Secret Sharings for Lattice-Based Threshold Signatures

Thomas Prest (joint work w/ PQShield & friends)

PQSHIELD

April 25, 2025

Lattice Signatures

PQ SHIELD

Easier to thresholdize ↓

	Hash-&-Sign	Fiat-Shamir
Convolution	Eagle [YJW23]	G+G [DPS23]
Rejection sampling	Phoenix [JRS24]	Dilithium [LDK+22]
Noise flooding	Plover [EEN+24]	Raccoon [dEK+23]

↑ More compact

Easier to thresholdize ↓

	Hash-&-Sign	Fiat-Shamir
Convolution	Eagle [YJW23]	G+G [DPS23]
Rejection sampling	Phoenix [JRS24]	Dilithium [LDK+22]
Noise flooding	Plover [EEN+24]	Raccoon [dEK+23]

↑ More compact

This talk: focus on Raccoon 🦝

- Masking-friendly [dPKPR24] and threshold-friendly [DKM+24]
- NIST PQC candidate [dEK+23], 2023-2024 (RIP in peace 🪦)
- Similar design also found in [ASY22, GKS24]

Raccoon: Schnorr over lattices

PQ SHIELD

Raccoon.Keygen$() \to \mathtt{sk}, \mathtt{vk}$

1. $\mathtt{vk} = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathtt{sk}$, for $\mathtt{sk}$ short.

Raccoon.Sign$(\mathtt{sk}, \mathtt{msg}) \to \mathtt{sig}$

1. Sample a short $\mathbf{r}$
2. $\mathbf{w} = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathbf{r}$
3. $c = H(\mathbf{w}, \mathtt{msg})$
4. $\mathbf{z} = \mathbf{r} + c \cdot \mathtt{sk}$
5. Output $\mathtt{sig} = (c, \mathbf{z})$

Raccoon.Verify$(\mathtt{vk}, \mathtt{msg}, \mathtt{sig})$

1. $\mathbf{w}' = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathbf{z} - c \cdot \mathtt{vk}$
2. Assert $H(\mathbf{w}', \mathtt{msg}) = c$
3. Assert $\mathbf{z}$ is short

Schnorr.Keygen$() \to \mathtt{sk}, \mathtt{vk}$

1. $\mathtt{vk} = g^{\mathtt{sk}}$, for $\mathtt{sk}$ uniform.

Schnorr.Sign$(\mathtt{sk}, \mathtt{msg}) \to \mathtt{sig}$

1. Sample r
2. $w = g^r$
3. $c = H(w, \mathtt{msg})$
4. $z = r + c \cdot \mathtt{sk}$
5. Output $\mathtt{sig} = (c, z)$

Schnorr.Verify$(\mathtt{vk}, \mathtt{msg}, \mathtt{sig})$

1. $w' = g^z \cdot \mathtt{vk}^{-c}$
2. Assert $H(\mathbf{w}', \mathtt{msg}) = c$

Security of Raccoon

Raccoon.Keygen$() \to \mathtt{sk}, \mathtt{vk}$

1. $\mathtt{vk} = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathtt{sk}$, for $\mathtt{sk}$ short.

Raccoon.Sign$(\mathtt{sk}, \mathtt{msg}) \to \mathtt{sig}$

1. Sample a short $\mathbf{r}$
2. $\mathbf{w} = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathbf{r}$
3. $c = H(\mathbf{w}, \mathtt{msg})$
4. $\mathbf{z} = \mathbf{r} + c \cdot \mathtt{sk}$
5. Output $\mathtt{sig} = (c, \mathbf{z})$

Raccoon.Verify$(\mathtt{vk}, \mathtt{msg}, \mathtt{sig})$

1. $\mathbf{w}' = \begin{bmatrix}\mathbf{A} & 1\end{bmatrix} \cdot \mathbf{z} - c \cdot \mathtt{vk}$
2. Assert $H(\mathbf{w}', \mathtt{msg}) = c$
3. Assert $\mathbf{z}$ is short

Security: Raccoon is EUF-CMA assuming:

1. **Hint-MLWE [KLSS23]** (next slide)
   - Implied by lack of rejection sampling
   - Ensures uniformity of the public key
2. **Self-target MSIS [KLS18]**
   - Unforgeability

PQ SHIELD

(Hint-)MLWE [KLSS23]

It is difficult to distinguish both distributions:

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} := \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \cdot \mathsf{sk}\right\}$$

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} \leftarrow \mathcal{R}_q^{k}\right\}$$

In Hint-MLWE, the adversary is additionally given Q "hints" of the shape:

$$(c_i, \mathbf{z}_i \leftarrow c_i \cdot \mathsf{sk} + \mathbf{r}_i), \quad \text{where } c_i \leftarrow \mathcal{C}, \mathbf{r}_i \leftarrow \chi_{\mathbf{r}}$$

PQ SHIELD

(Hint-)MLWE [KLSS23]

It is difficult to distinguish both distributions:

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} := \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \cdot \mathsf{sk}\right\}$$

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} \leftarrow \mathcal{R}_q^{k}\right\}$$

In Hint-MLWE, the adversary is additionally given Q "hints" of the shape:

$$(c_i, \mathbf{z}_i \leftarrow c_i \cdot \mathsf{sk} + \mathbf{r}_i), \quad \text{where } c_i \leftarrow \mathcal{C}, \mathbf{r}_i \leftarrow \chi_{\mathbf{r}}$$

Attack on Hint-MLWE

Assume $\forall i \in [Q], \|c_i\|^2 = \omega$. If we note $c^*(x) = c(x^{-1})$, we can recover sk by constructing this accumulator:

$$\begin{aligned} \mathsf{acc} &= \sum_i c_i^* \cdot \mathbf{z}_i \\ &= \sum_i c_i^* c_i \cdot \mathsf{sk} + \sum_i c_i^* \cdot \mathbf{r}_i \\ &\approx Q \cdot \omega \cdot \mathsf{sk} + O(\sqrt{Q \cdot \omega} \cdot \|\mathbf{r}\|) \end{aligned}$$

If $\|\mathbf{r}\| = o(\sqrt{Q \cdot \omega})$, rounding acc to the closest multiple of $Q \cdot \omega$ gives sk.

Hint-MLWE?

PQ SHIELD

(Hint-)MLWE [KLSS23]

It is difficult to distinguish both distributions:

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} := \begin{bmatrix} \mathbf{A} & \mathbf{I} \end{bmatrix} \cdot \mathsf{sk}\right\}$$

$$\left\{(\mathbf{A}, \mathbf{b}) | \mathbf{A} \leftarrow \mathcal{R}_q^{k \times \ell}, \mathsf{sk} \leftarrow \chi_{\mathsf{sk}}, \mathbf{b} \leftarrow \mathcal{R}_q^{k}\right\}$$

In Hint-MLWE, the adversary is additionally given Q "hints" of the shape:

$$(c_i, \mathbf{z}_i \leftarrow c_i \cdot \mathsf{sk} + \mathbf{r}_i), \quad \text{where } c_i \leftarrow \mathcal{C}, \mathbf{r}_i \leftarrow \chi_{\mathbf{r}}$$

Attack on Hint-MLWE

Assume $\forall i \in [Q], \|c_i\|^2 = \omega$. If we note $c^*(x) = c(x^{-1})$, we can recover sk by constructing this accumulator:

$$\begin{aligned} \mathsf{acc} &= \sum_i c_i^* \cdot \mathbf{z}_i \\ &= \sum_i c_i^* c_i \cdot \mathsf{sk} + \sum_i c_i^* \cdot \mathbf{r}_i \\ &\approx Q \cdot \omega \cdot \mathsf{sk} + O(\sqrt{Q \cdot \omega} \cdot \|\mathbf{r}\|) \end{aligned}$$

If $\|\mathbf{r}\| = o(\sqrt{Q \cdot \omega})$, rounding acc to the closest multiple of $Q \cdot \omega$ gives sk.

Security reduction, simplified [KLSS23, DKM+24]

If $\mathbf{sk}$ and $\mathbf{r}_i$ are sampled from gaussians of standard deviation σ_{sk} and $\sigma_{\mathbf{r}}$, then:

$$\text{Hint-MLWE}_{\mathcal{R}_q, k, \ell, \sigma_{\mathsf{sk}}, \sigma_{\mathbf{r}}, Q} \geq \text{MLWE}_{\mathcal{R}_q, k, \ell, \sigma_0}, \quad \text{where} \quad \frac{1}{\sigma_0^2} \approx 2\left(\frac{1}{\sigma_{\mathsf{sk}}^2} + \frac{Q \cdot \omega}{\sigma_{\mathbf{r}}^2}\right) \qquad (1)$$

Threshold Cryptography

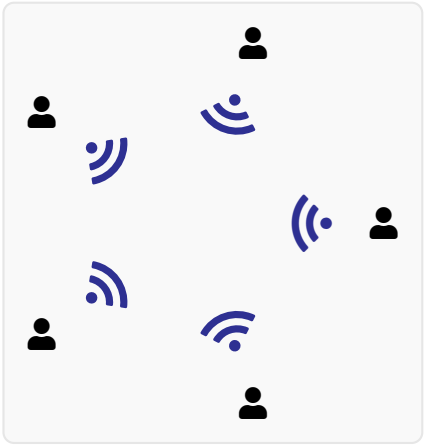
Main idea

PQ SHIELD

Distribute trust across devices ⇒ Increased resilience

		☠ Attacker: how many devices to compromise?	🥖 Attacker: how many devices to destroy?
1 device	**1** key	1 / 1	1 / 1
N devices	**1** key	1 / N	N / N
N devices	**N** keys	N / N	1 / N
N devices	**T-out-of-N** keys	T / N	(N - T + 1) / N

- → The two last solutions fall under **threshold cryptography**
- → Main focus of the NIST MPTC programme
- → Reminiscent of masking, but key differences in the attack model and properties



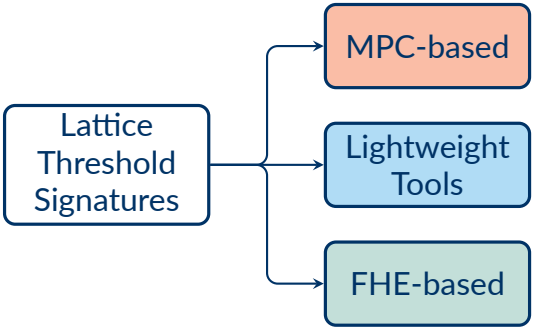
Communication

- Authenticated, reliable & synchronous broadcast channel
- Each *i* and *j* may share an authenticated private channel (via AEAD)

Syntax

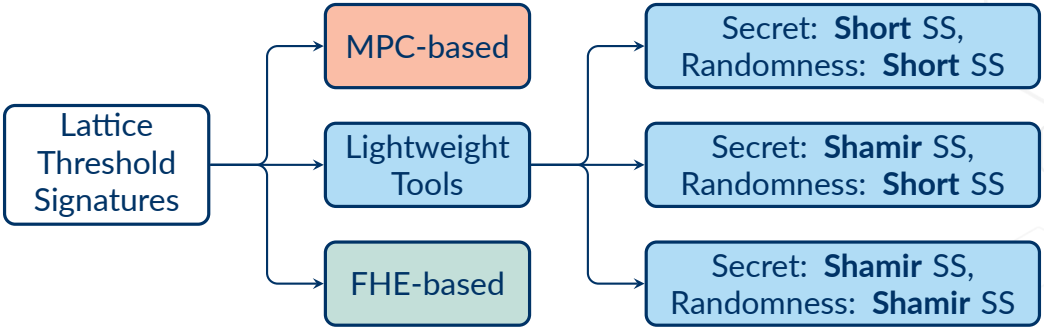
- One public key $\mathtt{vk}$
- Each user *i* has a secret key share $\mathtt{sk}_i$
- Signing is an interactive protocol between $|\mathcal{S}|$ signers
  - Our protocols are 3-4 rounds
  - $(|\mathcal{S}| < T) \Rightarrow \perp$
  - $(|\mathcal{S}| = T) \Rightarrow \mathtt{sig}$ a valid signature

Design choices



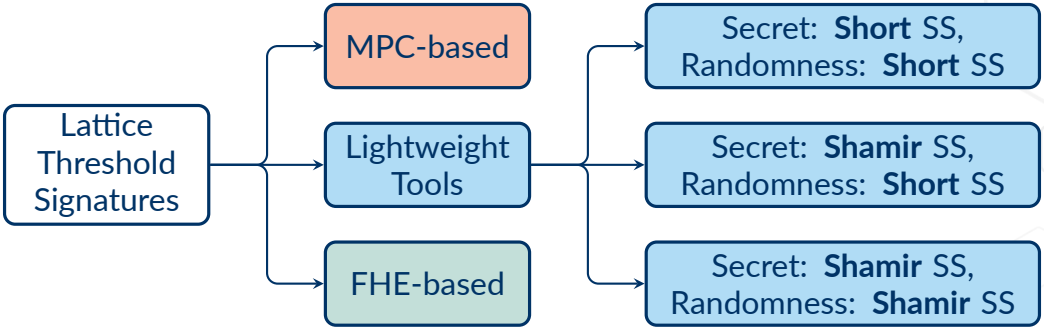
Paradigm	Size	Speed	Rounds	Comm/party
MPC	S	Slow	15	$\geq$ 1000 KB
Lightweight	S-M	Fast	2-4	$20 \rightarrow 56 \cdot T$ KB
FHE	M	As fast as FHE	2	$\geq$ 1000 KB

Design choices



Paradigm	Size	Speed	Rounds	Comm/party
MPC	S	Slow	15	$\geq$ 1000 KB
Lightweight	S-M	Fast	2-4	20 $\rightarrow$ 56 $\cdot$ T KB
FHE	M	As fast as FHE	2	$\geq$ 1000 KB

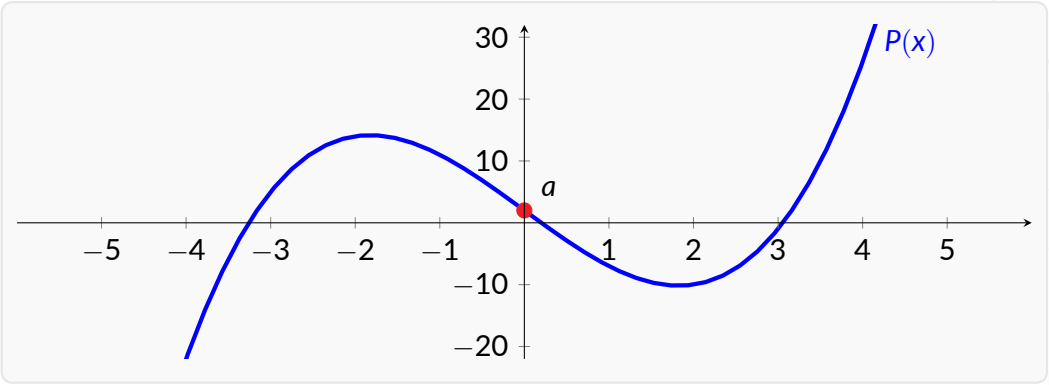
Design choices



Paradigm	Size	Speed	Rounds	Comm/party
MPC	S	Slow	15	$\geq$ 1000 KB
Lightweight	S-M	Fast	2-4	$20 \rightarrow 56 \cdot T$ KB
FHE	M	As fast as FHE	2	$\geq$ 1000 KB

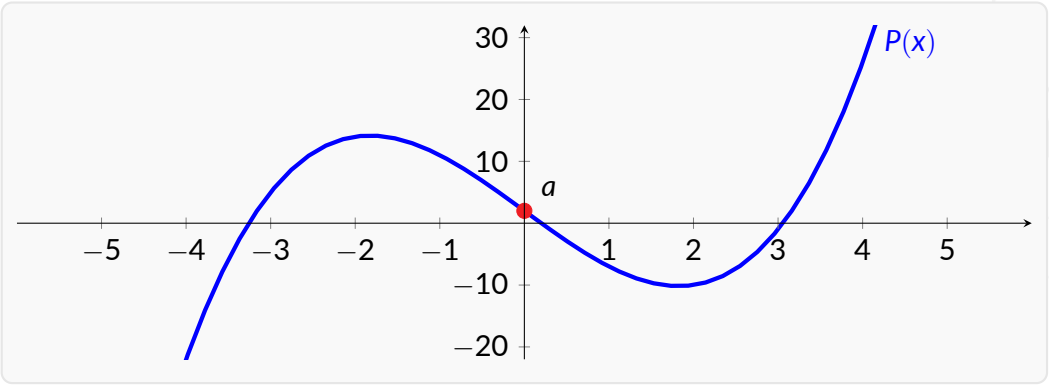
This talk.

So You Want to Thresholdize Raccoon?



Secret-sharing a secret $a \in \mathbb{Z}_p$:

- Generate $P(x)$ of degree at most $T - 1$ such that $P(0) = a$
- Each party $i \in \mathbb{Z}_p$ receives a share $a_i = P(i)$



Properties:

- With $< T$ shares, a is perfectly hidden
- With a set $\mathcal{S}$ of T shares, a can be recovered via Lagrange interpolation:

$$a = \sum_{i \in \mathcal{S}} \lambda_{i,\mathcal{S}} \cdot a_i, \quad \text{where} \quad \lambda_{i,\mathcal{S}} = \prod_{j \in \mathcal{S} \setminus \{i\}} \frac{j}{i-j} \tag{2}$$

Threshold Schnorr signatures

PQ SHIELD

Sparkle

Each signer i knows a share sk_i of sk.

→ **Round 1:**

1. Sample r_i
2. $w_i = g^{r_i}$
3. $\mathsf{com}_i = H_{\mathsf{com}}(w_i, \mathsf{msg}, \mathcal{S})$
4. Broadcast com_i

→ **Round 2:**

1. Broadcast w_i

→ **Round 3:**

1. $w = \prod_i w_i$
2. $c = H(\mathsf{vk}, \mathsf{msg}, w)$
3. $z_i = r_i + c \cdot \lambda_{i,\mathcal{S}} \cdot \mathsf{sk}_i$
4. Broadcast z_i

→ **Combine:** the final signature is $(c, z = \sum_{i \in \mathcal{S}} z_i)$

See [BN06, CKM23]

✓ This produces valid Schnorr signatures:

$$\begin{aligned} g^z &= g^{\sum_i z_i} \\ &= \left(g^{\sum_i r_i}\right) \cdot \left(g^{c \sum_i \lambda_{i,\mathcal{S}} \cdot \mathsf{sk}_i}\right) \\ &= w \cdot \mathsf{vk}^c \end{aligned}$$

Security: in z_i, r_i is uniform and perfectly hides $c \cdot \lambda_{i,\mathcal{S}} \cdot \mathsf{sk}_i$

⚠ Commit-then-reveal w_i to avoid ROS attacks [DEF+19, BLL+22] (we may ignore them for this talk)

? Can we transpose this to Raccoon?

PQ SHIELD

Insecure Threshold Raccoon

→ **Round 1:**

1. Sample short $\mathbf{r}_i$
2. $\mathbf{w}_i = \begin{bmatrix}\mathbf{A} & \mathbf{I}\end{bmatrix} \cdot \mathbf{r}_i$
3. $\mathtt{com}_i = H_{\mathtt{com}}(\mathbf{w}_i, \mathtt{msg}, \mathcal{S})$
4. Broadcast $\mathtt{com}_i$

→ **Round 2:**

1. Broadcast $\mathbf{w}_i$

→ **Round 3:**

1. $\mathbf{w} = \sum_i \mathbf{w}_i$
2. $c = H(\mathtt{vk}, \mathtt{msg}, \mathbf{w})$
3. $\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathtt{sk}_i$
4. Broadcast $\mathbf{z}_i$

→ **Combine:** the final signature is $(c, \mathbf{z} = \sum_{i \in \mathcal{S}} \mathbf{z}_i)$

✓ This gives valid Raccoon signatures (up to slight parameter changes)

PQ SHIELD

Insecure Threshold Raccoon

→ **Round 1:**

1. Sample short $\mathbf{r}_i$
2. $\mathbf{w}_i = \begin{bmatrix}\mathbf{A} & \mathbf{I}\end{bmatrix} \cdot \mathbf{r}_i$
3. $\mathtt{com}_i = H_{\mathtt{com}}(\mathbf{w}_i, \mathtt{msg}, \mathcal{S})$
4. Broadcast $\mathtt{com}_i$

→ **Round 2:**

1. Broadcast $\mathbf{w}_i$

→ **Round 3:**

1. $\mathbf{w} = \sum_i \mathbf{w}_i$
2. $c = H(\mathtt{vk}, \mathtt{msg}, \mathbf{w})$
3. $\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathtt{sk}_i$
4. Broadcast $\mathbf{z}_i$

→ **Combine:** the final signature is $(c, \mathbf{z} = \sum_{i \in \mathcal{S}} \mathbf{z}_i)$

✓ This gives valid Raccoon signatures (up to slight parameter changes)

⚠ Issue: when we consider

$$\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathtt{sk}_i, \qquad (3)$$

$\mathbf{r}_i$ is small but $c \cdot \lambda_i \cdot \mathtt{sk}_i$ is large.

- Breaks the security proof
- For a fixed i, with enough $\mathbf{z}_i$ of the form in (3) one can recover $\mathtt{sk}_i$

PQ SHIELD

Insecure Threshold Raccoon

→ **Round 1:**

1. Sample short $\mathbf{r}_i$
2. $\mathbf{w}_i = \begin{bmatrix}\mathbf{A} & \mathbf{I}\end{bmatrix} \cdot \mathbf{r}_i$
3. $\mathtt{com}_i = H_{\mathtt{com}}(\mathbf{w}_i, \mathtt{msg}, \mathcal{S})$
4. Broadcast $\mathtt{com}_i$

→ **Round 2:**

1. Broadcast $\mathbf{w}_i$

→ **Round 3:**

1. $\mathbf{w} = \sum_i \mathbf{w}_i$
2. $c = H(\mathtt{vk}, \mathtt{msg}, \mathbf{w})$
3. $\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathtt{sk}_i$
4. Broadcast $\mathbf{z}_i$

→ **Combine:** the final signature is $(c, \mathbf{z} = \sum_{i \in \mathcal{S}} \mathbf{z}_i)$

✓ This gives valid Raccoon signatures (up to slight parameter changes)

⚠ Issue: when we consider

$$\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathtt{sk}_i, \qquad (3)$$

$\mathbf{r}_i$ is small but $c \cdot \lambda_i \cdot \mathtt{sk}_i$ is large.

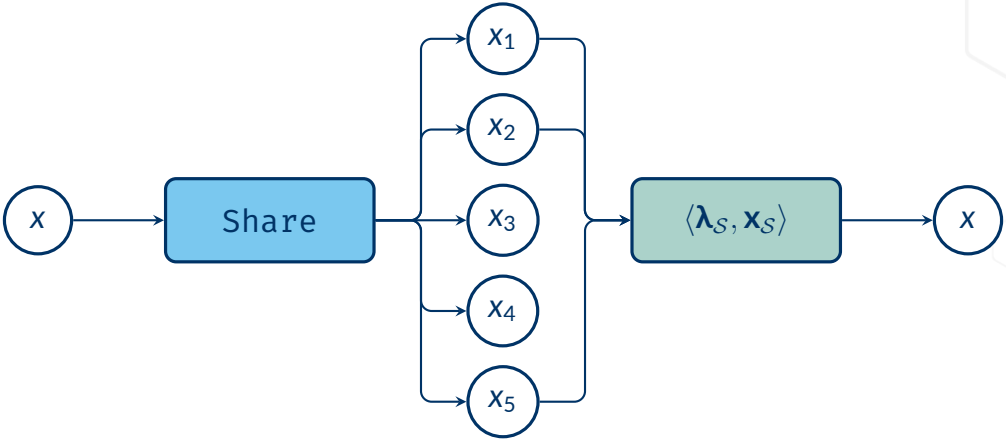
- Breaks the security proof
- For a fixed i, with enough $\mathbf{z}_i$ of the form in (3) one can recover $\mathtt{sk}_i$

? How do we solve this?

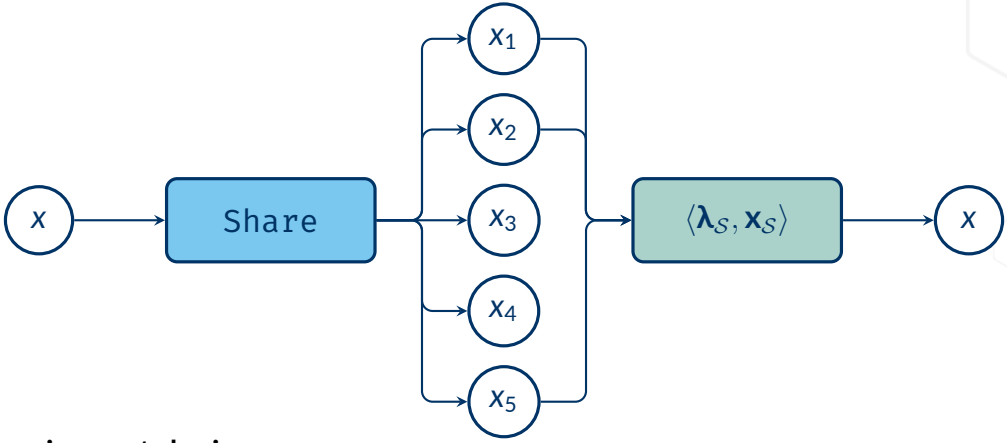
1. Add zero-share to $\mathbf{z}_i$ [DKM+24]
2. Use Shamir everywhere [ENP24]
3. Short secret sharings [**this talk!**]

Short Secret Sharings

Different types of secret sharings



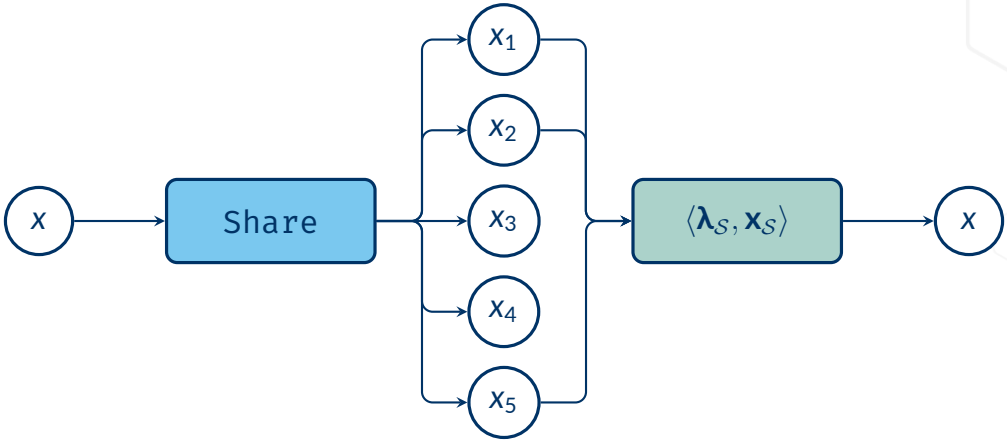
Different types of secret sharings



Shamir secret sharing:

- Share: $x_i = P(i)$, where $P(0) = x$
- The shares x_i and reconstruction vector $\boldsymbol{\lambda}_{\mathcal{S}}$ may be large

Different types of secret sharings



"Short" secret sharing: we require that:

1. If x is short, the shares x_i are short
2. The reconstruction vector $\boldsymbol{\lambda}_S$ is short

Example: N-out-of-N sharing where:

- $(x_i)_{1 \le i < N} \leftarrow D_\sigma^{N-1}$ and $x_N = x - \sum_{i<N} x_i$
- $\boldsymbol{\lambda}_S = (1, \ldots, 1)$

Threshold Raccoon w/ short secret sharing

PQ SHIELD

Threshold Raccoon, short shares

→ **Round 1:**

1. Sample short $\mathbf{r}_i$
2. $\mathbf{w}_i = \begin{bmatrix}\mathbf{A} & \mathbf{I}\end{bmatrix} \cdot \mathbf{r}_i$
3. $\mathsf{com}_i = H_{\mathsf{com}}(\mathbf{w}_i, \mathsf{msg}, \mathcal{S})$
4. Broadcast com_i

→ **Round 2:**

1. Broadcast $\mathbf{w}_i$

→ **Round 3:**

1. $\mathbf{w} = \sum_i \mathbf{w}_i$
2. $c = H(\mathsf{vk}, \mathsf{msg}, \mathbf{w})$
3. $\mathbf{z}_i = \mathbf{r}_i + c \cdot \lambda_i \cdot \mathsf{sk}_i$
4. Broadcast $\mathbf{z}_i$

→ **Combine:** the final signature is $(c, \mathbf{z} = \sum_{i \in \mathcal{S}} \mathbf{z}_i)$

Security

→ Even if a set of shares $(\mathsf{sk}_i)_{i \in \mathcal{C}}$ leak:

$$\mathsf{sk} | (\mathsf{sk}_i)_{i \in \mathcal{C}} \sim \sum_{i \in \mathcal{C}} \mathsf{sk}_i + D_{\sigma\sqrt{N - |\mathcal{C}|}}$$

→ Partial signature leak nothing

- $\mathbf{r}_i$ hides $c \cdot \lambda_i \cdot \mathsf{sk}_i$ as both are short
- We argue security via Hint-MLWE

Identifiable aborts

→ Each $\mathsf{vk}_i = \begin{bmatrix}\mathbf{A} & \mathbf{I}\end{bmatrix} \cdot \mathsf{sk}_i$ is a valid public key

→ Therefore each $(c, \mathbf{z}_i)$ is a valid partial signature

→ We get identifiable aborts for free!

Rest of this section and of this talk

PQ SHIELD

Three secret sharings based on set theory:

- → **Replicated secret sharing**
  - − Scales terribly
- → **Coupon collector secret sharing**
  - + Scales well
  - − Ramp (privacy threshold < correctness threshold)
- → **Vandermonde secret sharing**
  - + Scales well
  - + No ramp

Replicated Secret Sharing

PQ SHIELD

Replicated secret sharing

- We create one share $\mathbf{s}_J$ for each subset of $\{1, \ldots, N\}$ of size $N - T + 1$
  - A user $u \in \{1, \ldots, N\}$ is given $\mathbf{s}_J$ if and only if $u \in J$
  - The secret is $\mathbf{s} = \sum_J \mathbf{s}_J$
- **T-correctness:** for each share $\mathbf{s}_J$, exactly $T - 1$ users do not have it
- **$(T-1)$-privacy:** for any set $\mathtt{act}$ of size $|\mathtt{act}| = T - 1$, no member of $\mathtt{act}$ has the share $\mathbf{s}_{\{1,\ldots,N\}\setminus \mathtt{act}}$

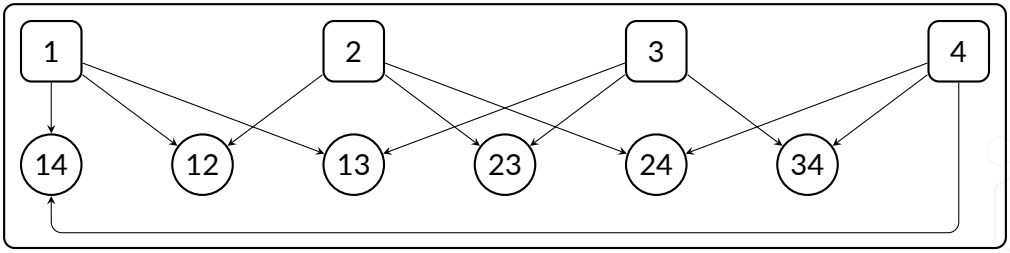


Figure 1: Illustration with $(N, T) = (4, 3)$.

Practical considerations

- **Number of shares:** $\binom{N}{N-T+1}$
- When signing, how do we assign shares to users? Here for $\texttt{act} = \{1, 3, 4\}$:
  - **Naive solution:** assign each share $\mathbf{s}_J$ to $u = \min(J)$
  - Other solutions might exist (wink)

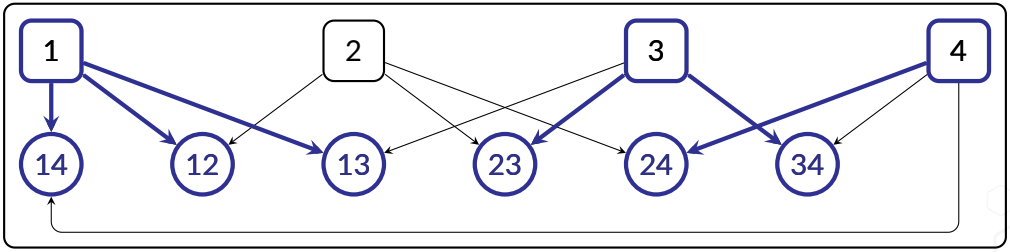


Figure 1: Illustration with $(N, T) = (4, 3)$.

Coupon Collector Secret Sharing

PQ SHIELD

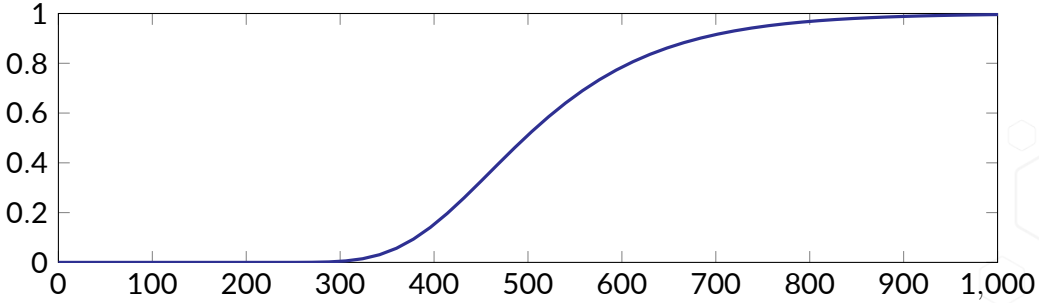
The coupon collector problem

Let $S = \{1, \ldots, n\}$. Starting at $i = 1$, we sample $x_i \leftarrow S$, until $\bigcup_i \{x_i\} = S$.

- The number of iterations of this sampling process follows a distribution T_n.
- The *coupon collector's problem* refers to the mathematical analysis of T_n.

Fact: $\mathbb{E}[T_n] = n\left(\frac{1}{1} + \frac{1}{2} + \cdots + \frac{1}{n}\right) \sim n \log n$.

Cumulative distribution graph of T_n for $n = 100$ (restricted):



Coupon collector secret sharing (CCSS)

PQ SHIELD

Lemma (Adapted from [Doe18])

If $\varepsilon_{\min} = \frac{\ln C}{\ln n}$, $\varepsilon_{\max} = \frac{C}{\ln n}$, *then:*

$$\mathbb{P}[T_n \leq T_{\min}] \leq e^{-C}, \quad \text{where } T_{\min} = \max\left((1-\varepsilon_{\min})\,(n-1)\,\ln n, n\right) \tag{4}$$

$$\mathbb{P}[T_n \geq T_{\max}] \leq e^{-C}, \quad \text{where } T_{\max} = (1+\varepsilon_{\max})\,n \ln n \tag{5}$$

Main idea

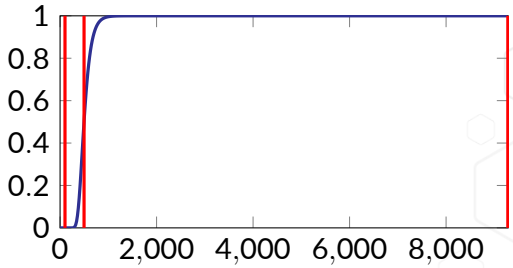
Sample n shares $\mathbf{s}_i$, set $\mathbf{s} = \sum_i \mathbf{s}_i$

- Each user receives a random share
- w.o.p. a set of $\leq T_{\min}$ users **cannot** recover all the shares
- w.o.p. a set of $\geq T_{\max}$ users **can** recover all the shares

Problem: $\frac{T_{\max}}{T_{\min}} \sim 1 + \varepsilon_{\max} + \varepsilon_{\min} \gg 1$.

For $n = 100$**:**

$(T_{\min}, \mathbb{E}[T_n], T_{\max}) = (102, 497, 9287)$.



PQ SHIELD

Optimization 1

s is now shared p times in parallel

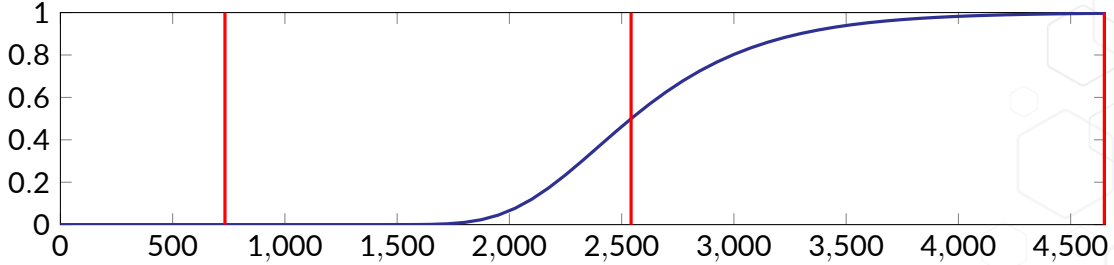
- → Each user receives one share of each sharing
- → Allows to relax correctness
- → We may decrease $\varepsilon_{\max}$ to $\frac{C/p}{\ln n}$

Optimization 2

Increase n by a factor q

- → Now each user receives n shares (per sharing)
- → "Amplify" asymptotic behavior

Example with $n\,q = 400$ and $p = 16$: we have $\frac{T_{\max}}{T_{\min}} \sim 1 + \frac{C/p + \ln C}{\ln(n\,q)}$



Vandermonde Secret Sharing

Vandermonde's identity

For $0 \leq c \leq N$:

$$\binom{N}{T} = \sum_{k=0}^{T} \binom{c}{k} \cdot \binom{N-c}{T-k} \tag{6}$$

Distribution theory interpretation: The sum of two binomials is a binomial:

$$B(m,p) + B(n,p) \sim B(m+n,p) \tag{7}$$

Set theory interpretation: let us note $\mathcal{S}_{S,T}$ the subsets of S of cardinality T.

- Any subset $\mathtt{act} \in \mathcal{S}_{\{1,\dots,N\},T}$ can be decomposed uniquely as:

$$\mathtt{act} = \mathtt{act}_L \sqcup \mathtt{act}_R, \quad \text{where} \begin{cases} \mathtt{act}_L \subseteq \{1,\dots,c\} \\ \mathtt{act}_R \subseteq \{c+1,\dots,N\} \end{cases} \tag{8}$$

- Eq. (6) follows from enumerating these decompositions.

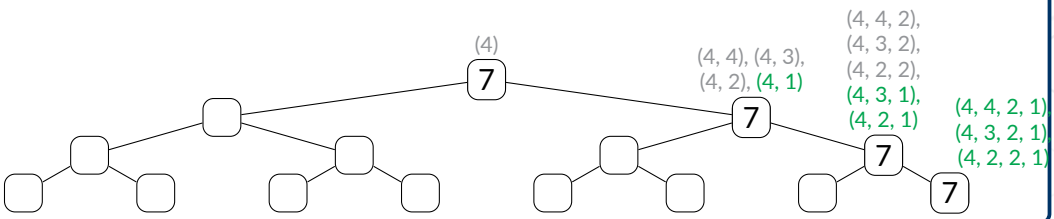
Vandermonde secret sharing [DDB95] turns this into a secret sharing:

- Enumerating all the possible disjunctions of the form in Eq. (8)
- For each disjunction, share the secret in two
  - Recursively share the first half across members of $\mathtt{act}_L$
  - Recursively share the second half across members of $\mathtt{act}_L$

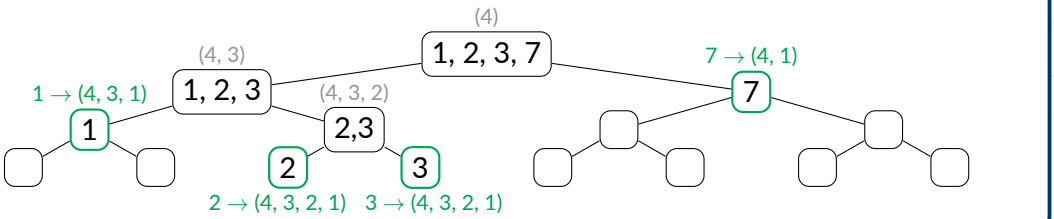
Example: 4-out-of-8

PQ SHIELD

Share with $(N, T) = (8, 4)$ from the point of view of user 7



Recover with $\texttt{act} = \{1, 2, 3, 7\}$

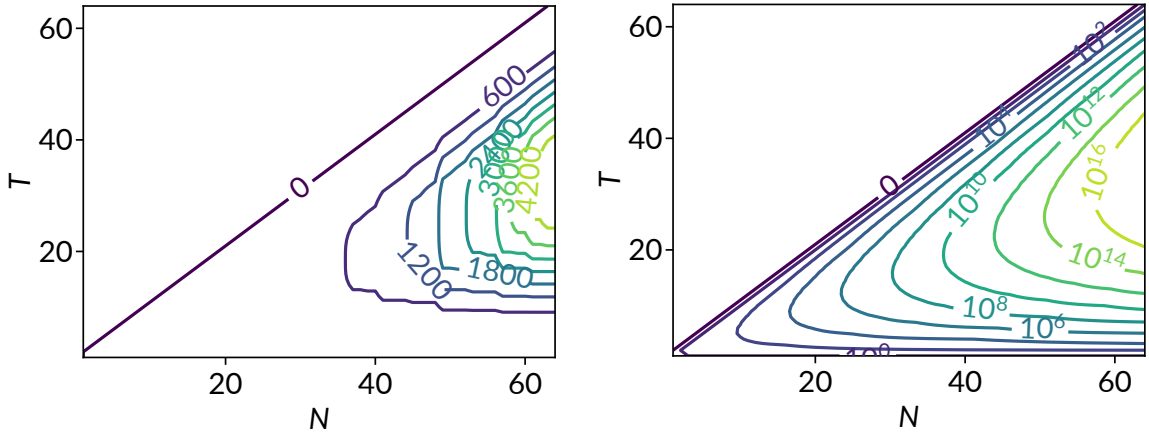


Algorithm 1 Share$(x, \mathcal{P}, T, \mathtt{idx} = (T)) \to \mathtt{Dict}$

$N = |\mathcal{P}|$
if $T = 1$ **then**
  return $\mathtt{Dict} \coloneqq \{user : \{\mathtt{idx} : x\} \mid user \in \mathcal{P}\}$
else
  $\mathtt{Dict} = \{user : \{:\} \mid user \in \mathcal{P}\}$. $c = \lfloor N/2 \rfloor$
  Parse $\mathcal{P} = \mathcal{P}_L \sqcup \mathcal{P}_R$, with $\mathcal{P}_L$ the c smallest elements of $\mathcal{P}$
  for $k = \max(0, T - N + c), \ldots, \min(c, T)$ **do**
    $\mathtt{idx}_L \coloneqq (\mathtt{idx}, k)$
    $\mathtt{idx}_R \coloneqq (\mathtt{idx}, T - k)$
    if $k = 0$ **then**
      $\mathtt{Dict} \coloneqq \mathtt{Dict} \cup$ Share$(x, \mathcal{P}_R, T, \mathtt{idx}_R)$
    else if $k = T$ **then**
      $\mathtt{Dict} \coloneqq \mathtt{Dict} \cup$ Share$(x, \mathcal{P}_L, T, \mathtt{idx}_L)$
    else
      $x_0 \leftarrow \chi$
      $x_1 \coloneqq (x - x_0) \bmod q$
      $\mathtt{Dict}_L \coloneqq$ Share$(x, \mathcal{P}_L, k, \mathtt{idx}_L)$
      $\mathtt{Dict}_R \coloneqq$ Share$(x, \mathcal{P}_R, T - k, \mathtt{idx}_R)$
      $\mathtt{Dict} \coloneqq \mathtt{Dict} \cup \mathtt{Dict}_L \cup \mathtt{Dict}_R$
  return Dict

Algorithm 2 Recover$(\mathcal{P}, \mathtt{act}, \mathtt{idx} = (T)) \to \mathtt{Dict}$

$N = |\mathcal{P}|, T = |\mathtt{act}|$
if $T = 1$ **then**
  return $\mathtt{Dict} \coloneqq \{user : \mathtt{idx} \mid user \in \mathcal{P}\}$
else
  $c = \lfloor N/2 \rfloor$. Parse $\mathcal{P} = \mathcal{P}_L \sqcup \mathcal{P}_R$, with $\mathcal{P}_L$ the c smallest elements of $\mathcal{P}$
  $k = |\mathcal{P}_L|, \mathtt{act}_L = \mathtt{act} \cap \mathcal{P}_L, \mathtt{act}_R = \mathtt{act} \cap \mathcal{P}_R$
  $\mathtt{idx}_L \coloneqq (\mathtt{idx}, k)$
  $\mathtt{idx}_R \coloneqq (\mathtt{idx}, T - k)$
  if $k = 0$ **then**
    return Recover$(\mathcal{P}_R, \mathtt{act}_R, \mathtt{idx}_R)$
  else if $k = T$ **then**
    return Recover$(\mathcal{P}_L, \mathtt{act}_L, \mathtt{idx}_L)$
  else
    $\mathtt{Dict}_L \coloneqq$ Recover$(\mathcal{P}_L, \mathtt{act}_L, \mathtt{idx}_L)$
    $\mathtt{Dict}_R \coloneqq$ Recover$(\mathcal{P}_R, \mathtt{act}_R, \mathtt{idx}_R)$
    return $\mathtt{Dict} \coloneqq \mathtt{Dict}_L \sqcup \mathtt{Dict}_R$



(a) **Vandermonde:** $O((N/\log N)^{\log N})$ shares/party

(b) **Replicated:** up to $\binom{N-1}{N-T} \approx 2^N$ shares/party

Figure 2: Contour plots of the number of shares/party, as a function of N and T (undef. for $T > N$).

Conclusion

Scheme	Shares/party	$\frac{T_{correctness}}{T_{privacy}}$	IA
Shamir	1	1	No
Replicated	2^N	1	Yes
Coupon Collector	$p \cdot q$	$1 + O\left(\frac{\kappa/p + \ln \kappa}{\ln(n\,q)}\right)$	Yes
Vandermonde	$O\left(\left(\frac{N}{\log N}\right)^{\log N}\right)$	1	Yes

Questions?

https://raccoonfamily.org
https://tprest.github.io

The Death Star Algorithm

How large is the sum of T vectors?

Consider T independent Gaussian vectors $\mathbf{x}_i \leftarrow D_\sigma^n$.
Let $\mathbf{x} = \sum_{i \in [T]} \mathbf{x}_i$. What can we say about $\|\mathbf{x}\|$?

How large is the sum of T vectors?

PQ SHIELD

Consider T independent Gaussian vectors $\mathbf{x}_i \leftarrow D_\sigma^n$.
Let $\mathbf{x} = \sum_{i \in [T]} \mathbf{x}_i$. What can we say about $\|\mathbf{x}\|$?

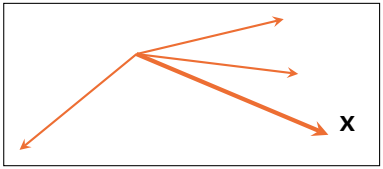


Figure 3: Average-case: $O(\sqrt{T})$

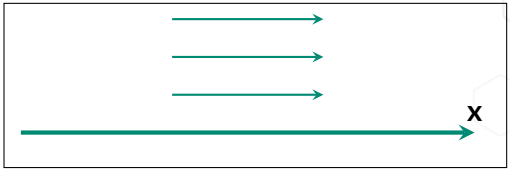
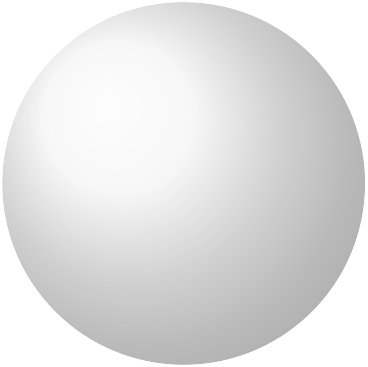


Figure 4: Worst-case: $O(T)$

- ✔ Signatures by honest signers would end up in Fig. 4
- ✖ But colluding signers could force the Fig. 3

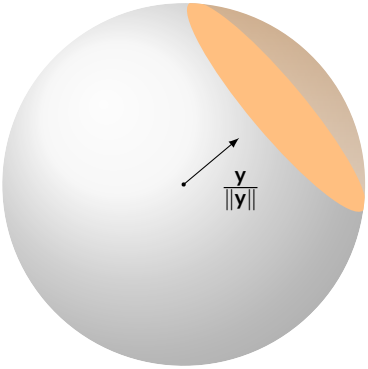
This will decrease security. Can we do better?

If $\mathbf{x}_i \leftarrow D_\sigma^n$, it is well known™ that:



If $\mathbf{x}_i \leftarrow D_\sigma^n$, it is well known™ that:

1. $\|\mathbf{x}_i\|$ is concentrated around its expected value $\sigma\sqrt{n}$

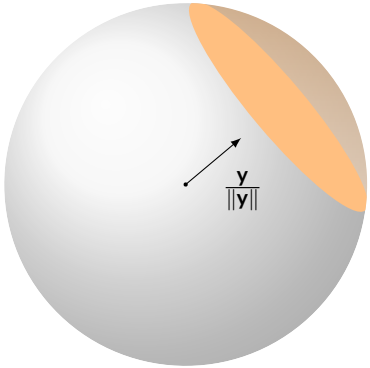


If $\mathbf{x}_i \leftarrow D_\sigma^n$, it is well known™ that:

1. $\|\mathbf{x}_i\|$ is concentrated around its expected value $\sigma\sqrt{n}$
2. For any vector $\mathbf{y}$:

$$\langle \mathbf{x}_i, \mathbf{y} \rangle < \sigma\sqrt{O(\lambda)}\,\|\mathbf{y}\| \qquad (9)$$

except with probability $\leq 2^{-\lambda}$



The Death Star Algorithm

1. For each signer i:
   1. If $\|\mathbf{x}_i\| \geq (1 + o(1))\sigma\sqrt{n}$, reject i
   2. If $\langle \mathbf{x}_i, \mathbf{y}_i \rangle \geq \sigma\sqrt{O(\lambda)}\,\|\mathbf{y}_i\|$, where $\mathbf{y}_i = \sum_{j \neq i} \mathbf{x}_j$, reject i

Lemma: for a set of non-rejected $(\mathbf{x}_i)_{i \in [T]}$, the sum $\mathbf{x} = \sum_i \mathbf{x}_i$ satistifes:

$$\|\mathbf{x}\| \leq \sigma \cdot T \cdot \sqrt{2 \log 2 \cdot \lambda} \tag{9}$$

$$+ \sigma \cdot \sqrt{T \cdot d} \cdot (1 + \varepsilon) \tag{10}$$

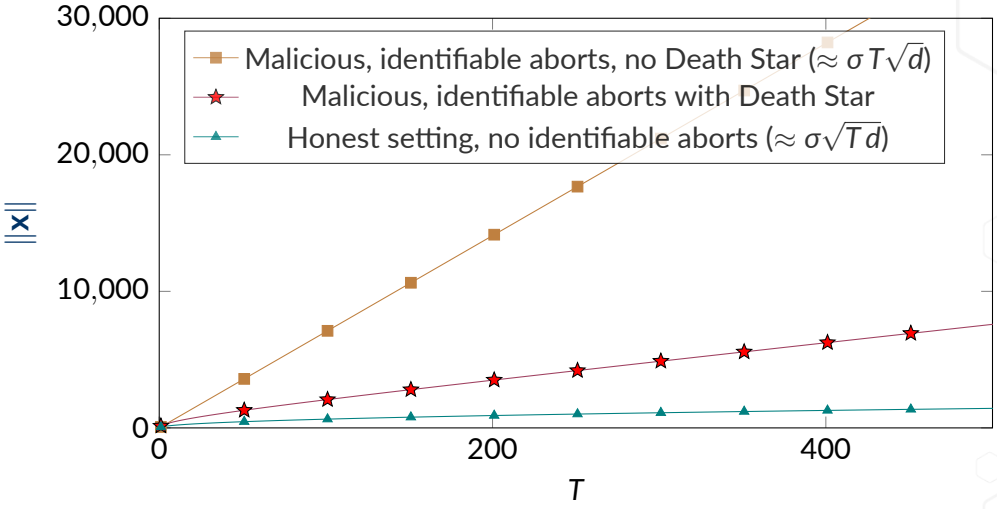


Figure 5: Norm of $\mathbf{x} = \sum_{i \in [T]} \mathbf{x}_i$, for $\sigma = 1$, dimension $n = 4096$, $\lambda = 128$ bits of security, and $1 \leq T \leq 1000$.

Shahla Atapoor, Karim Baghery, Daniele Cozzo, and Robi Pedersen.
VSS from distributed ZK proofs and applications.
In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part I*, volume 14438 of *LNCS*, pages 405–440. Springer, Singapore, December 2023.

Masayuki Abe and Serge Fehr.
Adaptively secure feldman VSS and applications to universally-composable threshold cryptography.
In Matthew Franklin, editor, *CRYPTO 2004*, volume 3152 of *LNCS*, pages 317–334. Springer, Berlin, Heidelberg, August 2004.

Shweta Agrawal, Damien Stehlé, and Anshu Yadav.
Round-optimal lattice-based threshold signatures, revisited.
In Mikolaj Bojanczyk, Emanuela Merelli, and David P. Woodruff, editors, *ICALP 2022*, volume 229 of *LIPIcs*, pages 8:1–8:20. Schloss Dagstuhl, July 2022.

Cecilia Boschini, Darya Kaviani, Russell W. F. Lai, Giulio Malavolta, Akira Takahashi, and Mehdi Tibouchi.
Ringtail: Practical two-round threshold signatures from learning with errors.
Cryptology ePrint Archive, Report 2024/1113, 2024.

Fabrice Benhamouda, Tancrède Lepoint, Julian Loss, Michele Orrù, and Mariana Raykova.
On the (in)security of ROS.
Journal of Cryptology, 35(4):25, October 2022.

Mihir Bellare and Gregory Neven.
Multi-signatures in the plain public-key model and a general forking lemma.
In Ari Juels, Rebecca N. Wright, and Sabrina De Capitani di Vimercati, editors, *ACM CCS 2006*, pages 390–399. ACM Press, October / November 2006.

Ran Canetti, Rosario Gennaro, Stanislaw Jarecki, Hugo Krawczyk, and Tal Rabin.
Adaptive security for threshold cryptosystems.
In Michael J. Wiener, editor, *CRYPTO'99*, volume 1666 of *LNCS*, pages 98–115. Springer, Berlin, Heidelberg, August 1999.

Elizabeth C. Crites, Chelsea Komlo, and Mary Maller.
Fully adaptive Schnorr threshold signatures.
In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part I*, volume 14081 of *LNCS*, pages 678–709. Springer, Cham, August 2023.

Yvo Desmedt, Giovanni Di Crescenzo, and Mike Burmester.
Multiplicative non-abelian sharing schemes and their application to threshold cryptography.
In Josef Pieprzyk and Reihaneh Safavi-Naini, editors, *ASIACRYPT'94*, volume 917 of *LNCS*, pages 21–32. Springer, Berlin, Heidelberg, November / December 1995.

Manu Drijvers, Kasra Edalatnejad, Bryan Ford, Eike Kiltz, Julian Loss, Gregory Neven, and Igors Stepanovs.
On the security of two-round multi-signatures.
In *2019 IEEE Symposium on Security and Privacy*, pages 1084–1101. IEEE Computer Society Press, May 2019.

Rafael del Pino, Thomas Espitau, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, Mélissa Rossi, and Markku-Juhani Saarinen.

Raccoon.

Technical report, National Institute of Standards and Technology, 2023.

available at https://csrc.nist.gov/Projects/pqc-dig-sig/round-1-additional-signatures.

Rafaël Del Pino, Shuichi Katsumata, Mary Maller, Fabrice Mouhartem, Thomas Prest, and Markku-Juhani O. Saarinen.

Threshold raccoon: Practical threshold signatures from standard lattice assumptions.

In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part II*, volume 14652 of *LNCS*, pages 219–248. Springer, Cham, May 2024.

Benjamin Doerr.

Probabilistic tools for the analysis of randomized optimization heuristics.

CoRR, abs/1801.06733, 2018.

Rafaël del Pino, Shuichi Katsumata, Thomas Prest, and Mélissa Rossi.

Raccoon: A masking-friendly signature proven in the probing model.

In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part I*, volume 14920 of *LNCS*, pages 409–444. Springer, Cham, August 2024.

Julien Devevey, Alain Passelègue, and Damien Stehlé.

G+G: A fiat-shamir lattice signature based on convolved gaussians.

In Jian Guo and Ron Steinfeld, editors, *ASIACRYPT 2023, Part VII*, volume 14444 of *LNCS*, pages 37–64. Springer, Singapore, December 2023.

Muhammed F. Esgin, Thomas Espitau, Guilhem Niot, Thomas Prest, Amin Sakzad, and Ron Steinfeld.

Plover: Masking-friendly hash-and-sign lattice signatures.

In Marc Joye and Gregor Leander, editors, *EUROCRYPT 2024, Part VII*, volume 14657 of *LNCS*, pages 316–345. Springer, Cham, May 2024.

Thomas Espitau, Shuichi Katsumata, and Kaoru Takemure.

Two-round threshold signature from algebraic one-more learning with errors.

In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 387–424. Springer, Cham, August 2024.

Thomas Espitau, Guilhem Niot, and Thomas Prest.

Flood and submerse: Distributed key generation and robust threshold signature from lattices.

In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 425–458. Springer, Cham, August 2024.

Craig Gentry, Shai Halevi, and Vadim Lyubashevsky.

Practical non-interactive publicly verifiable secret sharing with thousands of parties.

In Orr Dunkelman and Stefan Dziembowski, editors, *EUROCRYPT 2022, Part I*, volume 13275 of *LNCS*, pages 458–487. Springer, Cham, May / June 2022.

Kamil Doruk Gür, Jonathan Katz, and Tjerand Silde.

Two-round threshold lattice-based signatures from threshold homomorphic encryption.
In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part II*, pages 266–300. Springer, Cham, June 2024.


Stanislaw Jarecki and Anna Lysyanskaya.
Adaptively secure threshold cryptography: Introducing concurrency, removing erasures.
In Bart Preneel, editor, *EUROCRYPT 2000*, volume 1807 of *LNCS*, pages 221–242. Springer, Berlin, Heidelberg, May 2000.


Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders.
Phoenix: Hash-and-sign with aborts from lattice gadgets.
In Markku-Juhani Saarinen and Daniel Smith-Tone, editors, *Post-Quantum Cryptography - 15th International Workshop, PQCrypto 2024, Part I*, pages 265–299. Springer, Cham, June 2024.


Eike Kiltz, Vadim Lyubashevsky, and Christian Schaffner.
A concrete treatment of Fiat-Shamir signatures in the quantum random-oracle model.
In Jesper Buus Nielsen and Vincent Rijmen, editors, *EUROCRYPT 2018, Part III*, volume 10822 of *LNCS*, pages 552–586. Springer, Cham, April / May 2018.


Duhyeong Kim, Dongwon Lee, Jinyeong Seo, and Yongsoo Song.
Toward practical lattice-based proof of knowledge from hint-MLWE.
In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 549–580. Springer, Cham, August 2023.


Shuichi Katsumata, Michael Reichle, and Kaoru Takemure.

Adaptively secure 5 round threshold signatures from MLWE/MSIS and DL with rewinding.
In Leonid Reyzin and Douglas Stebila, editors, *CRYPTO 2024, Part VII*, volume 14926 of *LNCS*, pages 459–491. Springer, Cham, August 2024.


Vadim Lyubashevsky, Léo Ducas, Eike Kiltz, Tancrède Lepoint, Peter Schwabe, Gregor Seiler, Damien Stehlé, and Shi Bai.
CRYSTALS-DILITHIUM.
Technical report, National Institute of Standards and Technology, 2022.
available at https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022.


Yang Yu, Huiwen Jia, and Xiaoyun Wang.
Compact lattice gadget and its applications to hash-and-sign signatures.
In Helena Handschuh and Anna Lysyanskaya, editors, *CRYPTO 2023, Part V*, volume 14085 of *LNCS*, pages 390–420. Springer, Cham, August 2023.