Towards Breaking the Half-Barrier of Local Leakage-resilient Shamir's Secret Sharing

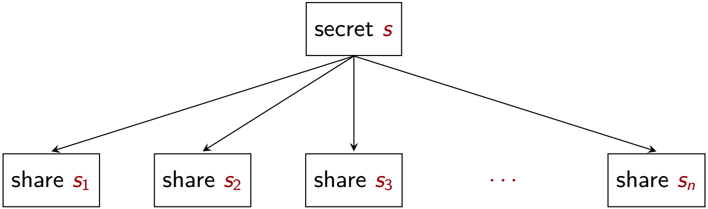
Hai H. Nguyen

ETH zürich

CRYPTO–2024

Threshold Secret Sharing [Shamir, Blakley]

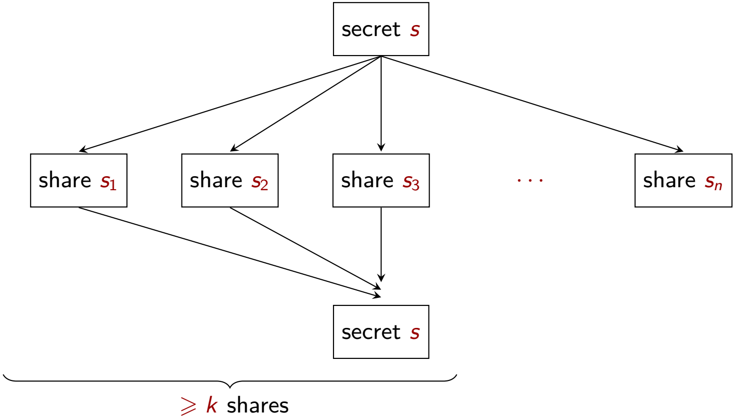
Sharing:



Threshold Secret Sharing [Shamir, Blakley]

Sharing:

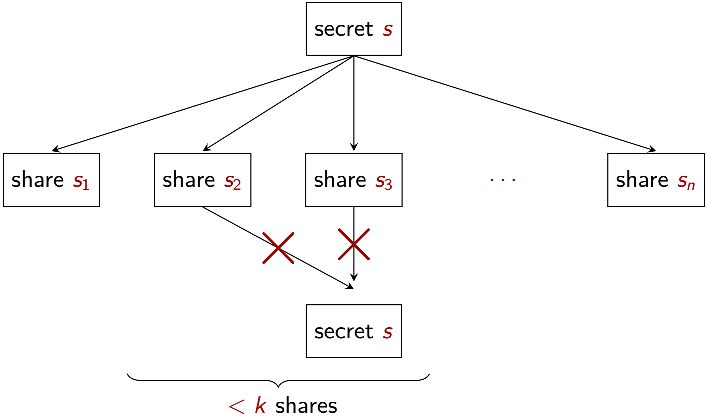
Reconstruction:



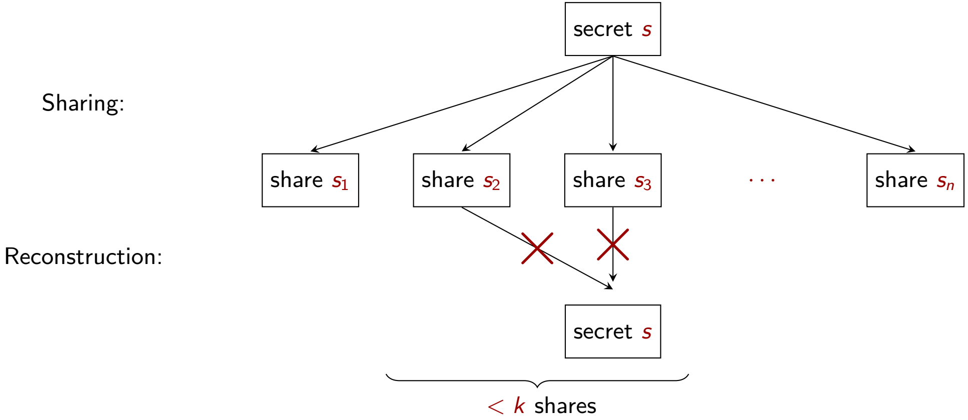
Threshold Secret Sharing [Shamir, Blakley]

Sharing:

Reconstruction:



Threshold Secret Sharing [Shamir, Blakley]

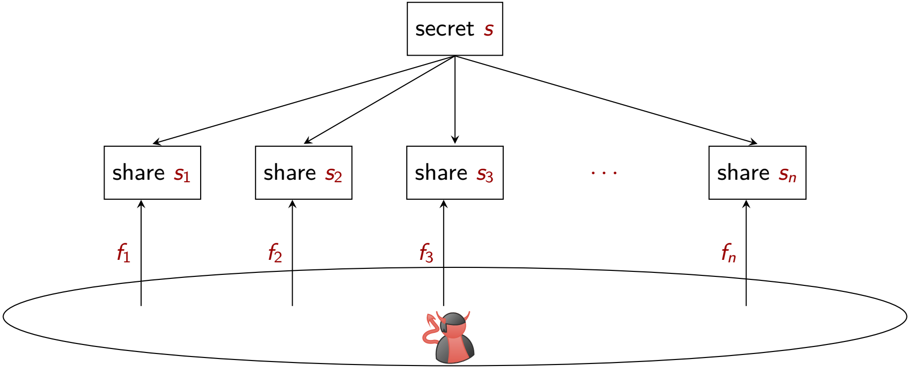


Concern: Side-channel attacks

- "All-or-nothing" no longer true
- Revealing partial information from every share

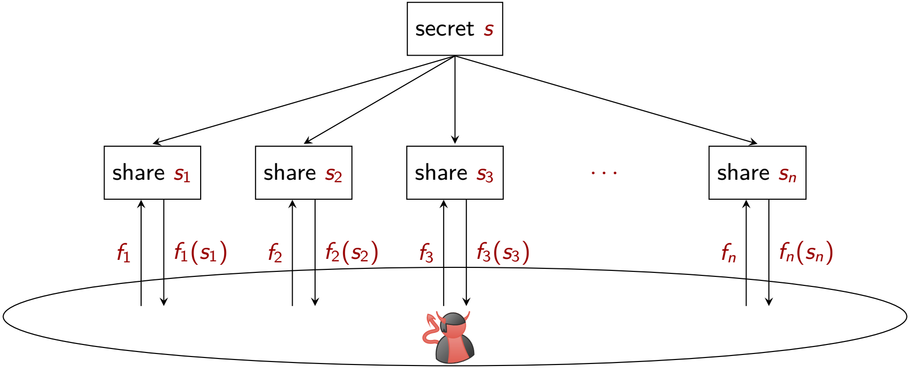
Local Leakage-resilient Secret Sharing

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



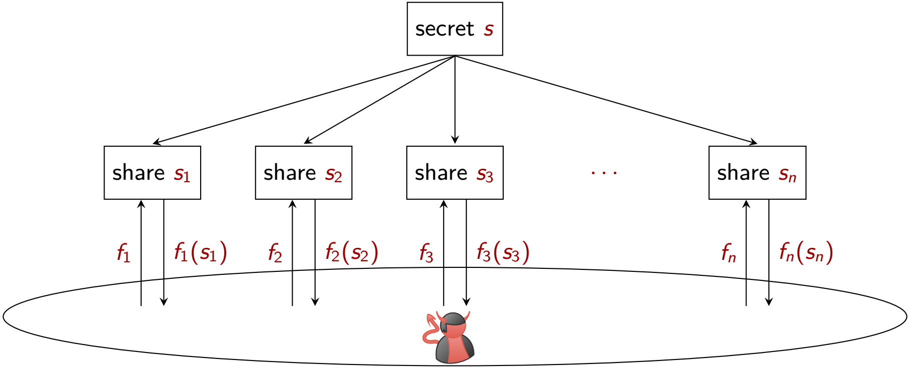
Local Leakage-resilient Secret Sharing

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



Local Leakage-resilient Secret Sharing

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

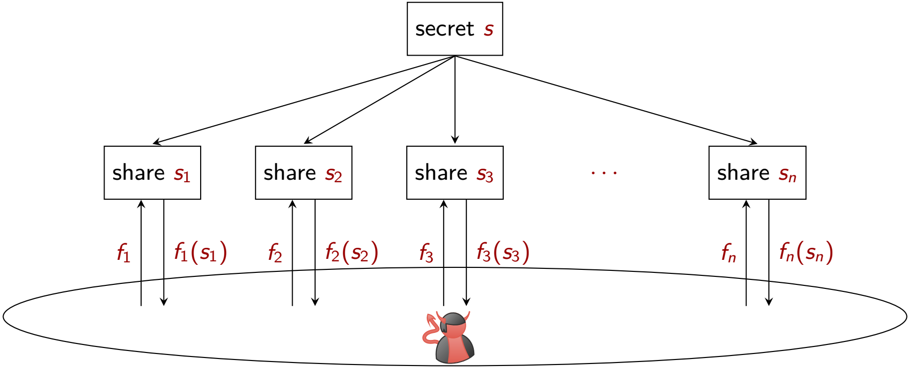


Example: Quadratic Residue Leakage

$$f_1 = f_2 = \ldots = f_n = \text{QR}, \text{ where } \text{QR}(x) = \begin{cases} 1 & \text{if } x = a^2 \text{ for some } a \in F_p, \\ 0 & \text{otherwise.} \end{cases}$$

Local Leakage-resilient Secret Sharing

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

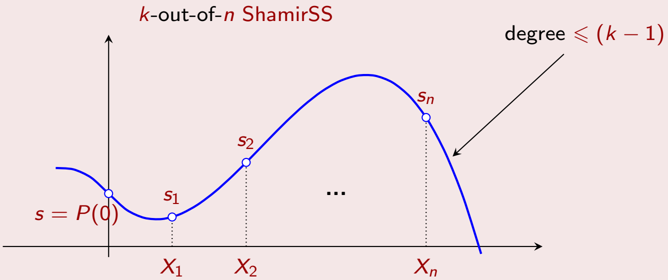


Example: Quadratic Residue Leakage

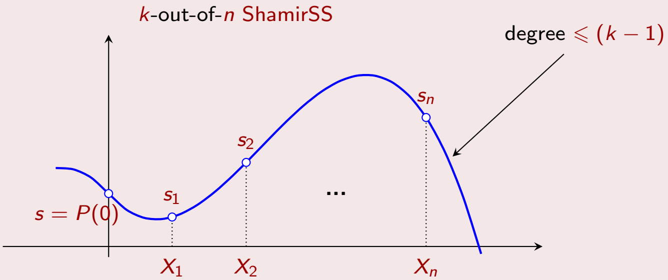
$$f_1 = f_2 = \ldots = f_n = \mathrm{QR}, \text{ where } \mathrm{QR}(x) = \begin{cases} 1 & \text{if } x = a^2 \text{ for some } a \in F_p, \\ 0 & \text{otherwise.} \end{cases}$$

ε-leakage resilience: $\Delta(\ \boldsymbol{f}(\text{share}(s)),\ \boldsymbol{f}(\text{share}(s'))\ ) \leqslant \varepsilon$ for all s, s'.

Local Leakage-resilient Shamir's Secret Sharing



Local Leakage-resilient Shamir's Secret Sharing



Applications: a useful primitive connected to many other fields

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

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	
KK'23	all	0.69	linear Fourier (no known barrier)
	balanced leakages	0.58	
	unbalanced leakages	small constant	

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	
KK'23	all	0.69	linear Fourier (no known barrier)
	balanced leakages	0.58	
	unbalanced leakages	small constant	
This work			higher-order Fourier

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	
KK'23	all	0.69	linear Fourier (no known barrier)
	balanced leakages	0.58	
	unbalanced leakages	small constant	
This work	QR leakage	any constant	higher-order Fourier

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	
KK'23	all	0.69	linear Fourier (no known barrier)
	balanced leakages	0.58	
	unbalanced leakages	small constant	
This work	QR leakage	any constant	higher-order Fourier
	almost all	any constant	

Prior Work and Our Contribution: Leakage Resilience

Goal: The smaller k/n, the better. Typical parameters for MPC applications are $1/2$ and $1/3$.

Paper	Local leakage family	Fractional threshold k/n	Techniques
BDIR'18	all	0.907	linear Fourier (known half barrier: QR leakage)
MPSW'21	all	0.868	
Journal of BDIR'18	all	0.85	
MNPSW'22	all	0.78	
KK'23	all	0.69	linear Fourier (no known barrier)
	balanced leakages	0.58	
	unbalanced leakages	small constant	
This work	QR leakage	any constant	higher-order Fourier
	almost all	any constant	

- Requires sufficiently large field, while others require n large (no matter what p is)
- Worst-case leakage remains open
- Extends to any MDS code-based secret sharing scheme

Prior Work and Our Contribution: Attacks

Consider k-out-of-n Shamir's secret sharing over a prime field F_p.

Paper	Attack	Distinguishing Advantage	Constraints
NS'20	t-bit random leakage	$1/2$	$\log p \leqslant t(n-k)/k$

Prior Work and Our Contribution: Attacks

Consider k-out-of-n Shamir's secret sharing over a prime field F_p.

Paper	Attack	Distinguishing Advantage	Constraints
NS'20	t-bit random leakage	$1/2$	$\log p \leqslant t(n-k)/k$
AMNNPSW'21	an explicit 1-bit local leakage (parity-of-parity attack)	$1/(2^k k!)$	$k \leqslant n < p$
MNPSWYY'22		$0.5 \cdot (2/\pi)^k$	

Prior Work and Our Contribution: Attacks

Consider k-out-of-n Shamir's secret sharing over a prime field F_p.

Paper	Attack	Distinguishing Advantage	Constraints
NS'20	t-bit random leakage	$1/2$	$\log p \leqslant t(n-k)/k$
AMNNPSW'21	an explicit 1-bit local leakage (parity-of-parity attack)	$1/(2^k k!)$	$k \leqslant n < p$
MNPSWYY'22		$0.5 \cdot (2/\pi)^k$	
CSTW'23	an explicit 3-bit local leakage	1	$k = O(\sqrt{n}),\ n = p - 1$

Prior Work and Our Contribution: Attacks

Consider k-out-of-n Shamir's secret sharing over a prime field F_p.

Paper	Attack	Distinguishing Advantage	Constraints
NS'20	t-bit random leakage	$1/2$	$\log p \leqslant t(n-k)/k$
AMNNPSW'21	an explicit 1-bit local leakage (parity-of-parity attack)	$1/(2^k k!)$	$k \leqslant n < p$
MNPSWYY'22		$0.5 \cdot (2/\pi)^k$	
CSTW'23	an explicit 3-bit local leakage	1	$k = O(\sqrt{n}),\ n = p - 1$
This work	an explicit 2-bit local leakage	1	$k = O(\sqrt{n}), n = \Theta(p)$

Prior Work and Our Contribution: Attacks

Consider k-out-of-n Shamir's secret sharing over a prime field F_p.

Paper	Attack	Distinguishing Advantage	Constraints
NS'20	t-bit random leakage	$1/2$	$\log p \leqslant t(n-k)/k$
AMNNPSW'21	an explicit 1-bit local leakage (parity-of-parity attack)	$1/(2^k k!)$	$k \leqslant n < p$
MNPSWYY'22		$0.5 \cdot (2/\pi)^k$	
CSTW'23	an explicit 3-bit local leakage	1	$k = O(\sqrt{n}),\ n = p-1$
This work	an explicit 2-bit local leakage	1	$k = O(\sqrt{n}), n = \Theta(p)$

Remarks

- Techniques: exponential sums, particularly Weil's bounds

Technical Highlights

Our New Analytical Proxy

Our New Proxy

$$\Delta(\ \boldsymbol{f}(\text{share}(0)),\ \boldsymbol{f}(\text{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell} \in \{0,1\}^n} \sum_{i=1}^{n} \left\| \tilde{f}_{i,\ell_i} \right\|_{U^{d+1}}$$

- share(s): set of all possible (random) shares of secret s
- Leakage function: $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, where $f_i \colon F_p \to \{0,1\}$
- Leakage distribution on s, denoted $\boldsymbol{f}(\text{share}(s))$:
  - samples $(s_1, s_2, \ldots, s_n) \leftarrow \text{share}(s)$
  - outputs $(f_1(s_1), f_2(s_2), \ldots, f_n(s_n))$
- Balanced leakage functions: $\tilde{f}_{i,\ell_i} = \mathbb{1}_{f_i^{-1}(\ell_i)} - \mathbb{1}_{-s+f_i^{-1}(\ell_i)}$

Our New Analytical Proxy

Our New Proxy

$$\Delta(\ \boldsymbol{f}(\text{share}(0)),\ \boldsymbol{f}(\text{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}\in\{0,1\}^n} \sum_{i=1}^{n} \left\| \tilde{f}_{i,\ell_i} \right\|_{U^{d+1}}$$

- $\text{share}(s)$: set of all possible (random) shares of secret s
- Leakage function: $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, where $f_i \colon F_p \to \{0,1\}$
- Leakage distribution on s, denoted $\boldsymbol{f}(\text{share}(s))$:
  - samples $(s_1, s_2, \ldots, s_n) \leftarrow \text{share}(s)$
  - outputs $(f_1(s_1), f_2(s_2), \ldots, f_n(s_n))$
- Balanced leakage functions: $\tilde{f}_{i,\ell_i} = \mathbb{1}_{f_i^{-1}(\ell_i)} - \mathbb{1}_{-s+f_i^{-1}(\ell_i)}$

Tools: Higher-order Fourier Analysis

- Gowers norms
- Generalized von Neumann inequality

Our New Analytical Proxy

Our New Proxy

$$\Delta(\ \boldsymbol{f}(\text{share}(0)),\ \boldsymbol{f}(\text{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}\in\{0,1\}^n} \sum_{i=1}^{n} \left\| \tilde{f}_{i,\ell_i} \right\|_{U^{d+1}}$$

- share(s): set of all possible (random) shares of secret s
- Leakage function: $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, where $f_i \colon F_p \to \{0,1\}$
- Leakage distribution on s, denoted $\boldsymbol{f}(\text{share}(s))$:
  - samples $(s_1, s_2, \ldots, s_n) \leftarrow \text{share}(s)$
  - outputs $(f_1(s_1), f_2(s_2), \ldots, f_n(s_n))$
- Balanced leakage functions: $\tilde{f}_{i,\ell_i} = \mathbb{1}_{f_i^{-1}(\ell_i)} - \mathbb{1}_{-s+f_i^{-1}(\ell_i)}$

Tools: Higher-order Fourier Analysis

- Gowers norms
- Generalized von Neumann inequality

Implication

Suffices to bound the Gower's norms of balanced leakage functions.

What's Higher-order Fourier Analysis?

What's Higher-order Fourier Analysis?

A generalization of (classical) linear Fourier analysis

What's Higher-order Fourier Analysis?

A generalization of (classical) linear Fourier analysis

Linear Fourier Analysis

- Developed at least a few centuries ago
- Studies how a function correlates with a "linear phase": $x \mapsto \exp(2\pi i \zeta x)$
- Counts simple linear patterns: 3-term arithmetic progressions (Roth's theorem) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)]$

Higher-order Fourier Analysis

- Developed in the last 25 years
- Studies how a function correlates with a "polynomial phase": $x \mapsto \exp(2\pi i \zeta x^2)$
- Counts more complex linear patterns: 4-term AP (Szemerédi's regularity lemma) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)\mathbb{1}_A(x+3y)]$

What's Higher-order Fourier Analysis?

A generalization of (classical) linear Fourier analysis

Linear Fourier Analysis

- Developed at least a few centuries ago
- Studies how a function correlates with a "linear phase": $x \mapsto \exp(2\pi i \zeta x)$
- Counts simple linear patterns: 3-term arithmetic progressions (Roth's theorem) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)]$

Higher-order Fourier Analysis

- Developed in the last 25 years
- Studies how a function correlates with a "polynomial phase": $x \mapsto \exp(2\pi i \zeta x^2)$
- Counts more complex linear patterns: 4-term AP (Szemerédi's regularity lemma) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)\mathbb{1}_A(x+3y)]$

n-Linear Form

Let $\Psi = (\psi_1, \psi_2, \ldots, \psi_n)$ be linear functions over t variables $\boldsymbol{x} = (x_1, x_2, \ldots, x_t)$ and $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, where $\psi_i \colon F^t \to F$, $f_i \colon F \to [-1, 1]$. Define

$$\Lambda_\Psi(f_1, f_2, \ldots, f_n) = \mathbb{E}_{\boldsymbol{x} \in F^t}[f_1(\psi_1(\boldsymbol{x})) \cdot f_2(\psi_2(\boldsymbol{x})) \cdots f_n(\psi_n(\boldsymbol{x}))]$$

What's Higher-order Fourier Analysis?

A generalization of (classical) linear Fourier analysis

Linear Fourier Analysis

- Developed at least a few centuries ago
- Studies how a function correlates with a "linear phase": $x \mapsto \exp(2\pi i \zeta x)$
- Counts simple linear patterns: 3-term arithmetic progressions (Roth's theorem) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)]$

Higher-order Fourier Analysis

- Developed in the last 25 years
- Studies how a function correlates with a "polynomial phase": $x \mapsto \exp(2\pi i \zeta x^2)$
- Counts more complex linear patterns: 4-term AP (Szemerédi's regularity lemma) $\mathbb{E}_{x,y}[\mathbb{1}_A(x)\mathbb{1}_A(x+y)\mathbb{1}_A(x+2y)\mathbb{1}_A(x+3y)]$

n-Linear Form

Let $\Psi = (\psi_1, \psi_2, \ldots, \psi_n)$ be linear functions over t variables $\boldsymbol{x} = (x_1, x_2, \ldots, x_t)$ and $\boldsymbol{f} = (f_1, f_2, \ldots, f_n)$, where $\psi_i \colon F^t \to F$, $f_i \colon F \to [-1, 1]$. Define

$$\Lambda_\Psi(f_1, f_2, \ldots, f_n) = \mathbb{E}_{\boldsymbol{x} \in F^t}[f_1(\psi_1(\boldsymbol{x})) \cdot f_2(\psi_2(\boldsymbol{x})) \cdots f_n(\psi_n(\boldsymbol{x}))]$$

- 3-term AP: $\Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A)$, where $\psi_1(x, y) = x$, $\psi_2(x, y) = x + y$, $\psi_3(x, y) = x + 2y$.
- 4-term AP: $\Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A)$, where additionally $\psi_4(x, y) = x + 3y$.

Main Ideas

Reduction to bounding linear forms

$$\Delta(\ \boldsymbol{f}(\mathrm{share}(0)),\ \boldsymbol{f}(\mathrm{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}} \sum_{i}^{n} \Lambda_{\Psi}(\tilde{f}_{i,\ell_1}, \tilde{f}_{i,\ell_2}, \ldots, \tilde{f}_{i,\ell_n}).$$

Main Ideas

Reduction to bounding linear forms

$$\Delta(\ \boldsymbol{f}(\mathrm{share}(0)),\ \boldsymbol{f}(\mathrm{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}} \sum_{i}^{n} \Lambda_{\Psi}(\tilde{f}_{i,\ell_1}, \tilde{f}_{i,\ell_2}, \ldots, \tilde{f}_{i,\ell_n}).$$

Theorem (Generalized von Neumann Inequality [GreenTao'10])

Let $\Psi = (\psi_1, \psi_2, \ldots, \psi_n)$ be a system of linear functions with Cauchy-Schwarz complexity d. Let $g_i : F_p \to [-1, 1]$ for every $i \in [n]$. Provided $p \geqslant d$, it holds that

$$\Lambda_{\Psi}(g_1, g_2, \ldots, g_n) \leqslant \min_{1 \leqslant i \leqslant n} \|g_i\|_{U^{d+1}}.$$

One of the key ingredients in the proof of the breakthrough result: "The primes contain arbitrarily long arithmetic progressions."

Main Ideas

Reduction to bounding linear forms

$$\Delta(\ \boldsymbol{f}(\mathrm{share}(0)),\ \boldsymbol{f}(\mathrm{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}} \sum_{i}^{n} \Lambda_{\Psi}(\tilde{f}_{i,\ell_1}, \tilde{f}_{i,\ell_2}, \ldots, \tilde{f}_{i,\ell_n}).$$

Theorem (Generalized von Neumann Inequality [GreenTao'10])

Let $\Psi = (\psi_1, \psi_2, \ldots, \psi_n)$ be a system of linear functions with Cauchy-Schwarz complexity d. Let $g_i : F_p \to [-1, 1]$ for every $i \in [n]$. Provided $p \geqslant d$, it holds that

$$\Lambda_{\Psi}(g_1, g_2, \ldots, g_n) \leqslant \min_{1 \leqslant i \leqslant n} \|g_i\|_{U^{d+1}}.$$

One of the key ingredients in the proof of the breakthrough result: "The primes contain arbitrarily long arithmetic progressions."

Applying this theorem extensively to all leakage values $\boldsymbol{\ell}$ and indices i yields

$$\Delta(\ \boldsymbol{f}(\mathrm{share}(0)),\ \boldsymbol{f}(\mathrm{share}(s))\ ) \leqslant \sum_{\boldsymbol{\ell}} \sum_{i=1}^{n} \left\| \tilde{f}_{i,\ell_i} \right\|_{U^{d+1}}.$$

Illustrative Example

Consider $n = 4$ parties, threshold $k = 4$ over prime field F_7 with evaluation places $\{1, 2, 3, 4\}$.

(Random) shares of secret 0

$$\text{share}(0) = \langle G_0 \rangle, \text{ where } G_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2^2 & 3^2 & 4^2 \\ 1 & 2^3 & 3^3 & 4^3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 2 \\ 1 & 1 & 6 & 1 \end{pmatrix}$$

$s_1 = x + y + z,\ s_2 = 2x + 4y + z,\ s_3 = 3x + 2y + 6z,\ s_4 = 4x + 2y + z$ for uniformly random x, y, z

Illustrative Example

Consider $n = 4$ parties, threshold $k = 4$ over prime field F_7 with evaluation places $\{1, 2, 3, 4\}$.

(Random) shares of secret 0

$$\text{share}(0) = \langle G_0 \rangle, \text{ where } G_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2^2 & 3^2 & 4^2 \\ 1 & 2^3 & 3^3 & 4^3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 2 \\ 1 & 1 & 6 & 1 \end{pmatrix}$$

$s_1 = x + y + z,\ s_2 = 2x + 4y + z,\ s_3 = 3x + 2y + 6z,\ s_4 = 4x + 2y + z$ for uniformly random x, y, z

Suppose the leakage function is QR. Let $A = \{a^2 \mid a \in F_7\} = \{0, 1, 4, 2\}$.

Probability of leakage being 1

$$\begin{aligned} \Pr[\boldsymbol{f}(\text{share}(0)) = \mathbf{1}] &= \mathbb{E}_{\boldsymbol{x},y,z}[\mathbb{1}_A(x+y+z)\mathbb{1}_A(2x+4y+z)\mathbb{1}_A(3x+2y+6z)\mathbb{1}_A(4x+2y+z)] \\ &= \Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) \end{aligned}$$

$$\Pr[\boldsymbol{f}(\text{share}(s)) = \mathbf{1}] = \Lambda_\Psi(\mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A}) \quad \text{since share}(s) = (s, s, \ldots, s) + \text{share}(0)$$

Illustrative Example

Consider $n = 4$ parties, threshold $k = 4$ over prime field F_7 with evaluation places $\{1, 2, 3, 4\}$.

(Random) shares of secret 0

$$\text{share}(0) = \langle G_0 \rangle, \text{ where } G_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2^2 & 3^2 & 4^2 \\ 1 & 2^3 & 3^3 & 4^3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 2 \\ 1 & 1 & 6 & 1 \end{pmatrix}$$

$s_1 = x + y + z,\ s_2 = 2x + 4y + z,\ s_3 = 3x + 2y + 6z,\ s_4 = 4x + 2y + z$ for uniformly random x, y, z

Suppose the leakage function is QR. Let $A = \{a^2 \mid a \in F_7\} = \{0, 1, 4, 2\}$.

Probability of leakage being 1

$$|\Pr[\boldsymbol{f}(\text{share}(0)) = \mathbf{1}] - \Pr[\boldsymbol{f}(\text{share}(s)) = \mathbf{1}]| = |\Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \Lambda_\Psi(\mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A})|$$

Illustrative Example

Consider $n = 4$ parties, threshold $k = 4$ over prime field F_7 with evaluation places $\{1, 2, 3, 4\}$.

(Random) shares of secret 0

$$\text{share}(0) = \langle G_0 \rangle, \text{ where } G_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2^2 & 3^2 & 4^2 \\ 1 & 2^3 & 3^3 & 4^3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 2 \\ 1 & 1 & 6 & 1 \end{pmatrix}$$

$s_1 = x + y + z,\ s_2 = 2x + 4y + z,\ s_3 = 3x + 2y + 6z,\ s_4 = 4x + 2y + z$ for uniformly random x, y, z

Suppose the leakage function is QR. Let $A = \{a^2 \mid a \in F_7\} = \{0, 1, 4, 2\}$.

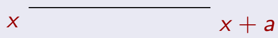
Probability of leakage being 1

$$|\Pr[\boldsymbol{f}(\text{share}(0)) = \mathbf{1}] - \Pr[\boldsymbol{f}(\text{share}(s)) = \mathbf{1}]| = |\Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) - \Lambda_\Psi(\mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A}, \mathbb{1}_{s+A})|$$

Not a linear form, but bounded by 4 linear forms:

$$\Lambda_\Psi(\mathbb{1}_A - \mathbb{1}_{s+A}, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A) + \Lambda_\Psi(\mathbb{1}, \mathbb{1}_A - \mathbb{1}_{s+A}, \mathbb{1}_A, \mathbb{1}_A) + \Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A - \mathbb{1}_{s+A}, \mathbb{1}_A) + \Lambda_\Psi(\mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A, \mathbb{1}_A - \mathbb{1}_{s+A})$$

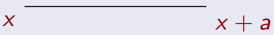
Gowers Norms

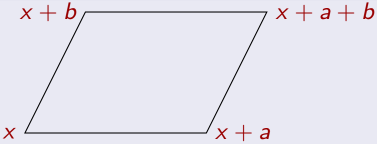


$$\|f\|_{U^1} = \mathbb{E}_{x,a}[f(x)f(x+a)]$$

Breaking the Half-barrier for QR Leakage & Almost all 1-bit Leakages

Gowers Norms

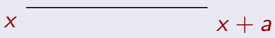


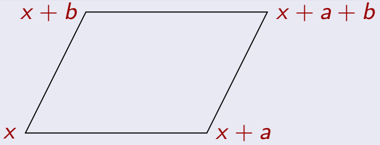


$\|f\|_{U^1} = \mathbb{E}_{x,a}[f(x)f(x+a)]$

$\|f\|_{U^2} = \mathbb{E}_{x,a,b}[f(x)f(x+a)f(x+b)f(x+a+b)]$

Gowers Norms





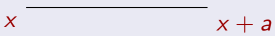
$\|f\|_{U^1} = \mathbb{E}_{x,a}[f(x)f(x+a)]$

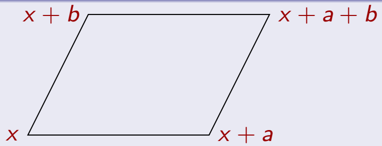
$\|f\|_{U^2} = \mathbb{E}_{x,a,b}[f(x)f(x+a)f(x+b)f(x+a+b)]$

Remark

Bounding the Gowers norms of an arbitrary function is challenging.

Gowers Norms





$\|f\|_{U^1} = \mathbb{E}_{x,a}[f(x)f(x+a)]$

$\|f\|_{U^2} = \mathbb{E}_{x,a,b}[f(x)f(x+a)f(x+b)f(x+a+b)]$

Remark

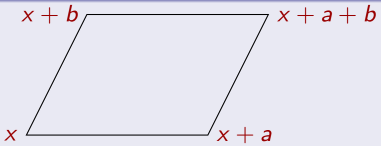
Bounding the Gowers norms of an arbitrary function is challenging.

Balanced quadratic leakage functions

$$\|\mathbb{1}_{\mathrm{QR}} - \mathbb{1}_{s+\mathrm{QR}}\|_{U^d} \leqslant \frac{1}{p^{\Theta(c_d)}} \text{ for all } s.$$

Technique: multiplicative character sums

Gowers Norms



$\|f\|_{U^1} = \mathbb{E}_{x,a}[f(x)f(x+a)]$

$\|f\|_{U^2} = \mathbb{E}_{x,a,b}[f(x)f(x+a)f(x+b)f(x+a+b)]$

Remark

Bounding the Gowers norms of an arbitrary function is challenging.

Balanced quadratic leakage functions

$$\|\mathbb{1}_{\mathrm{QR}} - \mathbb{1}_{s+\mathrm{QR}}\|_{U^d} \leqslant \frac{1}{p^{\Theta(c_d)}} \text{ for all } s.$$

Technique: multiplicative character sums

Random balanced leakage function

$$\|\mathbb{1}_A - \mathbb{1}_{s+A}\|_{U^d} = O_d\left(\frac{1}{p}\right) \text{ for all } s.$$

Technique: standard probabilistic methods

Summary and Open Problems

Takeaway

1. Develop a new analytic framework using higher-order Fourier analysis
   - cn-out-of-n Shamir secret sharing is leakage-resilient against almost all 1-bit local leakage
2. Present an explicit 2-bit leakage attack that determines the secret when $k = \Theta(\sqrt{n})$, $p = \Theta(n)$

Summary and Open Problems

Takeaway

1. Develop a new analytic framework using higher-order Fourier analysis
   - cn-out-of-n Shamir secret sharing is leakage-resilient against almost all 1-bit local leakage
2. Present an explicit 2-bit leakage attack that determines the secret when $k = \Theta(\sqrt{n})$, $p = \Theta(n)$

Open Problems

1. Leakage resilience
   - Breaking the half threshold for the worst-case leakage
   - What if p is not large enough, says $p = \Theta(n)$?
   - Multiple-bit leakages
   - Does randomizing the evaluation places help?
2. Attacks
   - 1-bit leakage attack
   - Higher threshold regime

Summary and Open Problems

Takeaway

1. Develop a new analytic framework using higher-order Fourier analysis
   - cn-out-of-n Shamir secret sharing is leakage-resilient against almost all 1-bit local leakage
2. Present an explicit 2-bit leakage attack that determines the secret when $k = \Theta(\sqrt{n})$, $p = \Theta(n)$

Open Problems

1. Leakage resilience
   - Breaking the half threshold for the worst-case leakage
   - What if p is not large enough, says $p = \Theta(n)$?
   - Multiple-bit leakages
   - Does randomizing the evaluation places help?
2. Attacks
   - 1-bit leakage attack
   - Higher threshold regime

Thank you!