Constructing Locally Leakage-resilient Linear Secret-sharing Schemes

Hemanta K. Maji   Anat Paskin-Cherniavsky   Tom Suad   Mingyuan Wang

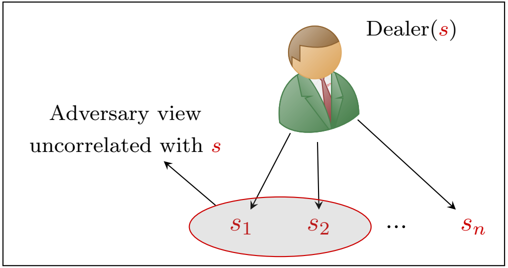
PURDUE UNIVERSITY

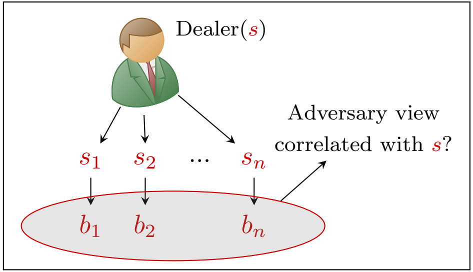
ARIEL UNIVERSITY

August, 2021 (CRYPTO–2021)

Local Leakage-resilient Secret-Sharing

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





Secret-sharing schemes

- Classical security ensures that any unauthorized set of shares is uncorrelated with the secret.
- What if an adversary leaks local information (e.g., one bit b_i) from every share through side-channel attacks? Is the secret still hidden given the leakage?
  - *Local leakage-resilient secret-sharing* ensures that the secret remains hidden.

Leakage-resilient Secret-sharing

A useful primitive connected to many other fields

- Repairing error-correcting codes
  [Guruswami Wootters STOC'16, Tamo Ye Barg FOCS'17, Guruswami Rawat SODA'17, ...]
- Secure multiparty computation protocol resilient to local leakage attacks
  [Benhamouda Degwekar Ishai Rabin CRYPTO'18, ...]
- Modular building block for other primitives (e.g., non-malleable secret-sharing)
  [Goyal Kumar STOC'18, Srinivasan Vasudevan CRYPTO'19, ...]
- ...

Leakage-resilient Secret-sharing

Construct new secret-sharing schemes that are leakage-resilient

Aggarwal Damgård Nielsen Obremski Purwanto Ribeiro Simkin CRYPTO'19,
Srinivasan Vasudevan CRYPTO'19,
Kumar Meka Sahai FOCS'19,
Chattopadhyay Goodman Goyal Kumar Li Meka Zuckerman FOCS'20

- Usually incurs significant overheads and loses algebraic structure (e.g, linearity).

Leakage-resilience of prominent secret-sharing schemes

Benhamouda Degkewar Ishai Rabin CRYPTO'18,
Nielsen Simkin EUROCRYPT'20,
Maji Nguyen Paskin-Cherniavsky Suad Wang EUROCRYPT'21,
Adams Maji Nguyen Nguyen Paskin-Cherniavsky Suad Wang ISIT'21

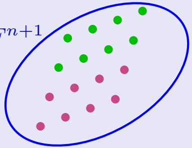
- Significant impact on real-world implementation
- Our work belongs to this line of research.

This Work

Massey Secret-sharing Scheme corresponding to a Random Linear Code

- Massey Secret-sharing corresponding to a code C:

$C \subseteq F^{n+1}$



$\Longrightarrow$

secret shares of s
$(s, s_1, \ldots, s_n) \leftarrow C$

secret shares of s'
$(s', s_1, \ldots, s_n) \leftarrow C$

  - Every linear secret-sharing is a Massey secret-sharing corresponding to some linear code.
    Shamir $\longleftrightarrow$ Reed-Solomon code
    Additive $\longleftrightarrow$ Parity code

- Random Linear Code:
  - The generator matrix $G \in F^{(k+1)\times(n+1)}$ is sampled uniformly at random.
  - Over sufficiently large field, a random matrix is MDS with overwhelming probability.
  - When G is MDS, Massey secret-sharing corresponding to G, is a threshold secret-sharing with n parties and reconstruction threshold $k+1$.

Main Result I

- Let λ be the security parameter, which represents the size of each secret share.
- Every secret share is an element from a prime field F, where $|F| \approx 2^{\lambda}$.
- m bits are leaked from every secret share.

Leakage-resilience of Massey Secret-Sharing

Let n be the number of parties. Let $k+1$ be the reconstruction threshold. Let m be any constant. If we have

$$k > n/2,$$

the Massey secret-sharing scheme corresponding to a random matrix $G \in F^{(k+1)\times(n+1)}$ is m-bit local leakage-resilient *except* with $\exp(-\Theta(n))$ probability.

- We do need $n < \lambda$ to ensure that G is MDS w.h.p.
- For example, $k = \frac{1}{3}\lambda$ and $n = \frac{1}{2}\lambda$.

Main Result II

A bottleneck for the existing analytic approaches

- Benhamouda Degwekar Ishai Rabin CRYPTO'18 introduced an innovative Fourier analytic approach, which is adopted by all existing works, to prove leakage-resilience.
- We show that this existing approach is bound to fail when $k < n/2$.
  - A Fourier analytic proxy is used to upper-bound the statistical distance.
  - We consider the leakage function to be the indicator function of quadratic residuosity.

$$L(x) = \begin{cases} 1 & x \text{ is a quadratic residue} \\ 0 & \text{otherwise} \end{cases}$$

  - For any linear secret sharing scheme, the analytic proxy is $\geqslant 1$ for this leakage function.
- Our first result is optimal w.r.t. the existing technical approach. Proving leakage-resilience (even against a single function) for $k < n/2$ requires significantly different ideas.
  - Motivation: MPC based on Shamir secret-sharing with $k < n/2$ is multiplication friendly.
  - Ongoing works: Prove leakage-resilience for any small leakage family $\mathcal{L}$.

Relevant Prior Works

Benhamouda Degwekar Ishai Rabin CRYPTO'18

For any MDS code G, Massey secret-sharing corresponding to G is leakage-resilient when m-bit is leaked from every share as long as $k > \delta_m \cdot n$.

- δ_m increases as m increases.
- $\delta_1 \approx 0.85$.

In particular, Shamir secret-sharing is 1-bit leakage-resilient if $k \geqslant 0.85n$.

	Construction	# of bits leaked m
BDIR'18	Any MDS G	$k > \delta_m \cdot n$
This work	Random G	$k > 0.5 \cdot n$

Relevant Prior Works

Maji Nguyen Paskin-Cherniavsky Suad Wang EUROCRYPT'21

- Shamir Secret-sharing with randomly chosen evaluation places.
- Only Physical-bit leakages.
- With overwhelming probability, Shamir Secret-sharing scheme with randomly chosen evaluation places is m-bit leakage-resilient even for $(k+1) = 2$, $n = \mathsf{poly}(\lambda)$, and any constant m.
  - Also employs the Fourier analytic approach and their results hold for the $k < n/2$ case.
  - This does not contradict the bottleneck we show as they only consider physical-bit leakage. (Testing whether a field element is a quadratic residue cannot be simulated by physical-bit leakage.)

	Construction	Leakage function	# of bits leaked m
BDIR'18	Any MDS G	general	$k > \delta_m \cdot n$
MNPSW'21	Random $G \leftarrow \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & U_1 & U_2 & \dots & U_n \\ 0 & U_1^2 & U_2^2 & \dots & U_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & U_1^k & U_2^k & \dots, & U_n^k \end{pmatrix}$	physical-bit	$(k+1) \geqslant 2$, $n = \mathsf{poly}(\lambda)$
This work	Random G	general	$k > 0.5 \cdot n$

Technical Overview

Leakage-resilience of Massey Secret Sharing

F is a prime field of size $\approx 2^{\lambda}$. The Massey secret-sharing scheme corresponding to a random matrix $G \in F^{(k+1)\times(n+1)}$ is local leakage-resilient as long as $k > n/2$.

Typical union bound (over leakage functions) would not work!

1. Fix a leakage function L and prove: "most G are secure against this L"
2. Union bound over all possible choices of L

Would not work! Why?

- Total number of leakage functions:
  - Assume 1-bit leakage from every share $L\colon F \to \{0,1\}$.
  - Number of leakage functions for every share: $2^{|F|}$.
  - Total number of leakage function: $\left(2^{|F|}\right)^{n} = 2^{|F|\cdot n}$.
- The size of the family of constructions:
  - Determined by the generator matrix $G \in F^{(k+1)\times(n+1)}$.
  - Number of constructions: $|F|^{(k+1)(n+1)} \approx 2^{\log(|F|)\cdot k\cdot n}$

Key Technical Observation

A New Set of Tests

- γ, σ, a are appropriate constants.
- A test is specified by a product space $\mathbf{V} = V_1 \times V_2 \times \cdots \times V_n \subseteq F^n$. (Every V_i is of size γ.)
- A codeword $\mathbf{c} \in F^n$ is "bad" (for the test $\mathbf{V}$) if a large fraction ($\geqslant \sigma$) of the coordinates fall into V_i.
$$\left|\{i \,:\, c_i \in V_i\}\right| \geqslant \sigma \cdot n.$$
- A code G passes the test if few ($< a^n$) codewords are "bad".

Intuition

- Fix a leakage function $(L_1, \cdots, L_n)$. V_i represents the set of large Fourier coefficients for L_i.
- If a code passes all tests, it is leakage-resilient.

  For any leakage function, only few ($< a^n$) codewords has many coordinates ($< \sigma \cdot n$) with large Fourier coefficients.

- Inspired by pseudorandomness literature.

Proof Overview

The number of tests is much smaller than the number of leakage functions!

- Number of tests $\mathbf{V} = V_1 \times V_2 \times \cdots \times V_n$: $\binom{|F|}{\gamma}^n \approx |F|^{\gamma \cdot n}$
- Number of leakage functions: $\left(2^{|F|}\right)^n$

Proof Overview

1. Fix a test $\mathbf{V} = V_1 \times V_2 \times \cdots \times V_n$, prove that "most G passes this test".
   - Combinatorial argument.
2. Use union bound (over test $\mathbf{V}$) to prove that most G passes <u>all</u> tests.
3. G passes all tests $\Longrightarrow$ G is leakage-resilient
   - Fourier analytic argument introduced by BDIR'18
   - Inherently requires $k > n/2$.

The Bottleneck

1/2 Barrier for the existing Fourier analytic approach

The existing Fourier analytic approach cannot prove leakage-resilience when $k \leqslant n/2$.

- In particular, it cannot prove leakage-resilience for one single function, i.e., the indicator function of quadratic residuosity.
- Intuition: Indicator function of quadratic residuosity is the function that maximizes the L_1 norm of the Fourier coefficients.

$$\arg\max_f \sum_{\alpha \in F} \left| \widehat{f}(\alpha) \right|.$$

Ongoing works

- For any small leakage family $\mathcal{L}$, a random code G is leakage-resilient to $\mathcal{L}$.
  - $\mathcal{L}$ could contain the indicator function of quadratic residuosity.
  - Rely on a purely combinatorial argument.
- Identifying the optimal attacks

Thanks!

Full version eprint.iacr.org/2020/1517