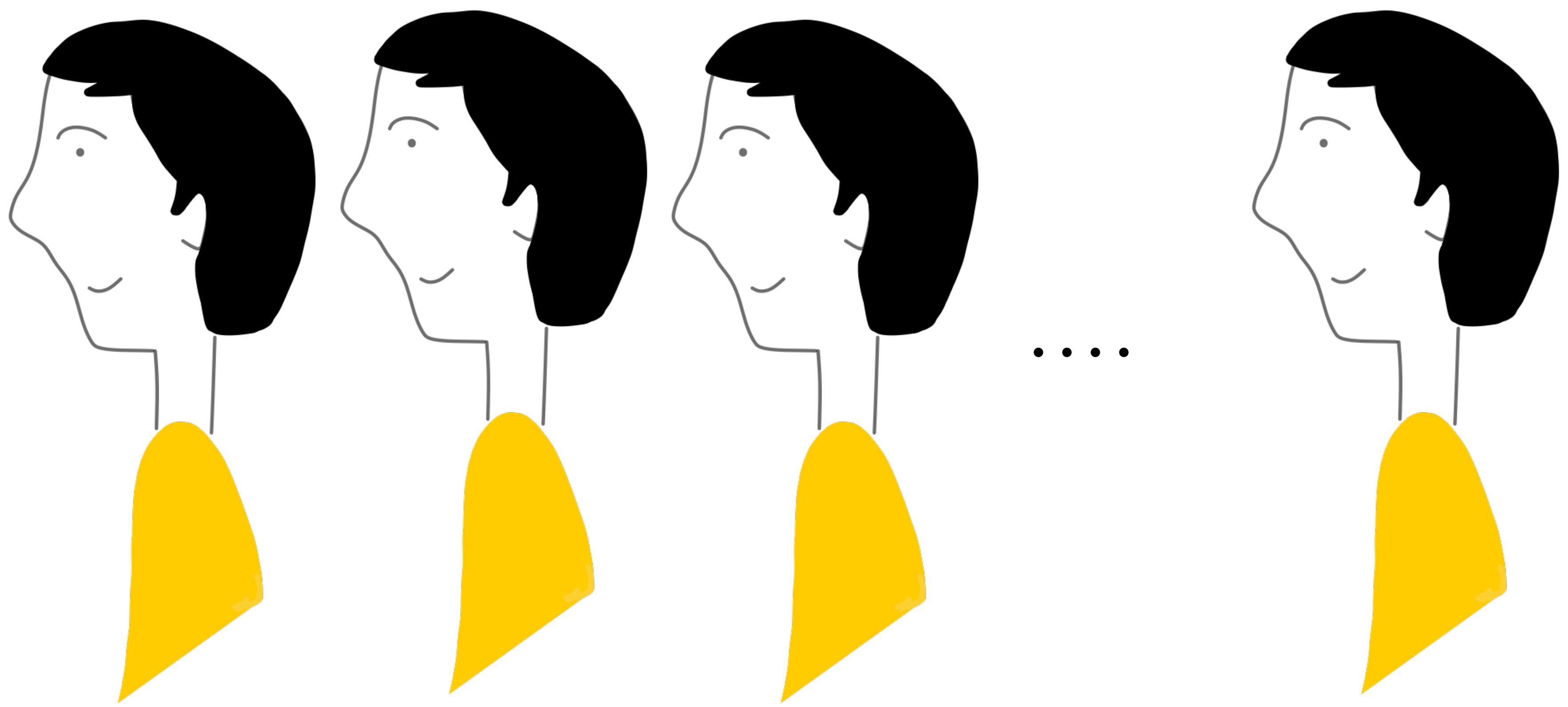
Linear Secret Sharing Schemes

(t, r, n)-**Linear Secret Sharing.** Let W be a module over $\mathfrak{R}$, $w \in W^k, \rho \in W^e$ and $M \in \mathfrak{R}^{h\times(k+e)}$.



$$\boxed{M \begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix}} \longrightarrow$$

t privacy and r reconstruction



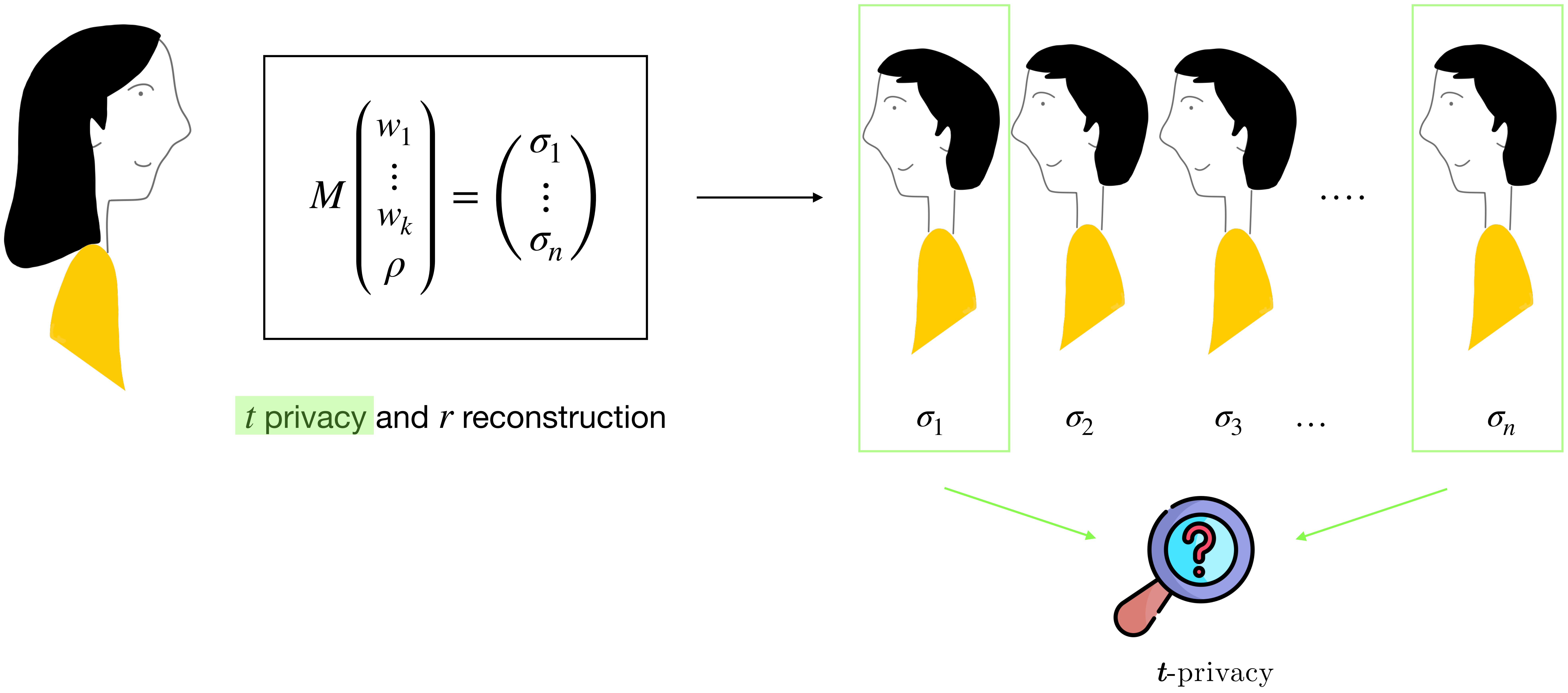
σ_1 σ_2 σ_3 $\ldots$ σ_n

Linear Secret Sharing Schemes

(t, r, n)**-Linear Secret Sharing.** Let W be a module over $\mathfrak{R}$, $w \in W^k, \rho \in W^e$ and $M \in \mathfrak{R}^{h\times(k+e)}$.

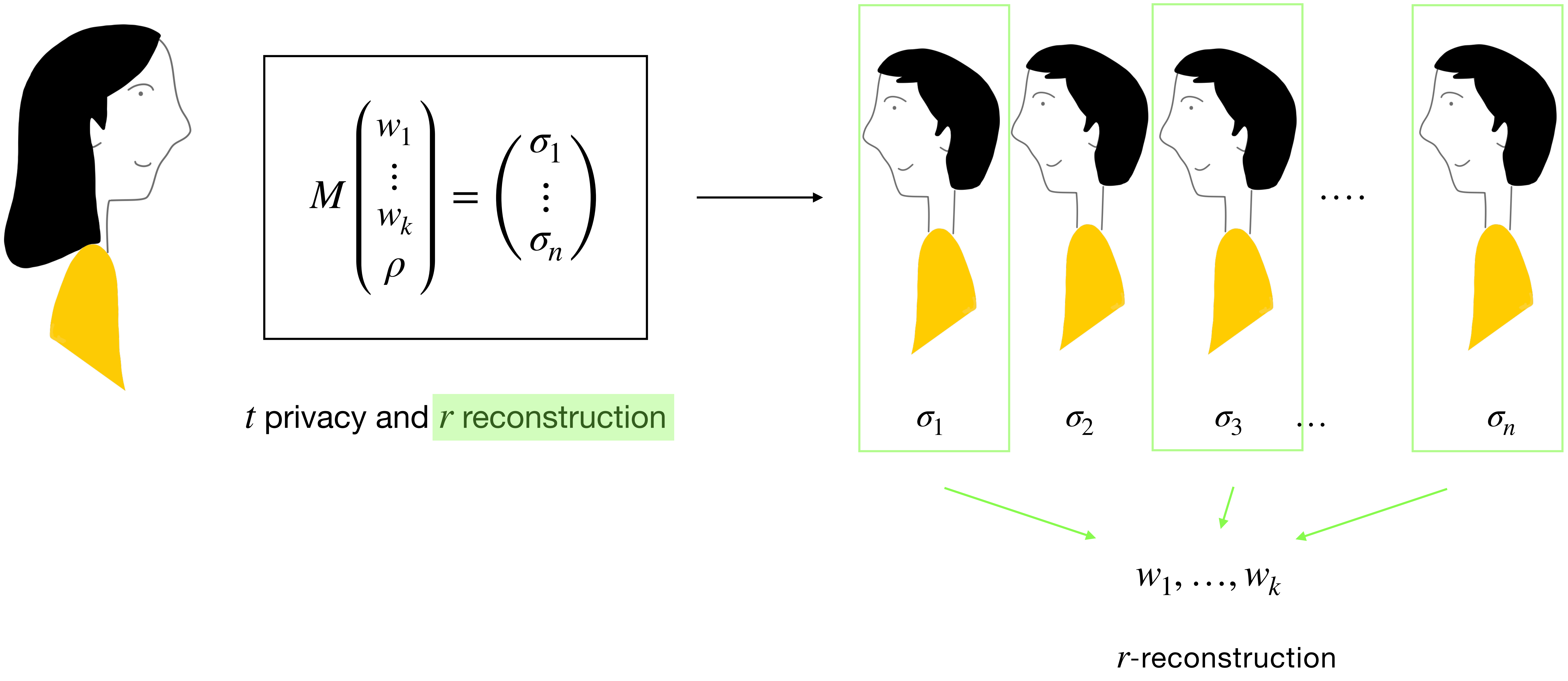
$$M\begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix}$$

t privacy and r reconstruction



Linear Secret Sharing Schemes

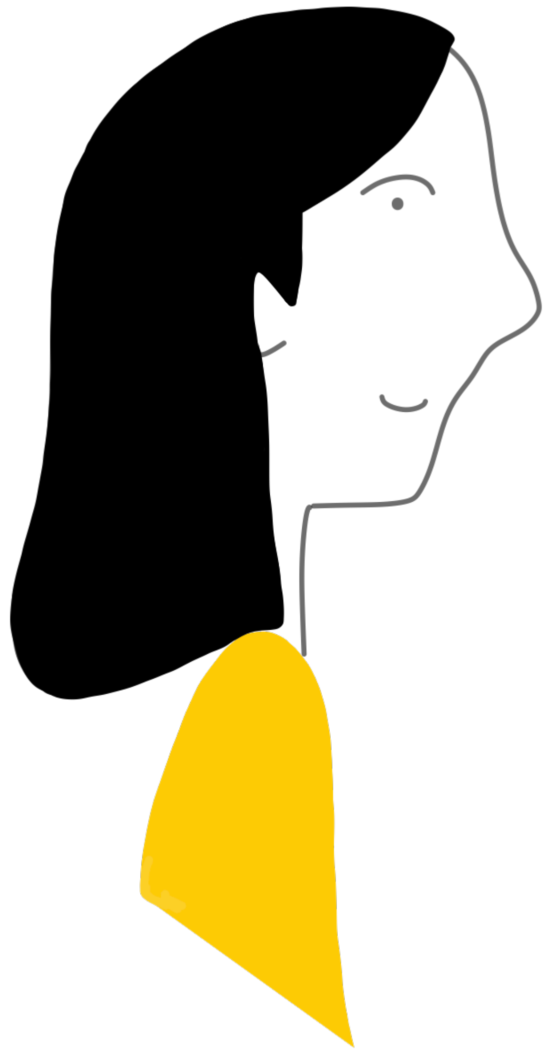
(t, r, n)**-Linear Secret Sharing.** Let W be a module over $\mathfrak{R}$, $w \in W^k, \rho \in W^e$ and $M \in \mathfrak{R}^{h\times(k+e)}$.



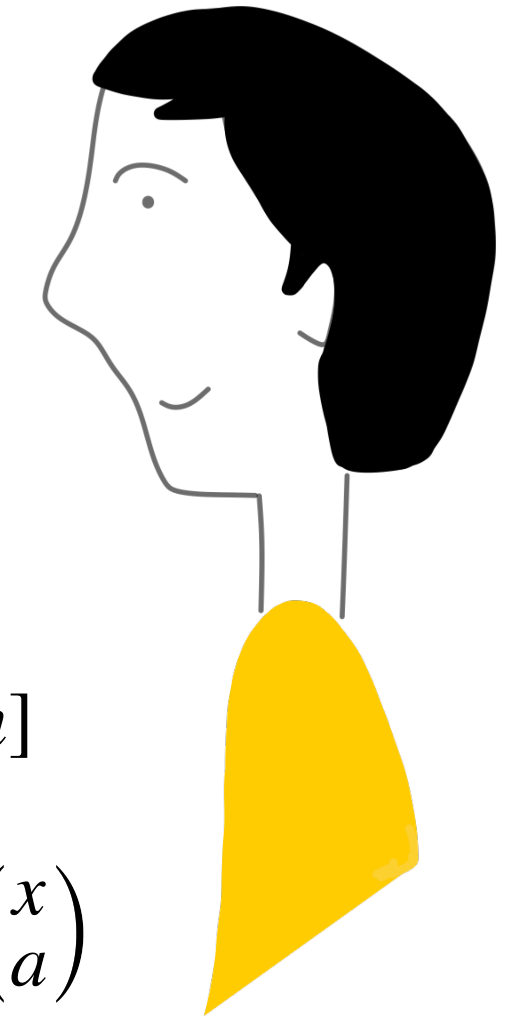
Σ-protocols through LSSS

W and X are modules over a ring $\mathfrak{R}$ and $F : W \to X$ is an homomorphism.
Let $M \in \mathfrak{R}^{h\times(k+e)}$ be the generator matrix of a $(1,r,n)$-LSSS over $\mathfrak{R}$ and let M_i be the rows generating the shares of participant i.

$$M \begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} \qquad M_i \begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = (\sigma_i)$$



I know w_i s.t. $x_i = F(w_i), \forall i \in [k]$



Random tape: ρ

$a = F(\rho)$ $\xrightarrow{\quad \boldsymbol{a} \quad}$

$\xleftarrow{\quad i \quad}$ $i \xleftarrow{\$} [n]$

$\sigma_i = M_i \begin{pmatrix} w \\ \rho \end{pmatrix}$ $\xrightarrow{\quad \sigma_i \quad}$ $F(\sigma_i) \overset{?}{=} M_i \begin{pmatrix} x \\ a \end{pmatrix}$

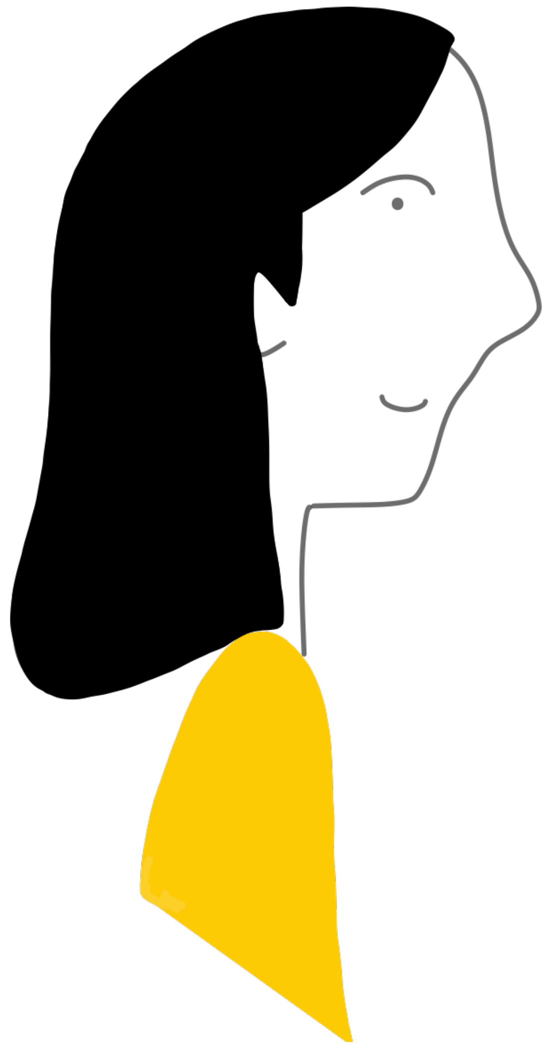
Σ-protocols through LSSS

W and X are modules over a ring $\mathfrak{R}$ and $F : W \to X$ is an homomorphism.

Let $M \in \mathfrak{R}^{h\times(k+e)}$ be the generator matrix of a $(1,r,n)$-LSSS over $\mathfrak{R}$ and let M_i be the rows generating the shares of participant i.

$$M\begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = \begin{pmatrix} \sigma_1 \\ \vdots \\ \sigma_n \end{pmatrix} \qquad M_i\begin{pmatrix} w_1 \\ \vdots \\ w_k \\ \rho \end{pmatrix} = (\sigma_i)$$

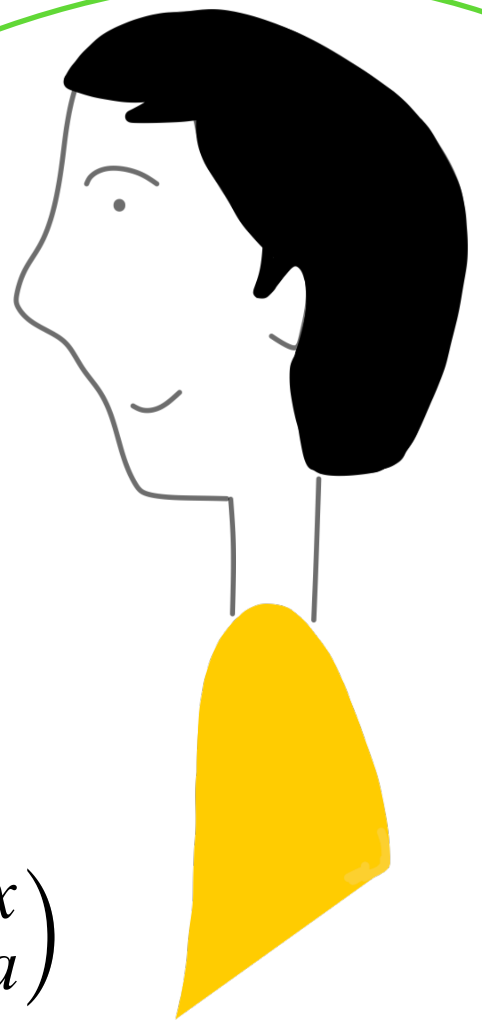
The communication complexity is determined by the share-size of the SSS



I know w_i s.t. $x_i = F(w_i), \forall i \in [k]$

Random tape: ρ

$a = F(\rho)$	$\xrightarrow{\boldsymbol{a}}$	
	$\xleftarrow{i}$	$i \leftarrow^{\$} [n]$
$\sigma_i = M_i\begin{pmatrix} w \\ \rho \end{pmatrix}$	$\xrightarrow{\sigma_i}$	$F(\sigma_i) =^? M_i\begin{pmatrix} x \\ a \end{pmatrix}$



- **Completeness:** F is an homomorphism + SS is linear.
- **r-Special Soundness:** Reconstruct from r conversations Soundness error $(r-1)/n$.
- **Honest-verifier zero-knowledge (HVZK):** t Privacy from the SSS.

Properties of the SSS

We need to construct a Secret Sharing Scheme such that:

- The SSS is linear
- Has $t = 1$ privacy and $r = 2$ reconstruction
- Large number of participants n
- Has small share-size
- Can be defined over any abelian group

Properties of the SSS

We need to construct a Secret Sharing Scheme such that:

- The SSS is linear
- Has $t = 1$ privacy and $r = 2$ reconstruction
- Large number of participants n
- Has small share-size $O(\log n)$. Note average share-size is $\geq \log n$ even for secret-size $k = 1$ [Cramer and Fehr 02]
- Can be defined over any abelian group

$(1,2,n)$**-Black-Box Secret Sharing** [Desmedt and Frankel 94]:
A Black-Box secret sharing scheme is a SSS that can be applied to any finite abelian group $\mathbb{G}$, obliviously to its structure.

Properties of the SSS

We need to construct a Secret Sharing Scheme such that:

- The SSS is linear
- Has $t = 1$ privacy and $r = 2$ reconstruction
- Large number of participants n
- Has small share-size $O(\log n)$. Note average share-size is $\geq \log n$ even for secret-size $k = 1$ [Cramer and Fehr 02]
- Can be defined over any abelian group

$(1,2,n)$**-Black-Box Secret Sharing** [Desmedt and Frankel 94]:
A Black-Box secret sharing scheme is a SSS that can be applied to any finite abelian group $\mathbb{G}$, obliviously to its structure.

Let $w \in \mathbb{G}^k$, $\rho \in \mathbb{G}^h$ and $\mathscr{M} = \{M_1, \ldots, M_n\}$ a family of matrices $M_i \in \mathbb{Z}^{h \times k}$, such that each participant $i \in [n]$ receives share σ_i.

$$M_i \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix} + \begin{pmatrix} \rho_1 \\ \vdots \\ \rho_h \end{pmatrix} = \sigma_i$$

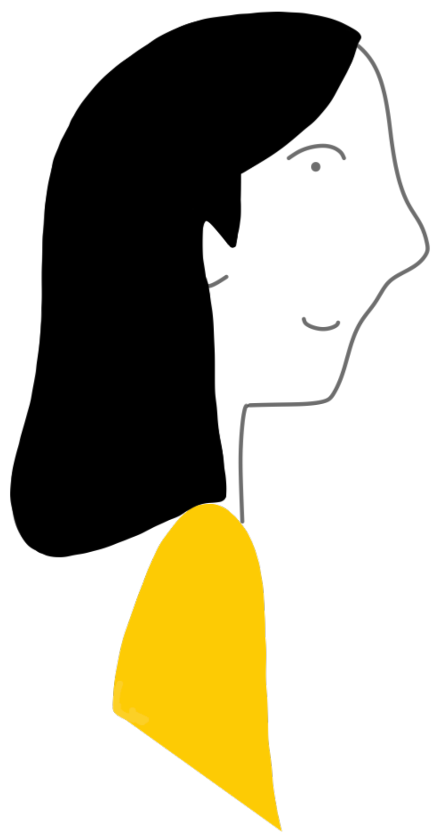
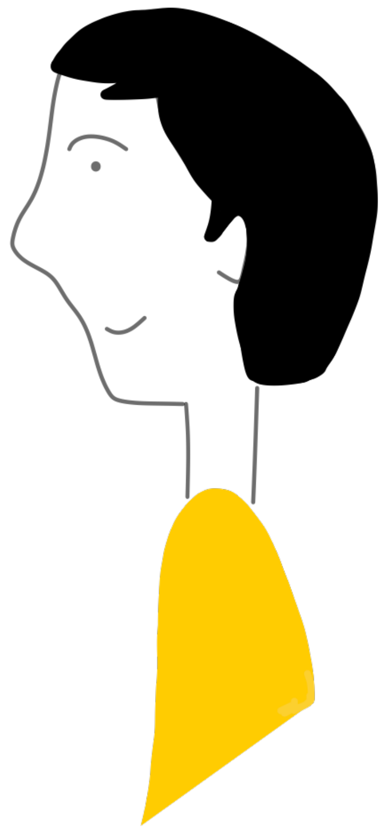
2 reconstruction $\Rightarrow M_i - M_j$ must have a pseudo-inverse such that $R_{i,j}(\sigma_i - \sigma_j) = \begin{pmatrix} w_1, \\ \vdots \\ w_k \end{pmatrix}$

Black-Box Secret Sharing Schemes

Let $\mathscr{M} = \{M_1, \ldots, M_n\}$ be a family of matrices such that $M_i - M_j$ has a pseudo-inverse such that $R_{i,j}(M_i - M_j) = I_k$

$k=1$ $\quad$ $N_1 = 1, N_2 = 0$

$k=2$ $\quad$ $N_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, N_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, N_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, N_4 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$

Black-Box Secret Sharing Schemes

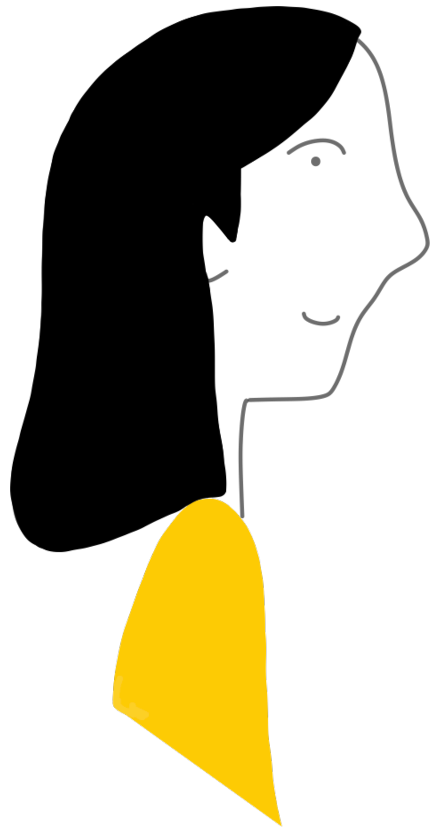
Let $\mathscr{M} = \{M_1, \ldots, M_n\}$ be a family of matrices such that $M_i - M_j$ has a pseudo-inverse such that $R_{i,j}(M_i - M_j) = I_k$

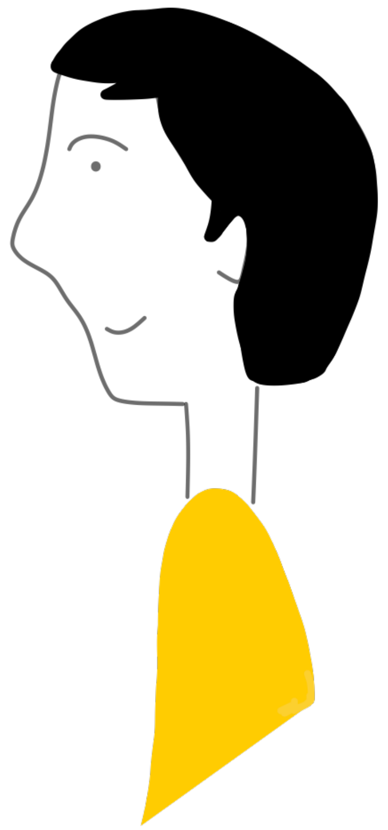
k=1 $$N_1 = 1, N_2 = 0$$

k=2 $$N_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, N_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, N_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, N_4 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

k=3 $$N_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, N_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, N_3 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, N_4 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$$N_5 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, N_6 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, N_7 = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, N_8 = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$





The matrices above define a (1,2,n)-BBSS schemes with $n = 8$, secrets in $\mathbb{G}^3$, and each share in $\mathbb{G}^3$.

Black-Box Secret Sharing Schemes

Let $\mathscr{M} = \{M_1, \ldots, M_n\}$ be a family of matrices such that $M_i - M_j$ has a pseudo-inverse such that $R_{i,j}(M_i - M_j) = I_k$

$k=1$ $\quad N_1 = 1, N_2 = 0$

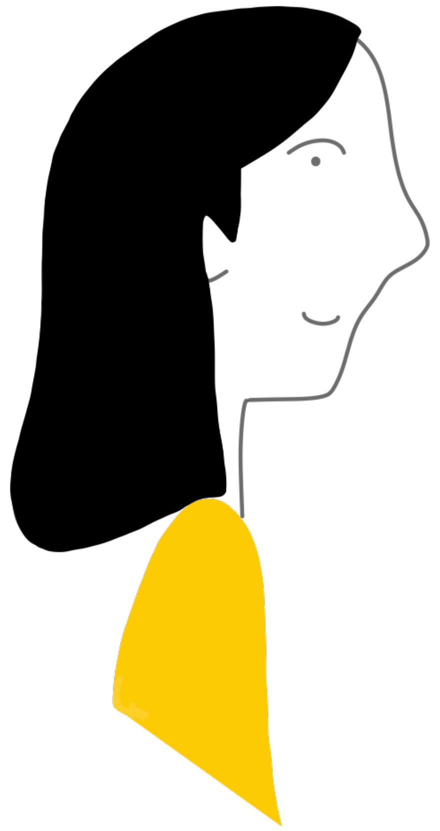
$k=2$ $\quad N_1 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, N_2$ $= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$

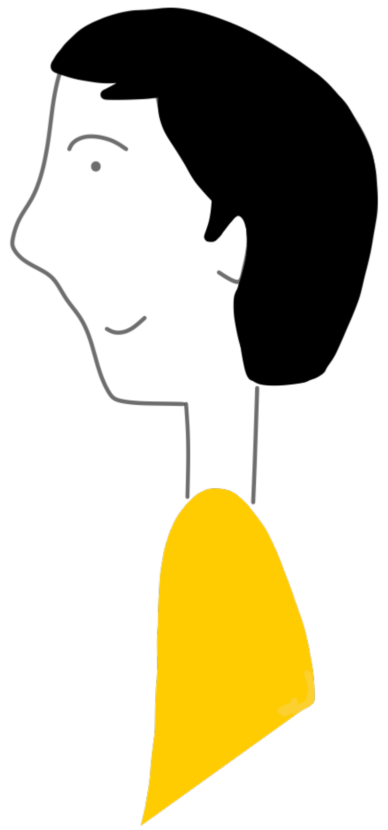
In general it is not known how to construct a family of 2^k matrices $k \times k$ for $k > 3$

$k=3$

$N_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, N_2 =$ $\begin{pmatrix} 0 & 0 & 1 \end{pmatrix}$ $\begin{pmatrix} 1 & 1 & 0 \end{pmatrix}, N_4 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

$N_5 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, N_6 = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, N_7 = \begin{pmatrix} 1 & 1 & 1 \\ -1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, N_8 = \begin{pmatrix} 1 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$





The matrices above define a (1,2,n)-BBSS schemes with $n = 8$, secrets in $\mathbb{G}^3$, and each share in $\mathbb{G}^3$.

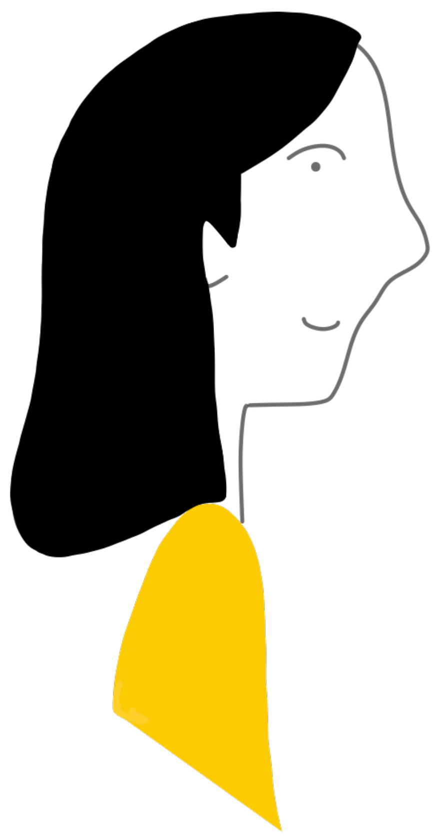
Construction of a (packed) BBSS

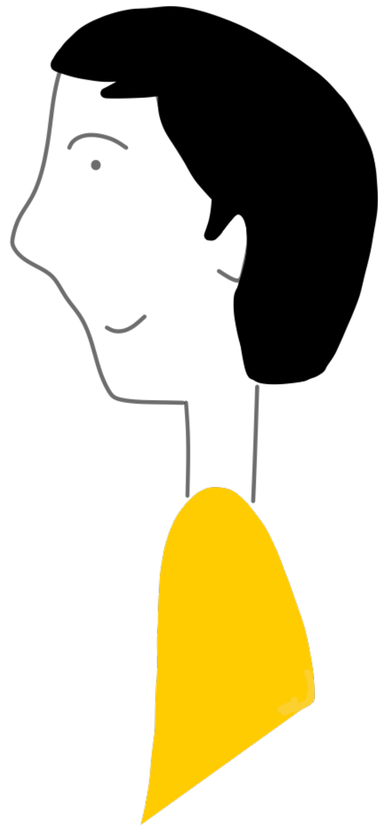
Let $\mathcal{N} = \{N_1, \ldots, N_8\}, N_i \in \mathbb{Z}^{3\times 3}$, for each $i \neq j \in [n]$, $N_i - N_j$ has a pseudo-inverse such that $R_{i,j}(N_i - N_j) = I_k$.

Let $n = 8^m$ be the number of participants, each participant $i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m$ $m > 0$
[Cramer and Damgård CRYPTO'09]

$$i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m \longleftrightarrow (N_{i,0}, \ldots, N_{i,m-1}),\ \text{where } N_{i,j} \in \mathcal{N}$$

$$M_i = \begin{pmatrix} N_{i,0} & & 0 \\ \vdots & \ddots & \\ N_{i,m-1} & & N_{i,0} \\ & \ddots & \vdots \\ 0 & & N_{i,m-1} \end{pmatrix} \in \mathbb{Z}^{3(k+m-1)\times k}$$





Construction of a (packed) BBSS

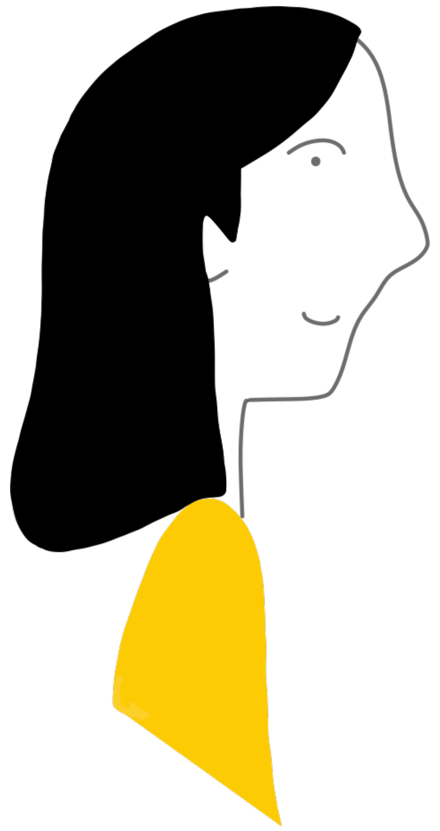
Let $\mathcal{N} = \{N_1, \ldots, N_8\}, N_i \in \mathbb{Z}^{3\times 3}$, for each $i \neq j \in [n]$, $N_i - N_j$ has a pseudo-inverse such that $R_{i,j}(N_i - N_j) = I_k$.

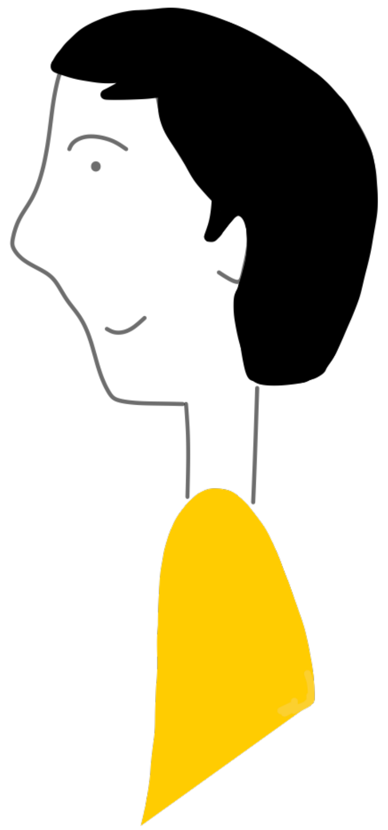
Let $n = 8^m$ be the number of participants, each participant $i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m$ $m > 0$
[Cramer and Damgård CRYPTO'09]

$$i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m \longleftrightarrow (N_{i,0}, \ldots, N_{i,m-1}), \text{ where } N_{i,j} \in \mathcal{N}$$

Let $i \neq j$ then we can assume $i_0 \neq j_0$ where $i = (i_0, \ldots, i_m), j = (j_0 \ldots, j_m) \in \{1,\ldots,8\}^m$

$$M_i = \begin{pmatrix} N_{i,0} & & 0 \\ \vdots & \ddots & \\ N_{i,m-1} & & N_{i,0} \\ & \ddots & \vdots \\ 0 & & N_{i,m-1} \end{pmatrix} \in \mathbb{Z}^{3(k+m-1)\times k} \qquad M_j = \begin{pmatrix} N_{j,0} & & 0 \\ \vdots & \ddots & \\ N_{j,m-1} & & N_{j,0} \\ & \ddots & \vdots \\ 0 & & N_{j,m-1} \end{pmatrix} \in \mathbb{Z}^{3(k+m-1)\times k}$$





Construction of a (packed) BBSS

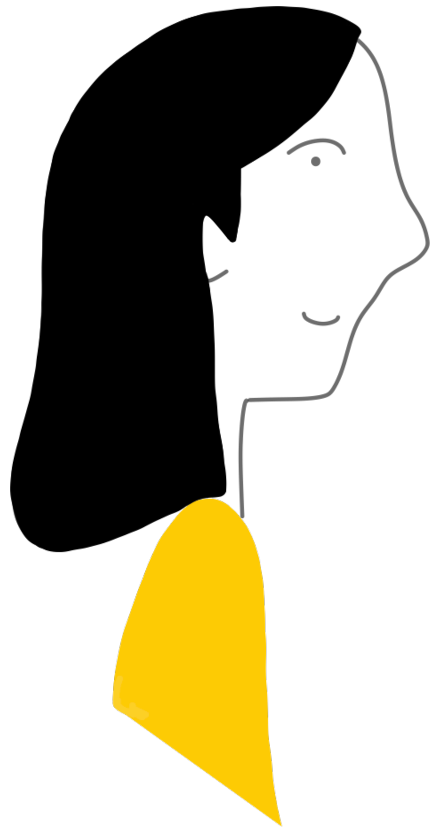
Let $\mathcal{N} = \{N_1, \ldots, N_8\}, N_i \in \mathbb{Z}^{3\times3}$, for each $i \neq j \in [n]$, $N_i - N_j$ has a pseudo-inverse such that $R_{i,j}(N_i - N_j) = I_k$. ★

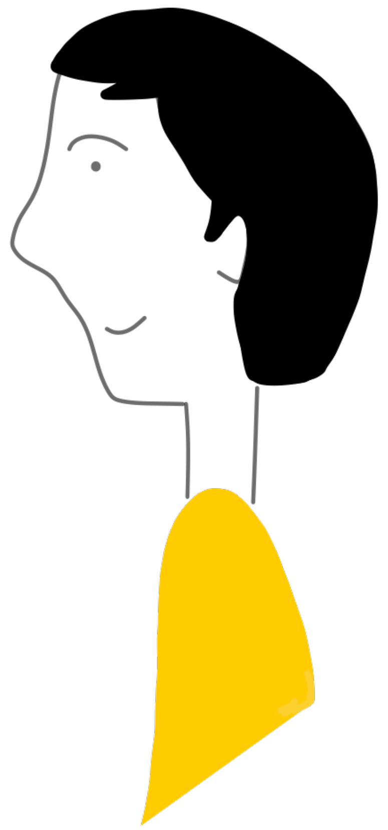
Let $n = 8^m$ be the number of participants, each participant $i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m$ $m > 0$
[Cramer and Damgård CRYPTO'09]

$$i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m \longleftrightarrow (N_{i,0}, \ldots, N_{i,m-1}), \text{ where } N_{i,j} \in \mathcal{N}$$

Let $i \neq j$ then we can assume $i_0 \neq j_0$ where $i = (i_0, \ldots, i_m), j = (j_0 \ldots, j_m) \in \{1,\ldots,8\}^m$

$$M_i = \begin{pmatrix} N_{i,0} & & 0 \\ \vdots & \ddots & \\ N_{i,m-1} & & N_{i,0} \\ & \ddots & \vdots \\ 0 & & N_{i,m-1} \end{pmatrix} - M_j = \begin{pmatrix} N_{j,0} & & 0 \\ \vdots & \ddots & \\ N_{j,m-1} & & N_{j,0} \\ & \ddots & \vdots \\ 0 & & N_{j,m-1} \end{pmatrix} \Rightarrow M_i - M_j = \begin{pmatrix} N_{i,0} - N_{j,0} & & 0 \\ \vdots & \ddots & \\ N_{i,m-1} - N_{j,m-1} & & N_{i,0} - N_{j,0} \\ & \ddots & \vdots \\ 0 & & N_{i,m-1} - N_{j,m-1} \end{pmatrix}$$





The family of matrices $\mathcal{M} = \{M_1, \ldots, M_n\}$ satisfies ★

Construction of a (packed) BBSS

Let $\mathcal{N} = \{N_1, \ldots, N_8\}, N_i \in \mathbb{Z}^{3\times 3}$, for each $i \neq j \in [n]$, $N_i - N_j$ has a pseudo-inverse such that $R_{i,j}(N_i - N_j) = I_k$.

Let $n = 8^m$ be the number of participants, each participant $i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m$ $m > 0$

[Cramer and Damgård CRYPTO'09]

$$i = (i_0, \ldots, i_{m-1}) \in \{0,\ldots,7\}^m \longleftrightarrow (N_{i,0}, \ldots, N_{i,m-1}), \text{ where } N_{i,j} \in \mathcal{N}$$

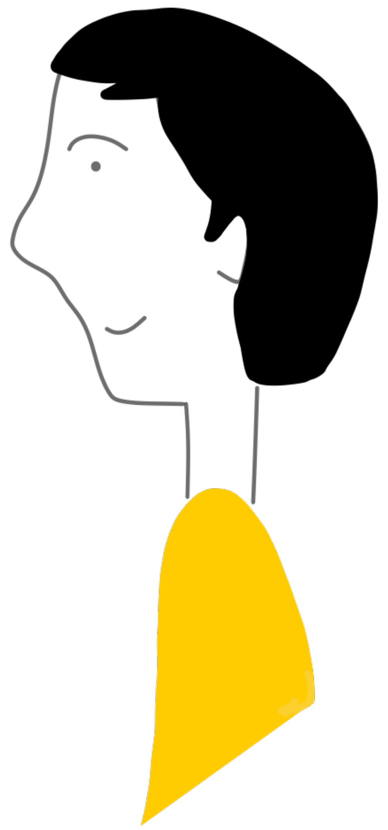
Let $i \neq j$ then we can assume $i_0 \neq j_0$ where $i = (i_0, \ldots, i_m), j = (j_0 \ldots, j_m) \in \{1,\ldots,8\}^m$

$$M_i = \begin{pmatrix} N_{i,0} & & 0 \\ \vdots & \ddots & \\ N_{i,m-1} & & N_{i,0} \\ & \ddots & \vdots \\ 0 & & N_{i,m-1} \end{pmatrix} \in \mathbb{Z}^{3(k+m-1)\times k}$$

The family of matrices $\mathcal{M} = \{M_1, \ldots, M_n\}$ satisfies

Proposition

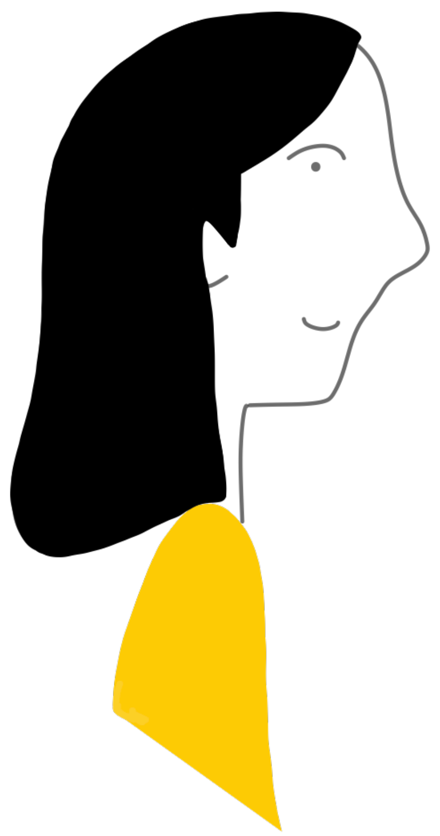
For $k \equiv 0 \mod 3$ and $n = 2^\lambda$, there exists a (1,2,n)-BBSS with share-size $h_* = k + \lambda - 3$.



Σ-protocols through BBSS

$\mathbb{G}_1$ and $\mathbb{G}_2$ are abelian groups and $F : \mathbb{G}_1 \to \mathbb{G}_2$ is an homomorphism.

I know $w_1, \ldots, w_k$ s.t.
$x_1 = F(w_1), \ldots, x_k = F(x_k)$



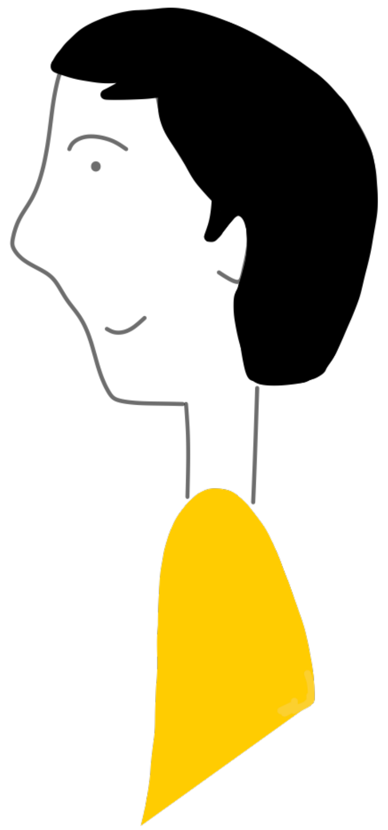
Σ-PROTOCOL

$(1,2,n)$**-BBSS**

For $k \equiv 0 \mod 3$ and $n = 2^\lambda$,
share-size $h_* = k + \lambda - 3$.

2-special soundness
soundness error $2^{-\lambda}$
communication complexity:
$k + \lambda - 3$ elements of
$\mathbb{G}_1$ and $\mathbb{G}_2$ (and λ bits for the challenge).

accept/reject

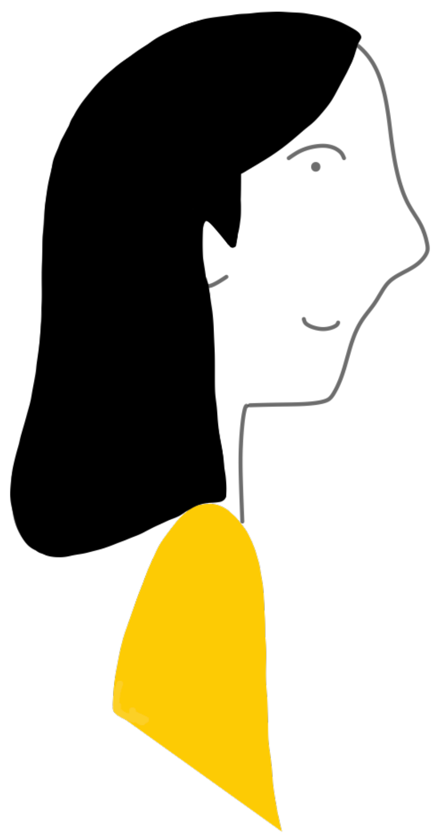


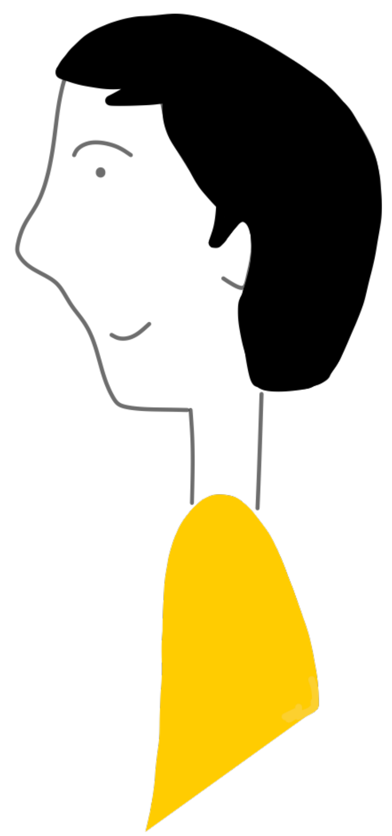
Class Groups

Let ℓ be an integer, let $\hat{G}$ be a finite commutative group and a cycle subgroup $G \subset \hat{G}$ of unknown order.
$G \cong F \times G^{\ell}$, where F is of order ℓ [Castagnos and Laguillaumie 15]

- **Proof of discrete logarithm:**
  $R_{DLCG,k} := \{(w, x) \in \mathbb{Z}^k \times G^k \mid g^{w_i} = x_i \ \forall i = 1,\ldots k\}$
- **Proof of plaintext and randomness knowledge CL_HSM:**
  $\psi : \mathbb{Z}_{\ell} \times \mathbb{Z} \to G^{\ell} \times G$, $\psi(m, r) = (g_{\ell}^{r}, \mathbf{pk}^{r} \cdot f^{m})$
  $R_{CL,k} := \{(m, r); (c, d) \in (\mathbb{Z} \times \mathbb{Z}_{\ell})^k \times (G^{\ell} \times G)^k \mid \psi(m_i, r_i) = (c_i, d_i) \ \forall i = 1,\ldots k\}$

Group homomorphisms





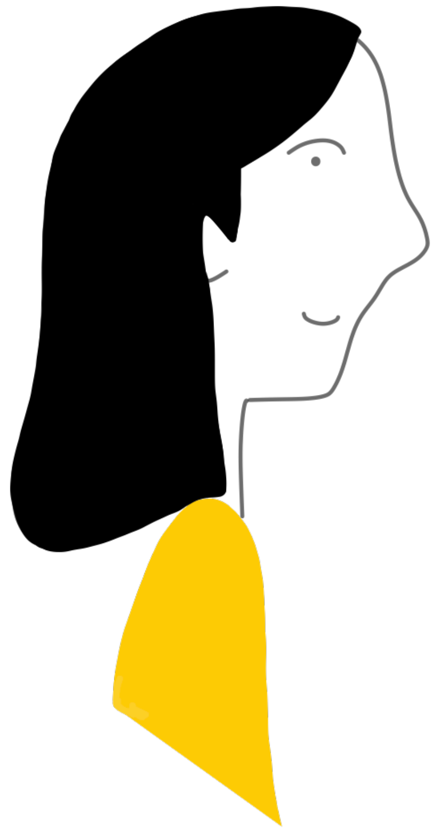
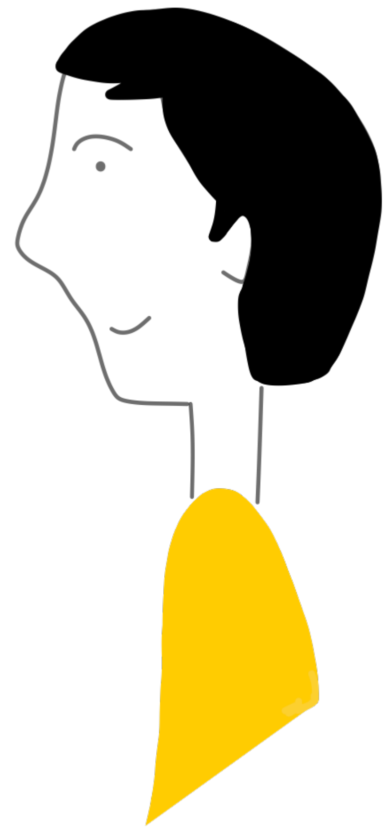
Class Groups

Let ℓ be an integer, let $\hat{G}$ be a finite commutative group and a cycle subgroup $G \subset \hat{G}$ of unknown order.
$G \cong F \times G^{\ell}$, where F is of order ℓ [Castagnos and Laguillaumie 15]

- **Proof of discrete logarithm:**
  $R_{DLCG,k} := \{(w, x) \in \mathbb{Z}^k \times G^k \mid g^{w_i} = x_i \ \forall i = 1, \ldots k\}$
- **Proof of plaintext and randomness knowledge CL_HSM:**
  $\psi : \mathbb{Z}_\ell \times \mathbb{Z} \to G^{\ell} \times G, \ \psi(m, r) = (g_\ell^r, \mathbf{pk}^r \cdot f^m)$
  $R_{CL,k} := \{(m, r); (c, d) \in (\mathbb{Z} \times \mathbb{Z}_\ell)^k \times (G^{\ell} \times G)^k \mid \psi(m_i, r_i) = (c_i, d_i) \ \forall i = 1, \ldots k\}$

Group homomorphisms

Proof of DL	Communication (bits)	Knowledge	Assumptions
Castagnos et al CRYPTO'19	$\lambda k(\log S + \lambda + \log \lambda)$	Yes	None
Castagnos et al PKC'20	$k(\log S + 2\lambda)$	Yes	Low order, Strong Root, Uniform random g
Braun et al CRYPTO'23	$k(\log S + 2\lambda)$	No	Rough Order
Our work	$(k + \lambda - 3)(\log S + \lambda + \log(k + \lambda + \log \min(\lambda, k))$	Yes	None

Other applications

- **ZK-ready functions:** Σ-protocol can be extended to ZK-ready functions [Cramer and Damgård CRYPTO'09]
- **Joye-Libert (JL'13):**

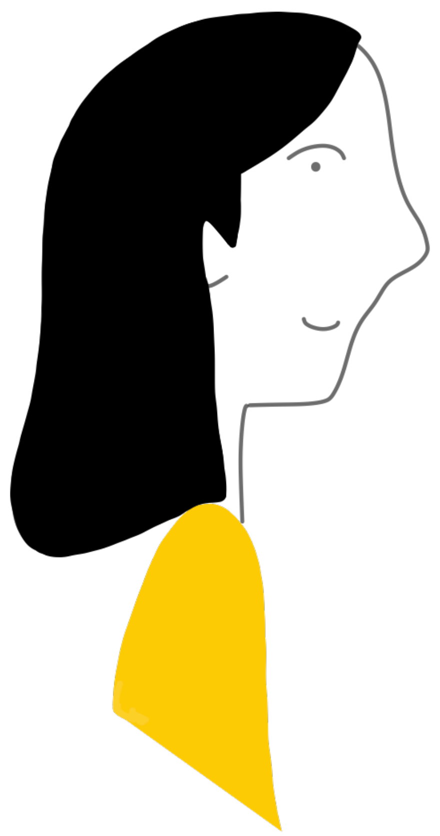
$$\begin{array}{rccc} f: & \mathbb{Z}_{2^\ell} \times \mathbb{Z}_N^* & \longrightarrow & \mathbb{Z}_N^* \\ & (u, s) & \mapsto & g^u \cdot s^{2^\ell} \end{array}$$

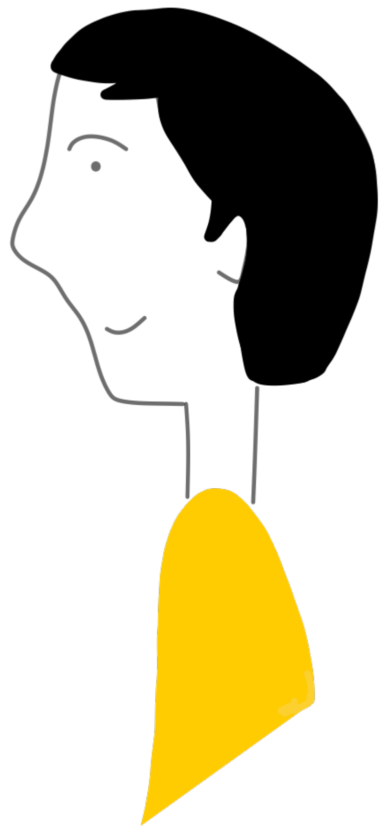
Σ-PROTOCOL JL

$(1,2,n)$**-BBSS**

For $k \equiv 0 \mod 3$ and $n = 2^\lambda$, share-size $h_* = k + \lambda - 3$.

2-special soundness
soundness error $2^{-\lambda}$
communication complexity: $k + \lambda - 3$ elements of $\mathbb{Z}_{2^\ell}$ and $\mathbb{Z}_N$ (and λ bits for the challenge).





Other applications

- **ZK-ready functions:** Σ-protocol can be extended to ZK-ready functions [Cramer and Damgård CRYPTO'09]
- **Joye-Libert (JL'13):**

$$\begin{array}{rccc} f: & \mathbb{Z}_{2^\ell} \times \mathbb{Z}_N^* & \longrightarrow & \mathbb{Z}_N^* \\ & (u, s) & \mapsto & g^u \cdot s^{2^\ell} \end{array}$$

Σ-PROTOCOL JL

$(1{,}2{,}n)$**-BBSS**

For $k \equiv 0 \mod 3$ a

share-size $h_* = k$ -

It can be improved!

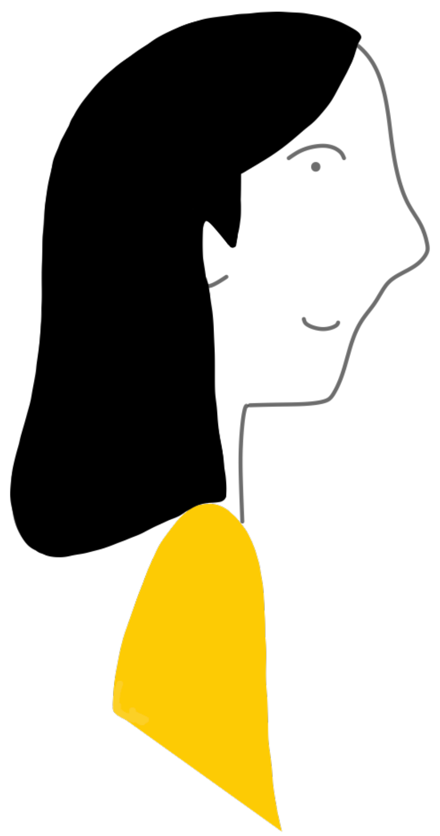
undness

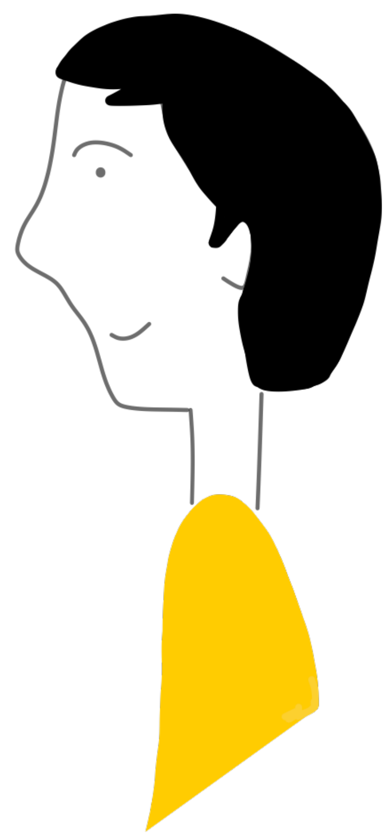
rror $2^{-\lambda}$

on complexity:

ements of

$\mathbb{Z}_{2^\ell}$ and $\mathbb{Z}_N$ (and λ bits for the challenge).





Other applications

- **ZK-ready functions:** Σ-protocol can be extended to ZK-ready functions [Cramer and Damgård CRYPTO'09]
- **Joye-Libert (JL'13):** We improve the Σ-protocol by using Shamir's secret sharing schemes over Galois Rings
  Ex. Attema *et al* TCC'22

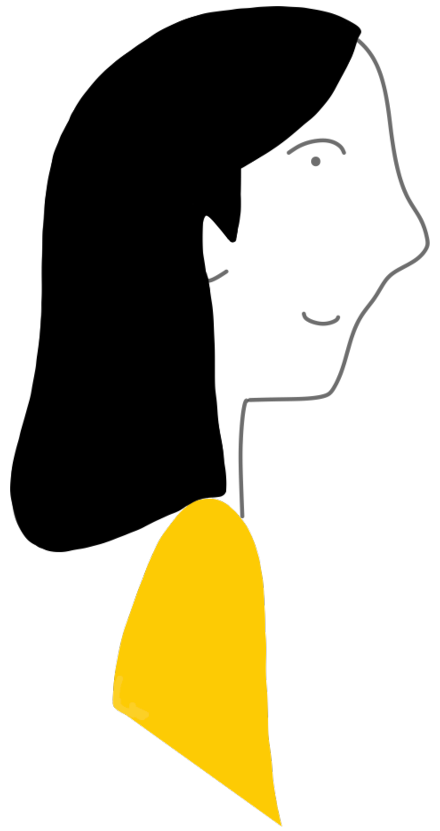
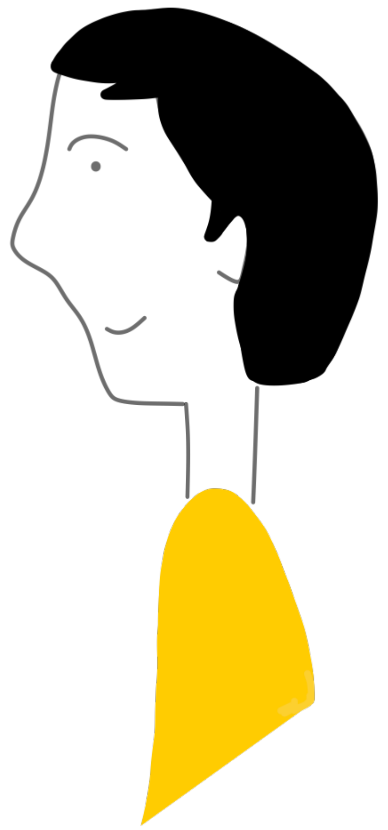
$$\begin{array}{rccc} f: & \mathbb{Z}_{2^\ell} \times \mathbb{Z}_N^* & \longrightarrow & \mathbb{Z}_N^* \\ & (u, s) & \mapsto & g^u \cdot s^{2^\ell} \end{array}$$

Σ-PROTOCOL JL

Shamir SS

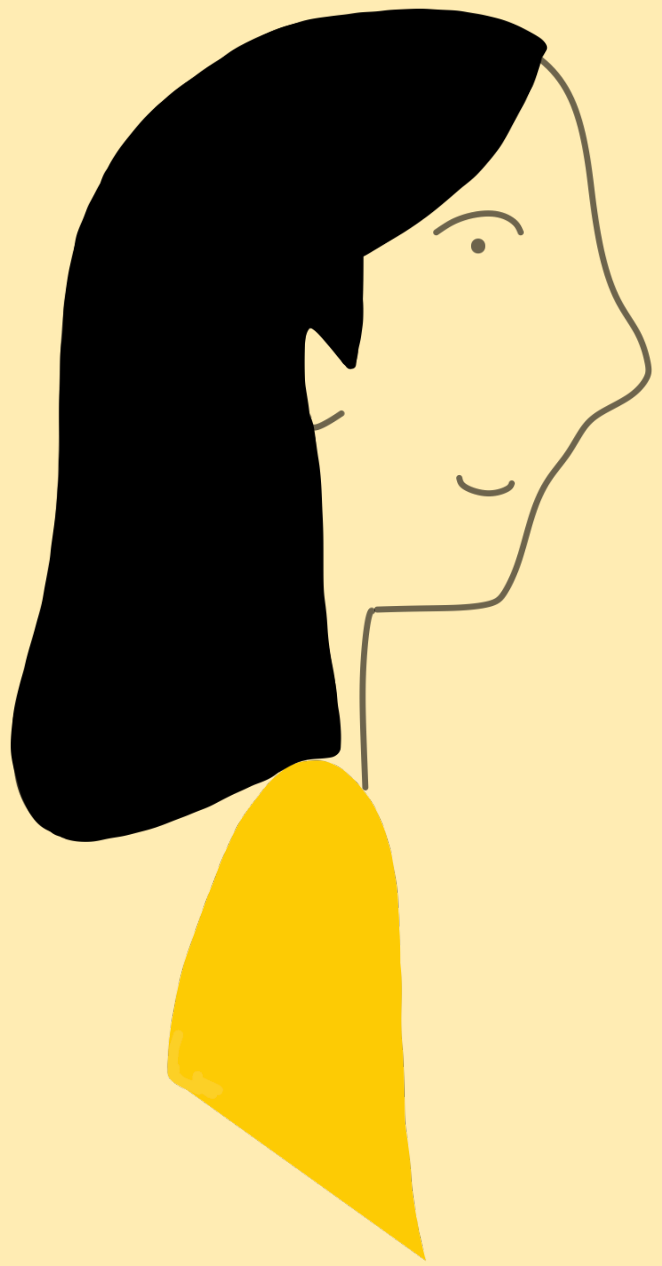
$(1, k+1, 2^k)$-Shamir's secret sharing scheme over Galois Rings

$(k+1)$-special soundness
soundness error 2^{-k}
communication complexity: k elements of $\mathbb{Z}_{2^\ell}$ and $\mathbb{Z}_N$ (and k bits for the challenge).

Conclusions

- Formalize the description of Σ-protocols proving knowledge of preimages of module homomorphisms, through any (t, r, n)-linear secret sharing scheme, including NI versions.
- General construction of a Σ-protocol proving knowledge of k preimages of group homomorphisms over any abelian group, even of unknown order.
- Application to Class Groups, improving previous works.
- Extension to ZK-ready functions and for Joye-Libert we present an improved construction of the Σ-protocol based on Galois Rings.



Conclusions

- Formalize the description of Σ-protocols proving knowledge of preimages of module homomorphisms, through any (t, r, n)-linear secret sharing scheme, including NI versions.
- General construction of a Σ-protocol proving knowledge of k preimages of group homomorphisms over any abelian group, even of unknown order.
- Application to Class Groups, improving previous works.
- Extension to ZK-ready functions and for Joye-Libert we present an improved construction of the Σ-protocol based on Galois Rings.

Acknowledgement: This work has been partially supported by the grant PIPF-2022/COM-25517, funded by the Madrid Regional Government, and by the projects SecuRing (PID2019-110873RJ-I00/MCIN/AEI/10.13039/501100011033), PRODIGY(TED2021-132464B-I00) funded by MCIN/AEI/10.13039/501100011033/ and the European Union NextGenerationEU/PRTR, and CONFIDENTIAL-6G funded by the European Union (GA 101096435).