Leakage-resilience of Shamir Secret-Sharing

Hemanta K. Maji

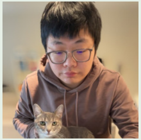
PURDUE UNIVERSITY

February 19, 2023

Co-authors: Purdue University

1. Hai H. Nguyen[G] (currently in post-doc market)

2. Mingyuan Wang[G] (currently a post-doc at UC-Berkeley)

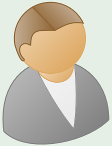


3. Xiuyu Ye[G]

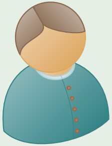
Co-authors: Purdue University

1. Albert Yu[G]

2. Donald Q. Adams[U]



3. Minh L. Nguyen[U]



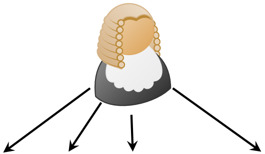
Co-authors: Ariel University

1. Anat Paskin-Cherniavsky

2. Tom Suad[G]

Secret-sharing Scheme

Secret s



Secret Shares: s_1 s_2 s_3 $\cdots$ s_n

Adversary Model

Obtains the secret shares of some subset of parties

Guarantees

1. If the subset is *authorized*: Reconstruct the secret
2. If the subset is *unauthorized*: Obtain no additional information about the secret

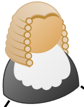
Numerous Applications in Cryptography & Distributed Computing

Threshold cryptography, Access control, and Secure storage & computation [Beimel–2011]

Local Leakage-resilience of Secret-sharing Schemes

[Benhamouda-Degwekar-Ishai-Rabin (CRYPTO–2018), Goyal-Kumar (STOC–2018)]

Secret s



Secret Shares: s_1 s_2 s_3 $\cdots$ s_n

$\mathcal{L}_1$ $\mathcal{L}_2$ $\mathcal{L}_3$ $\mathcal{L}_n$

ℓ_1 ℓ_2 ℓ_3 ℓ_n

Adversary Model

Obtains leakage $(\mathcal{L}_1, \mathcal{L}_2, \dots, \mathcal{L}_n)$ from secret shares $(s_1, s_2, \dots, s_n)$ respectively

Guarantees & Threat Assessment

1. Security: *Leakage (joint distribution) is independent* of the secret
2. Threat: *Advantage in distinguishing two secrets* using the leakage

Applications & Objectives

Useful Primitive

- (Connected to) Repairing error-correcting codes [Guruswami-Wootters (STOC 2016), Tamo-Ye-Barg (FOCS–2017), Guruswami-Rawat (SODA–2017)]
- Resilient Secure Computation & Storage [Benhamouda-Degwekar-Ishai-Rabin (CRYPTO–2018)]
- Modularly build other primitives (e.g., non-malleable secret-sharing) [Goyal-Kumar (STOC–2018), Srinivasan-Vasudevan (CRYPTO-2019)]

Applications & Objectives

Useful Primitive

- (Connected to) Repairing error-correcting codes [Guruswami-Wootters (STOC 2016), Tamo-Ye-Barg (FOCS–2017), Guruswami-Rawat (SODA–2017)]
- Resilient Secure Computation & Storage [Benhamouda-Degwekar-Ishai-Rabin (CRYPTO–2018)]
- Modularly build other primitives (e.g., non-malleable secret-sharing) [Goyal-Kumar (STOC–2018), Srinivasan-Vasudevan (CRYPTO-2019)]

Research Objective: Security & Threat Assessment

- Determine security threats
- Recommendations to make secret-sharing schemes more secure

Existing Literature

Construct new Secret-sharing Schemes

[Aggarwal-Damgård-Nielsen-Obremski-Purwanto-Ribeiro-Simkin (CRYPTO–2019), Srinivasan-Vasudevan (CRYPTO-2019), Kumar-Meka-Sahai (FOCS–2019), Chattopadhyay-Goodman-Goyal-Kumar-Li-Meka-Zuckerman (FOCS–2020)]

- Usually incurs significant overheads
- Loses algebraic structure (e.g., linearity and multiplication friendliness)

Existing Literature

Construct new Secret-sharing Schemes

[Aggarwal-Damgård-Nielsen-Obremski-Purwanto-Ribeiro-Simkin (CRYPTO–2019), Srinivasan-Vasudevan (CRYPTO-2019), Kumar-Meka-Sahai (FOCS–2019), Chattopadhyay-Goodman-Goyal-Kumar-Li-Meka-Zuckerman (FOCS–2020)]

- Usually incurs significant overheads
- Loses algebraic structure (e.g., linearity and multiplication friendliness)

Study Resilience of Prominent Secret-sharing Schemes

[Benhamouda-Degkewar-Ishai-Rabin (CRYPTO–2018), Nielsen-Simkin (EUROCRYPT–2020), Maji-Nguyen-PaskinCherniavsky-Suad-Wang (EUROCRYPT–2021), Maji-PaskinCherniavsky-Suad-Wang (CRYPTO–2021), Adams-Maji-Nguyen-Nguyen-PaskinCherniavsky-Suad-Wang (ISIT–2021), Maji-Nguyen-PaskinCherniavsky-Suad-Wang-Ye-Yu (TCC–2022), Maji-Nguyen-PaskinCherniavsky-Suad-Wang-Ye-Yu (ITC–2022), Maji-Nguyen-PaskinCherniavsky-Wang (ISIT–2022), Maji-Nguyen-PaskinCherniavsky-Yu (draft)]

- Significant impact on real-world security

Interesting Secret-sharing Schemes

Additive Secret-sharing Scheme (for n parties)

- Secret: $s \in F$
- Secret Shares: Random $(s_1, s_2, \ldots, s_n)$ conditioned on $s_1 + s_2 + \cdots + s_n = s$

Interesting Secret-sharing Schemes

Additive Secret-sharing Scheme (for n parties)

- Secret: $s \in F$
- Secret Shares: Random $(s_1, s_2, \dots, s_n)$ conditioned on $s_1 + s_2 + \cdots + s_n = s$

Shamir's Secret-sharing Scheme (for n parties & reconstruction threshold k)

- Secret: $s \in F$
- Secret Shares
    1. Pick a random F-polynomial $P(Z)$ such that: $\deg P < k$ and $P(0) = s$
    2. Pick arbitrary distinct evaluation places $X_1, X_2, \dots, X_n \in (F^*)^n$
    3. Define $s_1 = P(X_1)$, $s_2 = P(X_2)$, $\dots$, and $s_n = P(X_n)$

Interesting Secret-sharing Schemes

Additive Secret-sharing Scheme (for n parties)

- Secret: $s \in F$
- Secret Shares: Random $(s_1, s_2, \ldots, s_n)$ conditioned on $s_1 + s_2 + \cdots + s_n = s$

Shamir's Secret-sharing Scheme (for n parties & reconstruction threshold k)

- Secret: $s \in F$
- Secret Shares
  1. Pick a random F-polynomial $P(Z)$ such that: $\deg P < k$ and $P(0) = s$
  2. Pick arbitrary distinct evaluation places $X_1, X_2, \ldots, X_n \in (F^*)^n$
  3. Define $s_1 = P(X_1)$, $s_2 = P(X_2)$, $\ldots$, and $s_n = P(X_n)$

Research Objective

Determine the leakage resilience of these secret-sharing schemes

A Threat: Repairing Reed-Solomon Codes

Problem Definition

- Let $P(Z)$ be a random F-polynomial with $\deg P < k$
- Given: $(P(1), P(2), P(3), \ldots, P(|F^*|))$
- Objective: Recover $P(0)$

A Threat: Repairing Reed-Solomon Codes

Problem Definition

- Let $P(Z)$ be a random F-polynomial with $\deg P < k$
- Given: $(P(1), P(2), P(3), \ldots, P(|F^*|))$
- Objective: Recover $P(0)$

Traditional Strategy

1. Fetch $P(X_1), P(X_2), \ldots, P(X_k)$, for distinct evaluation places $X_1, X_2, \ldots, X_k \in F^*$
2. Use Lagrange Interpolation to reconstruct the polynomial $P(Z)$ and compute $P(0)$

A Threat: Repairing Reed-Solomon Codes

Problem Definition

- Let $P(Z)$ be a random F-polynomial with $\deg P < k$
- Given: $(P(1), P(2), P(3), \ldots, P(|F^*|))$
- Objective: Recover $P(0)$

Traditional Strategy

1. Fetch $P(X_1), P(X_2), \ldots, P(X_k)$, for distinct evaluation places $X_1, X_2, \ldots, X_k \in F^*$
2. Use Lagrange Interpolation to reconstruct the polynomial $P(Z)$ and compute $P(0)$

New Strategy [Guruswami-Wootters (STOC–2016)]

$$
\begin{tikzcd}
P(1) \arrow[d, dashed, "\mathcal{L}_1"] & P(2) \arrow[d, dashed, "\mathcal{L}_2"] & P(3) \arrow[d, dashed, "\mathcal{L}_3"] & \cdots & P(|F^*|) \arrow[d, dashed, "\mathcal{L}_{|F^*|}"] \\
\ell_1 \arrow[drr, dashed] & \ell_2 \arrow[dr, dashed] & \ell_3 \arrow[d, dashed] & & \ell_{|F^*|} \arrow[dll, dashed] \\
 & & s & &
\end{tikzcd}
$$

Research Questions

Security against Leakage Attacks

How to choose the Modulus and Evaluation Places of Shamir's Secret-sharing Scheme?

Definition: Leakage Resilience against a Leakage Family

1. For any leakage attack $\vec{\mathcal{L}}$ in the leakage family
2. For any two secrets s and s'
3. Advantage of distinguishing the secrets (using the leakage from the secret shares) is small

Research Questions

Security against Leakage Attacks

How to choose the Modulus and Evaluation Places of Shamir's Secret-sharing Scheme?

Definition: Leakage Resilience against a Leakage Family

1. For any leakage attack $\vec{\mathcal{L}}$ in the leakage family
2. For any two secrets s and s'
3. Advantage of distinguishing the secrets (using the leakage from the secret shares) is small

Threat posed by a Leakage Family

Give a leakage attack (in the family) that distinguishes two secrets with a significant advantage

Our Results: Leakage Model (Covered in Today's Talk)

Physical Bit Leakage [Ishai-Sahai-Wagner (CRYPTO–2003)]

- Field elements are stored in their binary representation
- Adversary can leak physical bits from the stored secret shares

Notation

- Security Parameter: Bit-length of the Secret Shares (represented by λ)

An Example

- Suppose $F = F_{31} = \{0, 1, 2, \ldots, 30\}$
- $\lambda = 5$
- For example, $6 = (00110)_2, \qquad 19 = (10011)_2.$

Remark

Entropy of Shamir's Secret-sharing Scheme: $k \cdot \lambda$ (roughly)

Our Results covered in Today's Talk: Security & Threat Assessment

Theorem (Monte-Carlo Construction)

Consider Shamir's Secret-sharing Scheme with random evaluation places. If the total leakage $m \cdot n$ *is less than the entropy* $k \cdot \lambda$*, then this scheme is resilient to* m *bit local leakage resilient from every secret share;* except *with* $\exp(-(k-1) \cdot \lambda)$ *probability*

Our Results covered in Today's Talk: Security & Threat Assessment

Theorem (Monte-Carlo Construction)

Consider Shamir's Secret-sharing Scheme with random evaluation places. If the total leakage $m \cdot n$ *is less than the entropy* $k \cdot \lambda$*, then this scheme is resilient to* m *bit local leakage resilient from every secret share;* except *with* $\exp(-(k-1)\cdot\lambda)$ *probability*

Theorem (Threat Assessment: Parity-of-Parity Attack)

If one is careless in choosing the modulus and evaluation places, then there is an attack that leaks one physical bit from each secret share and can distinguish two secrets with advantage $\geqslant (2/\pi)^k$

Our Results covered in Today's Talk: Security & Threat Assessment

Theorem (Monte-Carlo Construction)

Consider Shamir's Secret-sharing Scheme with random evaluation places. If the total leakage $m \cdot n$ *is less than the entropy* $k \cdot \lambda$, *then this scheme is resilient to* m *bit local leakage resilient from every secret share;* except *with* $\exp(-(k-1) \cdot \lambda)$ *probability*

Theorem (Threat Assessment: Parity-of-Parity Attack)

If one is careless in choosing the modulus and evaluation places, then there is an attack that leaks one physical bit from each secret share and can distinguish two secrets with advantage $\geqslant (2/\pi)^k$

Theorem (A Full Derandomization: Modulus Choice & Evaluation Places Recommendation)

Choose p *a Mersenne prime. Consider evaluation places* X_1, X_2 *satisfying* $X_2/X_1 = (0 \cdots 0 \underbrace{1 \cdots 1}_{\lambda/2\text{-bits}})_2$. *Then the corresponding* $[n = 2, k = 2]$ *Shamir's Secret-sharing Scheme is* $1/\sqrt{p}$ *leakage resilient against* $m = 1$ *physical bit leakage from each secret share*

Result 1: Leakage-resilience of Shamir Secret-sharing Scheme

Parameter Setting

1. Fix a constant $0 < d < \ln 2$
2. Choose number of parties n and the reconstruction threshold $k \geqslant 2$
3. Set insecurity tolerance $\varepsilon = 2^{-t}$
4. For all $\lambda > \lambda_0 := (t/k)\ln(t/k)$ and $m \leqslant k\lambda/n \ln^2 \lambda$

Randomized Shamir's Secret-sharing Scheme Construction

- Let F be a prime field such that $2^{\lambda-1} \leqslant |F| < 2^{\lambda}$
- Choose random and distinct evaluation places $X_1, X_2, \ldots, X_n \in F^*$
- Consider the corresponding $[n, k]$ Shamir's Secret-sharing Scheme over the field F

Leakage Family

Leak arbitrary m physical bits from every secret share

Monte Carlo Construction's Security

With probability $1 - \exp(-d \cdot (k-1) \cdot \lambda)$ over the the choice of the evaluation places, the resulting Shamir's secret-sharing scheme is resilient to the Leakage Family (within the security tolerance ε)

Technical Approach and Challenges

Proceeds via a Fourier-analytic Approach

Problem A: Understanding the Leakage Family

A tight estimation of an exponential sum of the form

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_S(\alpha)} \right|,$$

where (for a leakage function $f \colon F \to \{0,1\}$) $F \supseteq S := f^{-1}(0)$.

For example, if $f = \mathsf{LSB}$ (least significant bit) then $S = \{0, 2, 4, \ldots, p-1\}$ (for odd prime p)

Technical Approach and Challenges

Proceeds via a Fourier-analytic Approach

Problem A: Understanding the Leakage Family

A tight estimation of an exponential sum of the form

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_S(\alpha)} \right|,$$

where (for a leakage function $f\colon F \to \{0,1\}$) $F \supseteq S := f^{-1}(0)$.

For example, if $f = \mathsf{LSB}$ (least significant bit) then $S = \{0, 2, 4, \ldots, p-1\}$ (for odd prime p)

Problem B: Understanding the Secret-sharing Scheme

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

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

How many solutions $\vec{X} \in (F^*)^n$ exist of the equation above, such that $i \neq j \implies X_i \neq X_j$?

Tight Estimation of an Exponential Sum

Remark

- Suppose $f = \mathsf{LSB}$. Then, $S = f^{-1}(0) = \{0, 2, 4, \ldots, p-1\} \subseteq F$
- Observe S is an Arithmetic Progression – A set of the form $a + \Delta_1 \cdot b$
- Rank-2 Arithmetic Progression: A set of the form $a + \Delta_1 \cdot b + \Delta_2 \cdot c$. For example, the set $\{8, 9, 12, 13\}$
- If f is a physical bit leakage, then $f^{-1}(0)$ is
  "The union of a small number of Rank-2 Arithmetic Progressions"

For such sets, we prove the following "pseudorandomness property"

$$\sum_{\alpha \in F} \left| \widehat{\mathbb{1}_S}(\alpha) \right| \lesssim (1/\pi^2) \cdot \ln^3 \lambda$$

Estimate the Number of Solutions to a System of Equations

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

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

How many solutions $\vec{X} \in (F^*)^n$ exist of the equation above, such that $i \neq j \implies X_i \neq X_j$?

Our Approach

- Bézout's Theorem
- Upper bounds the number of solutions to (roughly) $k! \cdot p^{n-k}$

Result 2: Attack on Shamir's Secret-sharing Scheme

Parameter Setting

1. Suppose $p = 1 \mod k$ (that is, k divides $(p-1)$)
2. Let $\Omega := \{\omega, \omega^2, \ldots, \omega^k = 1\} \subseteq F^*$ be the solutions of the equation $Z^k - 1 = 0$
3. Vulnerable Evaluation Places: F^*/Ω

Attack on Careless Modulus and Evaluation Places Choice

Suppose $\{X_1, X_2, \ldots, X_n\}$ contains $\{\rho\omega, \rho\omega^2, \ldots, \rho\omega^k\}$ (for some $\rho \in F^*$). Then, one can leak every secret share's LSB to distinguish two secrets with $(2/\pi)^k$ advantage

Careless Evaluation Place Choice leads to Additive Secret-sharing Scheme

- Assume $p = 1 \mod k$
- Let $\{\omega, \omega^2, \ldots, \omega^k = 1\} \subseteq F^*$ be roots of the equation $Z^k - 1 = 0$
- Suppose $P(Z) = p_0 + p_1 Z + p_2 Z^2 + \cdots + p_{k-1} Z^{k-1}$ such that $p_0 = s$
- Suppose $X_1 = \rho\omega$, $X_2 = \rho\omega^2$, $\ldots$, $X_k = \rho\omega^k$, where $\rho \in F^*$

Observation

$$s_1 + s_2 + \cdots + s_k = \sum_{i=1}^{k} P(X_i) = ks$$

Proof Intuition

$$\begin{array}{llllll}
P(X_1) & = p_0 & + p_1\rho \cdot \left(\omega^1\right) & + p_2\rho^2 \cdot \left(\omega^1\right)^2 & \cdots & + p_{k-1}\rho^{k-1} \cdot \left(\omega^1\right)^{k-1} \\
P(X_2) & = p_0 & + p_1\rho \cdot \left(\omega^2\right) & + p_2\rho^2 \cdot \left(\omega^2\right)^2 & \cdots & + p_{k-1}\rho^{k-1} \cdot \left(\omega^2\right)^{k-1} \\
\vdots & & & & & \\
P(X_k) & = p_0 & + p_1\rho \cdot \left(\omega^k\right) & + p_2\rho^2 \cdot \left(\omega^k\right)^2 & \cdots & + p_{k-1}\rho^{k-1} \cdot \left(\omega^k\right)^{k-1}
\end{array}$$

Our Physical Bit Attack: The Parity-of-Parity Attack

- Consider the Additive Secret-sharing Scheme: Random secret shares $s_1, s_2, \ldots, s_k$ such that $s_1 + s_2 + \cdots + s_k = s$
- For $i \in \{1, 2, \ldots, k\}$, let ℓ_i represent whether the secret share s_i is odd or not
  - $\ell_i = 0 \iff s_i \in \{0, 2, 4, \ldots, p-1\}$
  - $\ell_i = 1 \iff s_i \in \{1, 3, 5, \ldots, p-3\}$

Parity of Parity Attack

Distinguisher outputs

$$\ell_1 \oplus \ell_2 \oplus \cdots \oplus \ell_k$$

Remark

The distinguisher does not “predict” the parity of the secret to be $\ell_1 \oplus \ell_2 \oplus \cdots \oplus \ell_k$

An Example: Additive Secret-sharing Scheme with $n = k = 2$

$s = 0$	(s_1, s_2)	$(0,0)$	$(1, p-1)$	$(2, p-2)$	$\cdots$	$(p-1, 1)$
	(ℓ_1, ℓ_2)	$(0,0)$	$(1,0)$	$(0,1)$	$\cdots$	$(0,1)$
	$\ell_1 \oplus \ell_2$	0	1	1	$\cdots$	1
$s = 1$	(s_1, s_2)	$(0,1)$	$(1,0)$	$(2, p-1)$	$\cdots$	$(p-1, 2)$
	(ℓ_1, ℓ_2)	$(0,1)$	$(1,0)$	$(0,0)$	$\cdots$	$(0,0)$
	$\ell_1 \oplus \ell_2$	1	1	0	$\cdots$	0

Distinguisher Behavior

- For $s = 0$, our distinguisher outputs 1 with probability $1 - 1/p$
- For $s = 1$, our distinguisher outputs 1 with probability $2/p$

Technical Problem: Discrepancy of Irwin-Hall Distribution

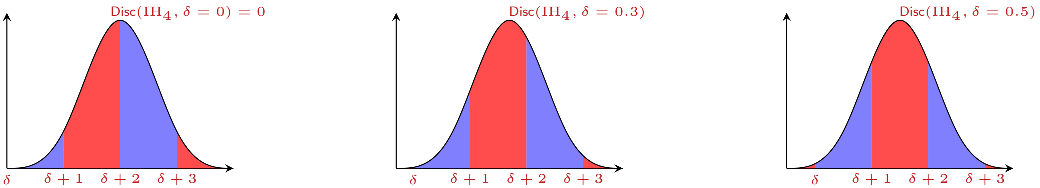
Definition (Irwin-Hall Distribution)

For $i \in \{1, 2, \dots\}$, the IH_i is the probability distribution over the sample space $[0, i)$ recursively defined as follows.

1. IH_1 is the uniform distribution over the sample space $[0, 1)$
2. For $i \geqslant 2$, the distribution IH_i is (the convolution) $\mathrm{IH}_{i-1} + \mathrm{IH}_1$

Definition (Discrepancy of a Probability Distribution)

$$\mathrm{disc}(\mathrm{IH}_i, \delta) := \left| \mathop{\mathbb{E}}_{x \sim \mathrm{IH}_i} \left[(-1)^{\lfloor x - \delta \rfloor} \right] \right| \qquad \mathrm{disc}(\mathrm{IH}_i) := \max_{\delta \in [0,1)} \mathrm{disc}(\mathrm{IH}_i, \delta)$$



Our Approach: Estimating an Exponential Sum

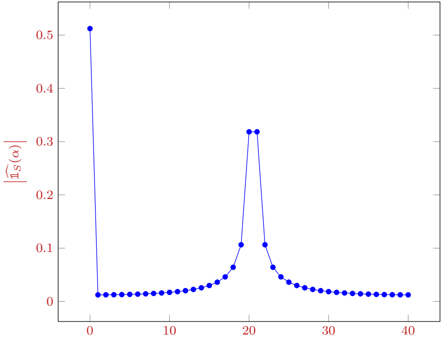
Recall: Connection to Distinguishing Advantage

$\mathrm{disc}(\mathrm{IH}_{k-1})$ is the distinguishing advantage of the Parity-of-Parity Distinguisher against the Additive Secret-sharing Scheme for $n = k$ parties.

Discrepancy Estimation

$$\mathrm{disc}(\mathrm{IH}_i) \geqslant (2/\pi)^i$$

Near-optimal [Benhamouda-Degkewar-Ishai-Rabin (CRYPTO–2018)]



Result 3: Derandomization – Modulus & Evaluation Places Recommendations

Parameter Setting

- Let p be a λ-bit Mersenne prime (For example, 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, etc.)
- F be the field of order p
- Let $n = k = 2$
- Let $X_1, X_2 \in F^*$, define $m = X_2/X_1$
- Suppose $(0 \cdots 0 \underbrace{1 \cdots 1}_{\lambda/2\text{-bits}})_2 \in \{m, -m, m^{-1}, -m^{-1}\}$

Leakage Family

Leak one physical bit from every secret share

A Full Derandomization

The corresponding $[n = 2, k = 2]$ Shamir's Secret-sharing Scheme is leakage resilient. Leakage attacks have a distinguishing advantage at most $1/\sqrt{p}$.

Remark

In general, extends to $n = k$ Shamir's Secret-sharing Scheme – achieving security (roughly) $(1/\sqrt{p})^{n/2}$

Technical Approach

Security against LSB Attacks

Consider an $[n = 2, k = 2]$ Shamir's Secret-sharing Scheme with evaluation places X_1 and X_2. Define $m = X_2/X_1$. Define $\varepsilon_{\mathsf{LSB}}(m)$ as the distinguishing advantage of the LSB leakage attack

Reduction to LSB Leakage

- Fix a Mersenne prime p
- Suppose an $[n = 2, k = 2]$ Shamir's Secret-sharing Scheme is leakage resilient to arbitrary physical bit attacks with distinguishing advantage ε
- Then, the following fact holds

$$\varepsilon = \max\left\{\varepsilon_{\mathsf{LSB}}(m), \varepsilon_{\mathsf{LSB}}(2 \cdot m), \varepsilon_{\mathsf{LSB}}(2^2 \cdot m), \dots, \varepsilon_{\mathsf{LSB}}(2^{\lambda-1} \cdot m)\right\}$$

What Remains

Develop a technique to determine whether $\varepsilon_{\mathsf{LSB}}(m)$ is small or not

Technical Problem Statement

We proceed via a Fourier-analytic approach and Identify interesting Combinatorial problems

Positive Set of Elements & Sign of Field Elements

Define the set of positive elements
$$P = \{0, 1, \ldots, (p-1)/2\}$$

Let $\mathrm{sgn}\colon F \to \{-1, +1\}$ defined below
$$\mathrm{sgn}(x) = \begin{cases} +1, & x \in P \\ -1, & \text{otherwise.} \end{cases}$$

(Nearly) Orthogonal and Pair-wise Orthogonal Functions

- Let $f, g\colon F \to \{-1, +1\}$ defined by $f(X) = \mathrm{sgn}(X)$ and $g(X) = \mathrm{sgn}(m \cdot X)$, where $m \in F^*$
- Our objective is to determine whether
$$\sum_{x \in F} f(x) \cdot g(x) \in [-\varepsilon \cdot p, \varepsilon \cdot p]$$

Connection?

Consider an $[n = 2, k = 2]$ Shamir Secret-sharing Scheme with evaluation places X_1 and X_2, satisfying $X_2/X_1 = m$. Then, $\varepsilon_{\mathsf{LSB}}(m) \leqslant \varepsilon$

Intuition of our Solution Strategy

Objective

For the interval P, we show that

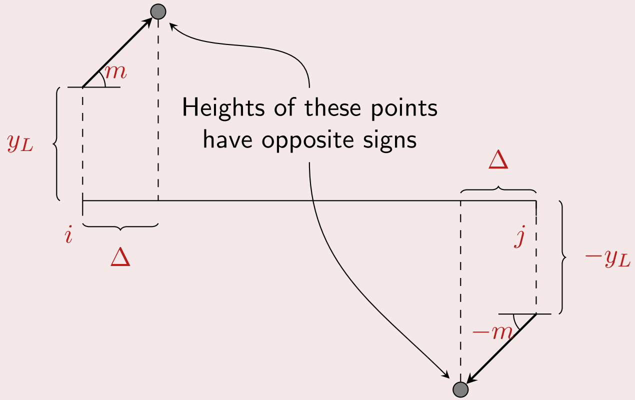
$$\sum_{x \in P} g(x) \in [-\varepsilon \cdot p, \varepsilon \cdot p],$$

where $g(X) = \mathrm{sgn}(m \cdot X)$

Solution Strategy

1. Consider the interval $P = \{0, 1, \ldots, (p-1)/2\}$
2. Suppose the height of the line $Y = m \cdot X$ is "close" at the end points of this interval
   - $y_L = m \cdot 0 = 0$
   - $y_R = m \cdot (p-1)/2$
   - The gap $y_L - y_R \in [-\alpha, \alpha]$, for a small α
3. Then, we will show that $\sum_{x \in P} g(x)$ is in the range $[-4\alpha, 4\alpha]$

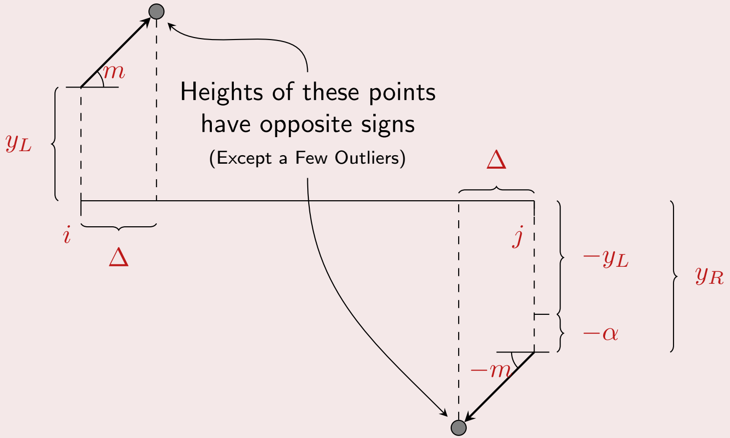
Signs of Lines: (Nearly) Balanced Windows



Conclusion

$$\sum_{x \in \{i, i+1, \ldots, j-1, j\}} g(x) = 0$$

Signs of Lines: (Nearly) Balanced Windows



Conclusion

$$\left| \sum_{x \in \{i, i+1, \ldots, j-1, j\}} g(x) \right| \leqslant 4\alpha$$

Signs of Lines: (Nearly) Balanced Windows

Main Technical Lemma

- Consider the interval $I = \{i, i+1, \ldots, j-1, j\}$
- Define $y_L = g(i)$
- Define $y_R = g(j)$
- Suppose $(y_L + y_R) \in [-\alpha, \alpha]$ or $y_L - y_R \in [-\alpha, \alpha]$
- Then

$$\left| \sum_{x \in I} g(x) \right| \leqslant 4\alpha$$

Safe and Unsafe Choices

Unsafe Choices

- m is a small odd number (for example, $3, 5, \ldots$)
- Has insecurity $\geqslant 1/2m$

Safe and Unsafe Choices

Unsafe Choices

- m is a small odd number (for example, $3, 5, \ldots$)
- Has insecurity $\geqslant 1/2m$

Safe Choices

- m is even and $m \leqslant \sqrt{p}$
- Has insecurity $\leqslant 1/\sqrt{p}$

Safe and Unsafe Choices

Unsafe Choices

- m is a small odd number (for example, $3, 5, \ldots$)
- Has insecurity $\geqslant 1/2m$

Safe Choices

- m is even and $m \leqslant \sqrt{p}$
- Has insecurity $\leqslant 1/\sqrt{p}$

Safe Choices

- $m = 2^i \cdot (0\cdots 0\,\underbrace{1\cdots 1}_{\lambda/2\text{-bits}})_2$, for all $i \in \{0, 1, \ldots, \lambda - 1\}$
- Has insecurity $\leqslant 1/\sqrt{p}$

What lies Ahead?

Open Problems

1. More secure Modulus and Evaluation Places choices for $[n = 2, k = 2]$ Shamir's Secret-sharing Scheme
2. The $[n = 3, k = 2]$ Shamir's Secret-sharing Scheme: Hashing properties of 3 "signs of lines"
   - Each "sign of line" is balanced
   - Each product of two "signs of lines" is balanced
   - The product of three "signs of lines" is balanced
3. Derandomization $[n, k]$ Shamir's Secret-sharing Scheme: Hashing properties of n "signs of $\deg < k$ curves"
   - For $i \in \{1, 2, \ldots, k\}$: The product of i "signs of curves" is balanced
4. More complex leakage classes
   - Multiple physical bits per secret share
   - Low complexity leakage

Thanks

Funding

- NSF CRII Award CNS–1566499
- NSF Awards CNS–1618822, CNS–2055605
- IARPA HECTOR project
- MITRE Innovation Program Academic Cybersecurity Research Award (2019–2020, 2020–2021)
- Ross-Lynn Research Scholar Grant (2021–2022)
- Purdue Research Foundation (PRF) Award (2017–2018)
- The Center for Science of Information, an NSF Science and Technology Center, Cooperative Agreement CCF–0939370

References (In Reverse Chronological Order)

[7] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Xiuyu Ye.
Leakage-resilience of shamir secret-sharing against physical-bit leakage: A full derandomization.
In *(Ongoing Work)*, 2023.

[6] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu.
Leakage-resilient linear secret-sharing against arbitrary bounded-size leakage family.
In *TCC*, 2022.

[5] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, Mingyuan Wang, Xiuyu Ye, and Albert Yu.
Tight estimate of the local leakage resilience of the additive secret-sharing scheme & its consequences.
In Dana Dachman-Soled, editor, *3rd Conference on Information-Theoretic Cryptography, ITC 2022, July 5-7, 2022, Cambridge, MA, USA*, volume 230 of *LIPIcs*, pages 16:1–16:19. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2022.

[4] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, and Mingyuan Wang.
Improved bound on the local leakage-resilience of shamir's secret sharing.
In *IEEE International Symposium on Information Theory, ISIT 2022, Espoo, Finland, June 26 - July 1, 2022*, pages 2678–2683. IEEE, 2022.

[3] Hemanta K. Maji, Hai H. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang.
Leakage-resilience of the shamir secret-sharing scheme against physical-bit leakages.
In Anne Canteaut and François-Xavier Standaert, editors, *EUROCRYPT 2021, Part II*, volume 12697 of *LNCS*, pages 344–374. Springer, Heidelberg, October 2021.

[2] Hemanta K. Maji, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang.
Constructing locally leakage-resilient linear secret-sharing schemes.
In Tal Malkin and Chris Peikert, editors, *CRYPTO 2021, Part III*, volume 12827 of *LNCS*, pages 779–808, Virtual Event, August 2021. Springer, Heidelberg.

[1] Donald Q. Adams, Hemanta K. Maji, Hai H. Nguyen, Minh L. Nguyen, Anat Paskin-Cherniavsky, Tom Suad, and Mingyuan Wang.
Lower bounds for leakage-resilient secret-sharing schemes against probing attacks.
In *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*, pages 976–981. IEEE, 2021.