Aarhus University

Verifiable Secret-Sharing Schemes

Irene Giacomelli

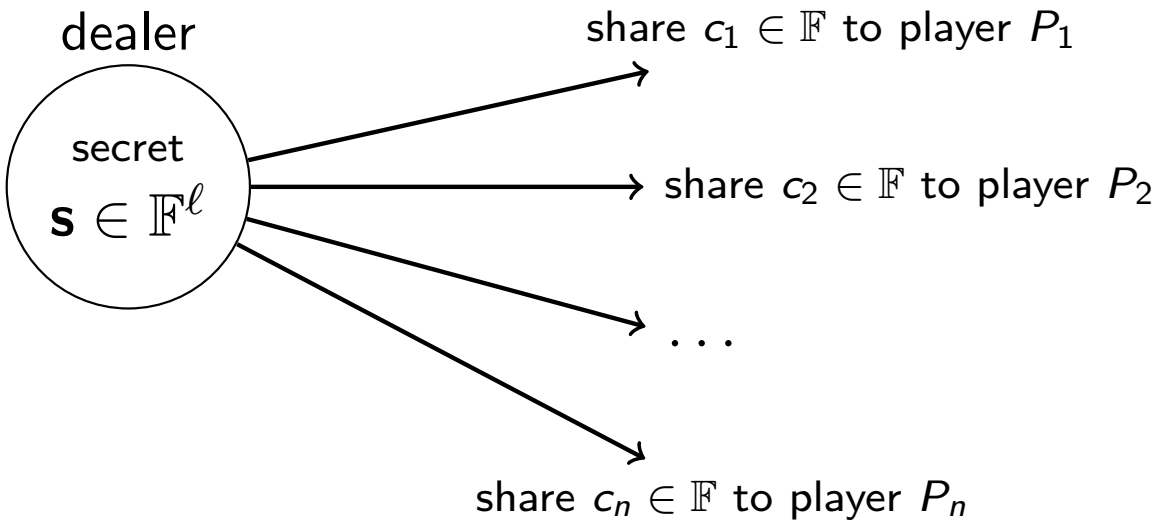
joint work with Ivan Damgård, Bernardo David and Jesper B. Nielsen

Aalborg, 30th June 2014

Packed Linear Secret-Sharing Scheme among n players

(t, r)-LSSS for secret $s \in \mathbb{F}^\ell$

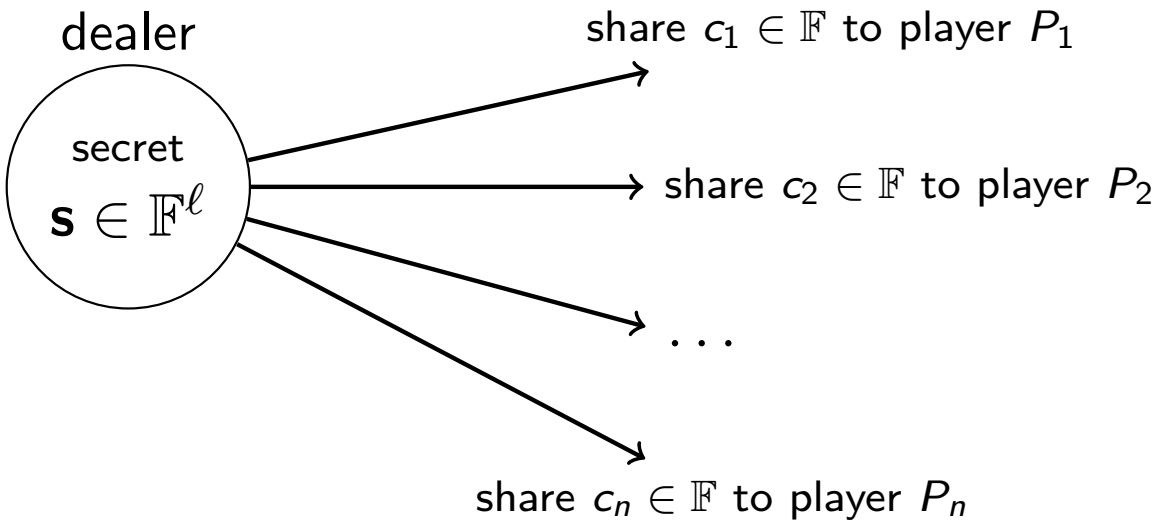
Sharing Phase:



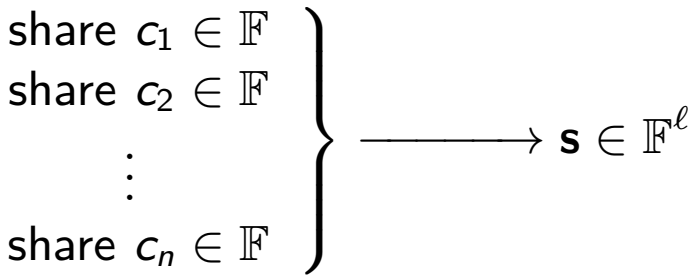
Packed Linear Secret-Sharing Scheme among n players

(t, r)-LSSS for secret $s \in \mathbb{F}^\ell$

Sharing Phase:



Reconstruction Phase:



Packed Linear Secret-Sharing Scheme among n players

(t, r)-LSSS for secret $s \in \mathbb{F}^\ell$

- t-**privacy**

$$\left.\begin{array}{l} \text{share } c_{i_1} \in \mathbb{F} \\ \text{share } c_{i_2} \in \mathbb{F} \\ \quad\vdots \\ \text{share } c_{i_t} \in \mathbb{F} \end{array}\right\} \longrightarrow \textbf{?}$$

- r-**reconstruction**

$$\left.\begin{array}{l} \text{share } c_{j_1} \in \mathbb{F} \\ \text{share } c_{j_2} \in \mathbb{F} \\ \quad\vdots \\ \text{share } c_{j_r} \in \mathbb{F} \end{array}\right\} \longrightarrow \mathbf{s} \in \mathbb{F}^\ell$$

An example: Shamir's scheme ($\ell = 1$) for n players

Let $\beta_1, \ldots, \beta_n$ be n distinct nonzero elements of $\mathbb{F}$,

$$\begin{array}{c} \text{secret} \\ s \in \mathbb{F} \end{array} \quad \rightsquigarrow \quad \begin{array}{c} D \text{ chooses} \\ f(x) = s + \sum_{i=1}^{t} a_i x^i \\ \text{random} \end{array} \quad \rightsquigarrow \quad \begin{array}{c} \text{shares:} \\ c_i = f(\beta_i) \\ i = 1, \ldots, n \end{array}$$

Note: Shamir's scheme has t-privacy and $(t+1)$-reconstruction.

An example: Shamir's scheme ($\ell = 1$) for n players

Let $\beta_1, \ldots, \beta_n$ be n distinct nonzero elements of $\mathbb{F}$,

$$\text{secret } s \in \mathbb{F} \quad \rightsquigarrow \quad \overset{D \text{ chooses}}{\overset{\text{random}}{f(x) = s + \sum_{i=1}^{t} a_i x^i}} \quad \rightsquigarrow \quad \text{shares: } c_i = f(\beta_i),\ i = 1, \ldots, n$$

Note: Shamir's scheme has t-privacy and $(t+1)$-reconstruction.

$$\begin{pmatrix} 1 & \beta_1 & \ldots & \beta_1^t \\ 1 & \beta_2 & \ldots & \beta_2^t \\ \vdots & \vdots & & \vdots \\ 1 & \beta_n & \ldots & \beta_n^t \end{pmatrix} \begin{pmatrix} s \\ a_1 \\ \vdots \\ a_t \end{pmatrix} = \begin{pmatrix} f(\beta_1) \\ f(\beta_2) \\ \vdots \\ f(\beta_n) \end{pmatrix}$$

An example: Shamir's scheme ($\ell = 1$) for n players

Let $\beta_1, \ldots, \beta_n$ be n distinct nonzero elements of $\mathbb{F}$,

$$\text{secret } s \in \mathbb{F} \quad \rightsquigarrow \quad \overset{D \text{ chooses}}{\overset{\text{random}}{f(x) = s + \sum_{i=1}^{t} a_i x^i}} \quad \rightsquigarrow \quad \text{shares: } c_i = f(\beta_i),\ i = 1, \ldots, n$$

Note: Shamir's scheme has t-privacy and $(t+1)$-reconstruction.

The set $\{(s, c_1, \ldots, c_n)\} =$

$$= \left\{ (f(0), f(\beta_1), \ldots, f(\beta_n)) \mid deg(f) \leq t \right\}$$

is a $[n+1, t+1]$-**Reed-Solomon code** over $\mathbb{F}$.

An example: Franklin and Yung's scheme ($\ell > 1$)

Let $\{\alpha_1, \ldots, \alpha_\ell\}$ and $\{\beta_1, \ldots, \beta_n\}$ be two disjoint sets of distinct elements of $\mathbb{F}$,

$$\text{secret } \mathbf{s} \in \mathbb{F}^\ell \quad \rightsquigarrow \quad \begin{array}{c} f(x) \in \mathbb{F}[x] \\ \text{random s.t.} \\ \deg(f) \leq t + \ell - 1 \\ \text{and} \\ f(\alpha_i) = \mathbf{s}[i] \\ \forall\, i = 1, \ldots, \ell \end{array} \quad \rightsquigarrow \quad \begin{array}{c} \text{shares:} \\ c_i = f(\beta_i) \\ i = 1, \ldots, n \end{array}$$

where $\mathbf{s} = \begin{pmatrix} \mathbf{s}[1] \\ \mathbf{s}[2] \\ \vdots \\ \mathbf{s}[\ell] \end{pmatrix}$

What kind of security?!

Assume the dealer is honest:

t-privacy $\longrightarrow$ security for the dealer against at most t corrupted curious players (**passive corruption**);

What kind of security?!

Assume the dealer is honest:

t-privacy $\longrightarrow$ security for the dealer against at most t corrupted curious players (**passive corruption**);

What happens if the corrupted players during the reconstruction phase provide faulty shares (**active corruption**)?!

robust reconstruction $\longrightarrow$ the set of the n shares determines the secret even if t of them are faulty (**robust SSS**)

What kind of security?!

Assume the dealer is honest:

t-privacy $\longrightarrow$ security for the dealer against at most t corrupted curious players (**passive corruption**);

What happens if the corrupted players during the reconstruction phase provide faulty shares (**active corruption**)?!

robust reconstruction $\longrightarrow$ the set of the n shares determines the secret even if t of them are faulty (**robust SSS**)

e.g. If $t < n/3$, Shamir's scheme is robust (Reed-Solomon decoding)

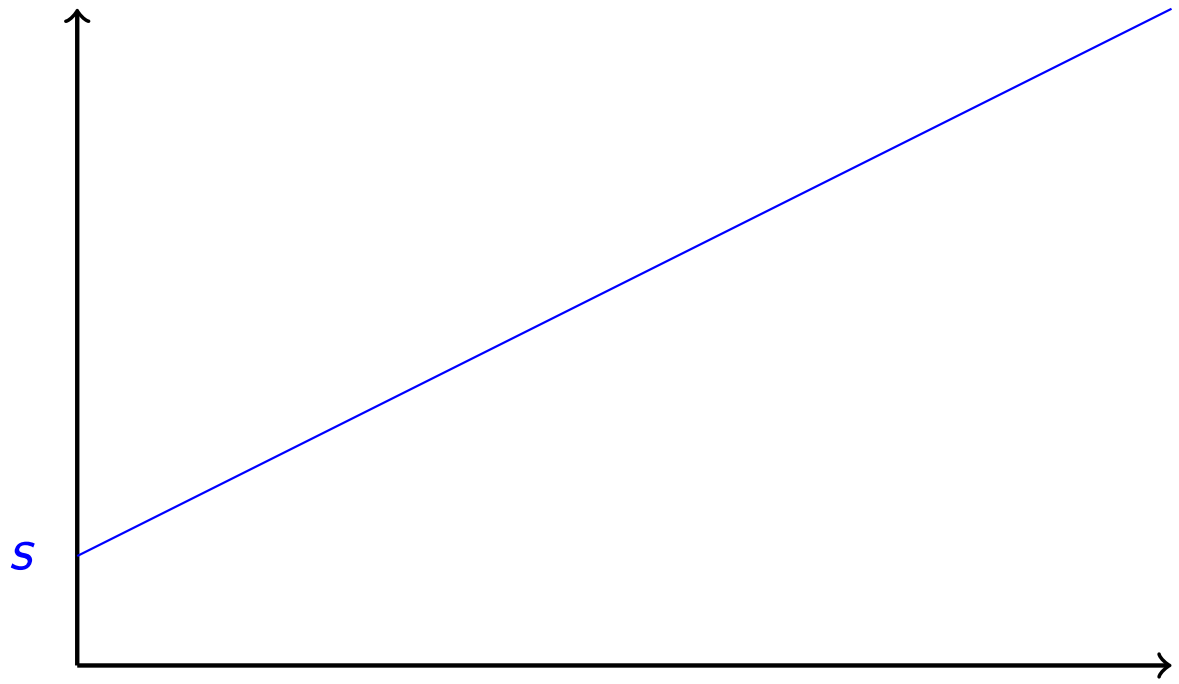
Security: the players' point of view

What happens if the dealer is not honest?!

Security: the players' point of view

What happens if the dealer is not honest?!

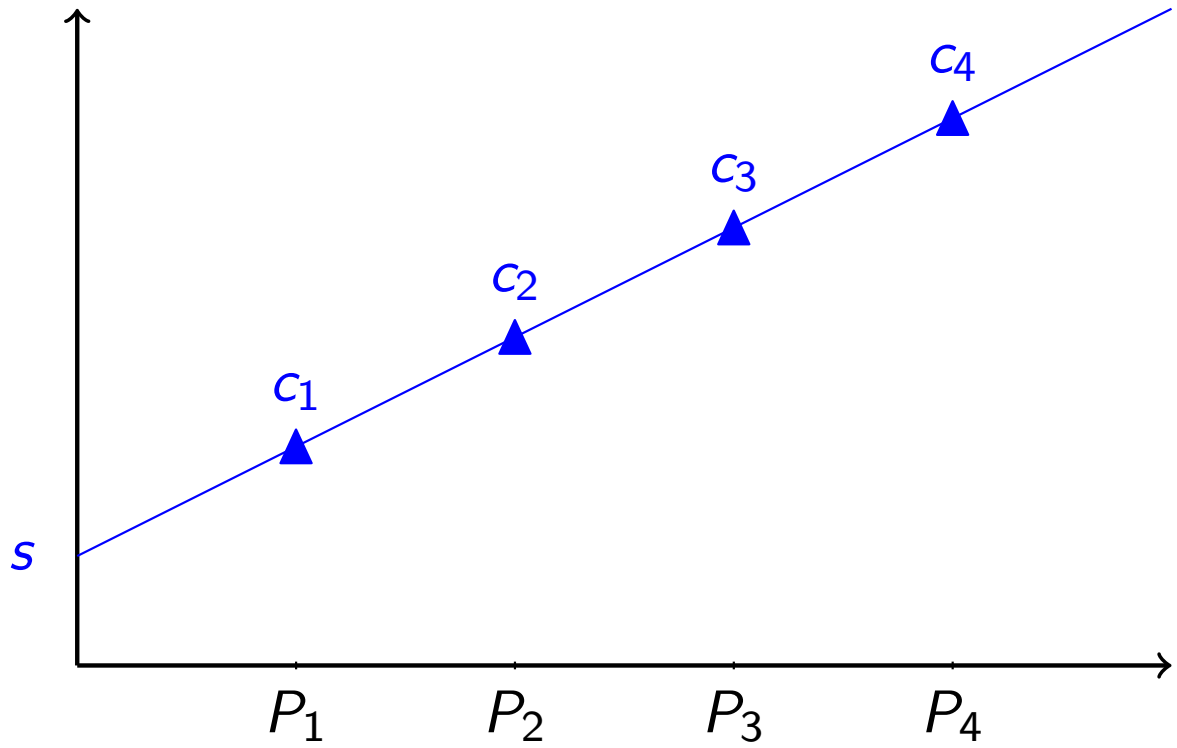
Consider Shamir's scheme with $n = 4$ and $t = 1$ ($r = 2$):



Security: the players' point of view

What happens if the dealer is not honest?!

Consider Shamir's scheme with $n = 4$ and $t = 1$ $(r = 2)$:



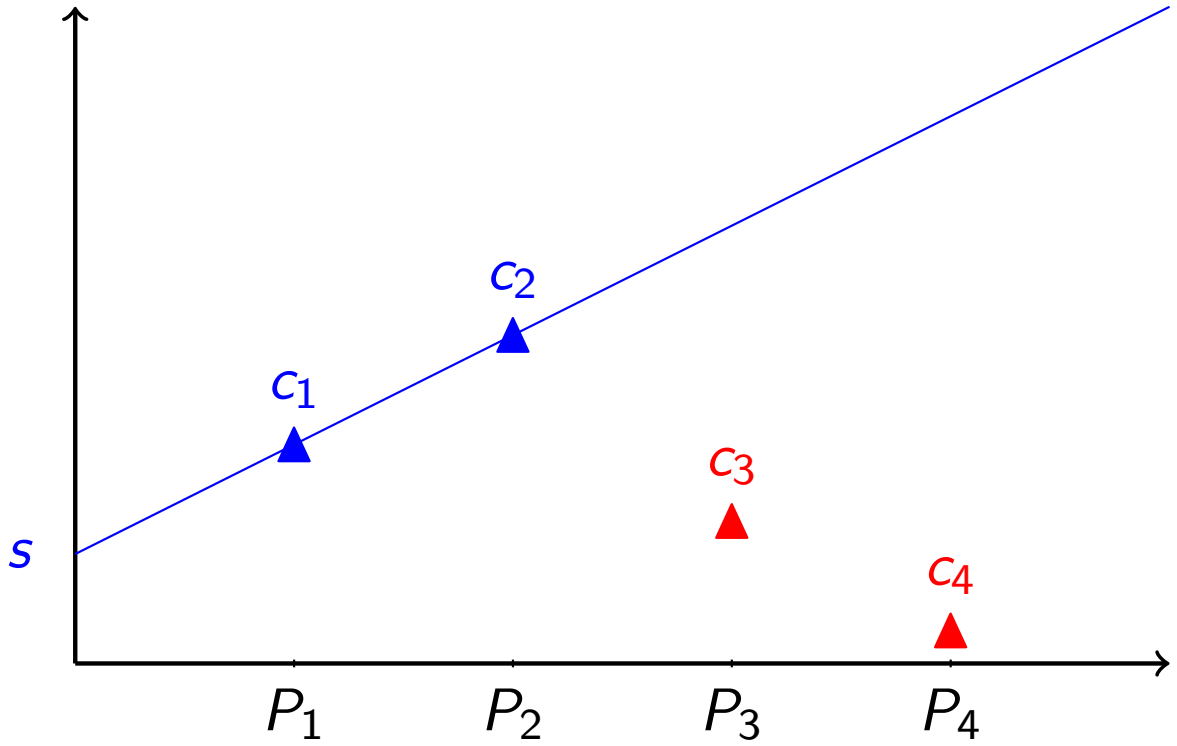
P_1, P_2 $\longrightarrow s$

P_3, P_4 $\longrightarrow s$

Security: the players' point of view

What happens if the dealer is not honest?!

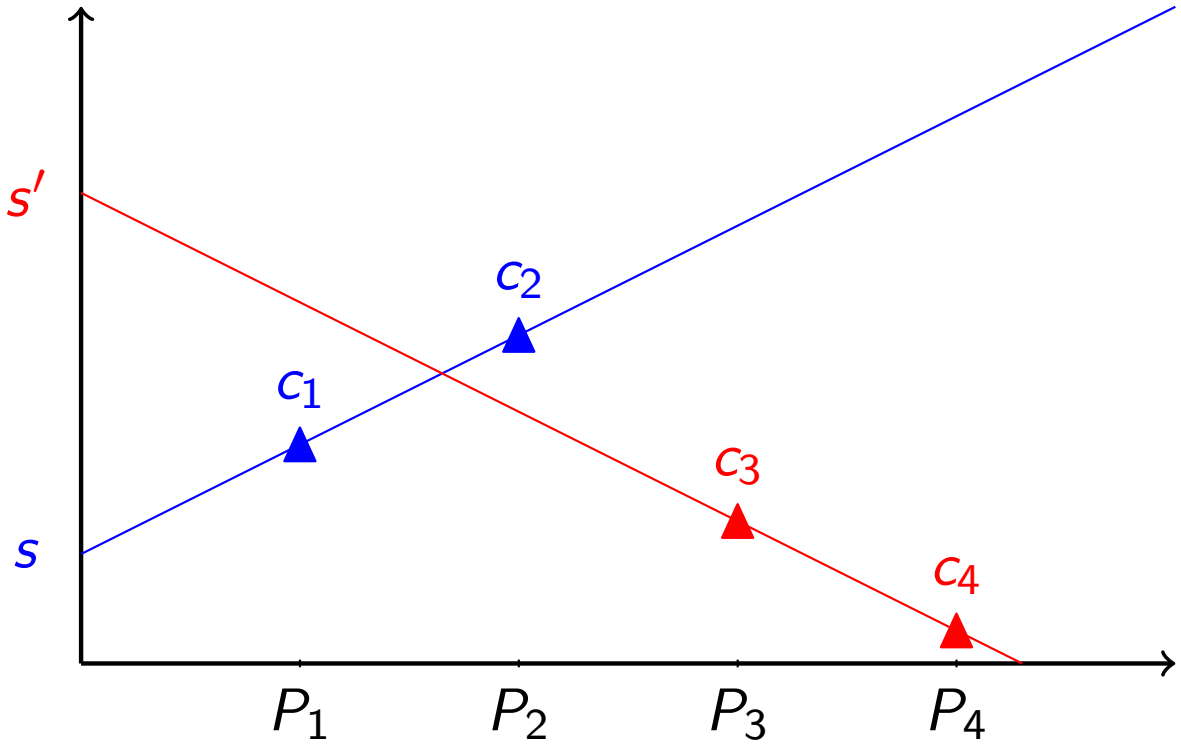
Consider Shamir's scheme with $n = 4$ and $t = 1$ $(r = 2)$:



Security: the players' point of view

What happens if the dealer is not honest?!

Consider Shamir's scheme with $n = 4$ and $t = 1$ $(r = 2)$:



$$\left.\begin{matrix} P_1 \\ P_2 \end{matrix}\right\} \longrightarrow s$$

$$\left.\begin{matrix} P_3 \\ P_4 \end{matrix}\right\} \longrightarrow s'$$

$$s \neq s'$$

Definition of VSSS:

A (t, r)-SSS among n players is **verifiable** if

- t-**privacy**: when the dealer is honest, any set of t players $\rightarrow$ no info about the secret.

$$\left.\begin{matrix} P_{i_1} \\ P_{i_2} \\ \vdots \\ P_{i_t} \end{matrix}\right\} \longrightarrow \textbf{?}$$

Definition of VSSS:

A (t, r)-SSS among n players is **verifiable** if

- t-**privacy**: when the dealer is honest, any set of t players $\rightarrow$ no info about the secret.

$$\left.\begin{matrix} P_{i_1} \\ P_{i_2} \\ \vdots \\ P_{i_t} \end{matrix}\right\} \longrightarrow ?$$

- r-**robust reconstruction**: when the dealer is corrupt,

  the sharing phase succeeds

  $\Downarrow$

  any set of r honest players reconstruct the same secret

For any $\{i_1, \ldots, i_r\} \neq \{j_1, \ldots, j_r\}$, if

$$\left.\begin{matrix} P_{i_1} \\ P_{i_2} \\ \vdots \\ P_{i_r} \end{matrix}\right\} \longrightarrow \mathbf{s} \in \mathbb{F}^{\ell} \qquad \text{and} \qquad \left.\begin{matrix} P_{j_1} \\ P_{j_2} \\ \vdots \\ P_{j_r} \end{matrix}\right\} \longrightarrow \mathbf{s}' \in \mathbb{F}^{\ell}$$

$$\Longrightarrow \mathbf{s} = \mathbf{s}'$$

A general construction from LSSS to VSSS:

(t, r)-LSSS for secret $\mathbf{s} \in \mathbb{F}^{\ell}$ $\Rightarrow$ (t, r)-VSSS for secrets $\{\mathbf{s}_1, \ldots, \mathbf{s}_{\ell}\} \subseteq \mathbb{F}^{\ell}$

A general construction from LSSS to VSSS:

(t, r)-LSSS for secret $\mathbf{s} \in \mathbb{F}^\ell$ $\Rightarrow$ (t, r)-VSSS for secrets $\{\mathbf{s}_1, \ldots, \mathbf{s}_\ell\} \subseteq \mathbb{F}^\ell$

Notation for (t, r)-LSSS for secret $\mathbf{s} \in \mathbb{F}^\ell$:

- $d = \ell + e$ (for some integer $e > 0$);
- $M \in \mathbb{F}^{n \times d}$
- $$\begin{aligned} \pi_\ell : \mathbb{F}^d &\longrightarrow \mathbb{F}^\ell \\ \mathbf{v} &\longmapsto (\mathbf{v}[1], \ldots, \mathbf{v}[\ell])^\top \end{aligned}$$

$$\text{secret } \mathbf{s} \in \mathbb{F}^\ell \rightsquigarrow \begin{array}{c} D \text{ chooses} \\ \mathbf{f} \in \mathbb{F}^d \text{ random} \\ \text{s.t. } \pi_\ell(\mathbf{f}) = \mathbf{s} \end{array} \rightsquigarrow \begin{array}{c} \text{shares:} \\ c_i = \mathbf{m}_i \cdot \mathbf{f} \\ i = 1, \ldots, n \end{array}$$

where $\mathbf{m}_i$ is the ith row of M.

The complexity

(t, r)-LSSS for secret $\mathbf{s} \in \mathbb{F}^\ell$ $\Rightarrow$ (t, r)-VSSS for secrets $\{\mathbf{s}_1, \ldots, \mathbf{s}_\ell\} \subseteq \mathbb{F}^\ell$

Assuming $\mathbb{F} = \{0, 1\}$ and $\ell = \Theta(n)$,

	secret bits shared	communication complexity
LSSS	ℓ	$\Theta(n)$
VSSS	ℓ^2	$\Theta(n^2)$

t-privacy in the LSSS $\Rightarrow$ t-privacy in the VSSS

Proposition:

If the dealer is honest, then for any set $C \subseteq \{1, \ldots, n\}$ such that $|C| \leq t$, the views

$$\left\{\mathbf{g}_i, \mathbf{h}^i\right\}_{i \in C}$$

give no info about the secrets held by the dealer.

$$\left.\begin{array}{ll} \text{view} & \mathbf{g}_{i_1}, \mathbf{h}^{i_1} \\ \text{view} & \mathbf{g}_{i_2}, \mathbf{h}^{i_2} \\ & \vdots \\ \text{view} & \mathbf{g}_{i_t}, \mathbf{h}^{i_t} \end{array}\right\} \longrightarrow \mathbf{?}$$

t-privacy in the LSSS $\Rightarrow$ t-privacy in the VSSS

Proposition:

If the dealer is honest, then for any set $C \subseteq \{1, \ldots, n\}$ such that $|C| \leq t$, the views

$$\left\{\mathbf{g}_i, \mathbf{h}^i\right\}_{i \in C}$$

give no info about the secrets held by the dealer.

If the dealer is honest, then for any set $C \subseteq \{1, \ldots, n\}$ such that $|C| \leq t$ and for any $\lambda_1, \ldots, \lambda_\ell$ in $\mathbb{F}$, the views

$$\left\{\mathbf{g}_i, \mathbf{h}^i, \sum_{k=1}^{\ell} \lambda_k \mathbf{s}^k\right\}_{i \in C}$$

give no extra info about the secrets held by the dealer.

r-robust reconstruction

$$\left.\begin{array}{c} r\text{-reconstruction in the LSSS} \\ + \\ \text{checks } \mathbf{m}_j \cdot \mathbf{h}^i = \mathbf{g}^j \cdot \mathbf{m}_i^\top \end{array}\right\} \Rightarrow r\text{-robust reconstruction in the VSSS}$$

r-robust reconstruction

$$\left.\begin{array}{c} r\text{-reconstruction in the LSSS} \\ + \\ \text{checks } \mathbf{m}_j \cdot \mathbf{h}^i = \mathbf{g}^j \cdot \mathbf{m}_i^\top \end{array}\right\} \Rightarrow r\text{-robust reconstruction in the VSSS}$$

Proposition

Assume that no player rejects. Then, even if the dealer is corrupt, any set of at least r honest players reconstruct the same secrets.

For any $\{i_1, \ldots, i_r\} \neq \{j_1, \ldots, j_r\}$, if

$$\left.\begin{array}{l} \text{view } \mathbf{g}_{i_1}, \mathbf{h}^{i_1} \\ \text{view } \mathbf{g}_{i_2}, \mathbf{h}^{i_2} \\ \vdots \\ \text{view } \mathbf{g}_{i_r}, \mathbf{h}^{i_r} \end{array}\right\} \rightarrow \{\mathbf{s}_1, \ldots, \mathbf{s}_\ell\} \subseteq \mathbb{F}^\ell \qquad \left.\begin{array}{l} \text{view } \mathbf{g}_{j_1}, \mathbf{h}^{j_1} \\ \text{view } \mathbf{g}_{j_2}, \mathbf{h}^{j_2} \\ \vdots \\ \text{view } \mathbf{g}_{j_r}, \mathbf{h}^{j_r} \end{array}\right\} \rightarrow \{\mathbf{s}'_1, \ldots, \mathbf{s}'_\ell\} \subseteq \mathbb{F}^\ell$$

$$\Longrightarrow \{\mathbf{s}_1, \ldots, \mathbf{s}_\ell\} = \{\mathbf{s}'_1, \ldots, \mathbf{s}'_\ell\}$$

Extensions:

- checking a public linear relation between the secrets
- generate shares of $\mathbf{0} \in \mathbb{F}^{\ell}$

Applications:

- MPC protocols
- Commitment Schemes
- ...

In these cases, we need to base the construction on a LSSS with t-strong multiplication such that

$n \to +\infty$

$|\mathbb{F}|$ constant

$t, \ell = \Theta(n)$

(e.g. AG Secret-Sharing Schemes!)