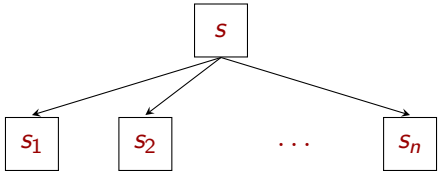
Leakage-resilient Linear Secret-sharing against arbitrary Bounded-size Leakage Family

Hemanta K. Maji Hai H. Nguyen Anat Paskin-Cherniavsky Tom Suad
Mingyuan Wang Xiuyu Ye Albert Yu

PURDUE UNIVERSITY ARIEL UNIVERSITY Berkeley UNIVERSITY OF CALIFORNIA

TCC–2022

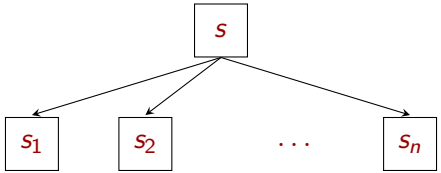
Secret-sharing



Correctness: any $\geqslant k$ shares can reconstruct s

Privacy: any $< k$ shares reveals no information about s

Secret-sharing



Correctness: any $\geqslant k$ shares can reconstruct s

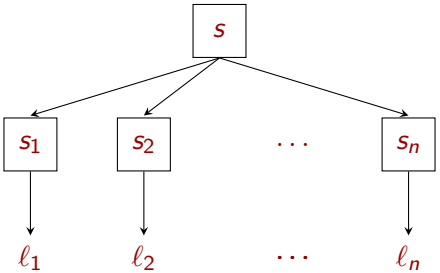
Privacy: any $< k$ shares reveals no information about s

Concern: Side-channel attacks

What if an adversary obtains partial information from secret shares?

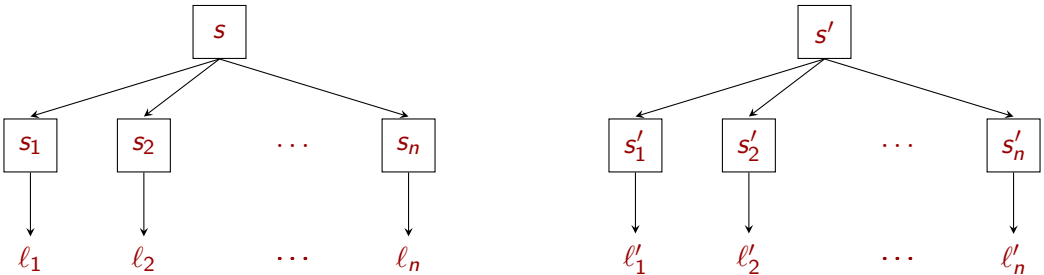
Local Leakage-resilient Secret-Sharing

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



Local Leakage-resilient Secret-Sharing

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



Leakage-resilience: $(\ell_1, \ell_2, \ldots, \ell_n) \approx (\ell'_1, \ell'_2, \ldots, \ell'_n)$

Leakage-resilient Secret-sharing

Construct new leakage-resilient schemes

[Aggarwal-Damgård-Nielsen-Obremski-Purwanto-Ribeiro-Simkin-19, Srinivasan-Vasudevan-19, Kumar-Meka-Sahai-19, Chattopadhyay-Goodman-Goyal-Kumar-Li-Meka-Zuckerman-20, Brian-Faonio-Obremski-Simkin-Venturi-20, Chandran-Kanukurthi-Obbattu-Sekar-22,...]

- Achieves higher leakage resilience.
- Usually incurs overheads + loses algebraic structure (e.g, linearity, multiplication friendly).

Prove the leakage-resilience of prominent schemes

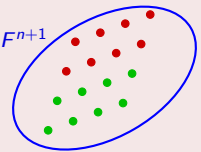
[Benhamouda-Degkewar-Ishai-Rabin-18, Nielsen-Simkin-20, Maji-PaskinCherniavsky-Suad-Wang-21, Maji-Nguyen-PaskinCherniavsky-Suad-Wang-21, Adams-Maji-Nguyen-Paskin-Cherniavsky-Suad-Wang-21, Maji-Nguyen-Paskin-Cherniavsky-Wang-22, Maji-Nguyen-Paskin-Cherniavsky-Suad-Wang-Ye-Yu-22]

- More precise risk assessment.
- Our work belongs to this line of research.

Model: Massey & Shamir Secret-sharing

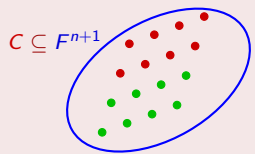
Massey Secret-sharing Scheme

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



Model: Massey & Shamir Secret-sharing

Massey Secret-sharing Scheme



To share a secret s:

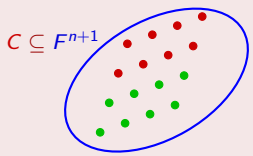
$(s_0, s_1, \ldots, s_n) \leftarrow C$

conditioned on $s_0 = s$,

$s_1, \ldots, s_n$ are secret shares

Model: Massey & Shamir Secret-sharing

Massey Secret-sharing Scheme



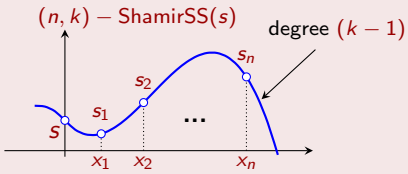
To share a secret s:

$(s_0, s_1, \ldots, s_n) \leftarrow C$

conditioned on $s_0 = s$,

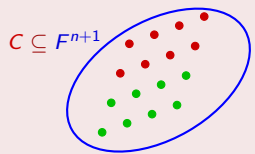
$s_1, \ldots, s_n$ are secret shares

Shamir Secret-sharing scheme



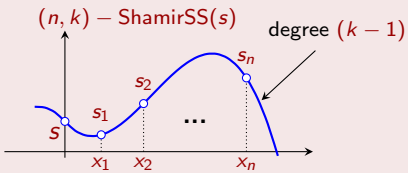
Model: Massey & Shamir Secret-sharing

Massey Secret-sharing Scheme



To share a secret s:
$(s_0, s_1, \ldots, s_n) \leftarrow C$
conditioned on $s_0 = s$,
$s_1, \ldots, s_n$ are secret shares

Shamir Secret-sharing scheme

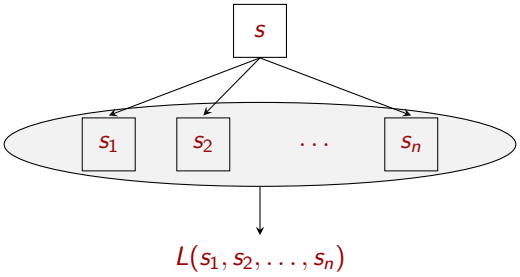


This work considers

1. Massey secret-sharing corresponding to a random linear code C.
   - The generator matrix $G^+ \in F^{k \times (n+1)}$ of C is sampled uniformly at random,
2. Shamir secret-sharing with random evaluation places.
   - $(x_1, x_2, \cdots, x_n)$ are sampled sequentially (without replacement) and uniformly at random.

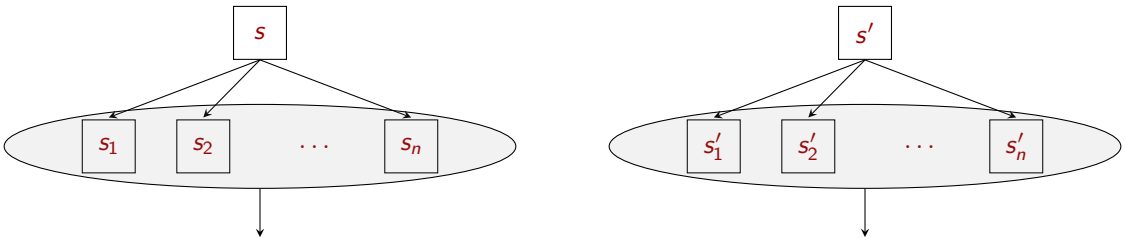
Model: Arbitrary Bounded-size Joint Leakage Family

m-bit Joint Leakage Function: $L\colon F^n \to \{0,1\}^m$



Model: Arbitrary Bounded-size Joint Leakage Family

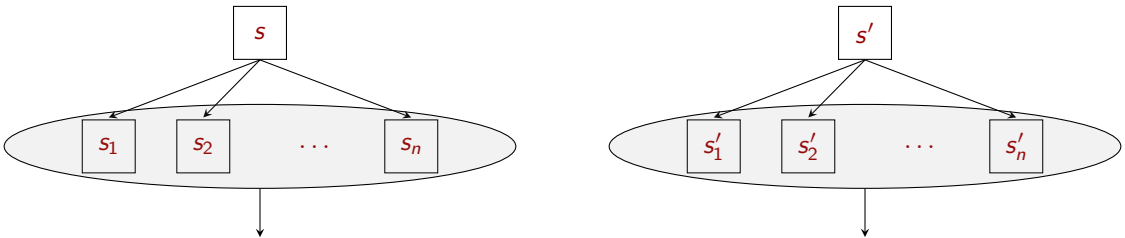
m-bit Joint Leakage Function: $L\colon F^n \to \{0,1\}^m$



Leakage-resilience: $L(s_1, s_2, \ldots, s_n) \approx L(s'_1, s'_2, \ldots, s'_n), \forall s, s' \in F$

Model: Arbitrary Bounded-size Joint Leakage Family

m-bit Joint Leakage Function: $L\colon F^n \to \{0,1\}^m$



Leakage-resilience: $L(s_1, s_2, \ldots, s_n) \approx L(s'_1, s'_2, \ldots, s'_n), \forall s, s' \in F$

Leakage-resilient Secret-Sharing

A secret-sharing is ε-leakage-resilient against $\mathcal{L}$ if

$$\mathrm{SD}\left(L(\mathrm{Share}(s)),\ L(\mathrm{Share}(s'))\right) \leqslant \varepsilon, \forall s, s' \in F, L \in \mathcal{L}.$$

Prior Work and Our Contribution

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$

Prior Work and Our Contribution

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$

Prior Work and Our Contribution

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$
MNPSW'21	Shamir secret-sharing with random evaluation places	physical-bit	$k \geqslant 2$, $n = \mathsf{poly}(\lambda)$

Prior Work and Our Contribution

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$
MNPSW'21	Shamir secret-sharing with random evaluation places	physical-bit	$k \geqslant 2$, $n = \mathrm{poly}(\lambda)$
MNPW'22	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.78 \cdot n$

Prior Work and Our Contribution

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$
MNPSW'21	Shamir secret-sharing with random evaluation places	physical-bit	$k \geqslant 2$, $n = \mathrm{poly}(\lambda)$
MNPW'22	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.78 \cdot n$
Our work	Massey secret-sharing of a random linear code	arbitrary bounded-size joint leakage	$k \geqslant 4$, $n = \mathrm{poly}(\lambda)$
	Shamir secret-sharing with random evaluation places	arbitrary bounded-size joint leakage	$k > 0.5 \cdot n$, $n = \mathrm{poly}(\lambda)$

Main Result I

- Let λ be the security parameter.
- Every secret share is an element of a field F, where $|F| \approx 2^{\lambda}$.
- Let n be the number of parties, k be the reconstruction threshold s.t. $n = \text{poly}(\lambda)$.
- Let $\mathcal{L}$ be any m-bit leakage family of size at most $|F|^{k-3.01}/8^m$.

Theorem (Leakage-resilience of Massey secret-sharing scheme)

Massey secret-sharing corresponding to a random generator matrix $\mathbf{G}^+ \in F^{k\times(n+1)}$ *is* $\exp(\Omega(-\lambda))$*-leakage-resilient against* $\mathcal{L}$ *except with probability* $\exp(\Omega(-\lambda))$.

Main Result I

- Let λ be the security parameter.
- Every secret share is an element of a field F, where $|F| \approx 2^{\lambda}$.
- Let n be the number of parties, k be the reconstruction threshold s.t. $n = \text{poly}(\lambda)$.
- Let $\mathcal{L}$ be any m-bit leakage family of size at most $|F|^{k-3.01}/8^m$.

Theorem (Leakage-resilience of Massey secret-sharing scheme)

Massey secret-sharing corresponding to a random generator matrix $\mathbf{G}^+ \in F^{k\times(n+1)}$ *is* $\exp(\Omega(-\lambda))$*-leakage-resilient against* $\mathcal{L}$ *except with probability* $\exp(\Omega(-\lambda))$.

Remarks: Our result

- requires $k \geqslant 4$ only,
- bypasses the bottleneck due to the existing Fourier approach,
- enables secure computation of secrets, and
- is near optimal (in terms of the size of the leakage family).

Main Result II

- Let λ be the security parameter.
- Every secret share is an element of a prime field F, where $|F| \approx 2^{\lambda}$.
- Let n be the number of parties, k be the reconstruction threshold s.t. $n = \text{poly}(\lambda)$.
- Let $\mathcal{L}$ be any m-bit leakage family of size at most $|F|^{2k-n-3.01}/8^m$.

Theorem (Leakage-resilience of Shamir secret-sharing)

k-out-of-n Shamir secret-sharing with random evaluation places is $\exp(\Omega(-\lambda))$-leakage-resilient against $\mathcal{L}$ except with probability $\exp(\Omega(-\lambda))$.

Main Result II

- Let λ be the security parameter.
- Every secret share is an element of a prime field F, where $|F| \approx 2^{\lambda}$.
- Let n be the number of parties, k be the reconstruction threshold s.t. $n = \mathrm{poly}(\lambda)$.
- Let $\mathcal{L}$ be any m-bit leakage family of size at most $|F|^{2k-n-3.01}/8^m$.

Theorem (Leakage-resilience of Shamir secret-sharing)

k-out-of-n Shamir secret-sharing with random evaluation places is $\exp(\Omega(-\lambda))$-leakage-resilient against $\mathcal{L}$ except with probability $\exp(\Omega(-\lambda))$.

Remarks: Our result

- requires $k > n/2$,
- is near-optimal due to the barrier of the existing Fourier approach.

Technical Overview: Massey Secret-sharing Result

Objective. Massey secret-sharing corresponding to random generator matrix $\mathbf{G}^+$ is leakage-resilient against any bounded-size leakage family $\mathcal{L}$ with high probability.

High-level Idea. Combinatorial argument + second-moment technique.

Technical Overview: Massey Secret-sharing Result

Objective. Massey secret-sharing corresponding to random generator matrix $\mathbf{G}^+$ is leakage-resilient against any bounded-size leakage family $\mathcal{L}$ with high probability.

High-level Idea. Combinatorial argument + second-moment technique.

1. **Reduction.** Suffices to prove that, for any subset $A \subseteq F^n$, the random variable $\mathbf{X}_{s,A}$ is small with high probability.

$$\mathbf{X}_{s,A} = \frac{1}{|F|^k} \cdot \left(\left| \langle \mathbf{G} \rangle \cap A \right| - \left| \left(\langle \mathbf{G} \rangle + s \cdot \vec{\mathbf{v}} \right) \cap A \right| \right)$$

Technical Overview: Massey Secret-sharing Result

Objective. Massey secret-sharing corresponding to random generator matrix $\mathbf{G}^+$ is leakage-resilient against any bounded-size leakage family $\mathcal{L}$ with high probability.

High-level Idea. Combinatorial argument + second-moment technique.

1. **Reduction.** Suffices to prove that, for any subset $A \subseteq F^n$, the random variable $\mathbf{X}_{s,A}$ is small with high probability.

$$\mathbf{X}_{s,A} = \frac{1}{|F|^k} \cdot \left(|\langle \mathbf{G} \rangle \cap A| - \left| \left(\langle \mathbf{G} \rangle + s \cdot \vec{\mathbf{v}} \right) \cap A \right| \right)$$

2. **Bounding using the second-moment technique.** $\Pr_{\mathbf{G}}[|\mathbf{X}_{\mathbf{s},\mathbf{A}}| \geqslant t] \leqslant \mathrm{E}[\mathbf{X}^2_{\mathbf{s},\mathbf{A}}]/t^2$
   - Bound the expectation of the second-moment of $\mathbf{X}_{\mathbf{s},\mathbf{A}}$ using a combinatorial approach (crucially relying on the fact G is a fully random matrix).

Technical Overview: Shamir Secret-sharing Result

Objective. Shamir secret-sharing with random evaluation places is leakage-resilient against any bounded-size leakage family $\mathcal{L}$ with high probability.

Bottleneck

- The generator matrix G for Shamir secret-sharing has less randomness.
- The idea used for Massey secret-sharing to bound $\mathrm{E}[\mathbf{X}_{\mathbf{s},\mathbf{A}}^2]$ seems to fail.

High-level Idea. Use existing Fourier-analytic approach with Bézout's theorem [MNPSW21] to bound the second-moment.

Summary

Relevant work	Secret-sharing scheme	Leakage family	Reconstruction threshold k
BDIR'18	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.85 \cdot n$
MPSW'21	Massey secret-sharing of a random linear code	arbitrary local	$k > 0.5 \cdot n$
MNPSW'21	Shamir secret-sharing with random evaluation places	physical-bit	$k \geqslant 2$, $n = \mathrm{poly}(\lambda)$
MNPW'22	Shamir secret-sharing with any fixed evaluation places	arbitrary local	$k > 0.78 \cdot n$
Our work	Massey secret-sharing of a random linear code	arbitrary bounded-size joint leakage	$k \geqslant 4$, $n = \mathrm{poly}(\lambda)$
	Shamir secret-sharing with random evaluation places	arbitrary bounded-size joint leakage	$k > 0.5 \cdot n$, $n = \mathrm{poly}(\lambda)$

Thanks!