Leakage-Resilience of Shamir's Secret Sharing: Identifying Secure Evaluation places

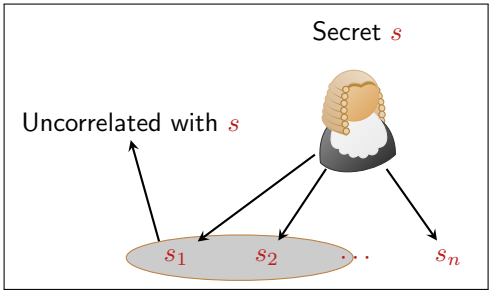
Jihun Hwang, Hemanta K. Maji, Hai H. Nguyen, Xiuyu Ye

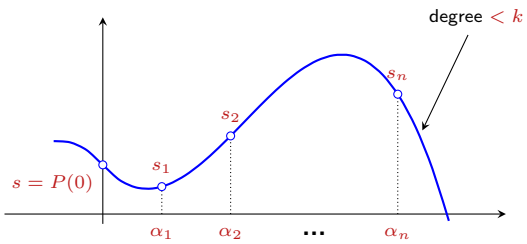
PURDUE UNIVERSITY

ETH zürich

Local Leakage Resilience of Shamir's secret-sharing

[Benhamouda-Degwekar-Ishai-Rabin CRYPTO'18, Goyal-Kumar STOC'18]





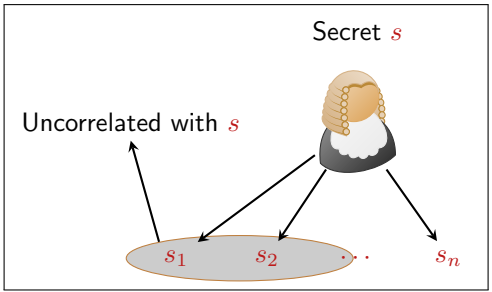
Shamir's secret sharing scheme

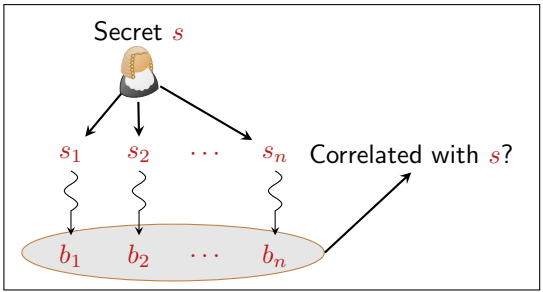
- Adversary does not achieve quorum: Learns nothing about the secret.
- Adversary achieves quorum: Reconstructs the secret.

These secret-sharings are widespread in secure storage/computation technologies and masking schemes.

Local Leakage Resilience of Shamir's secret-sharing

[Benhamouda-Degwekar-Ishai-Rabin CRYPTO'18, Goyal-Kumar STOC'18]





Shamir's secret sharing scheme

- Adversary does not achieve quorum: Learns nothing about the secret.
- Adversary achieves quorum: Reconstructs the secret.
- Adversary leaks partial information (e.g., least significant bit b_i) from every share, is the leakage statistically independent of the secret?

Motivation

Prior work 1 [Maji-Nguyen-PaskinCherniavsky-Suad-Wang-Yu-Ye-22]

For additive secret-sharing, leaking one bit from each share distinguishes secrets with advantage $\geqslant (2/\pi)^n$.

Prior work 2 [Maji-Nguyen-PaskinCherniavsky-Suad-Wang-21, Maji-Nguyen-PaskinCherniavsky-Ye-24]

Most evaluation places are leakage-resilient for Shamir's secret sharing.

- No secure explicit evaluation place is known.
- No classifier to determine whether specific evaluation places are secure or not.

For example, NIST can neither recommend nor certify the security of the evaluation places.

Our Research Question

Our Research Question

1. How to efficiently determine the security of specified evaluation places?
2. Can we find secure ones explicitly?

Linear leakages are easy to analyze (e.g. code reconstruction).

Technical Challenge

- Non-linear leakage (e.g. LSB).
  - Non-linear repair of Reed-Solomon Codes. [Con-Shutty-Tamo-W0otters-23, Con-Tamo-22]

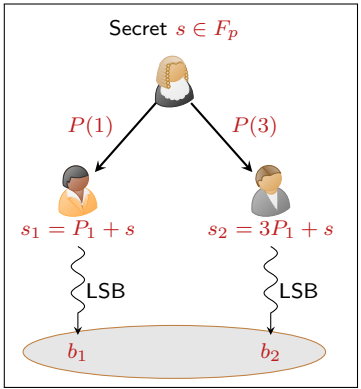
Our Results

Our Results

1. Classifier for secure evaluation places:
   - Shares of all parties are required to reconstruct the secret.
   - Against arbitrary single bit-probe in each share.
   - Mersenne and Fermat prime modulus.
2. Identify explicit secure evaluation places.

- Our characterization is "comprehensive".
- When vulnerable, we explicitly identify vulnerable secrets.

New Attack: For Evaluation places (1, 3)



- Fix an arbitrary prime field F_p.
- Shamir's scheme among two parties.

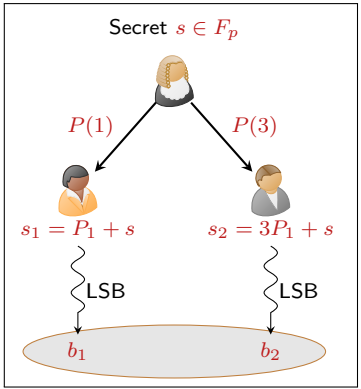
- Secret $s \in F_p$.
- Parties use the secret sharing polynomial $P(X) = P_1 \cdot X + s \in F_p[X]$, where P_1 is uniformly random from F_p.
- Evaluation places $\alpha_1 = 1, \alpha_2 = 3$.

- Corresponding shares are

$$(s_1, s_2) \in \left\{ (P_1 + s\ ,\ 3 \cdot P_1 + s) :\ P_1 \in F_p \right\}.$$

- Leakage: Least significant bits (LSB) (b_1, b_2) of the shares.

New Attack: For Evaluation places (1, 3)



- Fix an arbitrary prime field F_p.
- Shamir's scheme among two parties.

- Secret $s \in F_p$.
- Parties use the secret sharing polynomial $P(X) = P_1 \cdot X + s \ \in F_p[X]$, where P_1 is uniformly random from F_p.
- Evaluation places $\alpha_1 = 1, \alpha_2 = 3$.

- Corresponding shares are

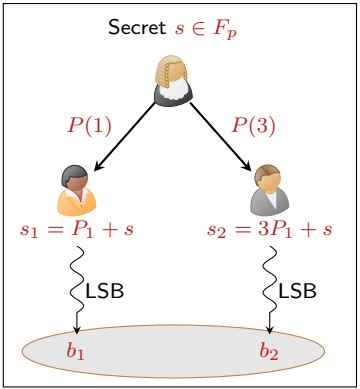
$$(s_1, s_2) \in \left\{ (P_1 + s \ , \ 3 \cdot P_1 + s) \ : \ P_1 \in F_p \right\}.$$

- Leakage: Least significant bits (LSB) (b_1, b_2) of the shares.

Baseline: Uniformly random secret $s \in F_p$

Leakage is independent and uniformly random. The probability that $b_1 \neq b_2$ is (roughly) $1/2$.

New Attack: For Evaluation places (1, 3)



What is an attack?

Some secret s is correlated with the joint distribution of (b_1, b_2).

In particular,

Sharing secret $s = 0$

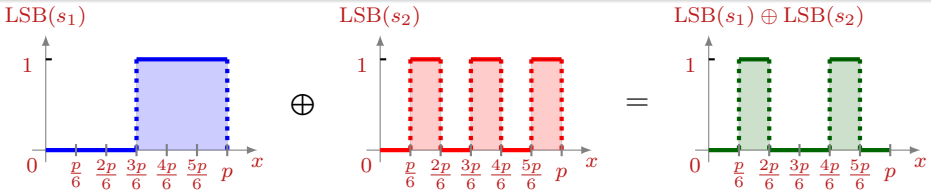
We prove: LSB of the shares is not uniformly distributed over $\{0,1\} \times \{0,1\}$.

New Attack: For Evaluation places (1, 3)

Our Analysis

Rewrite $s_1 = 2 \cdot x$ and $s_2 = 3 \cdot s_1 = 6 \cdot x$.

x	$[0, p/6)$	$[p/6, 2p/6)$	$[2p/6, 3p/6)$	$[3p/6, 4p/6)$	$[4p/6, 5p/6)$	$[5p/6, p)$
$b_1 = \mathrm{LSB}(s_1)$	0	0	0	1	1	1
$b_2 = \mathrm{LSB}(s_2)$	0	1	0	1	0	1



- b_1 and b_2 are different when $x \in [p/6, 2p/6)$ and $x \in [4p/6, 5p/6)$.
  - I.e., different with probability (roughly) $2/6 = 1/3$.

$\Longrightarrow$ LSB leakage is not independent of the secret.

This form of vulnerability generalizes to all (α_1, α_2).

Our Result: Identifying secure evaluation places against LSB Leakage

- Fix arbitrary prime field F_p.
- Shamir's scheme between two parties.
- Evaluation places $\alpha_1, \alpha_2 \in F_p$.

Our Classifier (LSB Leakage)

- Compute "small norm" $u, v \in \left\{-\lceil\sqrt{p}\rceil, \ldots, 0, 1, \ldots, \lceil\sqrt{p}\rceil\right\}$ satisfying $\alpha_1 \cdot \alpha_2^{-1} = u \cdot v^{-1}$ u, v are relatively prime.
- If uv is even, the evaluation places are secure.
- Otherwise (uv is odd), the evaluation places have $1/uv$ insecurity against LSB leakage from each share.

Evaluation places $(1, 3)$ are insecure

For any prime $p \geqslant 11$ and evaluation places satisfying $\alpha_1 : \alpha_2 = 1 : 3$ have insecurity $1/3$.

Technical Overview

Technical question

For a uniformly random $X \in F_p$, are the distributions $\mathrm{LSB}(\alpha_1 X)$ and $\mathrm{LSB}(\alpha_2 X)$ statistically independent?

Equivalently: Does $\sum_{X \in F_p} (-1)^{\mathrm{LSB}(\alpha_1 X)} \cdot (-1)^{\mathrm{LSB}(\alpha_2 X)}$ have a small/large magnitude?

Technical Overview

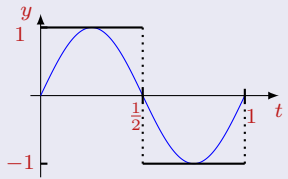
Technical question

For a uniformly random $X \in F_p$, are the distributions $\mathrm{LSB}(\alpha_1 X)$ and $\mathrm{LSB}(\alpha_2 X)$ statistically independent?

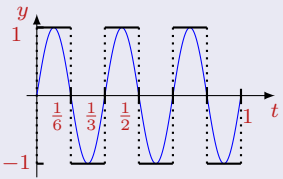
Equivalently: Does $\sum_{X \in F_p} (-1)^{\mathrm{LSB}(\alpha_1 X)} \cdot (-1)^{\mathrm{LSB}(\alpha_2 X)}$ have a small/large magnitude?

- Correlation E between distributions as inner product of two oscillatory $\{\pm 1\}$ sequence.
- Approximate this correlation by the similarity between two square wave functions,

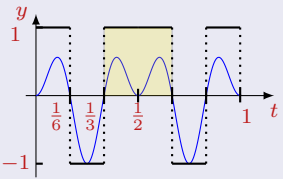
$$I_{u,v} = \int_0^1 \operatorname{sign}\sin(2\pi u \cdot t) \cdot \operatorname{sign}\sin(2\pi v \cdot t)\, \mathrm{d}t.$$



$\varphi(t) = \operatorname{sign}\sin(2\pi t)$



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



$\varphi(t) \cdot \varphi(3t)$

- Closed form of this integral

$$E \underset{1/\sqrt{p}}{\approx} I_{u,v} = \begin{cases} 0, & \text{if } uv \text{ is even,} \\ \frac{1}{uv} & \text{otherwise} \end{cases}.$$

Technical Overview

Technical question

For a uniformly random $X \in F_p$, are the distributions $\mathrm{LSB}(\alpha_1 X)$ and $\mathrm{LSB}(\alpha_2 X)$ statistically independent?

Equivalently: Does $\sum_{X \in F_p} (-1)^{\mathrm{LSB}(\alpha_1 X)} \cdot (-1)^{\mathrm{LSB}(\alpha_2 X)}$ have a small/large magnitude?

Remark: Exponential Sum

Answering this technical question is equivalent to estimating the following exponential sum

$$\sum_{X=0}^{p-1} \exp\left(\mathrm{i} \cdot \pi p \cdot \left(\left\{ \frac{\alpha_1 X}{p} \right\} + \left\{ \frac{\alpha_2 X}{p} \right\} \right) \right).$$

Note: $\{x\}$ represents the fractional part of the real x.

Our Result: Identifying secure evaluation places against PHYS Leakage

- Security parameter λ.
- Fix Mersenne $(p = 2^\lambda - 1)$ or Fermat $(p = 2^\lambda + 1)$ prime field F_p.
- Shamir's scheme among two parties.
- Evaluation places $\alpha_1, \alpha_2 \in F_p$.

Our Classifier (PHYS Leakage)

- For every $k \in \{0, 1, \ldots, \lambda - 1\}$,:
  - Check $(2^k\alpha_1, \alpha_2)$ is secure against LSB leakage
- If all checks pass, then (α_1, α_2) is secure.

Explicit Derandomization

Secure evaluation places:

$$\alpha_1 : \alpha_2 = 1 : 2^{\lfloor \lambda/2 \rfloor} - 1.$$

Secure evaluation places against PHYS Leakage 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 Λ in the above table represents the set of elements

$$\{\Lambda, \Lambda \cdot 2, \Lambda \cdot 2^2, \ldots, \Lambda \cdot 2^{\lambda-1}\}.$$

- Each element Λ in the above table stands for evaluation places $(1, \Lambda)$
- For example, the element 95 stands for

$$95 \cdot \langle 2 \rangle = \{95, 2 \cdot 95, 2^2 \cdot 95, \ldots, 2^{12} \cdot 95\}$$

Generalization

- Security parameter λ.
- Fix Mersenne $(p = 2^\lambda - 1)$ or Fermat $(p = 2^\lambda + 1)$ prime field F_p.
- Shamir's scheme among n parties where all parties are required to reconstruct the secret.
- Evaluation places $\alpha_1, \alpha_2, \ldots, \alpha_n \in F_p$.

Our Theorem (Generalization)

- For all $i \in \{1, 2, \ldots, n\}$, compute Lagrange multipliers $\beta_i = \left(\alpha_i \prod_{j \neq i} (\alpha_i - \alpha_j)\right)^{-1}$.
- If there exists $1 \leqslant i < j \leqslant n$ such that (β_i, β_j) is secure against PHYS leakage, then the evaluation places $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ are secure.

Derandomization

Pick Λ such that $(1, \Lambda)$ is declared "secure" by previous classifier. Then, $(\alpha_1, \ldots, \alpha_n)$ is leakage resilient for the following choice of evaluation places.

$$\alpha_1 = (n-1),$$
$$\alpha_2 = (n-1) - (1+\Lambda) = (n-2-\Lambda)$$
$$\alpha_j = (j-2) \cdot (1+\Lambda). \qquad \text{(For } j \in \{3, 4, 5, \ldots, n\}\text{)}$$

Summary

Our Results

- Classifiers to identify secure evaluation places for two party using Shamir's scheme and explicit derandomization.
  - Against LSB Leakage: Any prime field.
  - Against PHYS Leakage: Mersenne or Fermat prime field.
- Classifier to identify secure evaluation places for three or more parties where all parties are required for reconstruction.
  - Against PHYS Leakage: Mersenne or Fermat prime field.

Conclusion

Recall: Our correlation estimation recipe

1. **Small norm estimation.** Approximate a summation by an integral.
2. **Integral estimation.** Determine a closed-form expression.

Open Problems: Derandomization over prime field

- Multi-bit leakage: Connected to (generalizations of) Dedekind sums + Reciprocity laws.
- More general prime field: Modulus switching.
- General (n, k) : Well-principled mathematical formulation is lacking.

Conclusion

Recall: Our correlation estimation recipe

1. **Small norm estimation.** Approximate a summation by an integral.
2. **Integral estimation.** Determine a closed-form expression.

Open Problems: Derandomization over prime field

- Multi-bit leakage: Connected to (generalizations of) Dedekind sums + Reciprocity laws.
- More general prime field: Modulus switching.
- General (n, k) : Well-principled mathematical formulation is lacking.

Thank you!

Acknowledgement

This work is supported in part by the U.S. National Science Foundation under grants CNS-2055605 and CCF-2327981.