Improving the Security of Shamir's Secret-Sharing

Xiuyu Ye

Joint works with: Donald Q. Adams Hemanta K. Maji Hai H. Nguyen
Minh L. Nguyen Anat Paskin-Cherniavsky Tom Suad Mingyuan Wang Albert Yu

PURDUE
UNIVERSITY

June 10, 2023

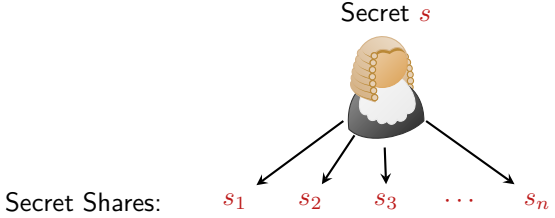
Protagonists: Relevant Secret-sharing Schemes

Additive Secret-sharing Scheme (n parties)

- Secret: $s \in F$.
- Secret Shares: Pick $(s_1, s_2, \ldots, s_{n-1})$ randomly from F and define $s_n = s - \sum_{i=1}^{n-1} s_i$.

Shamir's Secret-sharing Scheme ShamirSS$(n, k, \vec{X})$ (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 secret shares of each party $s_1 = P(X_1)$, $s_2 = P(X_2)$, $\ldots$, and $s_n = P(X_n)$

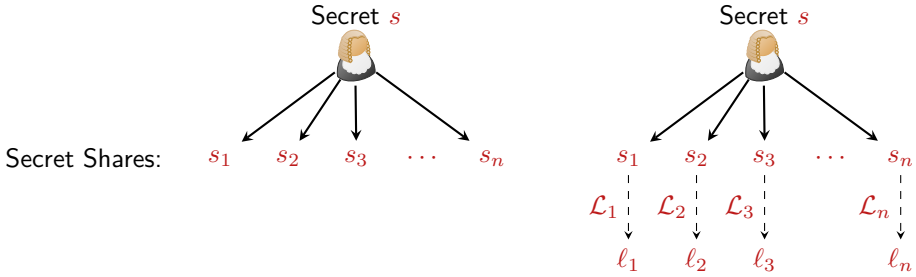


Fundamental to Nearly All Cryptography & Privacy

Applications of Shamir's secret-sharing scheme

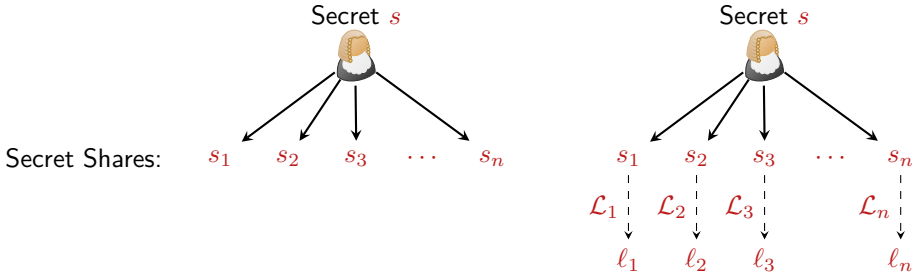
- Secure Computation [BenOr-Goldwasser-Wigderson (STOC–88),Chaum-Crépeau-Damgård (STOC–88), Rabin-BenOr (STOC–88), Cramer-Dåmgard-Ishai(TCC–05)]
- Threshold Cryptography [Desmedt (CRYPTO1987), Desmedt-Frankel(CRYPTO–1991), Gennaro-Rabin-Rabin (PODC–1998), Shoup (EUROCRYPT–2000)]
- Access Control [Naor-Wool(TPDS–1998), Goyal-Pandey-Sahai-Waters (CCS–2006), Waters (PKC–2011), Goyal-Kumar (CRYPTO–2018), Aggarwal-Damgard-Nielsen-Obremski-Purwanto-Ribeiro-Simkin(CRYPTO–2019)]
- Protection against Side Channel Attacks: Masking [Goubin-Martinelli(TCHES–2011), Coron-Prouff-Roche (CARDIS–2012), Cheng-Guilley-Carlet-Danger-Mesnager(TCHES–2021)]

Traditional Security Notion



Attack: Threshold Corruption (all or nothing) Leaking partial information

Traditional Security Notion



Attack: Threshold Corruption (all or nothing) Leaking partial information

Definition: Leakage Resilience against a Leakage Family

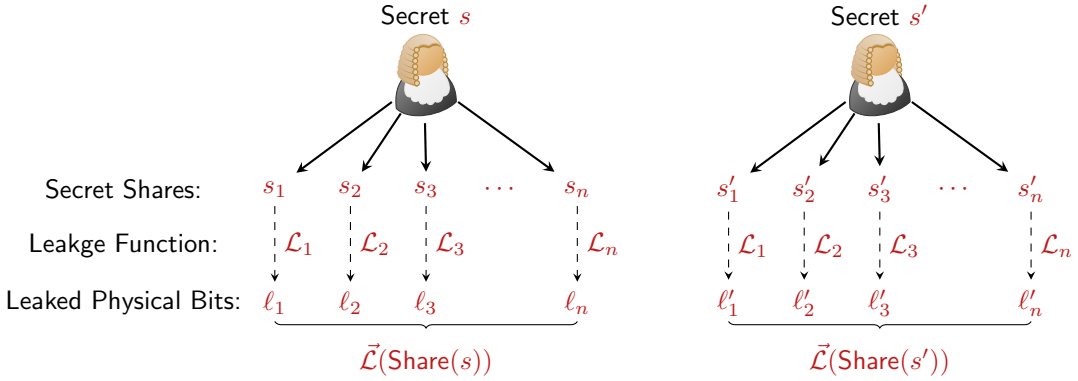
1. For any leakage attack $\vec{\mathcal{L}}$ in the leakage family
2. For any two secrets s and s'
3. Advantage of distinguishing the secrets (using the leakage from the secret shares) is small

$$\mathsf{SD}\left(\vec{\mathcal{L}}(\mathsf{Share}(s)) \ , \ \vec{\mathcal{L}}(\mathsf{Share}(s'))\right) < \text{small}$$

Adversarial Model (for 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



Threat Example 1: Parity-of-Parity Attack on Additive Secret-Sharing

- Secret Shares of Additive Secret-Sharing: Random $s_1, s_2, \ldots, s_k$ s.t. $s_1 + s_2 + \cdots + s_k = s$
- Attack: Leak the LSB of each secret share. ($\ell_i = \mathrm{LSB}(s_i)$)

$$\mathrm{LSB}(x) = \begin{cases} 0, & \text{if } x \in \{0, 2, 4, \ldots, p-1\} \\ 1, & \text{otherwise.} \end{cases}$$

- Parity of Parity Attack Distinguisher [Maji-Nguyen-PaskinCherniavsky-Suad-Wang (EUROCRYPT–2021)] outputs $\ell_1 \oplus \ell_2 \oplus \cdots \oplus \ell_k$

$s = 0$	(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

Threat Example 1: Parity-of-Parity Attack on Additive Secret-Sharing

- Secret Shares of Additive Secret-Sharing: Random $s_1, s_2, \ldots, s_k$ s.t. $s_1 + s_2 + \cdots + s_k = s$
- Attack: Leak the LSB of each secret share. ($\ell_i = \mathrm{LSB}(s_i)$)

$$\mathrm{LSB}(x) = \begin{cases} 0, & \text{if } x \in \{0, 2, 4, \ldots, p-1\} \\ 1, & \text{otherwise.} \end{cases}$$

- Parity of Parity Attack Distinguisher [Maji-Nguyen-PaskinCherniavsky-Suad-Wang (EUROCRYPT–2021)] outputs $\ell_1 \oplus \ell_2 \oplus \cdots \oplus \ell_k$

$s = 0$	(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

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

For additive secret-sharing scheme, there is an attack that leaks one physical bit from each secret share and can distinguish two secrets with advantage $\geqslant (2/\pi)^n$.
[Adams-Maji-Nguyen-Nguyen-PaskinCherniavsky-Suad-Wang (ISIT–2021), Maji-Nguyen-PaskinCherniavsky-Suad-Wang-Ye-Yu (ITC–2022)]

Threat Example 2: Careless Evaluation Place Choice for Shamir's secret-sharing

Vulnerability of Shamir against LSB Leakage

- 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 $\rho \in F^*$

Threat Example 2: Careless Evaluation Place Choice for Shamir's secret-sharing

Vulnerability of Shamir against LSB Leakage

- 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 $\rho \in F^*$

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

Observation

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

Research Question

Security against Leakage Attacks

- How to choose the Modulus and Evaluation Places for Shamir's Secret-sharing Scheme so it is leakage resilient?
- Adversarial model: Physical bit leakage from the secret shares

What is Known

Theorem (Monte-Carlo Construction [Maji-PaskinCherniavsky-Suad-Wang (CRYPTO–2021)])

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 from every secret share;* except *with* $\exp(-(k-1) \cdot \lambda)$ *probability*

What is Known

Theorem (Monte-Carlo Construction [Maji-PaskinCherniavsky-Suad-Wang (CRYPTO–2021)])

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 from every secret share;* except *with* $\exp(-(k-1) \cdot \lambda)$ *probability*

Security against Leakage Attacks

How to choose the Modulus and Evaluation Places of Shamir's Secret-sharing Scheme ShamirSS$(n, k, \vec{X})$?

Remark

[NIST] recently called for recommendations and guidelines to improve the security of multi-party threshold schemes.

Full Derandomization

- Derandomization is the problem we want to tackle today

Example of secure evaluation places for ShamirSS$(2, 2, \vec{X})$ when $p = 8191$

95	97	99	101	103	107	111	113	119	121	123	125	131	133	135
137	139	143	145	147	151	153	155	157	159	161	163	165	169	173
175	179	181	183	185	187	191	197	201	203	207	209	211	213	215
217	219	221	223	225	227	229	231	233	235	237	239	243	245	247
249	251	253	267	269	271	275	277	279	281	285	287	291	293	295
297	299	303	305	309	313	317	319	323	325	329	331	333	335	337
339	349	351	355	357	359	361	363	365	369	371	373	375	377	379
391	393	395	397	399	401	403	405	407	411	413	415	419	423	427
429	433	435	437	441	443	445	447	453	457	459	461	465	467	469
471	473	475	477	487	491	493	495	497	499	501	503	505	549	551
553	555	557	559	563	567	569	573	575	581	583	587	589	591	...

- Each element X in the above table represents the set of elements
$$\{X, X \cdot 2, X \cdot 2^2, \ldots, X \cdot 2^{\lambda-1}\}$$

- Each element X in the above table stands for evaluation places $(1, X)$
- For example, the element 95 stands for
$$\begin{aligned} 95 \cdot \langle 2 \rangle &= \{95, 2 \cdot 95, 2^2 \cdot 95, \ldots, 2^{12} \cdot 95\} \\ &= \{95, 190, 380, 760, 1520, 3040, 6080, 3969, 7938, 7685, 7179, 6167, 4143\} \end{aligned}$$

Question for Today's Technical Part of the Talk

Setting

- What evaluation places can make Shamir's secret-sharing scheme $(\mathsf{ShamirSS}(2,2,\vec{X}), \mathsf{ShamirSS}(3,2,\vec{X}))$ secure against $(m=1)$-bit leakage attack?

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

$$\mathsf{SD}\left(\vec{\mathcal{L}}(\mathsf{Share}(s))\ ,\ \vec{\mathcal{L}}(\mathsf{Share}(s'))\right) < \text{small}$$

New Result: Our Recommendation for Modulus & Evaluation Places

- Recommended Modulus: λ-bit Mersenne prime $p = 2^\lambda - 1$. (For example, 3, 7, 31, 127, 8191, 131071, 524287, 2147483647, etc.)
- Evaluation places:

Decision Algorithm to identify Secure Evaluation Places against Physical Bit attack

Input. Distinct evaluation places $X_1, X_2 \in F^*$, F is prime field of order p, a Mersenne prime

Output. Decide if ShamirSS$(2, 2, (X_1, X_2))$ is secure to all physical bit leakage attacks

Algorithm.

1. If there is $k \in \{0, 1, \ldots, \lambda - 1\}$ such that $2^k X_1 = X_2$: Return insecure
2. For $k \in \{0, 1, \ldots, \lambda - 1\}$:
   1. Call the decision algorithm to **find secure evaluation places against** LSB **attack for** ShamirSS$(2, 2, (2^k \cdot X_1, X_2))$
   2. If the algorithm returns "may be insecure," return may be insecure
3. Declare ShamirSS$(2, 2, (X_1, X_2))$ is secure against all physical bit attacks.

Algorithm to identify Secure Evaluation Places against LSB leakage

Decision Algorithm to identify Secure Evaluation Places against LSB attack

Input. Distinct evaluation places $X_1, X_2 \in F^*$

Output. Decide whether ShamirSS$(2, 2, (X_1, X_2))$ is secure to the LSB leakage attack

1. Define the equivalence class
$$[X_1 : X_2] := \left\{ (u, v) \colon u = \Lambda \cdot X_1, v = \Lambda \cdot X_2, \Lambda \in F^* \right\}.$$
Use the LLL[Lenstra–Lenstra–Lovász (1982)] algorithm to (efficiently) find $(u, v) \in [X_1 : X_2]$ such that for $B := \lceil 2^{3/4} \cdot \sqrt{p} \rceil$
$$u, v \in \{-B, -(B-1), \ldots, 0, 1, \ldots, (B-1), B\} \mod p.$$
2. Compute $g = \gcd(|u|_p, |v|_p)$.
3. If $|u|_p \cdot |v|_p / g^2$ is even: Declare ShamirSS$(2, 2, (X_1, X_2))$ is secure to LSB leakage attacks.
4. (Else) If $|u|_p \cdot |v|_p / g^2$ is odd and $|u|_p \cdot |v|_p / g^2 \geqslant \sqrt{p}$: Declare ShamirSS$(2, 2, (X_1, X_2))$ is secure to LSB leakage attacks
5. (Else) Declare ShamirSS$(2, 2, (X_1, X_2))$ against LSB attacks may be insecure

Algorithm to identify Secure Evaluation Places against LSB leakage

Notation: Length of a Finite Field Element

Consider an element $x \in F$, the prime field of order $p \geqslant 3$. Suppose $x = x' \mod p$, where $x' \in \{-(p-1)/2, \ldots, 0, 1, \ldots, (p-1)/2\} \subseteq \mathbb{Z}$. The *length of the element* is a function $|\cdot|_p \colon F \to \{0, 1, \ldots, (p-1)/2\}$ defined below.

$$|x|_p := \begin{cases} x', & \text{if } x' \in \{0, 1, \ldots, (p-1)/2\} \\ -x', & \text{if } x' \in \{-(p-1)/2, \ldots, -1\} \end{cases}$$

- For example, if $x = (p-1) \mod p$, then $x' = -1 \in \mathbb{Z}$ and $|x|_p = 1$.

Algorithm to identify Secure Evaluation Places against LSB leakage

Decision Algorithm to identify Secure Evaluation Places against LSB attack

Input. Distinct evaluation places $X_1, X_2 \in F^*$

Output. Decide whether ShamirSS$(2, 2, (X_1, X_2))$ is secure to the LSB leakage attack

1. Define the equivalence class
$$[X_1 : X_2] := \left\{ (u, v) \colon u = \Lambda \cdot X_1, v = \Lambda \cdot X_2, \Lambda \in F^* \right\}.$$
Use the LLL[Lenstra–Lenstra–Lovász (1982)] algorithm to (efficiently) find $(u, v) \in [X_1 : X_2]$ such that for $B := \lceil 2^{3/4} \cdot \sqrt{p} \rceil$
$$u, v \in \{-B, -(B-1), \ldots, 0, 1, \ldots, (B-1), B\} \mod p.$$
2. Compute $g = \gcd(|u|_p, |v|_p)$.
3. If $|u|_p \cdot |v|_p / g^2$ is even: Declare ShamirSS$(2, 2, (X_1, X_2))$ is secure to LSB leakage attacks.
4. (Else) If $|u|_p \cdot |v|_p / g^2$ is odd and $|u|_p \cdot |v|_p / g^2 \geqslant \sqrt{p}$: Declare ShamirSS$(2, 2, (X_1, X_2))$ is secure to LSB leakage attacks
5. (Else) Declare ShamirSS$(2, 2, (X_1, X_2))$ against LSB attacks may be insecure

From LSB to Sign

Definition: sign of lines

- We interpret the finite field F as the set of elements $\{0, 1, \ldots, p-1\}$.
- We introduce a Boolean function $\mathrm{sgn}_p \colon F \to \{\pm 1\}$ defined as follows.

$$\mathrm{sgn}_p(T) = \begin{cases} +1, & \text{if } T \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & \text{if } T \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases}$$

Reduction: LSB to Sign Leakage

Leaking the "LSB of each secret share" is equivalent to leaking the "sign of each secret share" (the leakage joint distributions are identical)

From LSB to Sign

Definition: sign of lines

- We interpret the finite field F as the set of elements $\{0, 1, \ldots, p-1\}$.
- We introduce a Boolean function $\mathrm{sgn}_p \colon F \to \{\pm 1\}$ defined as follows.

$$\mathrm{sgn}_p(T) = \begin{cases} +1, & \text{if } T \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & \text{if } T \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases}$$

Reduction: LSB to Sign Leakage

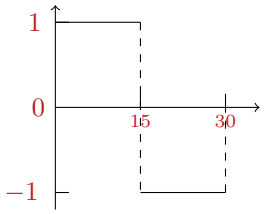
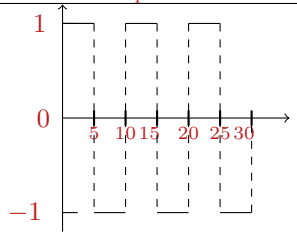
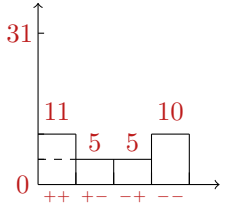
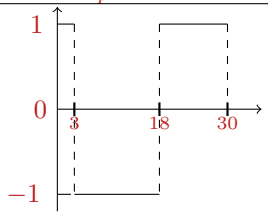
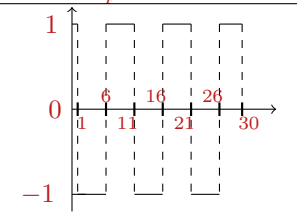
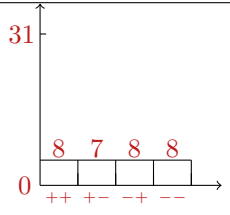
Leaking the "LSB of each secret share" is equivalent to leaking the "sign of each secret share" (the leakage joint distributions are identical)

Conclusion

If the frequencies of signs for secret $s = 0$ are not (close to) uniform, then there will be a secret with very different frequency of sign.

What would happen to evaluation places $(1, 3)$?

- Example: $p = 31, \mathsf{ShamirSS}(2, 2, (1, 3))$.

$s = 0$	$\mathrm{sgn}_p(T)$	$\mathrm{sgn}_p(3T)$	Frequency Plot
			
$s = 12$	$\mathrm{sgn}_p(T + 12)$	$\mathrm{sgn}_p(3T + 12)$	Frequency Plot
			

Orthogonality of Signs of Lines

Orthogonality of signs of lines

- **Uniformity of all frequencies** is equivalent as the line $\mathrm{sgn}_p(X_1 \cdot T)$ is (nearly) orthogonal to $\mathrm{sgn}_p(X_2 \cdot T)$. We call this **"orthogonality of signs of lines"**.
- Leakage resilient is equivalent to "orthogonality of signs of lines".

Problem

How do we know if $\mathrm{sgn}_p(X_1 \cdot T)$ and $\mathrm{sgn}_p(X_2 \cdot T)$ are orthogonal to each other?

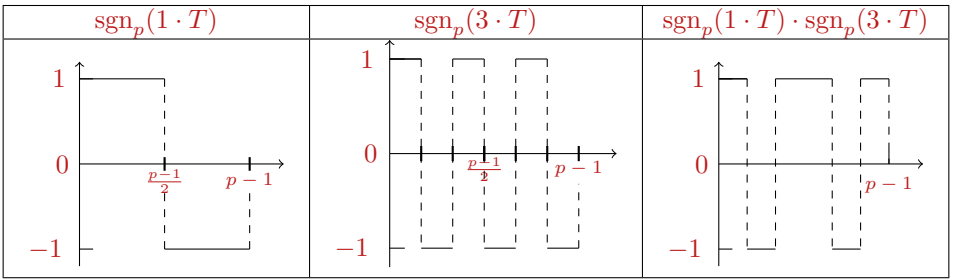
Orthogonality of Signs of Lines

Definition: Inner product of sign of lines

- We interpret the finite field F as the set of elements $\{0, 1, \ldots, p-1\}$.
- We introduce a Boolean function $\mathrm{sgn}_p \colon F \to \{\pm 1\}$ defined as follows.

$$\mathrm{sgn}_p(T) = \begin{cases} +1, & \text{if } T \in \{0, 1, \ldots, (p-1)/2\} \mod p \\ -1, & \text{if } T \in \{-(p-1)/2, \ldots, -1\} \mod p. \end{cases}$$

- Inner product: $\langle \mathrm{sgn}_p(X_1 \cdot T), \mathrm{sgn}_p(X_2 \cdot T) \rangle$



Orthogonality of Signs of Lines

What's next?

Estimating the exponential sum

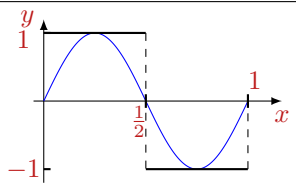
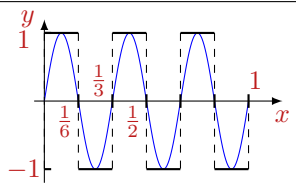
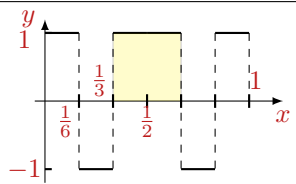
$$\Sigma := \sum_{T \in F} \mathrm{sgn}_p(X_1 \cdot T) \cdot \mathrm{sgn}_p(X_2 \cdot T).$$

Estimating the summation using integral

Definitions

- Define the periodic function $\varphi\colon \mathbb{R} \to \{\pm 1\}$ as $\varphi(t) := \operatorname{sgn}\sin(2\pi t)$.
- Family of square waves
- Define the integral

$$I := \int_0^1 \varphi(X_1 \cdot t) \cdot \varphi(X_2 \cdot t)\,\mathrm{d}t.$$

$\varphi(t) = \operatorname{sgn}\sin(2\pi t)$	$\varphi(3t) = \operatorname{sgn}\sin(2\pi \cdot 3 \cdot t)$	$\varphi(t) \cdot \varphi(3t)$
		

Quality of Estimation

Problem

- The quality of transferring from integral estimate to summation estimate depends on the number of oscillations in the function.
- It is proportional to $(|X_1|_p + |X_2|_p)/p$.
- The integral estimate is useless if the evaluation places are very large.

Dirichlet's Approximation Theorem

Solution

- Change basis from (X_1, X_2) to (u, v), where $X_1 : X_2 = u : v$ and $|u|_p, |v|_p$ are small
- How? Use **Dirichlet's Approximation Theorem**
- Instead of the inner product

$$\Sigma = \sum_{T \in F} \operatorname{sgn}_p(X_1 \cdot T) \cdot \operatorname{sgn}_p(X_2 \cdot T)$$

  we will estimate the following equivalent summation

$$\Sigma = \sum_{T \in F} \operatorname{sgn}_p(u \cdot T) \cdot \operatorname{sgn}_p(v \cdot T)$$

- Transference error: (proportional to) $(|u|_p + |v|_p)/p \leqslant 1/\sqrt{p}$

Dirichlet's Approximation Theorem

Solution

- Change basis from (X_1, X_2) to (u, v), where $X_1 : X_2 = u : v$ and $|u|_p, |v|_p$ are small
- How? Use **Dirichlet's Approximation Theorem**
- Instead of the inner product

$$\Sigma = \sum_{T \in F} \operatorname{sgn}_p(X_1 \cdot T) \cdot \operatorname{sgn}_p(X_2 \cdot T)$$

  we will estimate the following equivalent summation

$$\Sigma = \sum_{T \in F} \operatorname{sgn}_p(u \cdot T) \cdot \operatorname{sgn}_p(v \cdot T)$$

- Transference error: (proportional to) $(|u|_p + |v|_p)/p \leqslant 1/\sqrt{p}$

Is it efficient?

Dirichlet problem is inefficient to solve.

Dirichlet's Approximation Theorem

Solution

- Change basis from (X_1, X_2) to (u, v), where $X_1 : X_2 = u : v$ and $|u|_p, |v|_p$ are small
- How? Use **Dirichlet's Approximation Theorem**
- Instead of the inner product

$$\Sigma = \sum_{T \in F} \mathrm{sgn}_p(X_1 \cdot T) \cdot \mathrm{sgn}_p(X_2 \cdot T)$$

  we will estimate the following equivalent summation

$$\Sigma = \sum_{T \in F} \mathrm{sgn}_p(u \cdot T) \cdot \mathrm{sgn}_p(v \cdot T)$$

- Transference error: (proportional to) $(|u|_p + |v|_p)/p \leqslant 1/\sqrt{p}$

Is it efficient?

Dirichlet problem is inefficient to solve.

LLL to the rescue

- We introduce a slack of 1.68
- Solve it efficiently with LLL algorithm

Example of secure evaluation places for ShamirSS$(2, 2, \vec{X})$ when $p = 8191$

95	97	99	101	103	107	111	113	119	121	123	125	131	133	135
137	139	143	145	147	151	153	155	157	159	161	163	165	169	173
175	179	181	183	185	187	191	197	201	203	207	209	211	213	215
217	219	221	223	225	227	229	231	233	235	237	239	243	245	247
249	251	253	267	269	271	275	277	279	281	285	287	291	293	295
297	299	303	305	309	313	317	319	323	325	329	331	333	335	337
339	349	351	355	357	359	361	363	365	369	371	373	375	377	379
391	393	395	397	399	401	403	405	407	411	413	415	419	423	427
429	433	435	437	441	443	445	447	453	457	459	461	465	467	469
471	473	475	477	487	491	493	495	497	499	501	503	505	549	551
553	555	557	559	563	567	569	573	575	581	583	587	589	591	...

- Each element X in the above table represents the set of elements
$$\{X, X \cdot 2, X \cdot 2^2, \ldots, X \cdot 2^{\lambda-1}\}$$

- Each element X stands for the equivalence class of evaluation places $[1 : X]$
- For example, the element 95 stands for
$$\begin{aligned} 95 \cdot \langle 2 \rangle &= \{95, 2 \cdot 95, 2^2 \cdot 95, \ldots, 2^{12} \cdot 95\} \\ &= \{95, 190, 380, 760, 1520, 3040, 6080, 3969, 7938, 7685, 7179, 6167, 4143\} \end{aligned}$$

Thank you!

- We have the analogous result for ShamirSS$(3, 2, \vec{X})$ which allows one multiplication in GMW types MPC protocols
- We also have results for composite order fields

Generalize to any $n = k$

Security against arbitrary Physical Bit Leakage for ShamirSS$(n, n, \vec{X})$

Input. Distinct evaluation places $X_1, X_2, \ldots, X_n \in F^*$, F is a prime field of order $p = 2^\lambda - 1$.

Output. Determine whether ShamirSS$(n, n, \vec{X})$ is secure against physical bit leakage.

1. For each $i \in \{1, 2, \ldots, n\}$: Compute and save $\beta_i = \left(X_i \prod_{j \neq i}(X_i - X_j)\right)^{-1}$
2. For each $j \in \{1, 2, \ldots, n\}$:
   1. For each $\ell \in \{j+1, \ldots, n\}$:
      1. Check if (β_j, β_ℓ) are secure evaluation places for ShamirSS$(2, 2, (\beta_j, \beta_\ell))$ $\Leftarrow$
      2. If yes, return secure
3. Return may be insecure