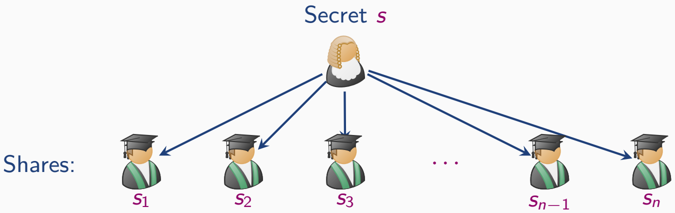
ETH zürich

Physical-bit Leakage Resilience of Linear Code-based Secret Sharing

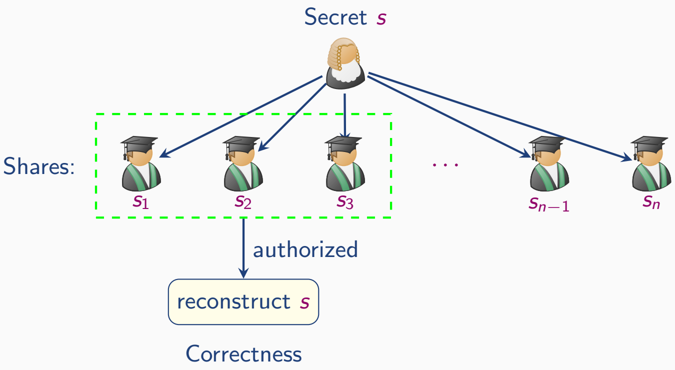
Hai H. Nguyen

EUROCRYPT 2025 - Madrid

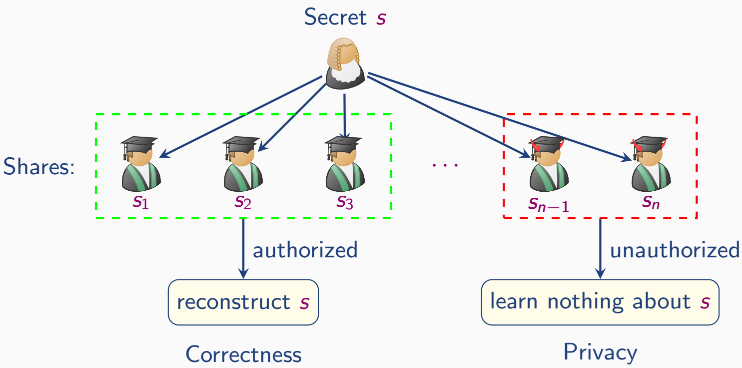
Secret Sharing [Shamir'79, Blakley'79]



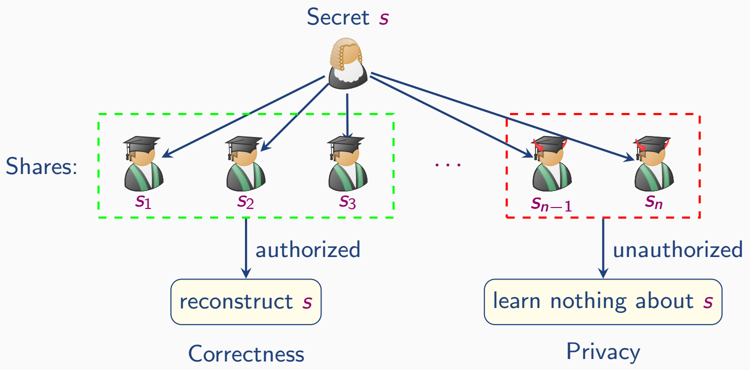
Secret Sharing [Shamir'79, Blakley'79]



Secret Sharing [Shamir'79, Blakley'79]



Secret Sharing [Shamir'79, Blakley'79]



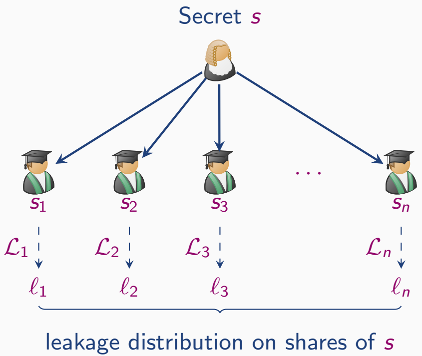
Concern: Side-Channel Attacks

1. Timing attacks, power analysis, Spectre, Meltdown
2. Reveal partial information from every share

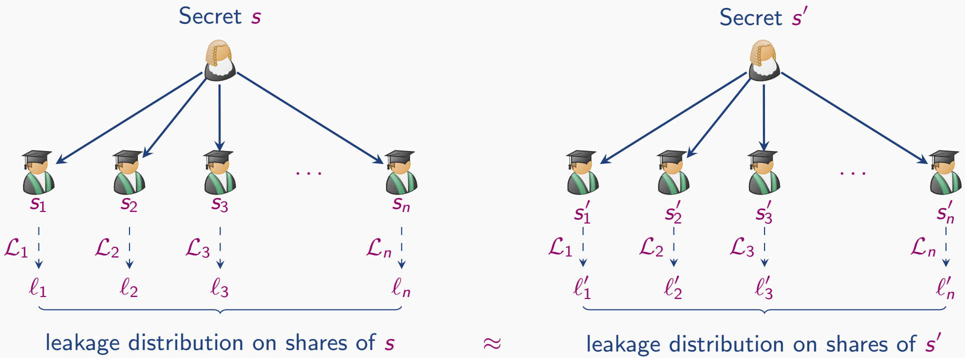
Research Question

Is the cryptographic scheme still secure under these attacks?

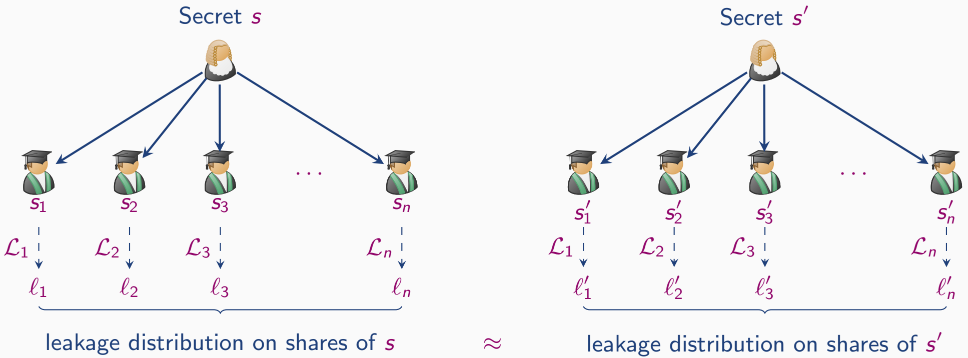
Local Leakage Resilience Secret Sharing [Benhamouda-Degwekar-Ishai-Rabin-18, Goyal-Kumar-18]



Local Leakage Resilience Secret Sharing [Benhamouda-Degwekar-Ishai-Rabin-18, Goyal-Kumar-18]



Local Leakage Resilience Secret Sharing [Benhamouda-Degwekar-Ishai-Rabin-18, Goyal-Kumar-18]



Applications: a useful primitive connected to many other fields

- Repairing error-correcting codes [Guruswami-Wootters-16,...]
- Resilient Secure Computation & Storage [Benhamouda-Degwekar-Ishai-Rabin-18, ...]
- Modular building block for other primitives [Goyal-Kumar-18,...]

Research Objectives

Objectives

Investigate the leakage resilience of linear code-based secret sharing (LCSS).

Why focus on LCSS? Widely used in many applications

What type of leakage? Probing attacks [Ishai-Sahai-Wagner-03]

Research Objectives

Objectives

Investigate the leakage resilience of linear code-based secret sharing (LCSS).

Why focus on LCSS? Widely used in many applications

What type of leakage? Probing attacks [Ishai-Sahai-Wagner-03]

Current State-of-the-Art [Maji-Nguyen-PaskinCherniavsky-Ye-24]

Shamir's schemes over binary extension fields with threshold 2 exhibit a dichotomy against any single-bit probing leakage: either perfectly secure or completely insecure.

Research Objectives

Objectives

Investigate the leakage resilience of linear code-based secret sharing (LCSS).

Why focus on LCSS? Widely used in many applications

What type of leakage? Probing attacks [Ishai-Sahai-Wagner-03]

Current State-of-the-Art [Maji-Nguyen-PaskinCherniavsky-Ye-24]

Shamir's schemes over binary extension fields with threshold 2 exhibit a dichotomy against any single-bit probing leakage: either perfectly secure or completely insecure.

Research Questions

- Is this dichotomy a general phenomenon?
- Can we precisely characterize when each scenario occurs?

Linear Code-based Secret Sharing Schemes

Secret Sharing Based on Linear Code $C \subseteq F^{n+1}$ (for n parties)

To share a secret $s \in F$,

- Sample a random codeword $(s, s_1, s_2, \ldots, s_n) \in C$,
- Distribute share s_i to party i.

Linear Code-based Secret Sharing Schemes

Secret Sharing Based on Linear Code $C \subseteq F^{n+1}$ (for n parties)

To share a secret $s \in F$,

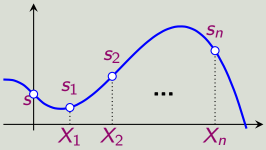
- Sample a random codeword $(s, s_1, s_2, \ldots, s_n) \in C$,
- Distribute share s_i to party i.

Example: Shamir's scheme for n parties and reconstruction threshold k

To share a secret $s \in F$,

1. Pick a random polynomial P:

   $\deg P < k, \;\; P(0) = s$
2. Distribute share $s_i = P(X_i)$ to party i



Code-based perspective. The corresponding linear code C is a Reed-Solomon code generated by

$$\begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ 0 & X_1 & X_2 & \cdots & X_n \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & X_1^{k-1} & X_2^{k-1} & \ldots & X_n^{k-1} \end{pmatrix}$$

Linear Code-based Secret Sharing Schemes

Secret Sharing Based on Linear Code $C \subseteq F^{n+1}$ (for n parties)

To share a secret $s \in F$,

- Sample a random codeword $(s, s_1, s_2, \ldots, s_n) \in C$,
- Distribute share s_i to party i.

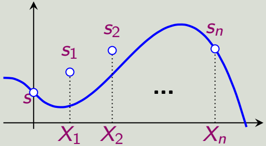
Example: GRS-based construction for n parties and reconstruction threshold k

To share a secret $s \in F$,

1. Pick a random polynomial P:

   $\deg P < k, \;\; P(0) = s$

2. Distribute share $s_i = v_i P(X_i)$ to party i



Code-based perspective. The corresponding linear code C is a GRS code generated by

$$\begin{pmatrix} 1 & v_1 & v_2 & \cdots & v_n \\ 0 & v_1 X_1 & v_2 X_2 & \cdots & v_n X_n \\ \vdots & \vdots & \ddots & \vdots & \\ 0 & v_1 X_1^{k-1} & v_2 X_2^{k-1} & \cdots & v_n X_n^{k-1} \end{pmatrix}$$

Leakage Model: Physical-Bit Leakage

Physical-Bit Leakage

- This work focuses on LCSS over binary extension fields using polynomial representation.
- Field elements in F_{2^λ} are stored as binary strings of length λ using their polynomial coefficients.
- The adversary can leak physical bits (coefficients) directly from the stored shares.

Example

$$\zeta^4 + \zeta + 1 \in \mathbb{F}_{2^5} \quad \Rightarrow \quad (1, 0, 0, 1, 1)$$

Stored as bits in memory:

Most significant $\longleftarrow$ $\boxed{1}\ \boxed{0}\ \boxed{0}\ \boxed{1}\ \boxed{1}$ $\longrightarrow$ Least significant

Adversary can probe bits directly

Our Contributions

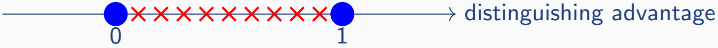
In a Nutshell

1. A dichotomy of leakage resilience
2. A complete characterization of leakage resilience via minimal codewords
3. A highly resilient GRS-based construction

Result I: Dichotomy

Theorem I: Dichotomy

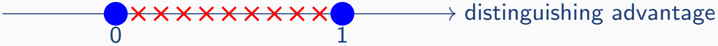
Every LCSS over binary extension fields is perfectly secure or completely insecure against any physical-bit leakage.



Result I: Dichotomy

Theorem I: Dichotomy

Every LCSS over binary extension fields is perfectly secure or completely insecure against any physical-bit leakage.



Comparison with [Maji-Nguyen-PaskinCherniavsky-Ye-24]. Generalizes the dichotomy in all dimensions

1. Shamir's scheme with threshold 2 to any LCSS scheme,
2. 1-bit physical leakage to any physical-bit leakage, no matter how many bits are leaked

Result II: Characterization

Theorem II: Our Characterization

Consider an LCSS based on a linear code C over F_{2^λ}. There is a one-to-one correspondence between

1. a (minimal) physical-bit leakage attack, and
2. a minimal codeword in the dual code of the binary image of C whose first λ coordinates $\neq 0^\lambda$.

Result II: Characterization

Theorem II: Our Characterization

Consider an LCSS based on a linear code C over F_{2^λ}. There is a one-to-one correspondence between

1. a (minimal) physical-bit leakage attack, and
2. a minimal codeword in the dual code of the binary image of C whose first λ coordinates $\neq 0^\lambda$.

Implication. Constructing a high leakage-resilient scheme by designing a code whose binary image's dual code has a large minimum distance

Insight: Generalizes Massey's characterization to leakage scenarios

Massey's characterization: for access structure of an LCSS

A minimal authorized set $\Leftrightarrow$ A minimal codeword in the dual code whose first coordinate is non-zero

Result III: GRS-based Leakage-Resilient Construction

Theorem III: A Monte-Carlo Construction

The LCSS based on $(n+1, k)$-GRS code over F_{2^λ} with randomized multipliers (and arbitrarily fixed evaluation points) is leakage-resilient, with overwhelming probability, when leaking total $(k-1)\lambda$ physical bits across all shares.

Result III: GRS-based Leakage-Resilient Construction

Theorem III: A Monte-Carlo Construction

The LCSS based on $(n+1, k)$-GRS code over F_{2^λ} with randomized multipliers (and arbitrarily fixed evaluation points) is leakage-resilient, with overwhelming probability, when leaking total $(k-1)\lambda$ physical bits across all shares.

Paper	Scheme	Finite field	Total leakage
MNPSW21	Shamir	prime field	$(k-1)\lambda$
MNPY24	Shamir	binary extension	$\frac{1}{2}(k-1)\lambda$
This work	GRS-based	binary extension	$(k-1)\lambda$

Technical Approach for Results I and II: Reduction to a Spanning Problem

Leakage Resilience Problem:

- LCSS based on a linear code $C \subseteq \mathbb{F}_{2^\lambda}^{n+1}$ with dimension k
- $G \in \mathbb{F}_2^{k\lambda \times (n+1)\lambda}$: generator matrix of $\mathcal{C}$ – the binary image of C
- A physical-bit leakage $\vec{\mathcal{L}}$: reveals bit positions $I \subseteq \{\lambda+1, \ldots, (n+1)\lambda\}$
- Question: Is the scheme resilient to $\vec{\mathcal{L}}$?

Technical Approach for Results I and II: Reduction to a Spanning Problem

Leakage Resilience Problem:

- LCSS based on a linear code $C \subseteq \mathbb{F}_{2^\lambda}^{n+1}$ with dimension k
- $G \in \mathbb{F}_2^{k\lambda \times (n+1)\lambda}$: generator matrix of $\mathcal{C}$ – the binary image of C
- A physical-bit leakage $\vec{\mathcal{L}}$: reveals bit positions $I \subseteq \{\lambda+1, \ldots, (n+1)\lambda\}$
- Question: Is the scheme resilient to $\vec{\mathcal{L}}$?

Our Reduction:

$$\mathrm{span}(G_{\mathrm{secret}}) \cap \mathrm{span}(G_i : i \in I) = \{\vec{0}\}?$$

where $G_{\mathrm{secret}} = \{G_1, \ldots, G_\lambda\}$ are the columns corresponding to the secret

Technical Approach for Results I and II: Reduction to a Spanning Problem

Leakage Resilience Problem:

- LCSS based on a linear code $C \subseteq \mathbb{F}_{2^\lambda}^{n+1}$ with dimension k
- $G \in \mathbb{F}_2^{k\lambda \times (n+1)\lambda}$: generator matrix of $\mathcal{C}$ – the binary image of C
- A physical-bit leakage $\vec{\mathcal{L}}$: reveals bit positions $I \subseteq \{\lambda+1, \dots, (n+1)\lambda\}$
- Question: Is the scheme resilient to $\vec{\mathcal{L}}$?

Our Reduction:

$$\mathrm{span}(G_{\mathrm{secret}}) \cap \mathrm{span}(G_i : i \in I) = \{\vec{0}\}?$$

where $G_{\mathrm{secret}} = \{G_1, \dots, G_\lambda\}$ are the columns corresponding to the secret

Implications:

- **Dichotomy:** trivial intersection $\rightarrow$ perfectly secure, non-trivial $\rightarrow$ completely insecure
- **Characterization:**
  - Non-trivial $\Leftrightarrow$ minimal codeword in $\mathcal{C}^\perp$ supported on $\{1, \dots, \lambda\} \cup I$ with nonzero secret part

Technical Approach: GRS-based Leakage-Resilient Construction

High-level Idea: Reduce to bounding the number of solutions to structured systems of equations.

Shamir's Setting: Random Evaluation Points (Multipliers = 1)

Fix $\vec{\alpha} \in F^n$ with at least k non-zero entries. Solve:

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_n \\ X_1^2 & X_2^2 & \cdots & X_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{k-1} & X_2^{k-1} & \cdots & X_n^{k-1} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- How many solutions $\vec{X} \in (F^*)^n$ with distinct X_i?
- Count roots of high-degree curves
- Use a Bézout-type theorem
  Answer: $\leqslant (k/2)! \cdot p^{n-k/2}$

GRS Setting: Random Multipliers (Fixed Evaluation Points)

Fix $\vec{\alpha} \in F^n$ with at least k non-zero entries. Solve:

$$\begin{pmatrix} V_1 x_1 & V_2 x_2 & \cdots & V_n x_n \\ V_1 x_1^2 & V_2 x_2^2 & \cdots & V_n x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ V_1 x_1^{k-1} & V_2 x_2^{k-1} & \cdots & V_n x_n^{k-1} \end{pmatrix} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

- How many solutions $\vec{V} \in (F^*)^n$?
- System is linear in $\vec{V}$
- Use rank-nullity theorem
  Answer: Exactly p^{n-k}

Takeaway: Randomizing multipliers gives us tighter bounds and simpler analysis.

Summary & Open Problems

Takeaways

- A dichotomy of leakage resilience: perfectly secure or completely insecure.
- A complete characterization of leakage resilience via minimal codewords
- A highly resilient GRS-based construction, significantly improving prior schemes

Summary & Open Problems

Takeaways

- A dichotomy of leakage resilience: perfectly secure or completely insecure.
- A complete characterization of leakage resilience via minimal codewords
- A highly resilient GRS-based construction, significantly improving prior schemes

Open Questions

- Derandomization: How to choose a deterministic set of evaluation points?
- More complex and practical leakage families:
  - Hamming weight leakage
  - Noisy leakage
- Breaking the half barrier for local leakage family (when $k/n \leqslant 1/2$)

Summary & Open Problems

Takeaways

- A dichotomy of leakage resilience: perfectly secure or completely insecure.
- A complete characterization of leakage resilience via minimal codewords
- A highly resilient GRS-based construction, significantly improving prior schemes

Open Questions

- Derandomization: How to choose a deterministic set of evaluation points?
- More complex and practical leakage families:
  - Hamming weight leakage
  - Noisy leakage
- Breaking the half barrier for local leakage family (when $k/n \leqslant 1/2$)

Thank you!