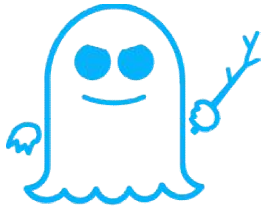
On the Local Leakage Resilience of Linear Secret Sharing Schemes

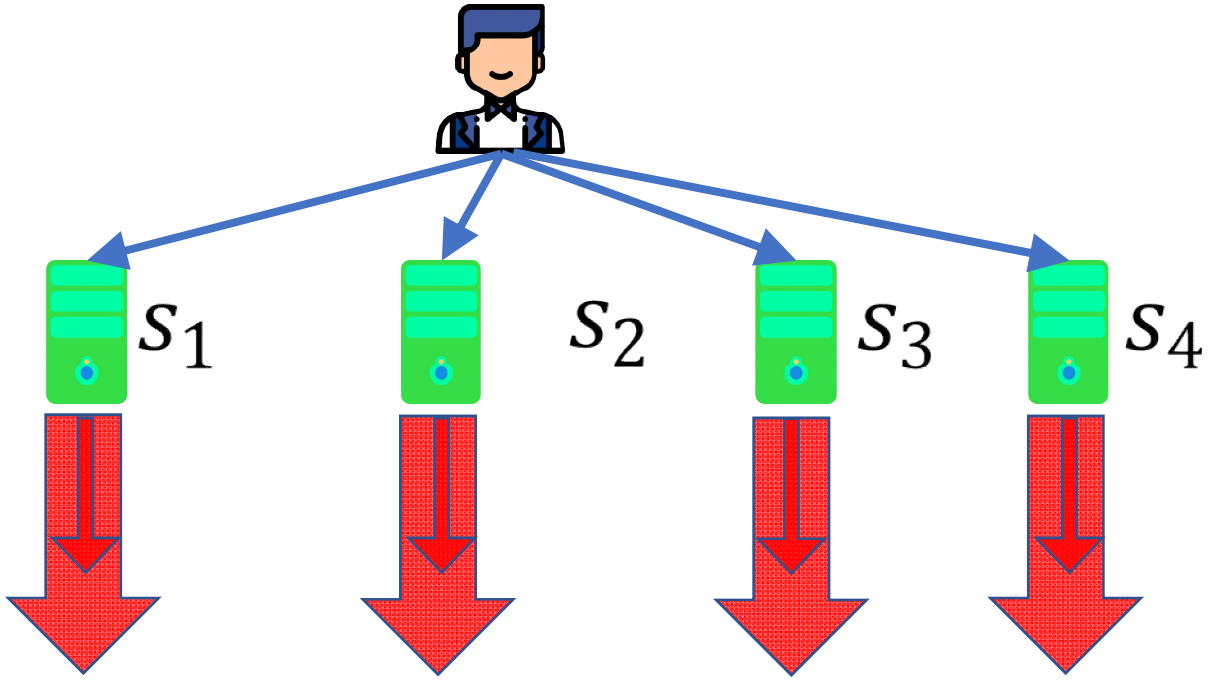
Akshay Degwekar
(MIT)

Joint with Fabrice Benhamouda (IBM Research),
Yuval Ishai (Technion) and Tal Rabin (IBM Research)



Leakage attacks can be devastating

Proposed Solution: Secret Sharing, MPC



A few full corruptions

All the servers?

Partial leak from all

Leakage Resilient Cryptography

[ISW03, MR04, DP07, DP08, AGV09, NS09, FRR+10, BKKV10, LLW11, BGJK12, DF12, BDL14, BGK14, GR15, DLZ15, GIMSS16 …]

- Strong leakage models
- Specially-designed schemes

Are **standard**

Additive
Shamir

Secret Sharing Schemes

Leakage Resilient?

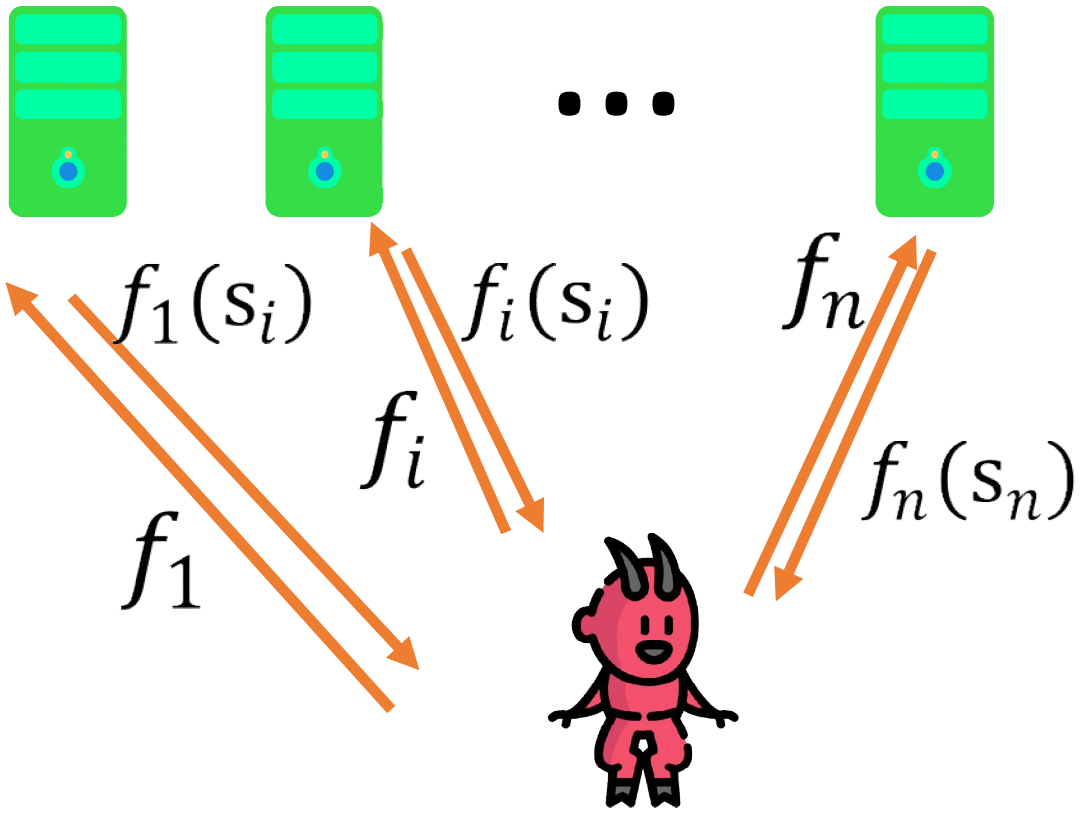
Limited General Results

Secret Sharing generically protects
against weak forms of leakage.

[DDF14] Noisy Leakage

[BIVW16] Low approximate degree leaks

Leakage Model: Local Leakage



Leak **any** partial information about state.

Output of each f_i is short

Restricted form of Only Computation Leaks[Micali-Reyzin04, GR12, BDL14], Bounded Comm. Leakage [GIMSS16]

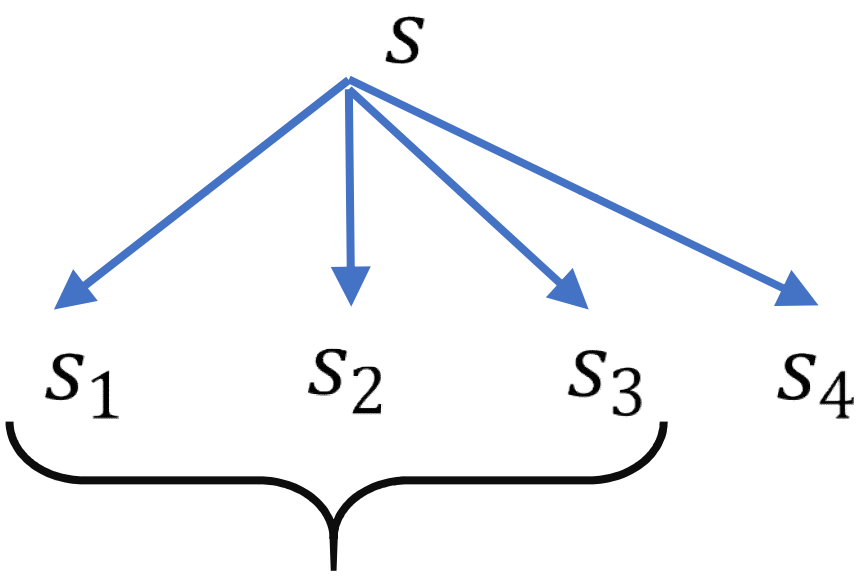
Is Local Leakage reasonable?

Local: Justified by physical separation

Shrinking: Timing, power, selective failures give limited information

Adversarial

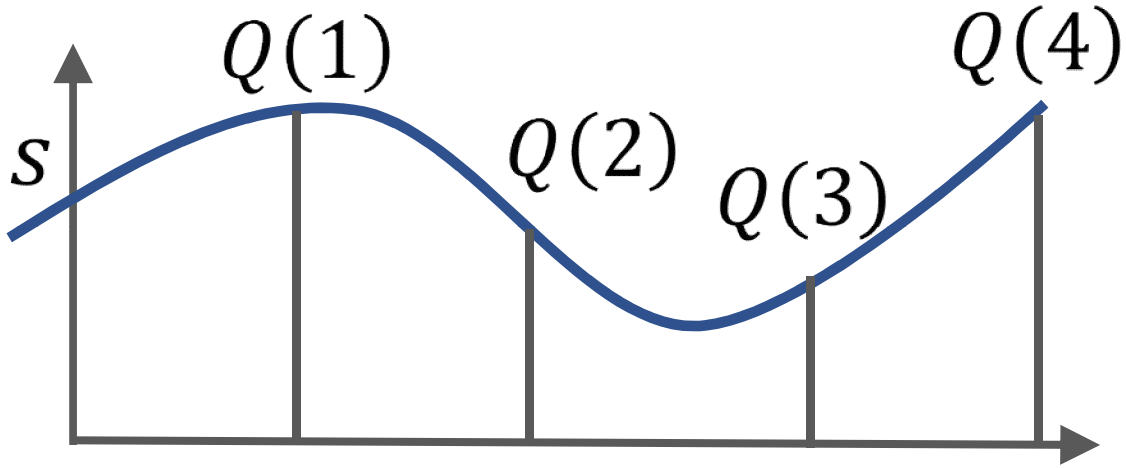
Additive Secret Sharing



Completely random

$$s = s_1 + s_2 + s_3 + s_4$$

Shamir Secret Sharing



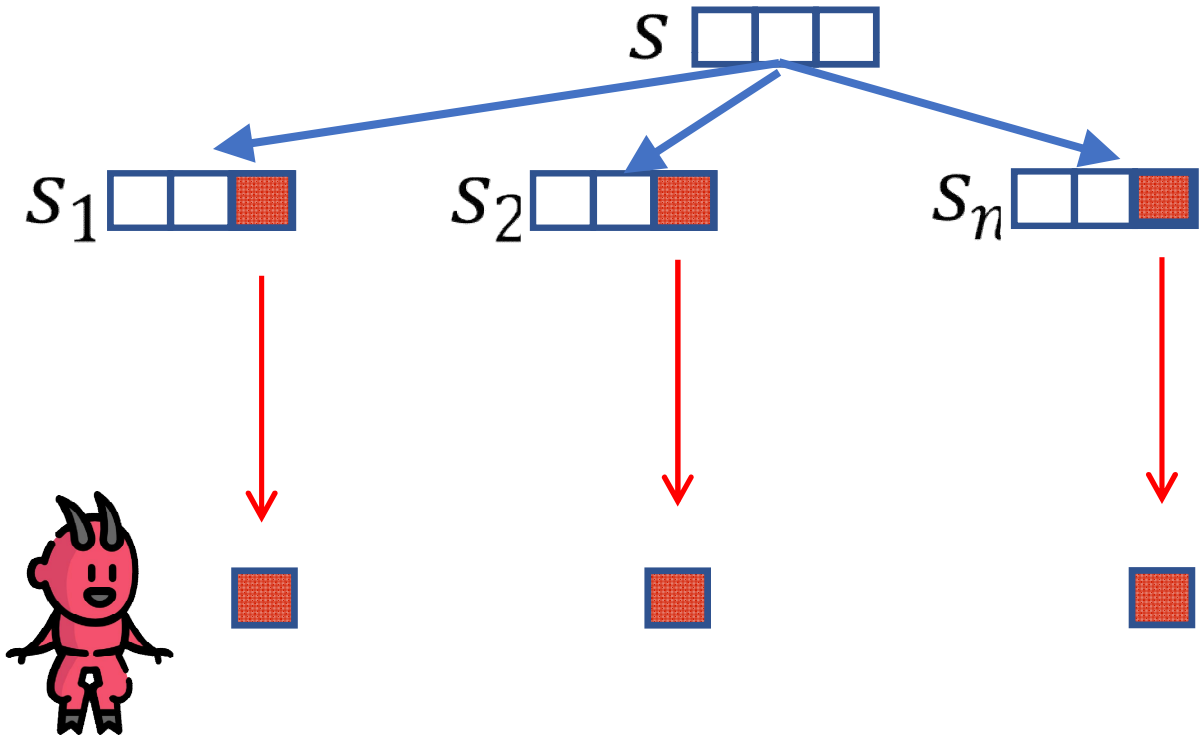
Random poly $Q(0) =$

Shares are evaluations

Threshold: Degree + 1 points to reconstruct

Is Additive Secret Sharing Local Leakage Resilient?

A. Not Necessarily. Field: $\mathbb{F}_{2^k}$



$$s = s_1 + s_2 \ldots + s_n$$

One bit each leaks
one bit of the secret!

How about Shamir ?

A. Not

Guruswami-Wootters 16: One bit per server can reconstruct the whole secret!

Regenerating Codes: When a server goes down, minimum communication you need to reconstruct.

$\mathbb{F}_{2^k}$: small additive subgroups

Other Fields?

Results Overview

Leakage Resilience of Additive &
Shamir Secret Sharing

Application: Leakage Resilience of GMW protocol

Application: Local Share Conversion

Results: Additive Secret Sharing

Prime order fields $\mathbb{F}_p$ are more leakage resilient

Thm.

Over $\mathbb{F}_p$, additive secret sharing is

local leakage-resilient.

$\Omega(\log p)$ bits of leakage, $\varepsilon = 2^{-\Omega(n)}$ distinguishing adv

n: number of servers

Results: Shamir Secret Sharing

Prime order fields $\mathbb{F}_p$ are more leakage resilient

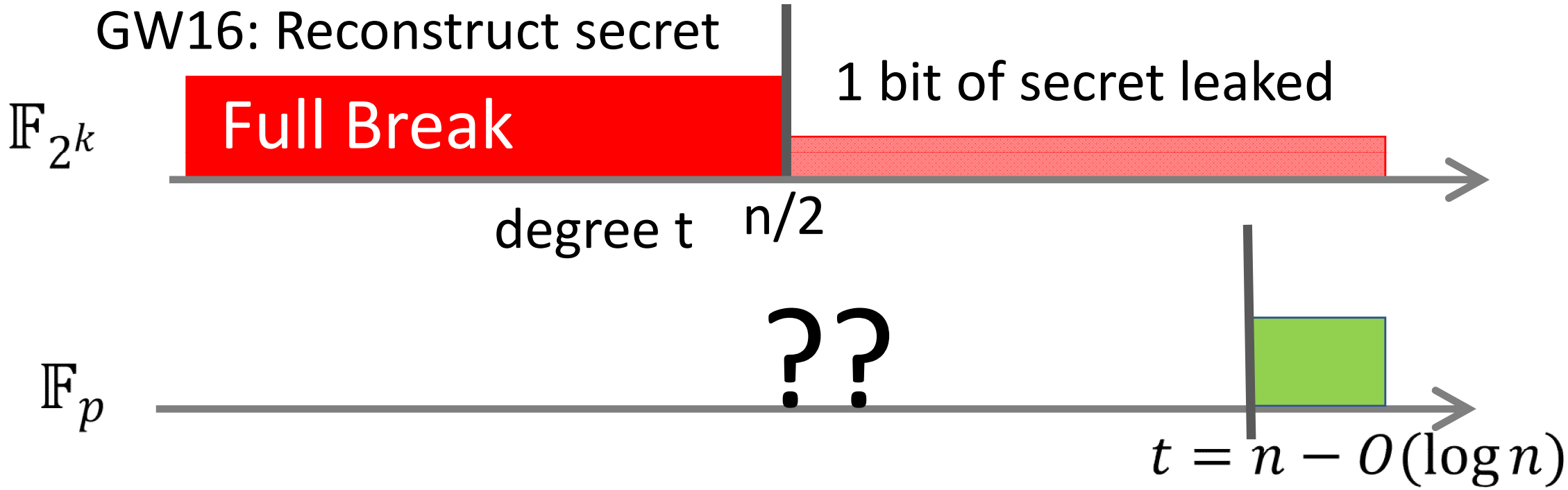
Thm.

Over $\mathbb{F}_p$, high threshold $t = n - O(\log n)$,

t-out-of-n Shamir scheme is leakage-resilient.

$\Omega(\log p)$ bits of leakage, $\varepsilon = 2^{-\Omega(n)}$ distinguishing advantage

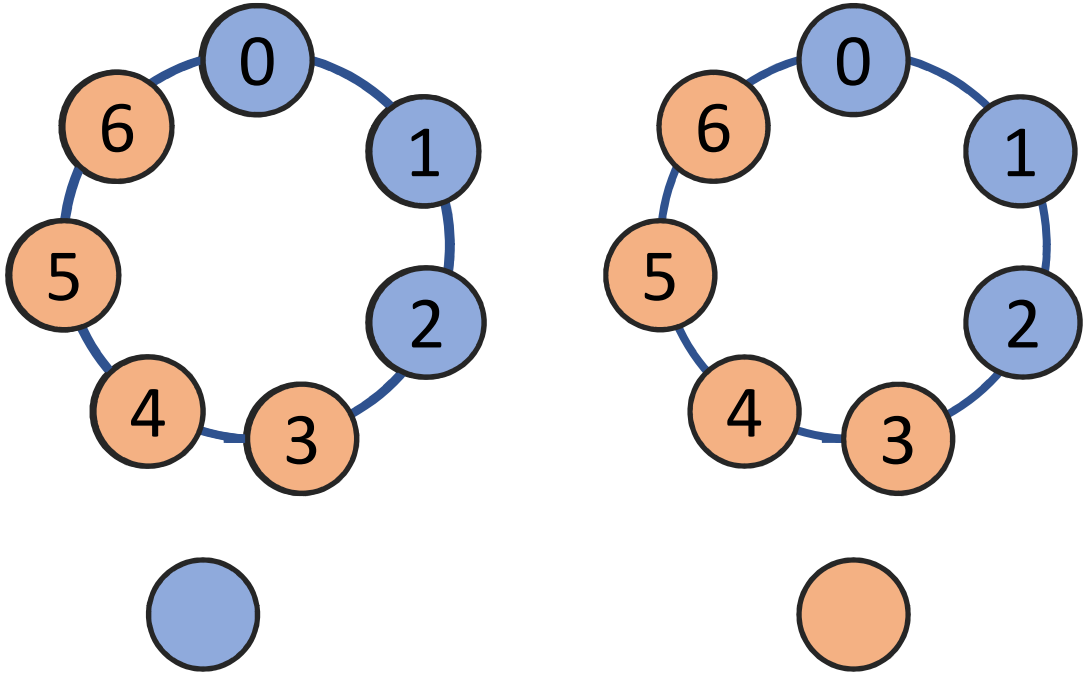
Fast MPC implementations use $\mathbb{F}_{2^k}$



Conjecture. For large n, $\frac{n}{100}$-out-of-n Shamir over $\mathbb{F}_p$ is local leakage-resilient.

Why large n? Approximate Subgroup Attack

$\mathbb{F}_7$

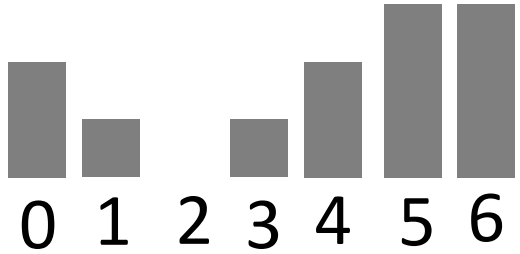


Random Secret

s_1, s_2 completely random

$s = s_1 + s_2$

$s \in \{0,1,2\} + \{3,4,5,6\}$



Generalizes to const. servers

Application: MPC

Honest-but-Curious GMW w/ preprocessed Beaver Triples

Goldreich-Micali-Wigderson87, Beaver91

Preprocessing	Secret Shared Inputs Beaver Triples for product gates
Computation	Addition: Locally Add Shares Multiplication: Use Beaver Triples

Application: MPC

Thm. Over field $\mathbb{F}_p$, GMW Protocol with "Beaver Triple preprocessing" is leakage-resilient:

a. (Corruptions) $n/2$ corruptions

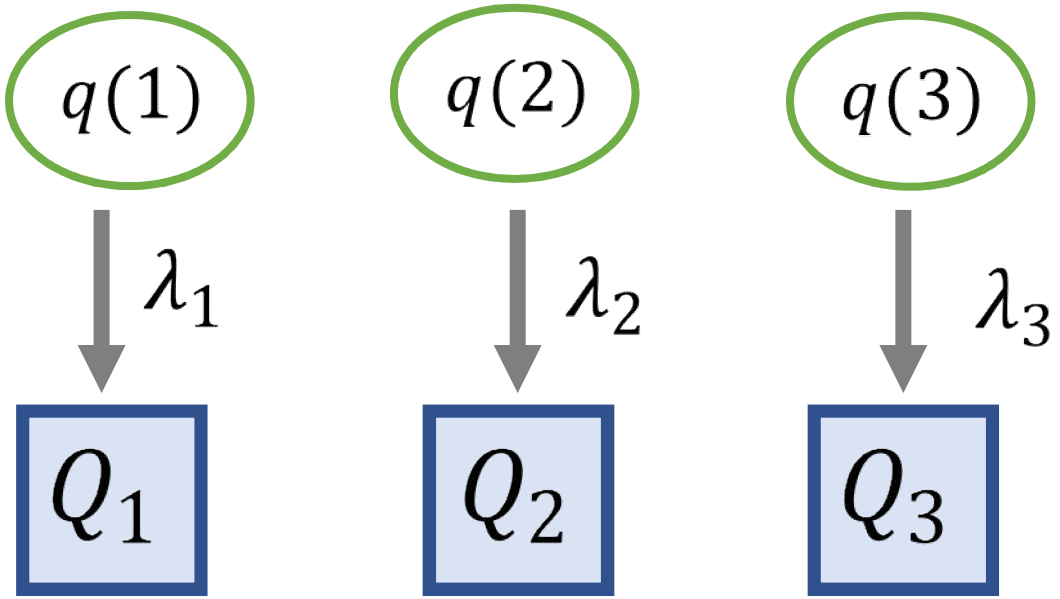
b. (Partial Leakage) $\Omega(\log p)$ bits of leakage.

Byproduct : On Local Share Conversion

[Beimel-Ishai-Kushilevitz-Orlov12]

Locally convert secret under one scheme to related secret under other scheme

Shamir → Additive (Secret unchanged)



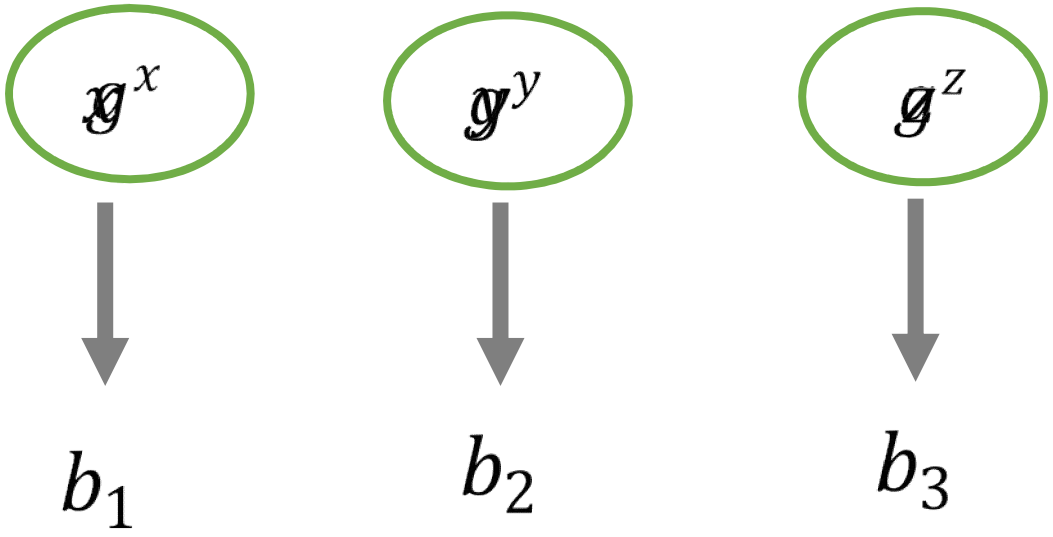
Lagrange Coefficients.

$$s = \lambda_1 q(1) + \lambda_2 q(2) + \lambda_3 q(3)$$

$$s = Q_1 + Q_2 + Q_3$$

Byproduct : On Local Share Conversion

Homomorphic Secret Sharing
(Boyle-Gilboa-Ishai16)



To get 3-server HSS:

$$g^x \cdot g^y \cdot g^z = g^b$$

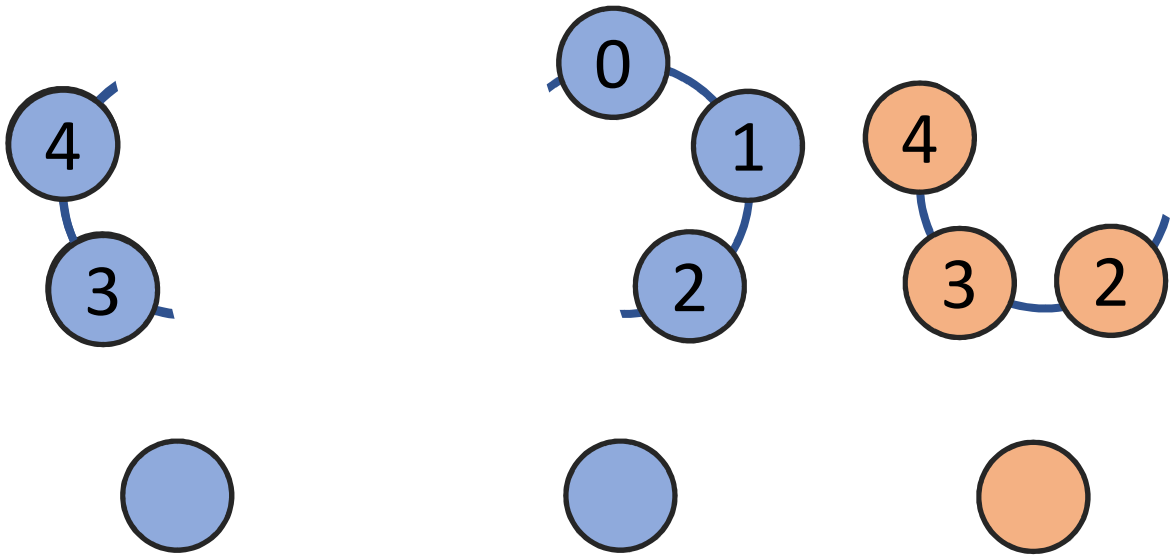
$$b = b_1 + b_2 + b_3$$

Thm: 3-party Additive over $\mathbb{F}_p$ ⇏ Additive over $\mathbb{F}_2$

Techniques

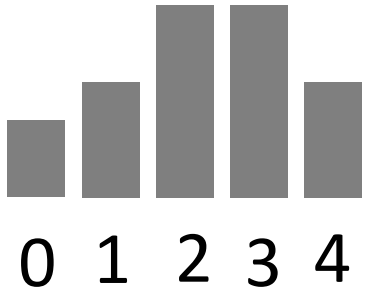
Prime order: $\mathbb{F}_5$

No subgroups



$$s \in \{4,3\} + \{0,1,2\} + \{2,3,4\}$$

Some information.



Want: s is close to random

Techniques $s \in \{4,3\} + \{0,1,2\} + \{2,3,4\}$

Cauchy-Davenport Theorem: Over $\mathbb{F}_p$,

$$|A_1 + A_2| \geq \min(p, |A_1| + |A_2| - 1)$$

Need: $A_1 + A_2$ is close to random on $\mathbb{F}_p$.

To show: For any $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}_p$ where $|A_i| \approx p/2^l$,

$A_1 + A_2 + \cdots + A_n$ is close to uniform on $\mathbb{F}_p$

Number Theory Techniques. Fourier Analysis over $\mathbb{F}_p$.

Summary

Prime order fields $\mathbb{F}_p$ are better against leakage

Thm: Additive & High threshold (t~n) Shamir over prime-order $\mathbb{F}_p$ are local leakage resilient.

Application: Honest-but-Curious GMW is leakage resilient.

Application: Local Share Conversion Impossibility results.

Conjecture: Shamir over $\mathbb{F}_p$ is leakage resilient when $t = {}^{n}/_{2}$


THANK
YOU
return

Usually in Leakage Resilience

Given Leakage Model,
Does ∃ Leakage Resilient Scheme?

[Cite many works on leakage.]

Here: Given existing schemes,
how Leakage Resilient are they?

Results:

Prime order fields $\mathbb{F}_p$ behave differently from $\mathbb{F}_{2^k}$!

Thm. For large n (no of servers), additive secret sharing over $\mathbb{F}_p$ is leakage-resilient to $\log p/4$- bits of leakage.

Thm. For large n, & $t = n - O(\log n)$ t-out-of-n Shamir secret sharing over $\mathbb{F}_p$ is leakage-resilient to $\log p/4$- bits of leakage.

Q: How Leakage Resilient are

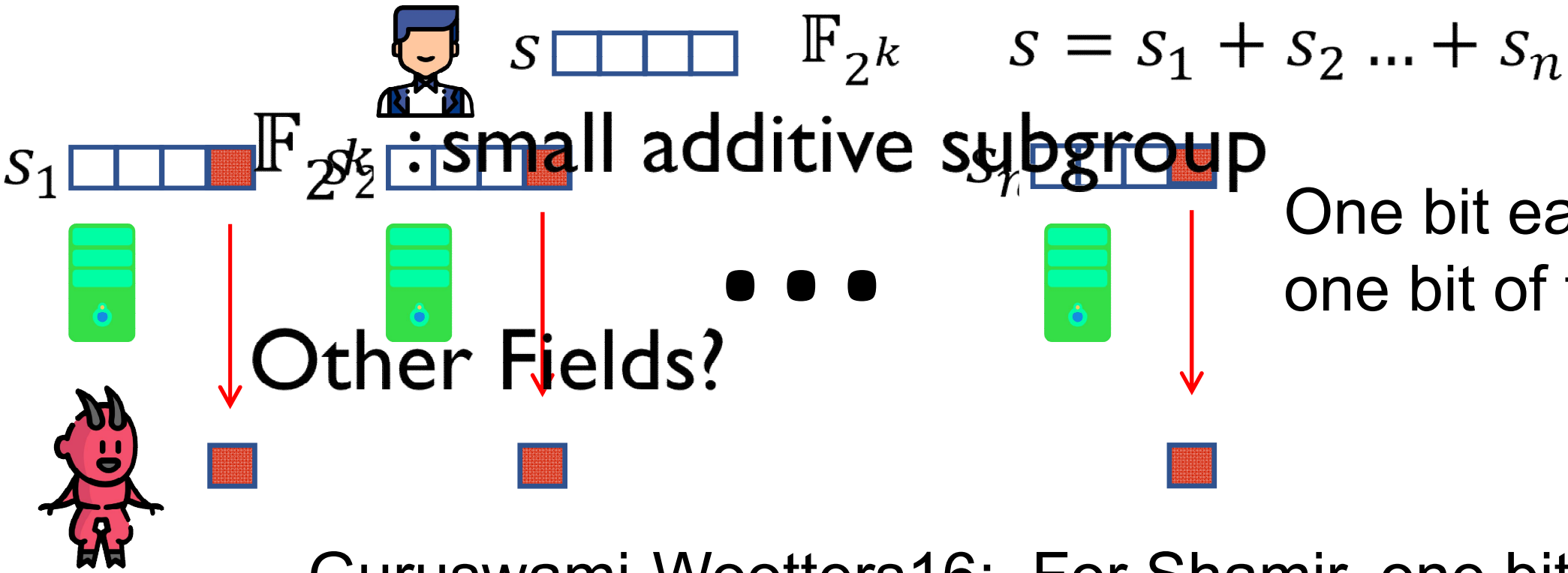
- Shamir & Additive Secret Sharing?
- GMW & BGW style MPC Protocols?

Why?

- Exist and are Used.
- Useful Properties: Homomorphisms.

Is Additive Secret Sharing Local Leakage Resili

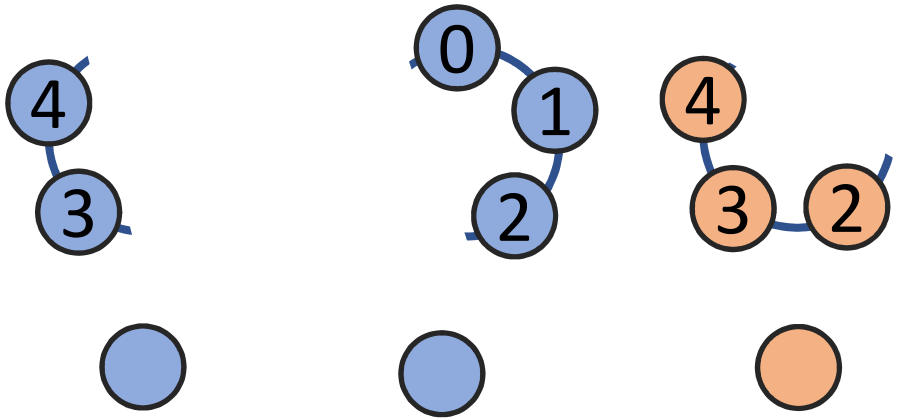
A. Not always.



One bit each leaks one bit of the secret!

Guruswami-Wootters16: For Shamir, one bit each allow full reconstruction of secret.

Techniques



To show:

Pr[ ] ≈ Pr[ ]

secret = 0 secret = 1

Leaks partition $\mathbb{F}_p$ into subsets.

To show: For any $A_1, A_2, \ldots, A_n \subseteq \mathbb{F}_p$ where $|A_i| \approx p/2^l$,

$A_1 + A_2 + \cdots + A_n$ is close to uniform on $\mathbb{F}_p$

Number Theory Techniques. Fourier Analysis over $\mathbb{F}_p$.

Application: Honest-but-Curious GMWs
w/ preprocessed Beaver Triples

$[x]$: Secret Shared

Preprocess

Secret Share Inputs $[x], [y], [z]$

Beaver Triples for product gates: $[a], [b], [ab]$

Compute:

Addition: Locally Add Shares $[w] = [x] + [y]$

Multiplication: $w = x \cdot y$. Use Beaver Triples

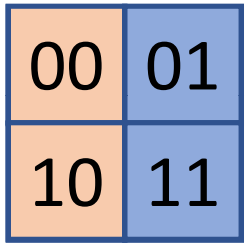
1. Compute and Publish $[x - a], [y - b]$
2. $[x \cdot y] = (x - a)(y - b) + [a](y - b) + (x - a)[b] + [ab]$

Techniques

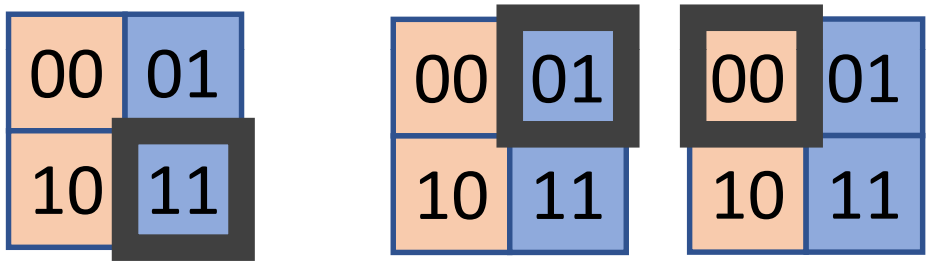
Doesn't work: $\mathbb{F}_4$

Attack: Leak lsb(share)

lsb(secret) = sum of leaks



Secret: 10 = 11 + 01 + 00



Leak reveals: Share's coset

The coset is a group.

Learn secret's coset.