Constructing Leakage-resilient Shamir's Secret Sharing: Over Composite Order Fields

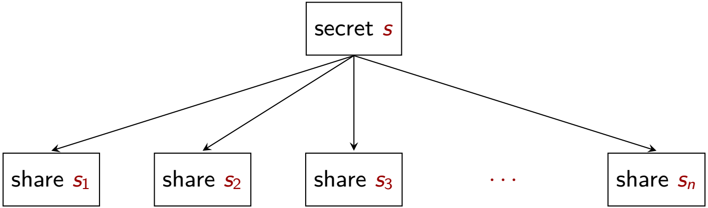
Hemanta K. Maji   Hai H. Nguyen   Anat Paskin-Cherniavsky   Xiuyu Ye

Purdue University   ETH zürich   Ariel University

EUROCRYPT–2024

Threshold Secret Sharing [Shamir, Blakley]

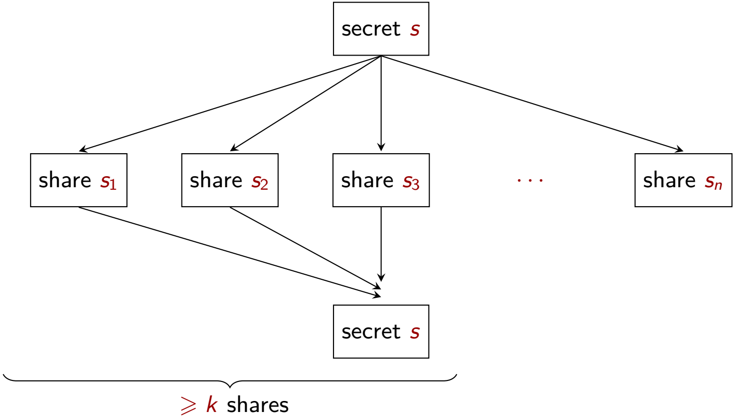
Sharing:



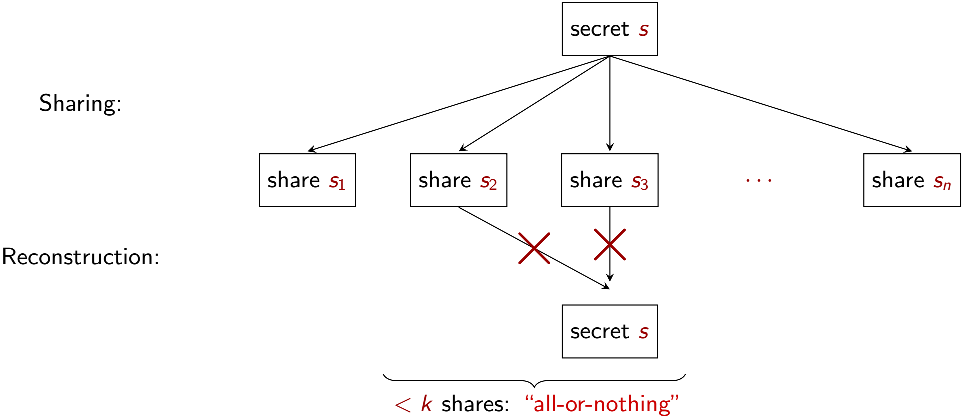
Threshold Secret Sharing [Shamir, Blakley]

Sharing:

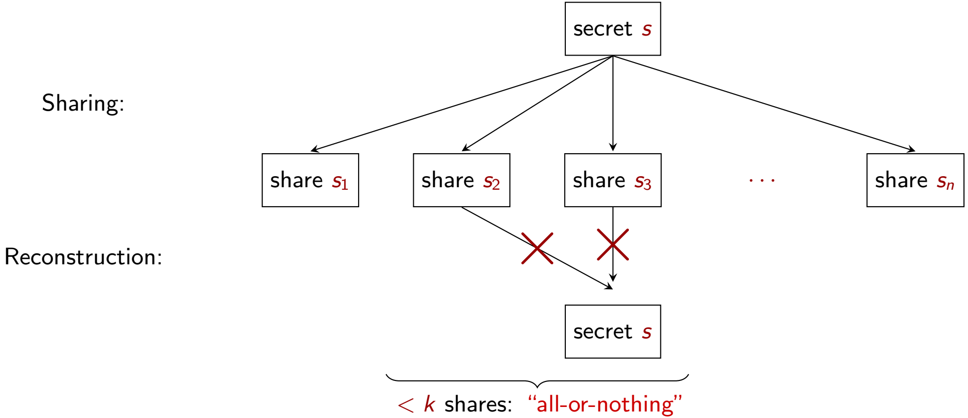
Reconstruction:



Threshold Secret Sharing [Shamir, Blakley]



Threshold Secret Sharing [Shamir, Blakley]

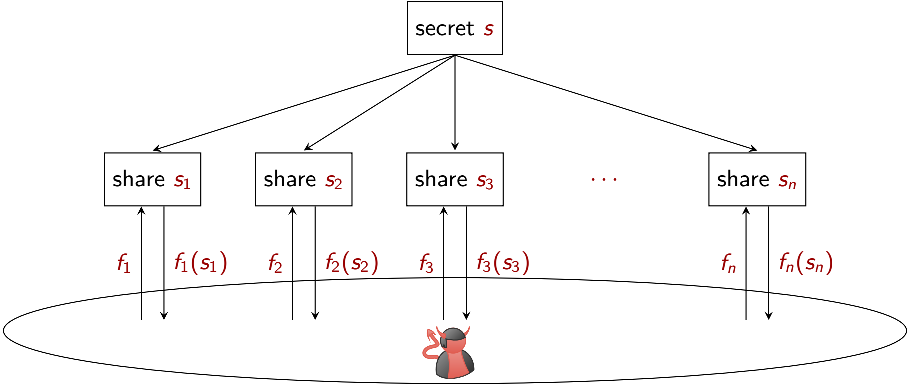


Concern: Side-channel attacks

- "All-or-nothing" no longer true
- Revealing partial or full information from every share

Local Leakage-resilient Secret Sharing

[Benhamouda-Degwekar-Ishai-Rabin-18, Goyal-Kumar-18]



Leakage resilience: Adversary view is essentially uncorrelated with the secret s.

Our Research Problem

Research Question

How to securely instantiate Shamir's scheme against leakage attacks?

Our Research Problem

Research Question

How to securely instantiate Shamir's scheme against leakage attacks?

1. Why Shamir? Because it is everywhere.

Our Research Problem

Research Question

How to securely instantiate Shamir's scheme against leakage attacks?

1. Why Shamir? Because it is everywhere.
2. What leakage? We consider probing attacks [Ishai-Sahai-Wagner-03].

Our Research Problem

Research Question

How to securely instantiate Shamir's scheme against leakage attacks?

1. Why Shamir? Because it is everywhere.
2. What leakage? We consider probing attacks [Ishai-Sahai-Wagner-03].

Current state-of-the-art [Maji-Nguyen-PaskinCherniavsky-Suad-Wang-21]

Shamir's secret sharing over prime fields with random evaluation places is leakage-resilient.

Our Research Problem

Research Question

How to securely instantiate Shamir's scheme against leakage attacks?

1. Why Shamir? Because it is everywhere.
2. What leakage? We consider probing attacks [Ishai-Sahai-Wagner-03].

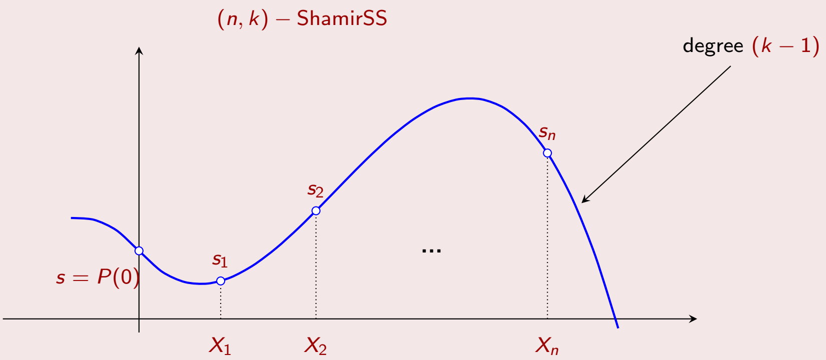
Current state-of-the-art [Maji-Nguyen-PaskinCherniavsky-Suad-Wang-21]

Shamir's secret sharing over prime fields with random evaluation places is leakage-resilient.

Question

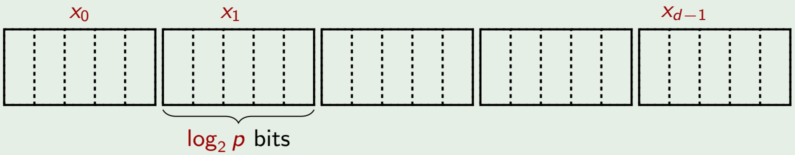
How about composite order fields?

Model: Shamir's Secret Sharing



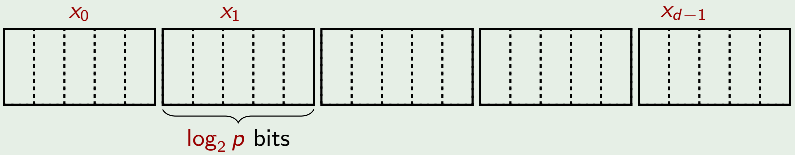
Leakage Model: Physical Bit Probing [Ishai-Sahai-Wagner-03]

Representation of every field element $x \in F_{p^d}$



Leakage Model: Physical Bit Probing [Ishai-Sahai-Wagner-03]

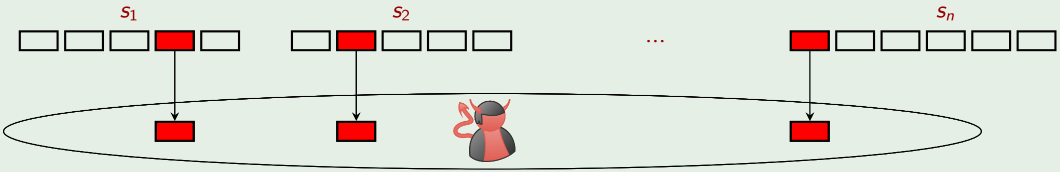
Representation of every field element $x \in F_{p^d}$



Leakage model

The adversary gets physical bits leakage from every share.

Example: single block leakage (a $log_2 p$ physical bits leakage)



Main Result I

Theorem (Randomized construction for composite order fields)

Let $\lambda = d\lceil \log_2 p \rceil$ *be the security parameter.*

If the total leakage $\leqslant \rho(k-1)\lambda$, *where* $\rho = \begin{cases} 1 - 1/p & \text{if } 2 \leqslant p \leqslant k-1, \\ 1 & \text{otherwise,} \end{cases}$

random evaluation places yield leakage-resilient Shamir's scheme.

Main Result I

Theorem (Randomized construction for composite order fields)

Let $\lambda = d\lceil \log_2 p \rceil$ *be the security parameter.*

If the total leakage $\leqslant \rho(k-1)\lambda$, *where* $\rho = \begin{cases} 1 - 1/p & \text{if } 2 \leqslant p \leqslant k-1, \\ 1 & \text{otherwise,} \end{cases}$

random evaluation places yield leakage-resilient Shamir's scheme.

Remarks

Our result holds for any $k \geqslant 2$ and large characteristic-2 fields.

1. Enables leakage-resilient secure computation using GMW-style protocols.

Main Result I

Theorem (Randomized construction for composite order fields)

Let $\lambda = d\lceil \log_2 p \rceil$ *be the security parameter.*

If the total leakage $\leqslant \rho(k-1)\lambda$*, where* $\rho = \begin{cases} 1 - 1/p & \text{if } 2 \leqslant p \leqslant k-1, \\ 1 & \text{otherwise,} \end{cases}$

random evaluation places yield leakage-resilient Shamir's scheme.

Remarks

Our result holds for any $k \geqslant 2$ and large characteristic-2 fields.

1. Enables leakage-resilient secure computation using GMW-style protocols.

Comparison with the result over prime fields [MNPSW-21]

- $\rho = 1$ for prime fields.
- The permissible leakage tolerance may be slightly smaller for composite order fields.

Main Result II

Theorem (Classifying evaluation places: a dichotomy)

Against single block leakage, $(n, 2)$-Shamir's scheme is either perfectly secure or completely insecure.

Main Result II

Theorem (Classifying evaluation places: a dichotomy)

Against single block leakage, $(n, 2)$-Shamir's scheme is either perfectly secure or completely insecure.

Classifying Secure Evaluation Places Algorithm for Single Block Leakages

- **Input:** Distinct evaluation places $X_1, X_2, \ldots, X_n \in F_{p^d}$.
- **Output:** Whether $(n, 2)$-Shamir's secret sharing with evaluation places $X_1, X_2, \ldots, X_n$ are secure.
- **Algorithm:**
  1. Compute the set of shift factors S (of size d).
  2. If exist $\eta_1, \eta_2, \ldots, \eta_n \in S$ such that $X_1\eta_1, X_2\eta_2, \ldots, X_n\eta_n$ are F_p-linearly dependence, then return "insecure".
  3. Otherwise, return "secure".

Main Result II

Theorem (Classifying evaluation places: a dichotomy)

Against single block leakage, $(n, 2)$-Shamir's scheme is either perfectly secure or completely insecure.

Classifying Secure Evaluation Places Algorithm for Single Block Leakages

- **Input:** Distinct evaluation places $X_1, X_2, \ldots, X_n \in F_{p^d}$.
- **Output:** Whether $(n, 2)$-Shamir's secret sharing with evaluation places $X_1, X_2, \ldots, X_n$ are secure.
- **Algorithm:**
  1. Compute the set of shift factors S (of size d).
  2. If exist $\eta_1, \eta_2, \ldots, \eta_n \in S$ such that $X_1\eta_1, X_2\eta_2, \ldots, X_n\eta_n$ are F_p-linearly dependence, then return "insecure".
  3. Otherwise, return "secure".

Comparison with [Hwang-Maji-Nguyen-Ye-24]

- Consider similar problems over Mersenne/Fermat prime fields, one-bit leakage per share.
- Derandomize the construction over prime fields.

Prior Works

Relevant work	Finite Field F	Evaluation Places	Leakage family	Bounds on k
BDIR'18&21	prime	any	local	$k \geqslant 0.85n$
MNPSW'21	prime	random	physical bit	$k \geqslant 2$
MNPW'22	prime	any	local	$k \geqslant 0.78n$
MNPSWYY'22	prime	random	bounded joint	$k > 0.5n$
KK'23	prime	any	local	$k \geqslant 0.69n$
This work	composite	random	physical bit	$k \geqslant 2$

Table 1: Summary of prior works and ours for 1-bit leakage, where $\lambda = \log_2 |F|$.

Technical Overview

Extend the analysis of [MNPSW'21] to composite order fields: Fourier analysis & probabilistic method.

Reductions

1. For any leakage function, for any two secrets, the distinguishing advantage is small over randomly chosen evaluation places.

$$\mathrm{E}_{\vec{X}}\ \mathrm{SD}\left(f(s)\ ,\ f(s')\right) \leqslant \mathrm{E}_{\vec{X}} \sum_{\vec{t}\in\{0,1\}^n} \sum_{\vec{\alpha}\in F^n\setminus\{0\}} \left(\prod_{i=1}^{n} \left|\widehat{\mathbb{1}_{t_i}}(\alpha_i)\right|\right) \cdot \Pr_{\vec{X}}\left[\vec{\alpha} \in C_{\vec{X}}^{\perp}\right] \leqslant \exp(-\Theta(\lambda))$$

2. Applying standard probabilistic techniques (union bound and Markov inequality) yields most evaluation places are secure.

Bound on the Number of Solutions of a System of Equations

System of equations

Fix $\vec{\alpha} \in (F_{p^d}^*)^k$, consider the following system of equations

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_k \\ X_1^2 & X_2^2 & \cdots & X_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^k & X_2^k & \cdots & X_k^k \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \iff \begin{cases} f_1(\vec{X}) = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_k X_k & = 0 \\ f_2(\vec{X}) = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \cdots + \alpha_k X_k^2 & = 0 \\ \vdots \\ f_k(\vec{X}) = \alpha_1 X_1^k + \alpha_2 X_2^k + \cdots + \alpha_k X_k^k & = 0 \end{cases}$$

How many solutions $\vec{X} \in (F_{p^d}^*)^k$ satisfying X_i's are distinct?

Bound on the Number of Solutions of a System of Equations

System of equations

Fix $\vec{\alpha} \in (F_{p^d}^*)^k$, consider the following system of equations

$$\begin{pmatrix} X_1 & X_2 & \cdots & X_k \\ X_1^2 & X_2^2 & \cdots & X_k^2 \\ \vdots & \vdots & \ddots & \vdots \\ X_1^k & X_2^k & \cdots & X_k^k \end{pmatrix} \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_k \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \iff \begin{cases} f_1(\vec{X}) = \alpha_1 X_1 + \alpha_2 X_2 + \cdots + \alpha_k X_k & = 0 \\ f_2(\vec{X}) = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \cdots + \alpha_k X_k^2 & = 0 \\ \vdots \\ f_k(\vec{X}) = \alpha_1 X_1^k + \alpha_2 X_2^k + \cdots + \alpha_k X_k^k & = 0 \end{cases}$$

How many solutions $\vec{X} \in (F_{p^d}^*)^k$ satisfying X_i's are distinct?

Bound on the number of solutions

- Employ a contemporary Bézout-like theorem over composite order fields [Bafna-Sudan-Velusamy-Xiang-21].
  - Maji et al. used [Wooley-96] result for prime fields.
- Subtlety arises for composite order fields
  - A naive analysis would not work.

Bézout-like Theorems

Definition

Consider $f_i \in F_{p^d}[X_1, X_2, \ldots, X_k]$ of degree d_i for $1 \leqslant i \leqslant k$.
An $\vec{a} \in F_{p^d}^k$ is an *isolated zero* of the square system $\vec{f} = \vec{0}$, if $\vec{f}(\vec{a}) = \vec{0}$ but $J(\vec{f}; \vec{a}) \neq 0$.

Jacobian

$$J(\vec{f}) = \det \left(\frac{\partial f_j}{\partial X_i} \right)_{i,j \in \{1,2,\ldots,k\}} \in F_{p^d}[X_1, X_2, \ldots, X_k].$$

Theorem ([Wooley'96] for prime fields, [Zhao'12,BZXV'21] for composite order fields)

The number of isolated zeroes of the system of equations $\vec{f} = \vec{0}$ *is at most* $d_1 \cdot d_2 \cdots d_k$.

How the proof in [MNPSY'21] works?

Consider $k = 3$, $\vec{\alpha} = \vec{1}$, and a prime field F_p with large p.

$$J(\vec{f}) = \det \begin{pmatrix} 1 & 1 & 1 \\ 2X_1 & 2X_2 & 2X_3 \\ 3X_1^2 & 3X_2^2 & 3X_3^2 \end{pmatrix} = 6(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$$

$J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct. So #solutions = #isolated zeroes.

Illustrating Examples

How the proof in [MNPSY'21] works?

Consider $k = 3$, $\vec{\alpha} = \vec{1}$, and a prime field F_p with large p.

$$J(\vec{f}) = \det \begin{pmatrix} 1 & 1 & 1 \\ 2X_1 & 2X_2 & 2X_3 \\ 3X_1^2 & 3X_2^2 & 3X_3^2 \end{pmatrix} = 6(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$$

$J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct. So #solutions = #isolated zeroes.

Over composite order fields

1. When $p > k = 3$, the same idea works since $J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct.
2. When $p = 2$, the same analysis does not work since $J(\vec{f}, \vec{a}) = 0$ for every $\vec{a}$.

Illustrating Examples

How the proof in [MNPSY'21] works?

Consider $k = 3$, $\vec{\alpha} = \vec{1}$, and a prime field F_p with large p.

$$J(\vec{f}) = \det \begin{pmatrix} 1 & 1 & 1 \\ 2X_1 & 2X_2 & 2X_3 \\ 3X_1^2 & 3X_2^2 & 3X_3^2 \end{pmatrix} = 6(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$$

$J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct. So $\#$solutions $= \#$isolated zeroes.

Over composite order fields

1. When $p > k = 3$, the same idea works since $J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct.
2. When $p = 2$, the same analysis does not work since $J(\vec{f}, \vec{a}) = 0$ for every $\vec{a}$.

Our solution when $p = 2$

1. Remove equation with even power
2. Fix X_3 arbitrarily, consider a new system $g_1 = X_1 + X_2 + c_1$, and $g_2 = X_1^3 + X_2^3 + c_2$.

$$J(\vec{g}) = \det \begin{pmatrix} 1 & 1 \\ 3X_1^2 & 3X_2^2 \end{pmatrix} = 3(X_1 - X_2)(X_1 + X_2) = 3(X_1 - X_2)^2$$

Illustrating Examples

How the proof in [MNPSY'21] works?

Consider $k = 3$, $\vec{\alpha} = \vec{1}$, and a prime field F_p with large p.

$$J(\vec{f}) = \det \begin{pmatrix} 1 & 1 & 1 \\ 2X_1 & 2X_2 & 2X_3 \\ 3X_1^2 & 3X_2^2 & 3X_3^2 \end{pmatrix} = 6(X_1 - X_2)(X_2 - X_3)(X_3 - X_1)$$

$J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct. So #solutions = #isolated zeroes.

Over composite order fields

1. When $p > k = 3$, the same idea works since $J(\vec{f}, \vec{X}) \neq 0$ iff X_i's are distinct.
2. When $p = 2$, the same analysis does not work since $J(\vec{f}, \vec{a}) = 0$ for every $\vec{a}$.

What if $p = 3$?

1. $J(\vec{g}, \vec{X}) = 0$ iff $X_1 = X_2$ or $X_1 + X_2 = 0$ – a new and unexpected way of making Jacobian zero.
2. $J(\vec{g})$ is a *generalized Vandermonde determinant*. We prove that the number of zeroes is small.
   - Identifying their zeroes is an open research problem in Mathematics.

Summary

Theorem (Randomized construction for composite order fields)

Random evaluation places yield leakage-resilient Shamir's scheme.

Theorem (Classifying evaluation places: a dichotomy)

1. *Against single block leakage, $(n, 2)$-Shamir is either perfectly secure or completely insecure.*
2. *Given evaluation places $(X_1, X_2, \ldots, X_n)$, our algorithm classifies them as secure or not.*

Summary

Theorem (Randomized construction for composite order fields)

Random evaluation places yield leakage-resilient Shamir's scheme.

Theorem (Classifying evaluation places: a dichotomy)

1. *Against single block leakage, $(n, 2)$-Shamir is either perfectly secure or completely insecure.*
2. *Given evaluation places $(X_1, X_2, \ldots, X_n)$, our algorithm classifies them as secure or not.*

Thank you!