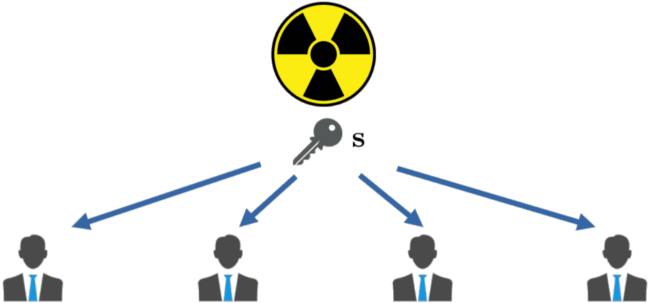
New Bounds on the Local Leakage Resilience of Shamir's Secret Sharing Scheme

Ohad Klein[1] and **Ilan Komargodski**[1,2]

[1] Department of Computer Science, Hebrew University
[2] NTT research

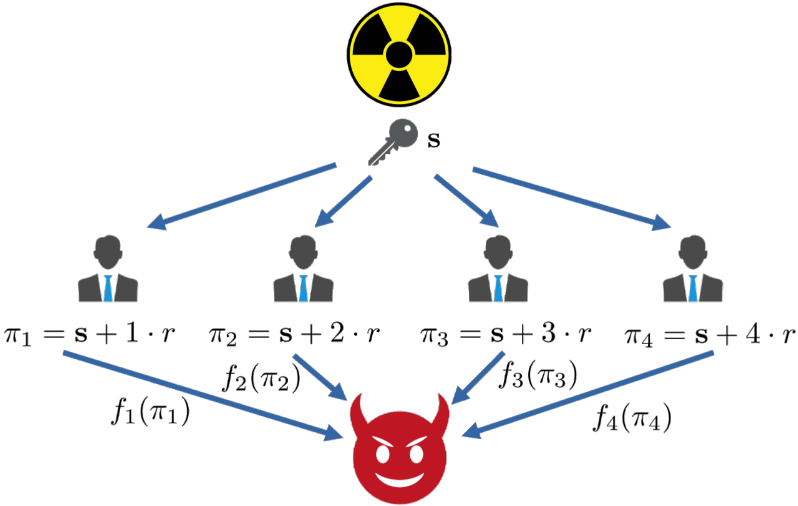
August 21, 2023

Secret Sharing (t out of n)



$\pi_1 = \mathbf{s} + 1 \cdot r$ $\pi_2 = \mathbf{s} + 2 \cdot r$ $\pi_3 = \mathbf{s} + 3 \cdot r$ $\pi_4 = \mathbf{s} + 4 \cdot r$

Local Leakage Resillient Secret Sharing



Applications of Leakage Resilient Secret Sharing

Main Application (Conjectured Benhamouda, Degwekar, Ishai, Rabin '18)

BGW protocol for **MPC** (Ben-Or, Goldwasser, Wigderson '88) is more secure than currently known.

Applications of Leakage Resilient Secret Sharing

Main Application (Conjectured Benhamouda, Degwekar, Ishai, Rabin '18)

BGW protocol for **MPC** (Ben-Or, Goldwasser, Wigderson '88) is more secure than currently known.

Security against local leakage attacks:

- Adversary can leak a small amount of information from each honest party, in addition to controlling malicious parties.
- Adversary obtains only negligible information of secret input.

Applications of Leakage Resilient Secret Sharing

Main Application (Conjectured Benhamouda, Degwekar, Ishai, Rabin '18)

BGW protocol for **MPC** (Ben-Or, Goldwasser, Wigderson '88) is more secure than currently known.

Security against local leakage attacks:

- Adversary can leak a small amount of information from each honest party, in addition to controlling malicious parties.
- Adversary obtains only negligible information of secret input.

Leakage Resilience is Not Trivial

There are popular MPC protocols which are broken under local leakage attacks.

Applications of Leakage Resilient Secret Sharing

Main Application (Conjectured Benhamouda, Degwekar, Ishai, Rabin '18)

BGW protocol for **MPC** (Ben-Or, Goldwasser, Wigderson '88) is more secure than currently known.

Security against local leakage attacks:

- Adversary can leak a small amount of information from each honest party, in addition to controlling malicious parties.
- Adversary obtains only negligible information of secret input.

Leakage Resilience is Not Trivial

There are popular MPC protocols which are broken under local leakage attacks.

- Leakage resilient circuit compilers.
- Threshold cryptographic systems.

Definition of Secret Sharing (t out of n)

$\mathbf{s}$ denotes secret, π_i denotes share. Assume $\mathbf{s}, \pi_i \in \mathbb{F}_q$.

Definition (Secret Sharing, t out of n)

A randomized algorithm $\mathbf{s} \mapsto (\pi_1, \ldots, \pi_n)$ s.t.

- **Reconstruction:** Any t shares determine $\mathbf{s}$ uniquely.
- **Indistinguishability:** Knowledge of less than t shares reveals nothing about $\mathbf{s}$.

Definition of Secret Sharing (t out of n)

$\mathbf{s}$ denotes secret, π_i denotes share. Assume $\mathbf{s}, \pi_i \in \mathbb{F}_q$.

Definition (Secret Sharing, t out of n)

A randomized algorithm $\mathbf{s} \mapsto (\pi_1, \ldots, \pi_n)$ s.t.

- **Reconstruction:** Any t shares determine $\mathbf{s}$ uniquely.
- **Indistinguishability:** Knowledge of less than t shares reveals nothing about $\mathbf{s}$.

Shamir's Secret Sharing Example (3 out of 5)

Let $r_1, r_2 \sim \mathbb{F}_q$ uniformly random.

$$\pi_1 = \mathbf{s} + 1 \cdot r_1 + 1^2 \cdot r_2,$$
$$\pi_2 = \mathbf{s} + 2 \cdot r_1 + 2^2 \cdot r_2,$$
$$\vdots$$
$$\pi_5 = \mathbf{s} + 5 \cdot r_1 + 5^2 \cdot r_2.$$

Definition of Leakage Resilient Secret Sharing

$\mathbf{s}$ denotes secret, π_i denotes share. Assume $\mathbf{s}, \pi_i \in \mathbb{F}_q$.

Definition (Leakage Resilient SS)

SS is resilient against leakage functions $f_1, \ldots, f_n$ if
knowledge of $\mathbf{Leak} = (f_1(\pi_1), \ldots, f_n(\pi_n))$ reveals almost nothing about $\mathbf{s}$.

Definition of Leakage Resilient Secret Sharing

s denotes secret, π_i denotes share. Assume $\mathbf{s}, \pi_i \in \mathbb{F}_q$.

Definition (Leakage Resilient SS)

SS is resilient against leakage functions $f_1, \ldots, f_n$ if
knowledge of **Leak** $= (f_1(\pi_1), \ldots, f_n(\pi_n))$ reveals almost nothing about **s**.

Various Security Models

- f_i outputs a few bits.
- f_i depends on several shares.
- f_i easy to compute.

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ leakage resilient if:

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ **leakage resilient if:**

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.92n$. (BDIR '18)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ **leakage resilient if:**

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.92n$. (BDIR '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.78n$. (Maji, Nguyen, Paskin-C., Wang '22)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ **leakage resilient if:**

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.92n$. (BDIR '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.78n$. (Maji, Nguyen, Paskin-C., Wang '22)
- $f_i : \mathbb{F}_p \to \{0,1\}^{\epsilon \lg(p)}$ output 'physical' bits of π_i, and $t \geq \epsilon n$. (M., N., P-C., Suad, W. '21)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ **leakage resilient if:**

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.92n$. (BDIR '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.78n$. (Maji, Nguyen, Paskin-C., Wang '22)
- $f_i : \mathbb{F}_p \to \{0,1\}^{\epsilon \lg(p)}$ output 'physical' bits of π_i, and $t \geq \epsilon n$. (M., N., P-C., Suad, W. '21)
- Random linear SS is resilient against $f_i : \mathbb{F}_p \to \{0,1\}$ if $t \geq (0.5+\epsilon)n$. (MPSW '20)

Applications vs. Previous Results

What is missing for MPC application?

Shamir's secret sharing is resilient for $t = (1-\epsilon)n/2$. (Security against passive adversary.)
Shamir's secret sharing is resilient for $t = (1-\epsilon)n/3$. (Active adversary.)

Theorems

Shamir's SS is $\exp(-n^c)$ **leakage resilient if:**

- $f_i : \mathbb{F}_p \to \{0,1\}^{\lg(p)/4}$ and $t \geq n - n^{1/4}$. (Benhamouda, Degwekar, Ishai, Rabin '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.92n$. (BDIR '18)
- $f_i : \mathbb{F}_p \to \{0,1\}$ and $t \geq 0.78n$. (Maji, Nguyen, Paskin-C., Wang '22)
- $f_i : \mathbb{F}_p \to \{0,1\}^{\epsilon \lg(p)}$ output 'physical' bits of π_i, and $t \geq \epsilon n$. (M., N., P-C., Suad, W. '21)
- Random linear SS is resilient against $f_i : \mathbb{F}_p \to \{0,1\}$ if $t \geq (0.5+\epsilon)n$. (MPSW '20)
- $\exists$ non-linear SS against $f_i : \mathbb{F}_p \to \{0,1\}^{0.99 \lg(p)}$, $\forall$ access structure. (Srinivasan, Vasudevan '19)

• • •

Limitations of Linear Leakage Resilience

Shamir SS with small t is not leakage resilient

$\forall$ linear SS with threshold t, $\exists$ one-bit leakage functions with $I(\mathbf{s}; \mathbf{Leak}) \geq \exp(-t)$.

$\Longrightarrow$ Leakage resilience may hold only if t, n are large.

Limitations of Linear Leakage Resilience

Shamir SS with small t is not leakage resilient

$\forall$ linear SS with threshold t, $\exists$ one-bit leakage functions with $I(\mathbf{s}; \mathbf{Leak}) \geq \exp(-t)$.
$\implies$ Leakage resilience may hold only if t, n are large.

Shamir SS with $q = 2^k$ is not resilient (Guruswami Wootters '15)

If $q = 2^k$ equals $n = 2t$, then $\mathbf{s}$ is **completely** determined by $(f_i(\pi_i))_{i=1}^n$ for $f_i : \mathbb{F}_q \to \{0, 1\}$.
$\implies$ Leakage resilience makes sense primarily over $\mathbb{F}_p$.

Limitations of Linear Leakage Resilience

Shamir SS with small t is not leakage resilient

$\forall$ linear SS with threshold t, $\exists$ one-bit leakage functions with $I(\mathbf{s}; \mathbf{Leak}) \geq \exp(-t)$.

$\implies$ Leakage resilience may hold only if t, n are large.

Shamir SS with $q = 2^k$ is not resilient (Guruswami Wootters '15)

If $q = 2^k$ equals $n = 2t$, then $\mathbf{s}$ is **completely** determined by $(f_i(\pi_i))_{i=1}^n$ for $f_i : \mathbb{F}_q \to \{0, 1\}$.

$\implies$ Leakage resilience makes sense primarily over $\mathbb{F}_p$.

t and n are of same order of magnitude (Nielsen Simkin '19)

$\exists c > 0$ s.t. if $t < cn/\log(n)$, $\exists$ one-bit leakage functions with $I(\mathbf{s}; \mathbf{Leak}) \geq c$.

$\implies$ Leakage resilience essentially requires $t = \Omega(n)$.

Our results

Let $s \mapsto \pi$ be linear SS. **Leak** $= (f_1(\pi_1), \ldots, f_n(\pi_n))$ for $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}$. $p = 2^{o(n)}$.

Theorem (Main)

For all secrets $s_1, s_2 \in \mathbb{F}_p$,

$$\mathrm{SD}(\textbf{Leak} \mid \mathbf{s} = s_1 \ , \ \textbf{Leak} \mid \mathbf{s} = s_2) \leq \text{New Proxy}.$$

Our results

Let $s \mapsto \pi$ be linear SS. **Leak** $= (f_1(\pi_1), \ldots, f_n(\pi_n))$ for $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}$. $p = 2^{o(n)}$.

Theorem (Main)

For all secrets $s_1, s_2 \in \mathbb{F}_p$,

$$\mathrm{SD}(\textbf{Leak} \mid \mathbf{s} = s_1 \ , \ \textbf{Leak} \mid \mathbf{s} = s_2) \leq \text{New Proxy}.$$

Corollary (General Bound)

Shamir's secret sharing is Leakage Resilient once $t \geq 0.69n$.

Our results

Let $s \mapsto \pi$ be linear SS. **Leak** $= (f_1(\pi_1), \ldots, f_n(\pi_n))$ for $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}$. $p = 2^{o(n)}$.

Theorem (Main)

For all secrets $s_1, s_2 \in \mathbb{F}_p$,

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2) \leq \text{New Proxy}.$$

Corollary (General Bound)

Shamir's secret sharing is Leakage Resilient once $t \geq 0.69n$.

Corollary (Bound for Hard-Cases)

If $\Pr[f_i = 0] = 1/2 \pm \epsilon$ then Shamir's secret sharing is Leakage Resilient once $t \geq 0.58n$.

Our results

Let $s \mapsto \pi$ be linear SS. **Leak** $= (f_1(\pi_1), \ldots, f_n(\pi_n))$ for $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}$. $p = 2^{o(n)}$.

Theorem (Main)

For all secrets $s_1, s_2 \in \mathbb{F}_p$,

$$\mathrm{SD}(\textbf{Leak} \mid \mathbf{s} = s_1 \ , \ \textbf{Leak} \mid \mathbf{s} = s_2) \leq \text{New Proxy}.$$

Corollary (General Bound)

Shamir's secret sharing is Leakage Resilient once $t \geq 0.69n$.

Corollary (Bound for Hard-Cases)

If $\Pr[f_i = 0] = 1/2 \pm \epsilon$ then Shamir's secret sharing is Leakage Resilient once $t \geq 0.58n$.

Corollary (Going below $t = n/2$)

If $\Pr[f_i = 0] < \epsilon$ then Shamir's secret sharing is Leakage Resilient once $t \geq 0.01n$.

Main Result

Let $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}$. Let $I \subseteq [n]$. Define

$$f(I) := \max_{s \in \mathbb{F}_p} \left| \Pr\left[\bigoplus_{i \in I} f_i(\pi_i) = 0 \,\middle|\, \mathbf{s} = s \right] - \Pr\left[\bigoplus_{i \in I} f_i(\pi_i) = 0 \right] \right| .$$

Theorem (New Proxy)

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2)^4 \le p^{O(1)} \sum_{I \subseteq [n]} f(I)^2.$$

Previous Proxy (BDIR '19)

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2) \le \mathit{Proxy} \ge p^{-O(1)} \sum_{I \subseteq [n]} f(I).$$

Main Result

Let $f_1, \dots, f_n \colon \mathbb{F}_p \to \{0,1\}$. Let $I \subseteq [n]$. Define

$$f(I) := \max_{s \in \mathbb{F}_p} \left| \Pr\left[\bigoplus_{i \in I} f_i(\pi_i) = 0 \,\middle|\, \mathbf{s} = s \right] - \Pr\left[\bigoplus_{i \in I} f_i(\pi_i) = 0 \right] \right| .$$

Theorem (New Proxy)

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \;,\; \mathbf{Leak} \mid \mathbf{s} = s_2)^4 \le p^{O(1)} \sum_{I \subseteq [n]} f(I)^2 .$$

Previous Proxy (BDIR '19)

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \;,\; \mathbf{Leak} \mid \mathbf{s} = s_2) \le \mathit{Proxy} \ge p^{-O(1)} \sum_{I \subseteq [n]} f(I) .$$

Previous Barrier (MPSW '19)

$\exists$ functions $f_1, \dots, f_n$ with $\mathit{Proxy} \ge 1$ whenever $t \le n/2$. Even if $\Pr[f_i = 0] \approx 0$.

(Heuristic) Interpretation of Main Result

Suppose attackers wish to distinguish

$$\mathbf{s} = 0 \qquad \text{and} \qquad \mathbf{s} = 1.$$

(Heuristic) Interpretation of Main Result

Suppose attackers wish to distinguish

$$\mathbf{s} = 0 \qquad \text{and} \qquad \mathbf{s} = 1.$$

Given independent statistical information: samples $s_j \in \{0, 1\}$ and $\epsilon_j \in [-1, 1]$ with guarantee

$$\mathrm{Cov}(\mathbf{s}, s_j) = \epsilon_j, \qquad j = 1 \ldots \ell.$$

Aggregating all information, maximum likelihood of $\mathbf{s}$ gives (optimal) advantage

$$\mathop{\mathbb{E}}_{s_1,\ldots,s_\ell} \left| \Pr\left[\mathbf{s} = 0 \mid s_1, \ldots, s_\ell\right] - \Pr\left[\mathbf{s} = 1 \mid s_1, \ldots, s_\ell\right] \right| = \Theta\left(\sum_j \epsilon_j^2\right).$$

(Heuristic) Interpretation of Main Result

Suppose attackers wish to distinguish

$$\mathbf{s} = 0 \qquad \text{and} \qquad \mathbf{s} = 1.$$

Given independent statistical information: samples $s_j \in \{0, 1\}$ and $\epsilon_j \in [-1, 1]$ with guarantee

$$\mathrm{Cov}(\mathbf{s}, s_j) = \epsilon_j, \qquad j = 1 \dots \ell.$$

Aggregating all information, maximum likelihood of $\mathbf{s}$ gives (optimal) advantage

$$\mathop{\mathbb{E}}_{s_1,\dots,s_\ell} \Big| \Pr[\mathbf{s} = 0 \mid s_1, \dots, s_\ell] - \Pr[\mathbf{s} = 1 \mid s_1, \dots, s_\ell] \Big| = \Theta\Big(\sum_j \epsilon_j^2\Big).$$

Suggested attack

Given the leakage, compute $s_I = \bigoplus_{i \in I} f_i(\pi_i)$. Covariance of s_I with $\mathbf{s}$ is $\epsilon_I = p^{O(1)} f(I)$.
Using MLE, advantage is

$$\sum_I \epsilon_I^2 = p^{O(1)} \sum_I f(I)^2.$$

Open problems

Conjecture (Benhamouda, Degwekar, Ishai, Rabin '18)

Shamir SS over $\mathbb{F}_p$ with $t/n = \alpha > 0$ and **arbitrary** 1-bit leakage from each share satisfies

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2) \leq \exp(-O_\alpha(n)). \quad (1)$$

Open problems

Conjecture (Benhamouda, Degwekar, Ishai, Rabin '18)

Shamir SS over $\mathbb{F}_p$ with $t/n = \alpha > 0$ and **arbitrary** 1-bit leakage from each share satisfies

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2) \leq \exp(-O_\alpha(n)). \quad (1)$$

Problem (indistinguishability using XOR)

Under same conditions, prove

$$f([n]) = \max_{s \in \mathbb{F}_p} \left| \Pr\left[\bigoplus_{i=1}^{n} f_i(\pi_i) = 0 \,\middle|\, \mathbf{s} = s \right] - \Pr\left[\bigoplus_{i=1}^{n} f_i(\pi_i) = 0 \right] \right| = \exp(-O_\alpha(n)).$$

$*$ Currently known only for $\alpha > 1/2$.

Open problems

Conjecture (Benhamouda, Degwekar, Ishai, Rabin '18)

Shamir SS over $\mathbb{F}_p$ with $t/n = \alpha > 0$ and **arbitrary** 1-bit leakage from each share satisfies

$$\mathrm{SD}(\mathbf{Leak} \mid \mathbf{s} = s_1 \ , \ \mathbf{Leak} \mid \mathbf{s} = s_2) \leq \exp(-O_\alpha(n)). \quad (1)$$

Problem (indistinguishability using XOR)

Under same conditions, prove

$$f([n]) = \max_{s \in \mathbb{F}_p} \left| \Pr\left[\bigoplus_{i=1}^{n} f_i(\pi_i) = 0 \,\middle|\, \mathbf{s} = s \right] - \Pr\left[\bigoplus_{i=1}^{n} f_i(\pi_i) = 0 \right] \right| = \exp(-O_\alpha(n)).$$

$*$ Currently known only for $\alpha > 1/2$.

Problem (Generalize to multi-bit leakage)

Find useful bound for (1) when $f_1, \ldots, f_n \colon \mathbb{F}_p \to \{0,1\}^m$ for $m > 1$.

Thank You!