Finally!

A Compact Lattice-Based Threshold Signature

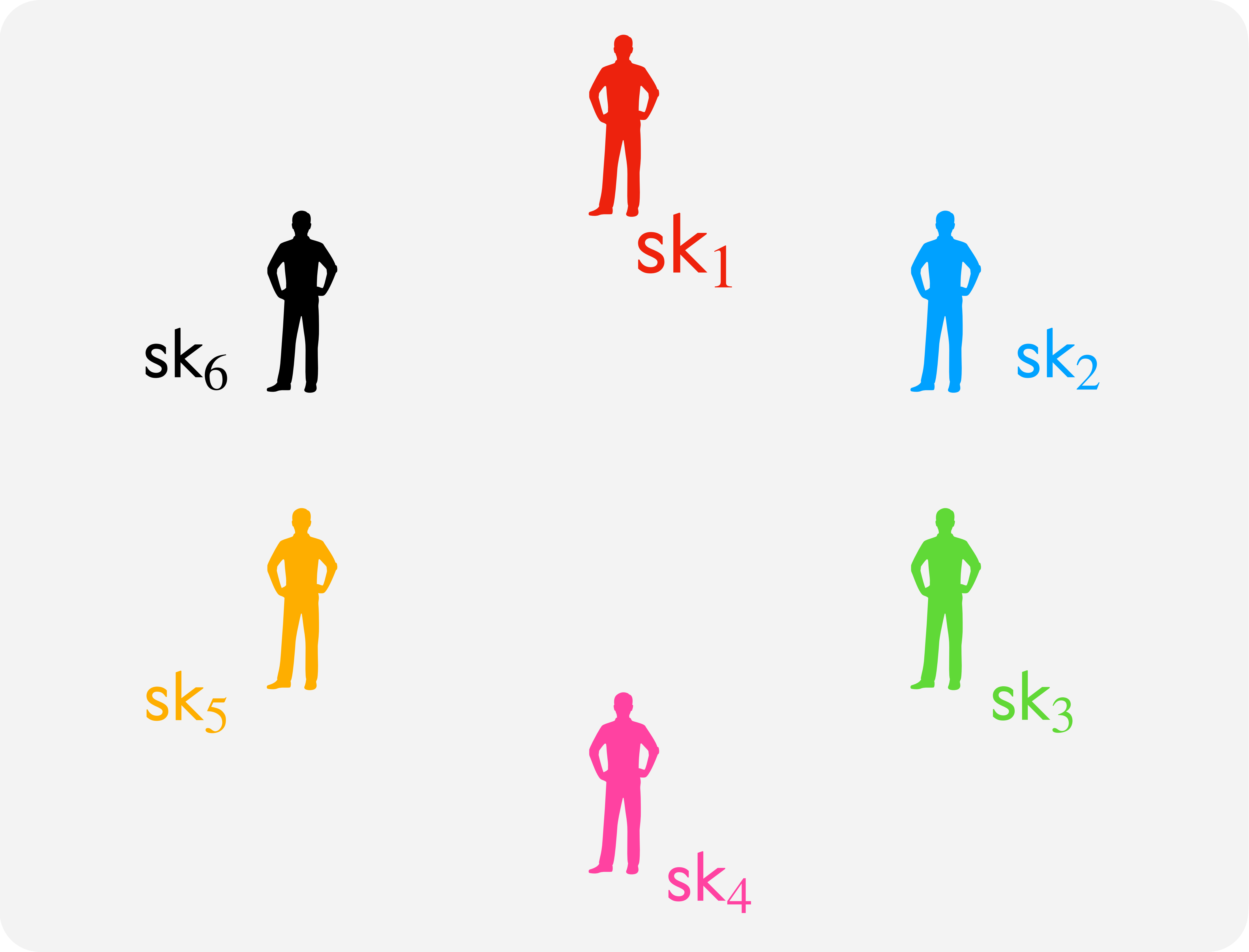
Rafael del Pino, joint work with *Guilhem Niot*

PKC 2025

1. Background

(T-out-of-N) threshold signatures
What are they?

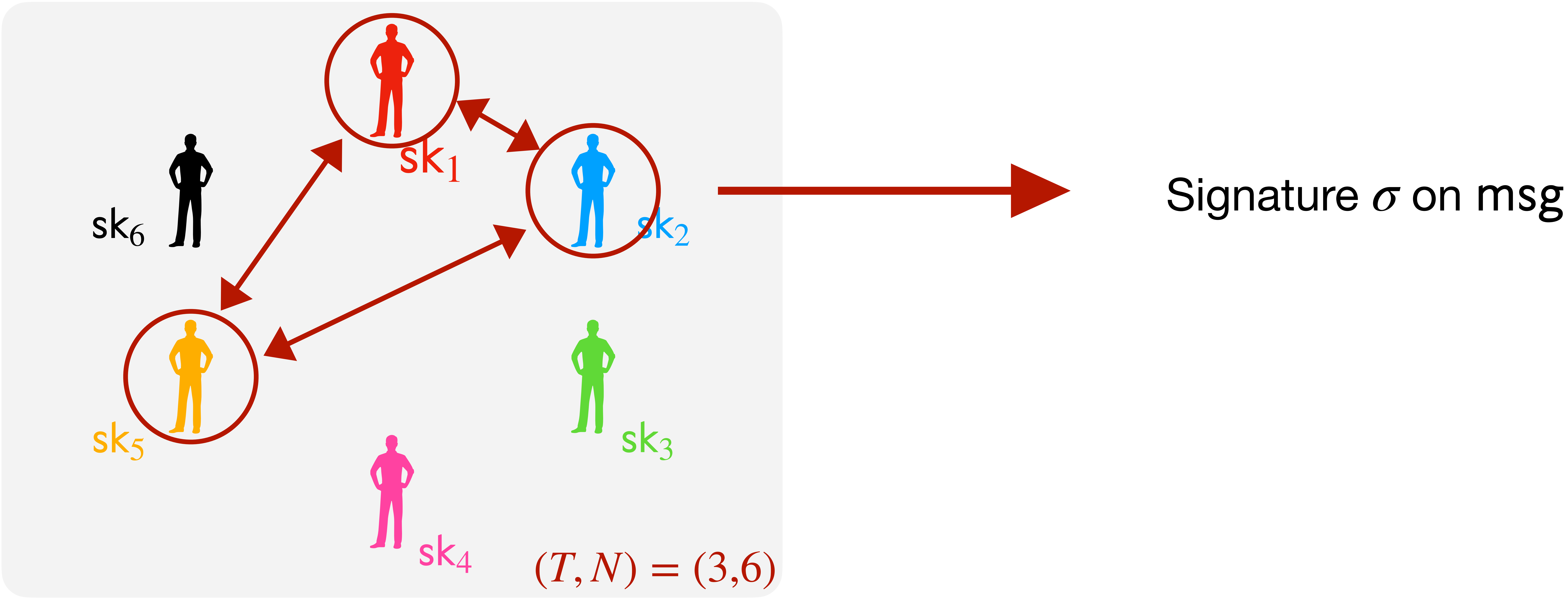
An interactive protocol to distribute signature generation.



- Global verification key vk
- 1 partial signing key sk_i per party
- T-out-of-N:
  - Any T out of N parties can collaborate to sign a message under vk.
  - $T-1$ parties cannot sign.

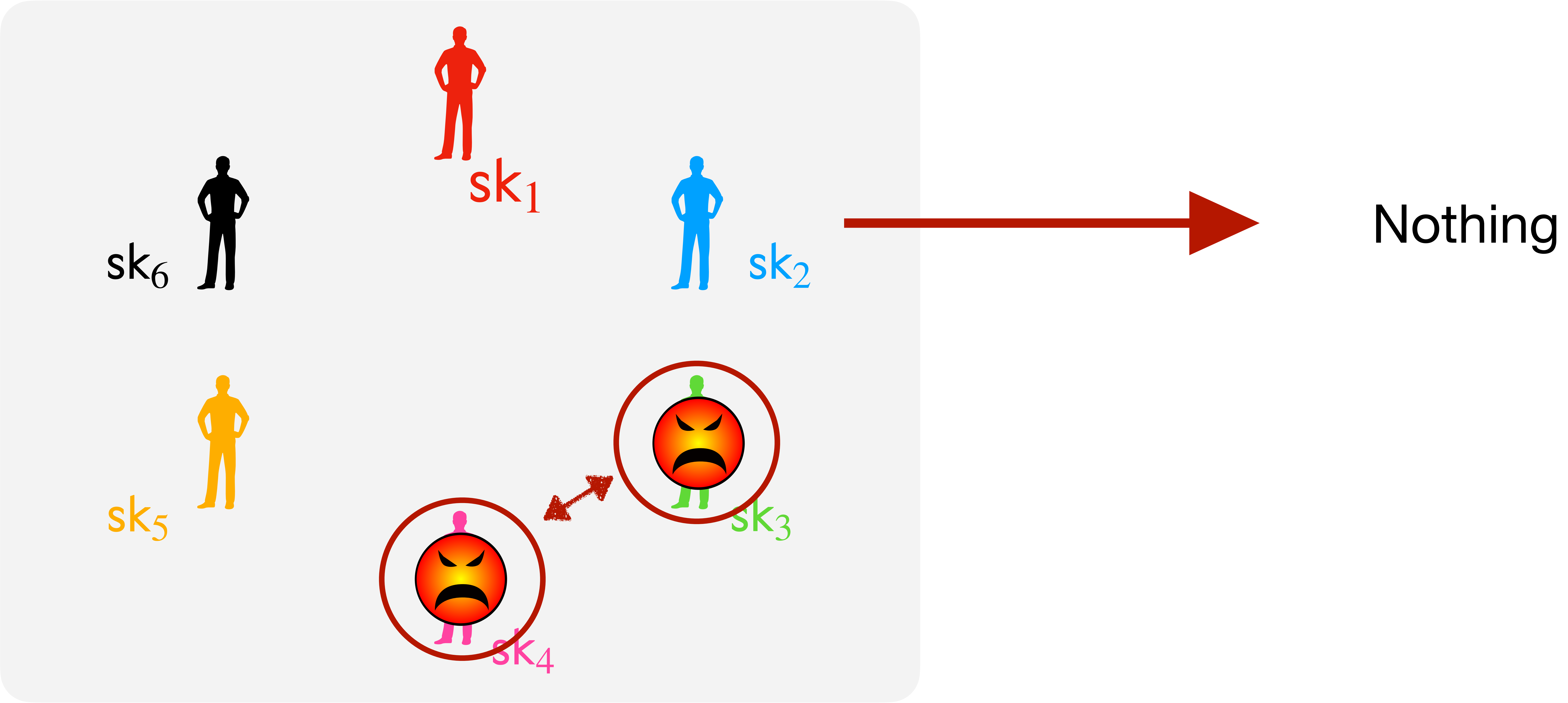
(T-out-of-N) threshold signatures
What are they?

An interactive protocol to distribute signature generation.



(T-out-of-N) threshold signatures
What are they?

An interactive protocol to distribute signature generation.



Lattice-based Threshold Signatures

An active field of research.

Threshold Raccoon: Practical Threshold Signatures from Standard Lattice Assumptions

Rafael del Pino[1], Shuichi Katsumata[1,2], Mary Maller[1,3], Fabrice Mouhartem[4], Thomas Prest[1], Markku-Juhani Saarinen[1,5]

Two-Round Threshold Signature from Algebraic One-More Learning with Errors

Thomas Espitau[1], Shuichi Katsumata[1,2], Kaoru Takemure* [1,2]

Ringtail: **Practical Two-Round Threshold Signatures from Learning with Errors**

Cecilia Boschini, *ETH Zürich, Switzerland*
Darya Kaviani, *UC Berkeley, USA*
Russell W. F. Lai, *Aalto University, Finland*
Giulio Malavolta, *Bocconi University, Italy*
Akira Takahashi, *JPMorgan AI Research & AlgoCRYPT CoE, USA*
Mehdi Tibouchi, *NTT Social Informatics Laboratories, Japan*

***Flood and Submerse*: Distributed Key Generation and Robust Threshold Signature from Lattices**

Thomas Espitau[1], Guilhem Niot[1,2], and Thomas Prest[1]

Two-round n-out-of-n and Multi-Signatures and Trapdoor Commitment from Lattices⋆

Ivan Damgård[1], Claudio Orlandi[1], Akira Takahashi[1], and Mehdi Tibouchi[2]

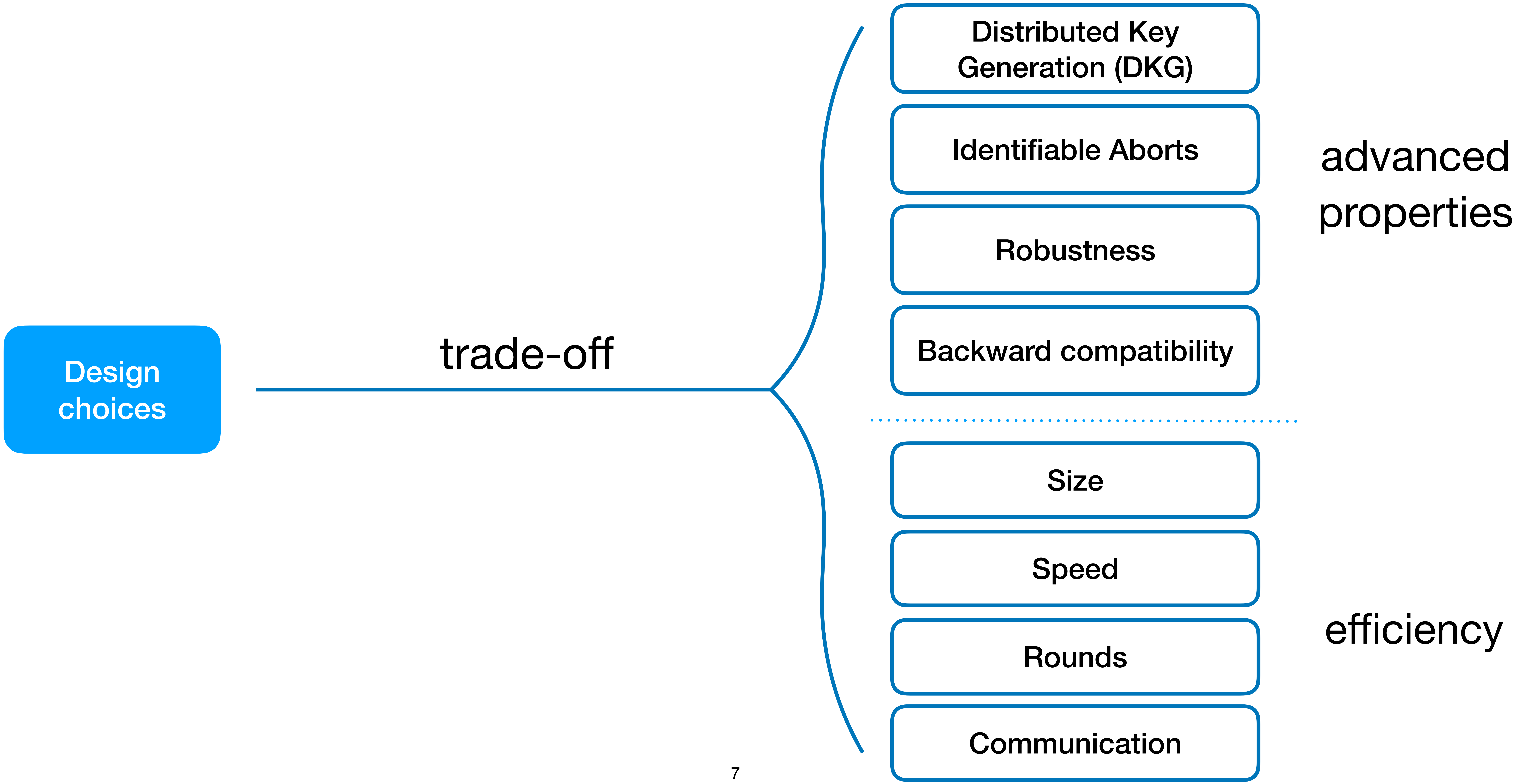
MuSig-L: Lattice-Based Multi-Signature With Single-Round Online Phase⋆

Cecilia Boschini[1], Akira Takahashi[2], and Mehdi Tibouchi[3]

Two-Round Threshold Lattice-Based Signatures from Threshold Homomorphic Encryption⋆

Kamil Doruk Gur[1], Jonathan Katz[2⋆⋆], and Tjerand Silde[3⋆⋆⋆]

Designing a threshold scheme



Designing a threshold scheme

Lattice-based Threshold Signatures

Candidate schemes

	Hash & Sign	Fiat-Shamir
Gaussian Sampling	Eagle [YJW23]	G+G [DPS23]
Rejection Sampling	Phoenix [JRS24]	Dilithium [LDK+22]
Noise Flooding	Plover [EEN+24]	Raccoon [dEK+24]

Easier to thresholdize

More compact

This talk: Dilithium threshold variant.

Lattice-based Threshold Signatures

An active field of research, with different designs.

Thresholdization technique	Size	Speed	Rounds	Comm/party
MPC	S	Slow	15	≥ 1MB
FHE	M	As fast as FHE	2	≥ 1MB
Tailored	S-M	Fast	2-4	20 kB $\rightarrow 56T$ kB

This talk: Tailored

Dilithium-like

Two-round n-out-of-n and Multi-Si
Trapdoor Commitment from Lattices*

Ivan Damgård[1], Claudio Orlandi[1], Akira Takahashi[1], and Mehdi Tibouchi[2]

$\rightarrow$ more compact and T-out-of-N?

2. Compact Dilithium-like Threshold Signatures

Finally! A Compact Lattice-Based Threshold Signature

Rafael del Pino[1] and Guilhem Niot[1,2]

Designing a threshold scheme

Fiat-Shamir with Aborts signature

$\mathsf{FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Fiat-Shamir with Aborts signature

$\mathsf{FSwA}\,.\,\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

$\mathsf{Rej}(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \rightarrow \mathbf{z} \mid \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

In the ROM, the distribution of signatures of the above scheme is independent of the secret sk.

$\rightarrow$ allows to prove unforgeability

Fiat-Shamir with Aborts signature

$\mathsf{Rej}(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \,|\, \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\dfrac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

$\mathsf{FSwA}.\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

$\mathsf{FSwA}.\mathsf{Verify}(\mathsf{vk}, \mathsf{msg}, \mathsf{sig} = (c, \mathbf{z}))$

- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{z} - c \cdot \mathsf{vk}$
- Assert $c = H(\mathbf{w}, \mathsf{msg})$
- Assert $\mathbf{z}$ short

In the ROM, the distribution of signatures of the above scheme is independent of the secret sk.

$\to$ allows to prove unforgeability

Fiat-Shamir with Aborts signature

Rej$(\mathbf{v}, \chi_r, \chi_z, M) \to \mathbf{z} \mid \perp$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\dfrac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

Ideal$(\chi_z, M) \to \mathbf{z} \mid \perp$

- $\mathbf{z} \leftarrow \chi_{\mathbf{z}}$
- $b \leftarrow \mathscr{B}\left(\dfrac{1}{M}\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

For proper parameters, Rej$(\mathbf{v}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M) \sim$ Ideal$(\chi_{\mathbf{z}}, M)$.

$\rightarrow$ distribution of $\mathbf{z}$ is independent of the secret value $\mathbf{v}$

Threshold FSwA signature? N-out-of-N

$\mathsf{FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Threshold FSwA signature? N-out-of-N

$\mathsf{FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Intuition N-out-of-N setting: $\mathsf{sk} = \sum_i \mathsf{sk}_i$

$\mathsf{TH\text{-}FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

Round 1:

- Sample a short $\mathbf{r}_i$
- $\mathbf{w}_i = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}_i$
- Broadcast $\mathsf{cmt}_i = H_{\mathsf{cmt}}(\mathbf{w}_i)$

Threshold FSwA signature? N-out-of-N

$\mathsf{FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Intuition N-out-of-N setting: $\mathsf{sk} = \sum_i \mathsf{sk}_i$

$\mathsf{TH\text{-}FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

Round 1:

- Sample a short $\mathbf{r}_i$
- $\mathbf{w}_i = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}_i$
- Broadcast $\mathsf{cmt}_i = H_{\mathsf{cmt}}(\mathbf{w}_i)$

Round 2:

- Broadcast $\mathbf{w}_i$

Threshold FSwA signature? N-out-of-N

$\mathsf{FSwA}.\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Intuition N-out-of-N setting: $\mathsf{sk} = \sum_i \mathsf{sk}_i$

$\mathsf{TH\text{-}FSwA}.\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \rightarrow \mathsf{sig}$

Round 1:

- Sample a short $\mathbf{r}_i$
- $\mathbf{w}_i = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}_i$
- Broadcast $\mathsf{cmt}_i = H_{\mathsf{cmt}}(\mathbf{w}_i)$

Round 2:

- Broadcast $\mathbf{w}_i$

Round 3:

- $\mathbf{w} = \sum_i \mathbf{w}_i$
- $c = H(\mathbf{w}, \mathsf{msg})$
- Broadcast $\mathbf{z}_i = \mathsf{Rej}(c \cdot \mathsf{sk}_i, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r}_i)$

Combine: the final signature is

$$(c, \textstyle\sum_{i \in S} \mathbf{z}_i)$$

Threshold FSwA signature? N-out-of-N

$\mathsf{FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

Intuition N-out-of-N setting: $\mathsf{sk} = \sum_i \mathsf{sk}_i$

We need sk_i small for rejection sampling!

We have to reveal $\mathbf{w}_i$ even when we reject!

$\mathsf{TH\text{-}FSwA.Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

Round 1:

- Sample a short $\mathbf{r}_i$
- $\mathbf{w}_i = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}_i$
- Broadcast $\mathsf{cmt}_i = H_{\mathsf{cmt}}(\mathbf{w}_i)$

Round 2:

- Broadcast $\mathbf{w}_i$

Round 3:

- $\mathbf{w} = \sum_i \mathbf{w}_i$
- $c = H(\mathbf{w}, \mathsf{msg})$
- Broadcast $\mathbf{z}_i = \mathsf{Rej}(c \cdot \mathsf{sk}_i, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r}_i)$

Combine: the final signature is

$$(c, \textstyle\sum_{i \in S} \mathbf{z}_i)$$

Revealing w_i in case of rejection

Previous solutions

- DualMS [Chen24]: Hide w_i by adding an extra noise $[\ B\ I\ ].r'$
  - Essentially doubles signature size
- [DFPSX23]: Directly prove that w_i does not leak information
  - Requires very high entropy or reduces to "weak" problem

Revealing w_i in case of rejection

Our Solution:

- For a fixed v,
  [A I].z is indistinguishable from uniform
  = [A I].r is indistinguishable from uniform

Rej$(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \mid \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

Revealing w_i in case of rejection

Our Solution:

Suppose:

- For rejected samples : I can distinguish A.z from uniform

Rej$(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \mid \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

Revealing w_i in case of rejection

Rej$(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \mid \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

Our Solution:

Suppose:

- For rejected samples : I can distinguish A.z from uniform
- For accepted samples: I cannot distinguish A.z from uniform

Revealing w_i in case of rejection

Rej$(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \rightarrow \mathbf{z} | \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$
- Return $\mathbf{z}$

Our Solution:

Suppose:

- For rejected samples : I can distinguish A.z from uniform
- For accepted samples: I cannot distinguish A.z from uniform
- Then I can distinguish A.z from uniform ! (if rejection probability is non negligible)

Revealing w_i in case of rejection

Rej$(\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \,|\, \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_{\mathbf{z}}(\mathbf{z})}{M\chi_{\mathbf{r}}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$

Lemma: Rejected w_i is indistinguishable from uniform if:

- [A I].r is indistinguishable from uniform.
- [A I].z is indistinguishable from uniform.

Revealing w_i in case of rejection

Rej($\mathbf{v}, \chi_r, \chi_z, M; \mathbf{r}) \to \mathbf{z} \mid \perp$

- $\mathbf{z} = \mathbf{v} + \mathbf{r}$
- $b \leftarrow \mathscr{B}\left(\max\left(\frac{\chi_\mathbf{z}(\mathbf{z})}{M\chi_\mathbf{r}(\mathbf{r})}, 1\right)\right)$
- If $b = 0$ then $\mathbf{z} = \perp$

Lemma: Rejected w_i is indistinguishable from uniform if:

- [A I].r is indistinguishable from uniform. **LWE**
- [A I].z is indistinguishable from uniform. **LWE**

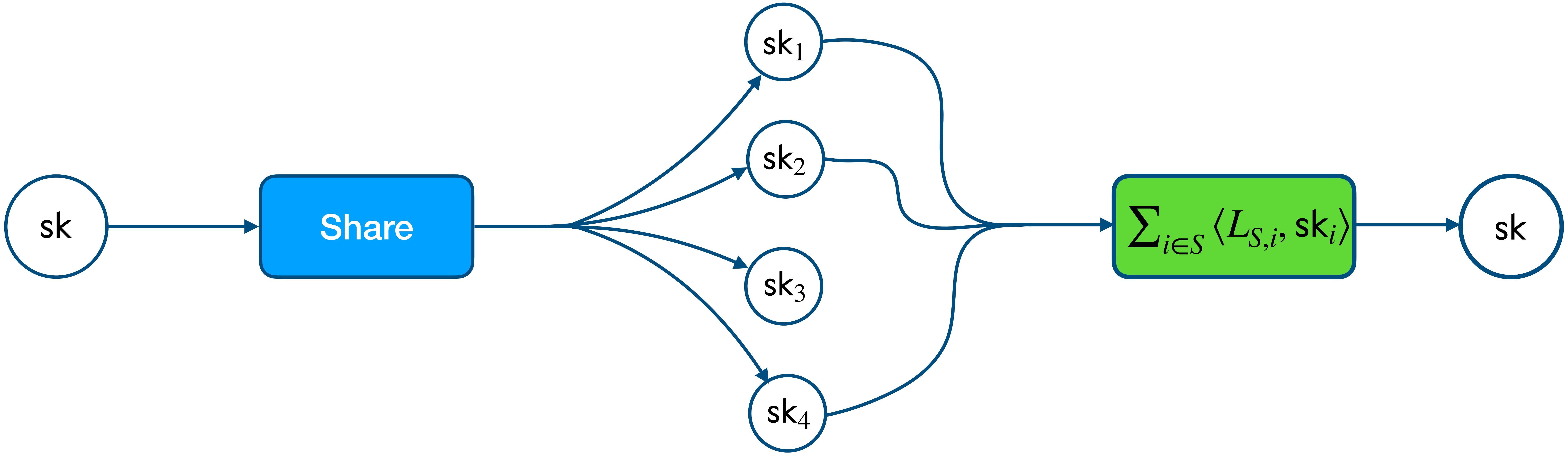
3. T-out-of-N short secret sharing

How to Shortly Share a Short Vector

DKG with Short Shares and Application to Lattice-Based Threshold Signatures with Identifiable Aborts

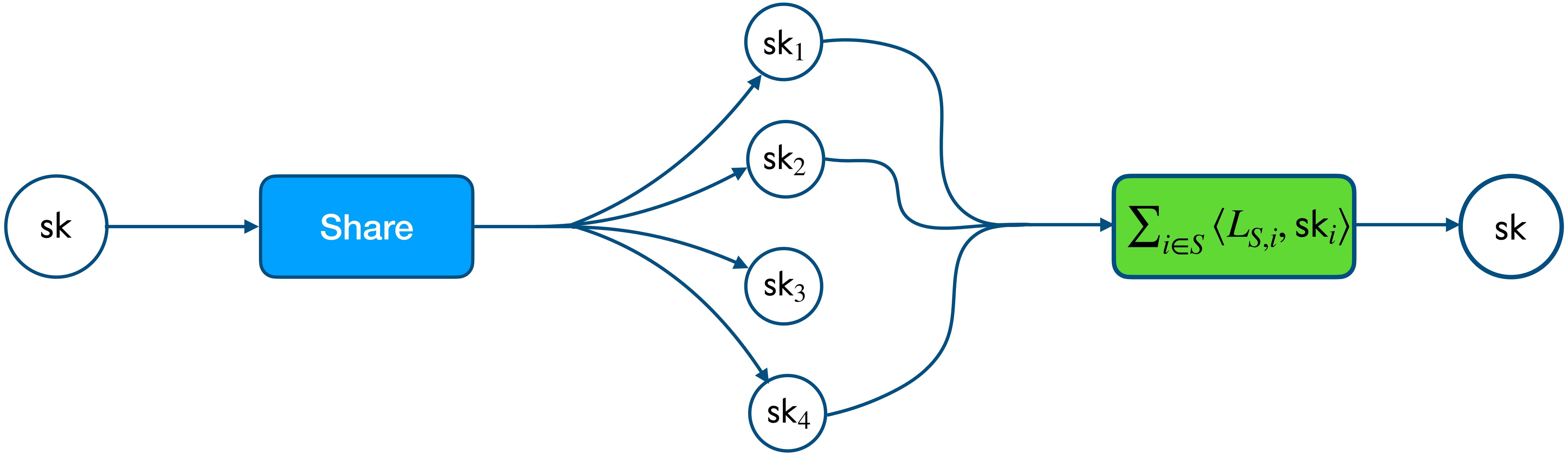
Rafael del Pino[1], Thomas Espitau[1], Guilhem Niot[1,2], and Thomas Prest[1]

Short secret sharing for T<N



- Individual pool of short shares $\mathsf{sk}_i = (\mathbf{s}_i^{(1)}, \mathbf{s}_i^{(2)}, \ldots)$
- T shares: can recover sk
  - Reconstruction vector $L_{S,i}$ with small coefficients
- $\leq T-1$ shares: can't recover sk

Short secret sharing for T<N



- Individual pool of short shares $\mathsf{sk}_i = (\mathbf{s}_i^{(1)}, \mathbf{s}_i^{(2)}, \ldots)$
- T shares: can recover sk
  - Reconstruction vector $L_{S,i}$ with small coefficients
- $\leq T - 1$ shares: can't recover sk

Example: N-out-of-N sharing (one share per party)

- $\mathsf{sk}_1, \ldots, \mathsf{sk}_N \leftarrow \mathscr{D}_\sigma^N$ and $\mathsf{sk} = \sum_i \mathsf{sk}_i$
- $L_{S,i} = 1$

Extends to T-out-of-N by having several shares per party.

Threshold FSwA signature?

$\mathsf{FSwA}.\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

- $\mathbf{r} \leftarrow \chi_{\mathbf{r}}$
- $\mathbf{w} = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}$
- $c = H(\mathbf{w}, \mathsf{msg})$
- $\mathbf{z} = \mathsf{Rej}(c \cdot \mathsf{sk}, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r})$
- If $\mathbf{z} = \perp$ then **restart**
- Return $(c, \mathbf{z})$

- How to support T-out-of-N?

  $\rightarrow$ Use short secret sharing

$\mathsf{TH\text{-}FSwA}.\mathsf{Sign}(\mathsf{sk}, \mathsf{msg}) \to \mathsf{sig}$

Round 1:

- Sample a short $\mathbf{r}_i$
- $\mathbf{w}_i = [\mathbf{A} \quad \mathbf{I}] \cdot \mathbf{r}_i$
- Broadcast $\mathsf{cmt}_i = H_{\mathsf{cmt}}(\mathbf{w}_i)$

Round 2:

- Broadcast $\mathbf{w}_i$

Round 3:

- $\mathbf{w} = \sum_i \mathbf{w}_i$
- $c = H(\mathbf{w}, \mathsf{msg})$
- Broadcast $\mathbf{z}_i = \mathsf{Rej}(c \cdot \langle L_{S,i}, \mathsf{sk}_i \rangle, \chi_{\mathbf{r}}, \chi_{\mathbf{z}}, M; \mathbf{r}_i)$

Combine: the final signature is

$$(c, \textstyle\sum_{i \in S} \mathbf{z}_i)$$

Solution: Replicated Secret Sharing

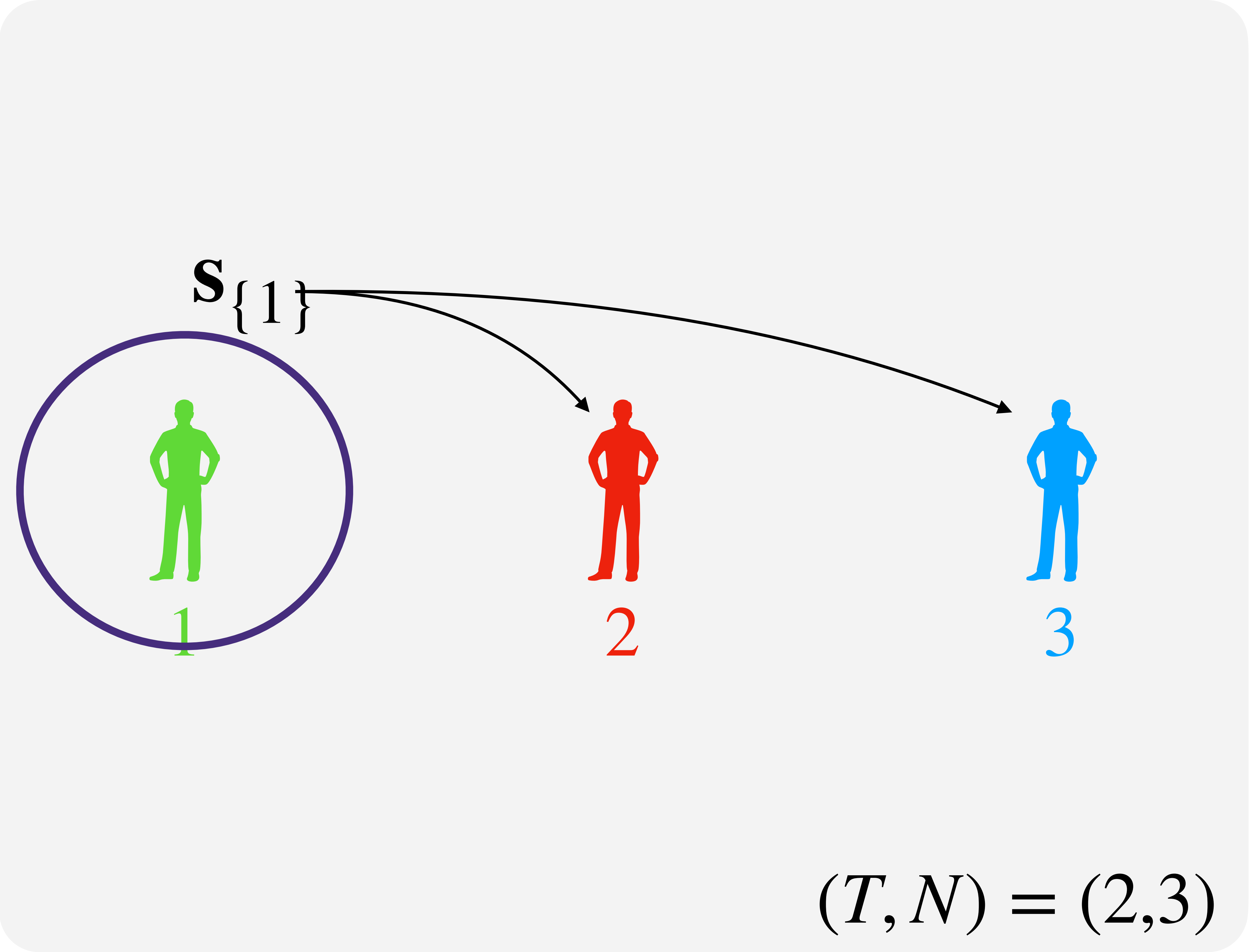
Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

Solution: Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathcal{T}$ of $T - 1$ parties, sample a uniform share $\mathbf{s}_{\mathcal{T}}$.

2. Distribute $\mathbf{s}_{\mathcal{T}}$ to the parties in $[N] \backslash \mathcal{T}$.

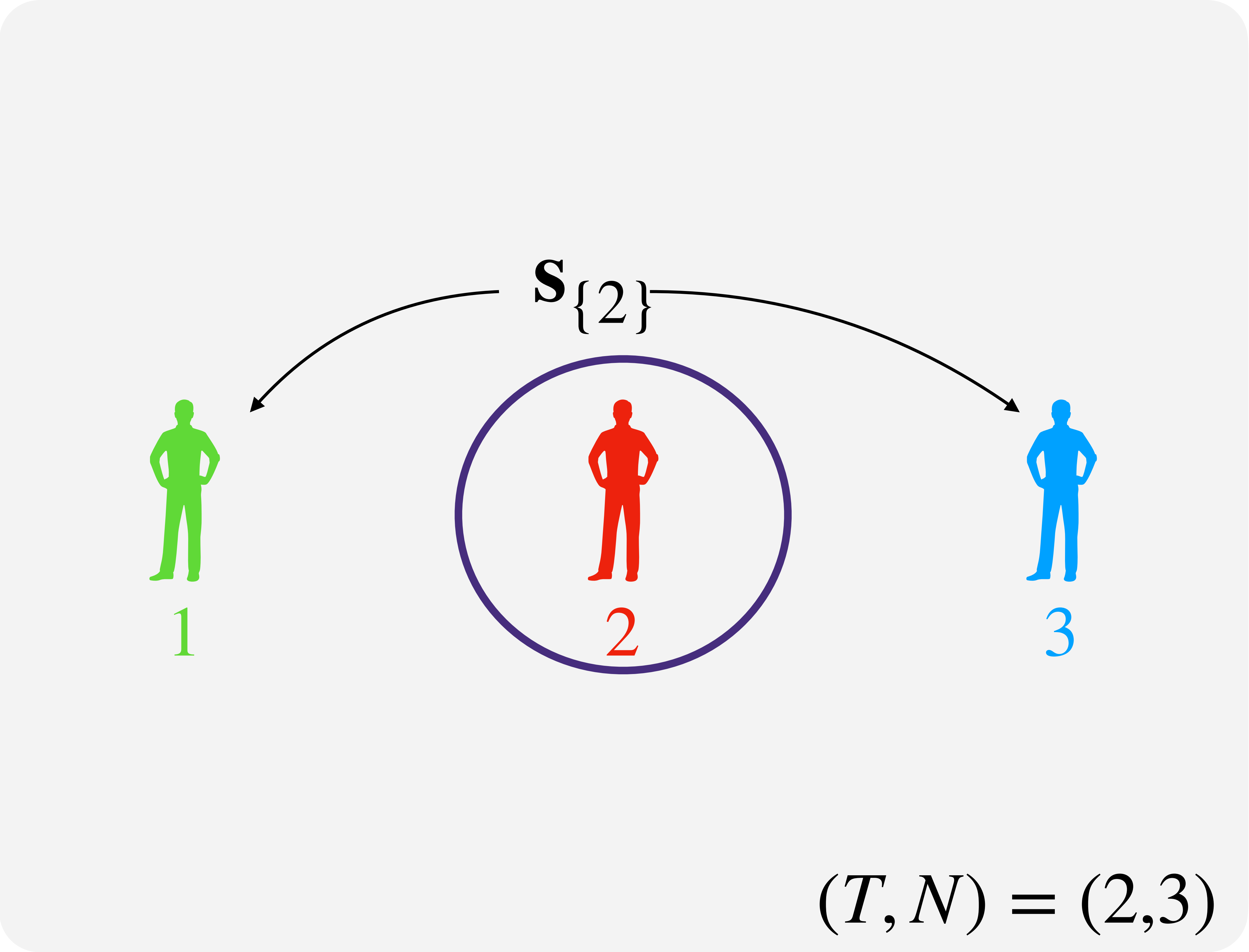


Solution: Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathcal{T}$ of $T-1$ parties, sample a uniform share $\mathbf{s}_{\mathcal{T}}$.

2. Distribute $\mathbf{s}_{\mathcal{T}}$ to the parties in $[N]\backslash\mathcal{T}$.

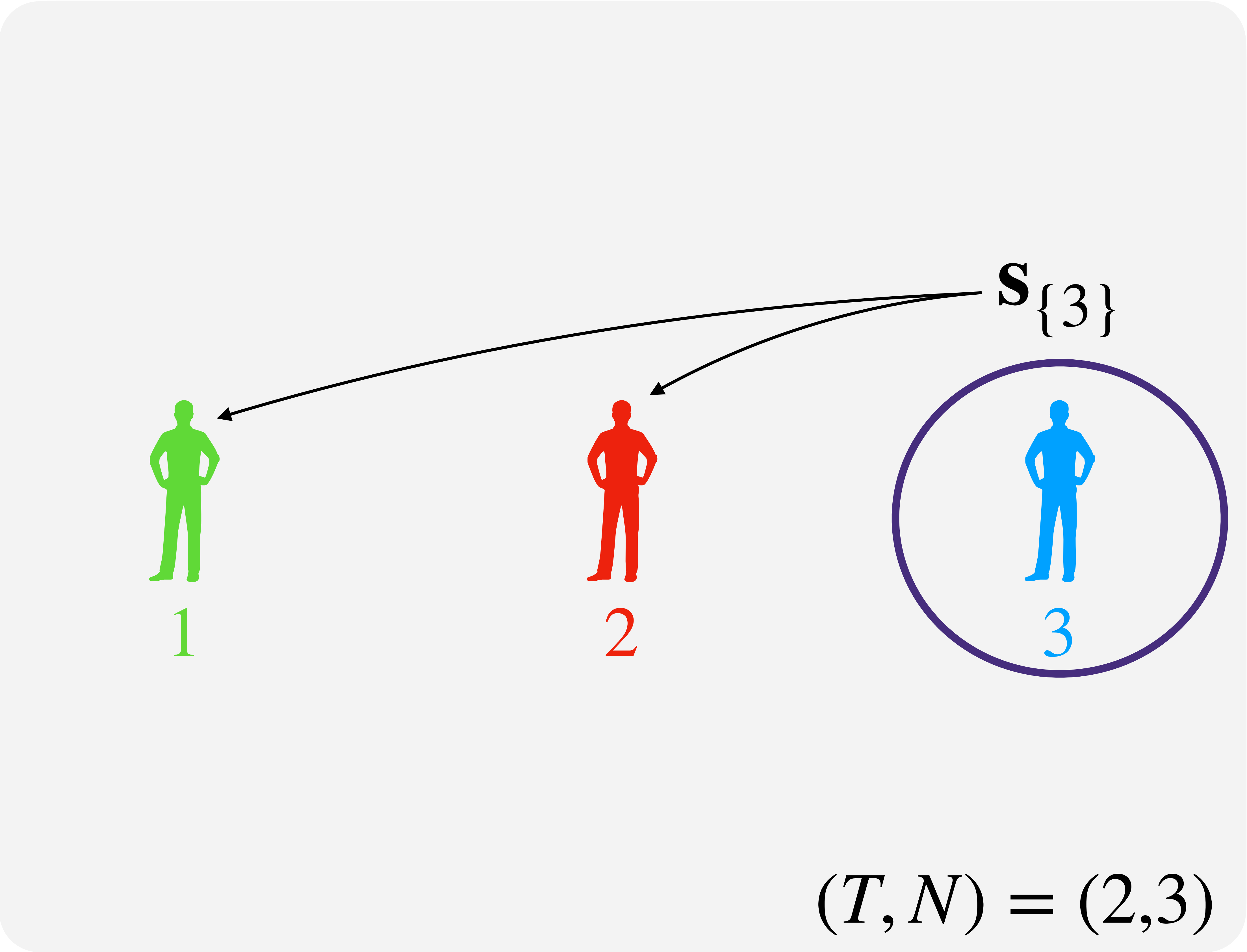


Solution: Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathcal{T}$ of $T-1$ parties, sample a uniform share $\mathbf{s}_{\mathcal{T}}$.

2. Distribute $\mathbf{s}_{\mathcal{T}}$ to the parties in $[N] \backslash \mathcal{T}$.



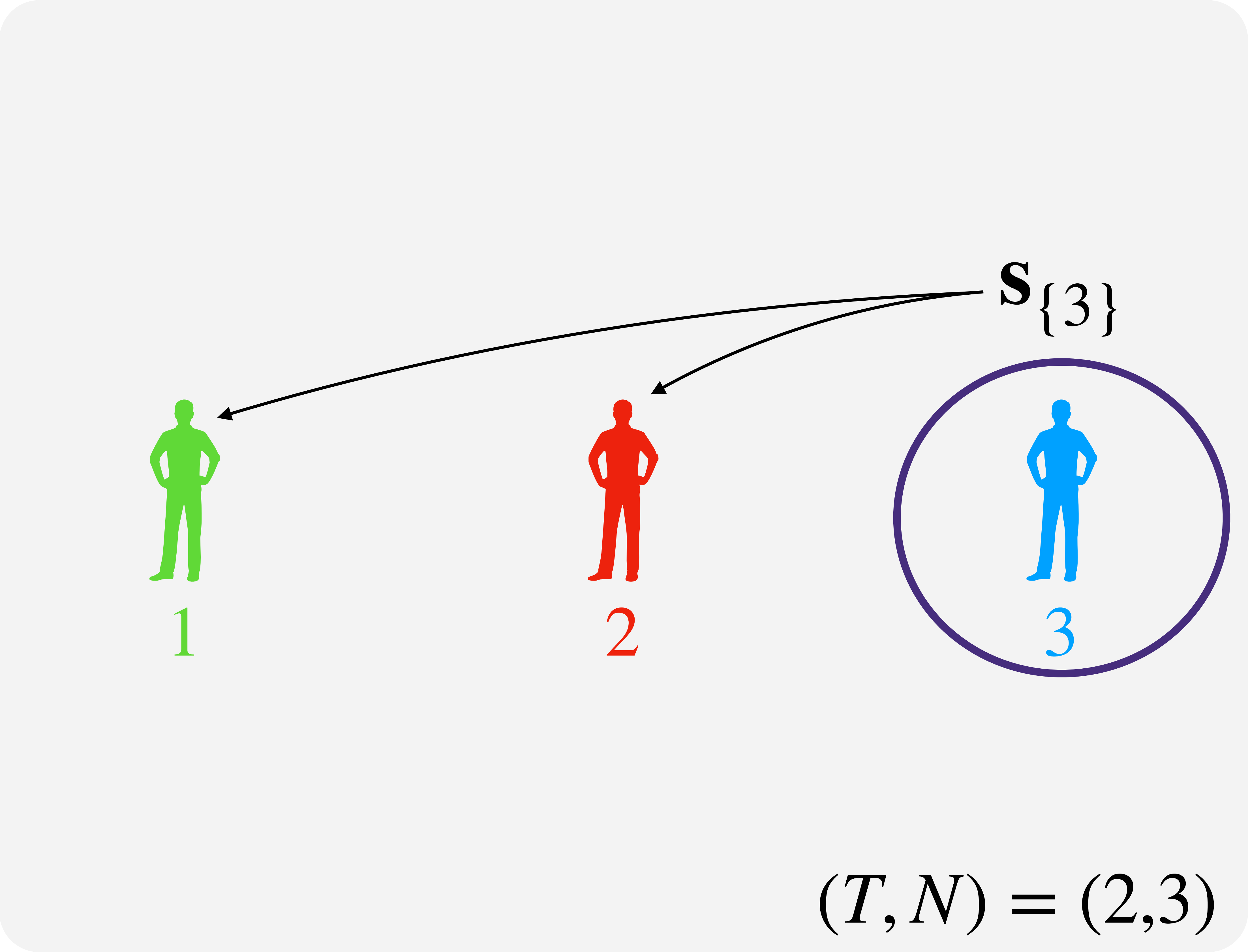
Solution: Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathscr{T}$ of $T-1$ parties, sample a uniform share $\mathbf{s}_{\mathscr{T}}$.

2. Distribute $\mathbf{s}_{\mathscr{T}}$ to the parties in $[N]\backslash\mathscr{T}$.

3. Define sk $= \sum_{\mathscr{T}} \mathbf{s}_{\mathscr{T}}$.



Solution: Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathcal{T}$ of $T-1$ parties, sample a uniform share $\mathbf{s}_{\mathcal{T}}$.
2. Distribute $\mathbf{s}_{\mathcal{T}}$ to the parties in $[N] \backslash \mathcal{T}$.
3. Define $\mathsf{sk} = \sum_{\mathcal{T}} \mathbf{s}_{\mathcal{T}}$.

Properties:

- Reconstruction coefficients 0 or 1
- When $< T$ corrupted parties, at least one $\mathbf{s}_{\mathcal{T}}$ remains hidden.

→ guarantees that sk remains protected

Solution: Short Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathcal{T}$ of $T-1$ parties, sample a short share $\mathbf{s}_{\mathcal{T}}$.
2. Distribute $\mathbf{s}_{\mathcal{T}}$ to the parties in $[N]\backslash\mathcal{T}$.
3. Define sk $= \sum_{\mathcal{T}} \mathbf{s}_{\mathcal{T}}$.

Properties:

- Reconstruction coefficients 0 or 1
- When $< T$ corrupted parties, at least one $\mathbf{s}_{\mathcal{T}}$ remains hidden.

  → guarantees that [A I].sk looks uniform (MLWE assumption)

Solution: Short Replicated Secret Sharing

Idea: sample a share for all maximal sets that should not be able to sign, and give it to everyone else.

1. For any set $\mathscr{T}$
   sample a short

2. Distribute $\mathbf{s}_{\mathscr{T}}$ t
   $[N] \backslash \mathscr{T}$.

3. Define sk $= \sum_{\mathscr{T}} \mathbf{s}_{\mathscr{T}}$.

Caveat: This scheme has a number of shares that is equal to $\binom{N}{T-1}$.

efficients 0 or 1

pted parties, at least one $\mathbf{s}_{\mathscr{T}}$ remains hidden.

→ guarantees that [A I].sk looks uniform (MLWE assumption)

Threshold FSwA signature

For $N \leq 8$,

<table>
<tr><th>Distributions</th><th>Speed</th><th>Rounds</th><th>| vk |</th><th>| sig |</th><th>Total communication</th></tr>
<tr><td>Gaussians</td><td rowspan="2">Fast</td><td rowspan="2">3</td><td>2.6 kB</td><td>2.7 kB</td><td>5.6 kB</td></tr>
<tr><td>Uniforms</td><td>3.1 kB</td><td>4.8 kB</td><td>13.5 kB</td></tr>
</table>

Comparable to Dilithium size: 2.4kB at NIST level II!

Conclusion

Conclusion

- **Introduced Finally, a 3-round compact lattice-based threshold signature**
  - Up to 8 parties
  - Signature size 2.7kB (comparable to Dilithium, 2.4kB)
- **Future work?**
  - 2-round?
  - Tackle malicious behavior? Adaptive security?

Questions?