

Near-Optimal Non-malleable Codes and Leakage Resilient Secret Sharing Schemes

Sruthi Sekar

Advisors: Bhavana Kanukurthi, Manjunath Krishnapur



Thesis Colloquium

Today's Talk

Paper: Adaptive Extractors and their Application to Leakage Resilient Secret Sharing

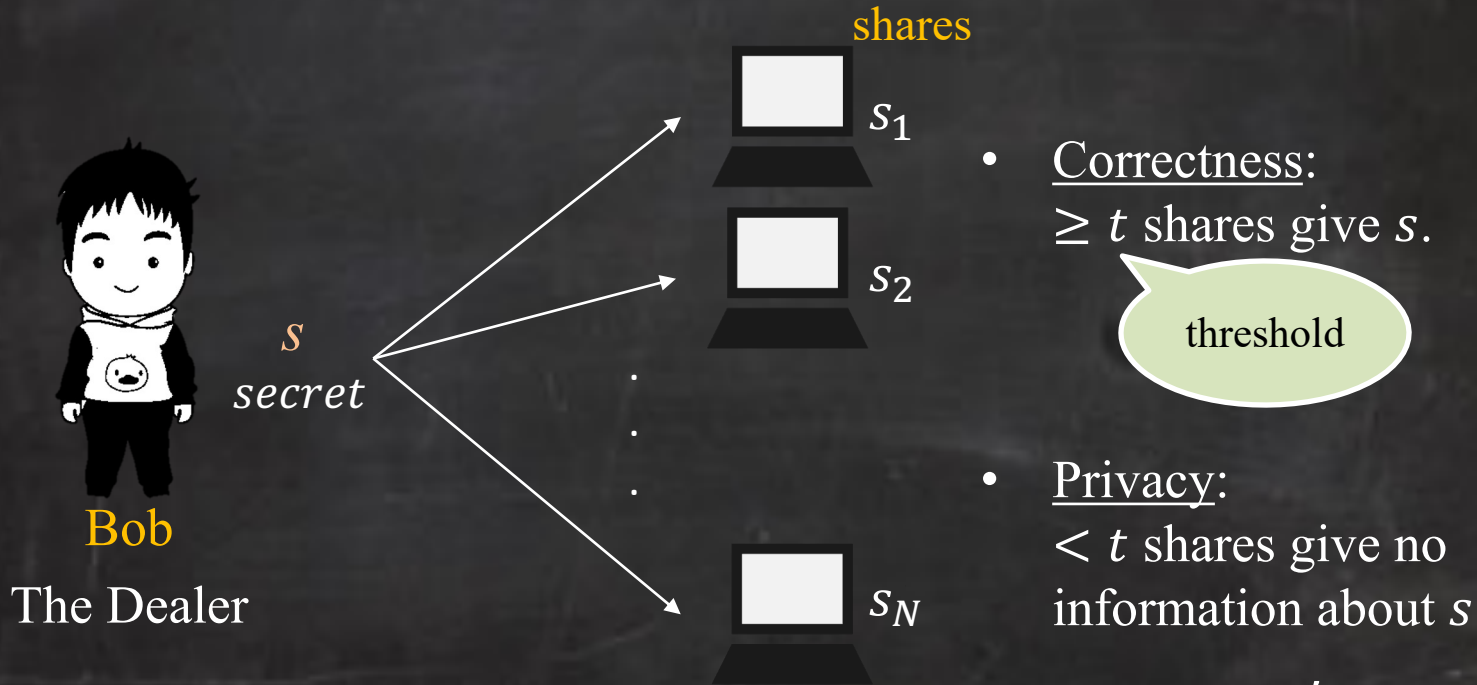
Published at: CRYPTO 2021

Joint Work with: Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu

- Define Leakage Resilient Secret Sharing
- Important Parameters and State of Art
- Our Construction
- Security Proof

Secret Sharing Schemes

Shamir and Blakely (1979)



$$\forall s, s' \\ (< t \text{ shares of } s) \approx (< t \text{ shares of } s')$$

Shamir Secret Sharing



LEAKAGE ATTACKS [Kocher(1996)]

What if in addition to $t - 1$ shares, adversary gets arbitrary bounded bits from other shares too?

[Guruswami, Wooters (2016)]: Shamir breaks, given 1-bit leakage on remaining shares.

- Confidentiality
- Privacy

$p(i_1), \dots, p(i_{t-1})$

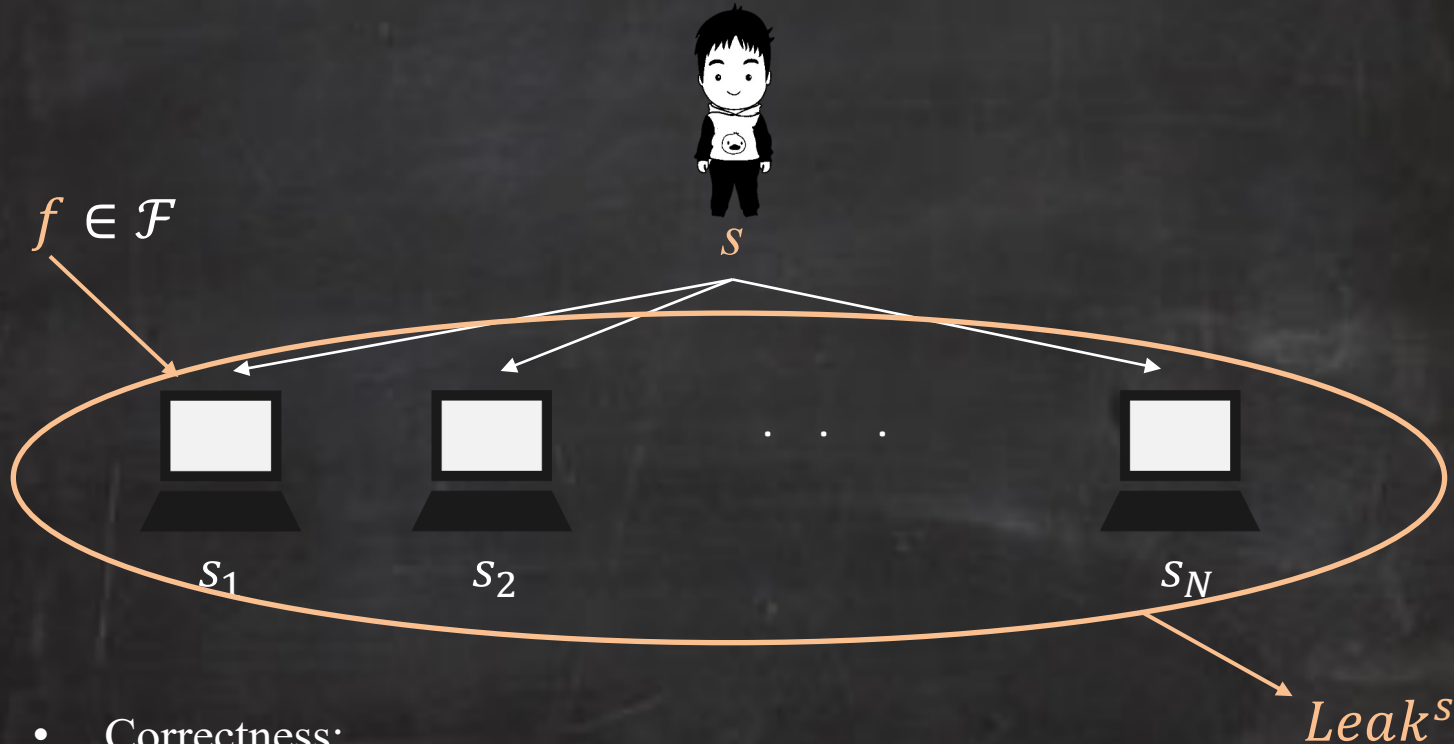
$\equiv$

$y_1, \dots, y_{t-1}$
(picked uniformly from $\mathbb{Z}_q$)

Shares

Leakage Resilient Secret Sharing

Dziembowski and Pietrzak (2007)



- Correctness:
 $\geq t$ shares give s .
- Leakage Resilience: $\mathcal{F}$ be some family of functions on the shares.

$$\forall s, s' \text{ } Leak^s \approx Leak^{s'}$$

Leakage Resilient Secret Sharing

Parameters

- Share Size: Measures size of the largest share amongst all N shares.

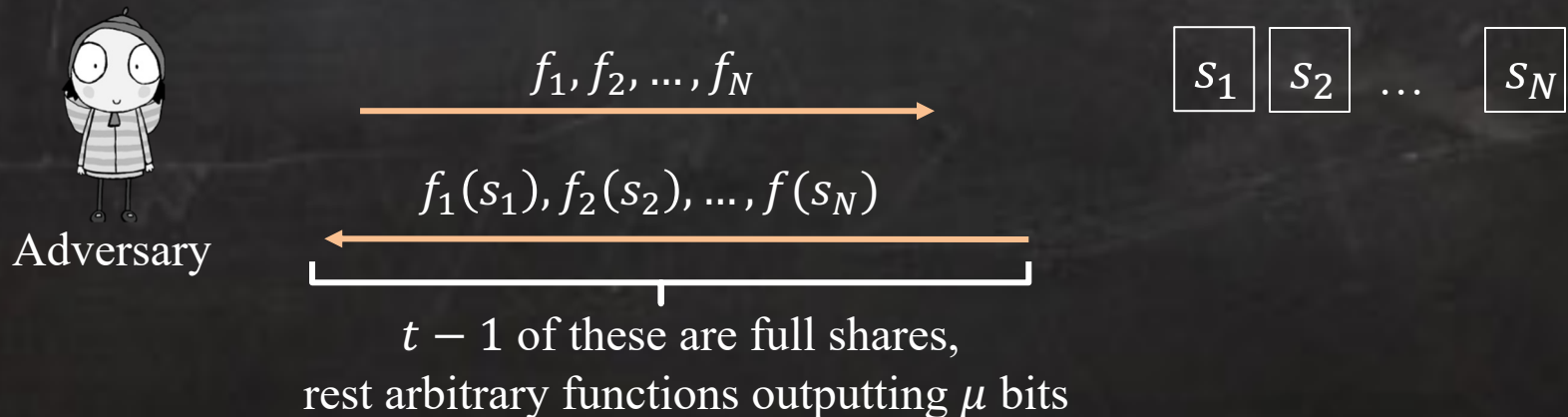
Smaller Share Size $\Rightarrow$ Lower Redundancy

Best we can hope for: *message length* + μ

Leakage bits
allowed per share

- Leakage Model/Family: Determines the leakage queries allowed by adversary. Adaptive vs Non-adaptive, Independent vs Joint

Non-Adaptive Independent Leakage

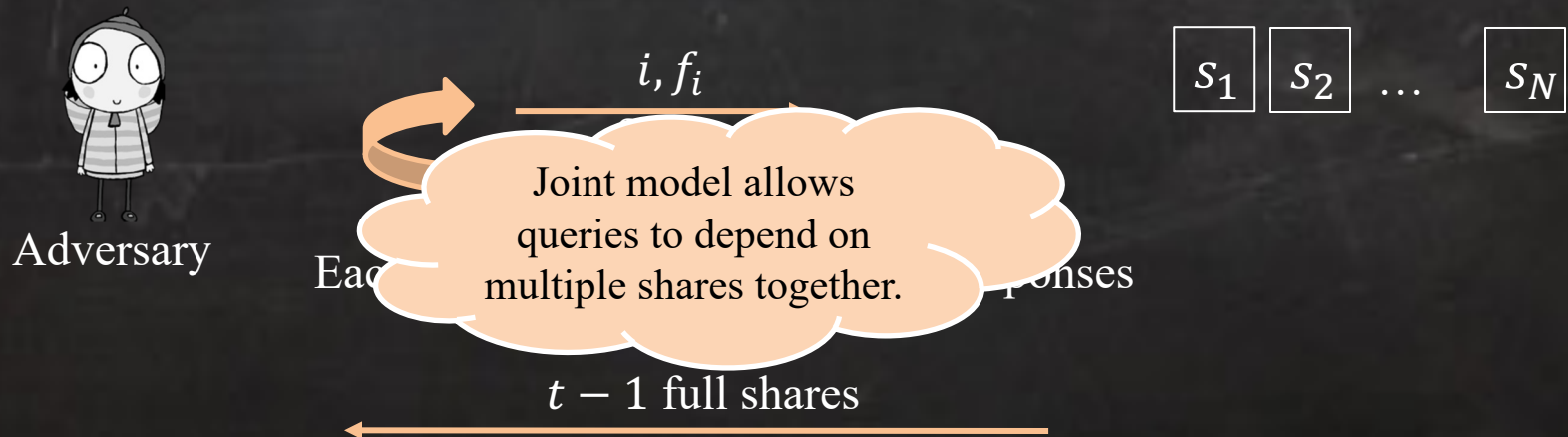


Leakage Resilient Secret Sharing

Parameters

- Share Size: Measures size of the largest share amongst all N shares.
- Leakage Model/Family: Determines the leakage queries allowed by adversary. Adaptive vs Non-adaptive, Independent vs Joint

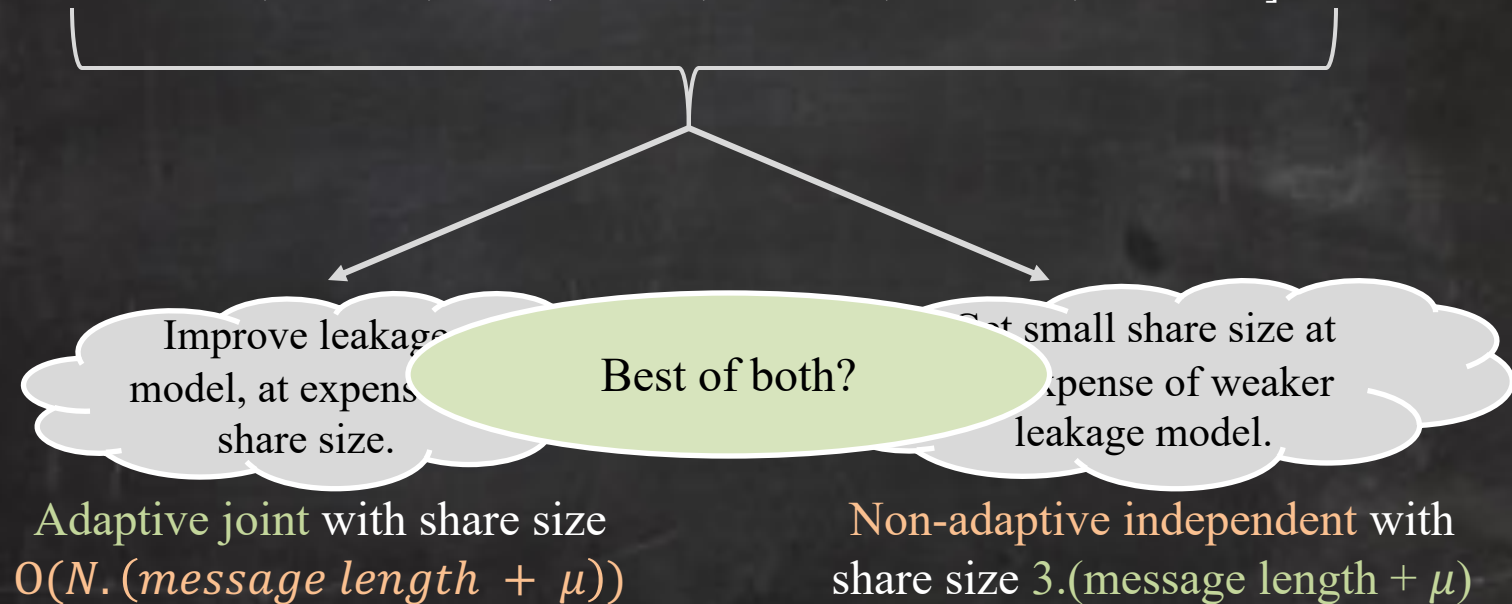
Adaptive Independent Leakage



Leakage Resilient Secret Sharing

State of Art

- Long line of research: [DDV10, LL12, GK18, BDIR18, SV19, ADN+19, KMS19, FV19, BFV19, LCG+19, CGG+20, BFO+20]



Our Result: Adaptive joint model with share size of $O((message\ length + \mu))$

Today's Talk

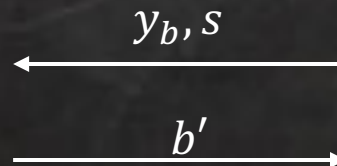
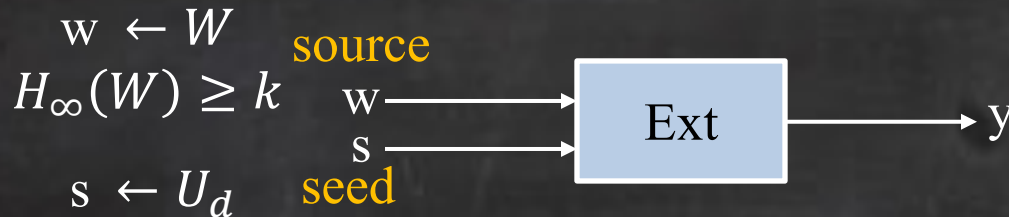
- Define Leakage Resilient Secret Sharing
- Important Parameters and State of Art
- Our Construction: for adaptive independent model
- Security Proof

Building Blocks

Adaptive Extractors

RANDOMNESS EXTRACTORS

[Nissan and Zuckerman, 1996]



Challenger

- Pick $s \leftarrow U_d, w \leftarrow W$ and a random bit b
- Set $y_0 = \text{Ext}(w; s)$
- Pick $y_1 \leftarrow U_l$

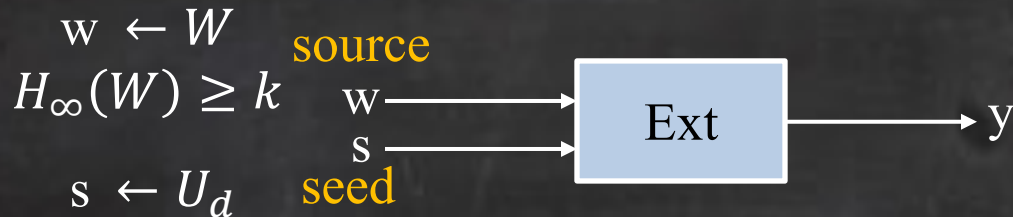
Security: $\Pr[b' = b] = \frac{1}{2} + \epsilon$

Building Blocks

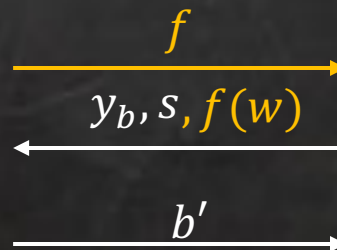
Adaptive Extractors

AVERAGE-CASE RANDOMNESS EXTRACTORS

[Nissan and Zuckerman, 1996]



Adversary



Challenger

- Pick $s \leftarrow U_d$, $w \leftarrow W$ and a random bit b
- Set $y_0 = \text{Ext}(w; s)$
- Pick $y_1 \leftarrow U_l$

Security: $\Pr[b' = b] = \frac{1}{2} + \epsilon$

Building Blocks

Adaptive Extractors

AVERAGE-CASE RANDOMNESS EXTRACTORS

Example: Leftover Hash (Impagliazzo, Levin, Luby, 1989)

$$q \log |\mathbb{F}| = k - 2 \log \frac{1}{\epsilon}$$

Define $\text{Ext}: \mathbb{F}_p \times (\mathbb{F}_p \times \mathbb{F}_p) \rightarrow \mathbb{F}_q$ as: $\text{Ext}(w, (a, b)) := (aw + b) \bmod q$
is an average case extractor for k -entropic sources!

What if adversary gets leakage on
 w , dependent on y_b and s ?

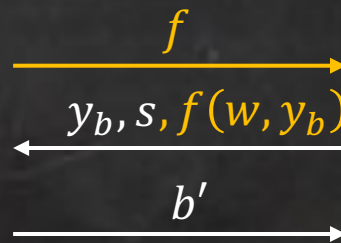
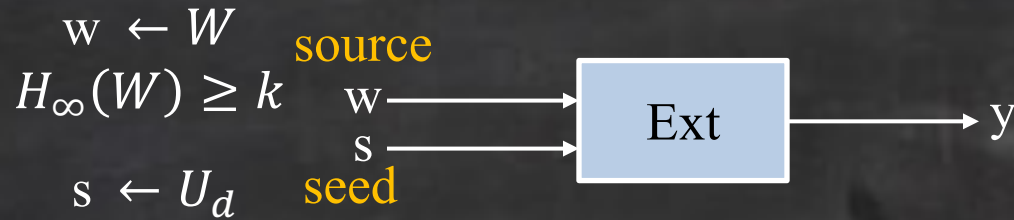
$$f(w, y_b, s) := 1_{\text{Ext}(w; s) = y_b}$$

BREAK

Building Blocks

Adaptive Extractors

Adaptive Randomness Extractors



Challenger

- Pick $s \leftarrow U_d, w \leftarrow W$ and a random bit b
- Set $y_0 = \text{Ext}(w; s)$
- Pick $y_1 \leftarrow U_l$

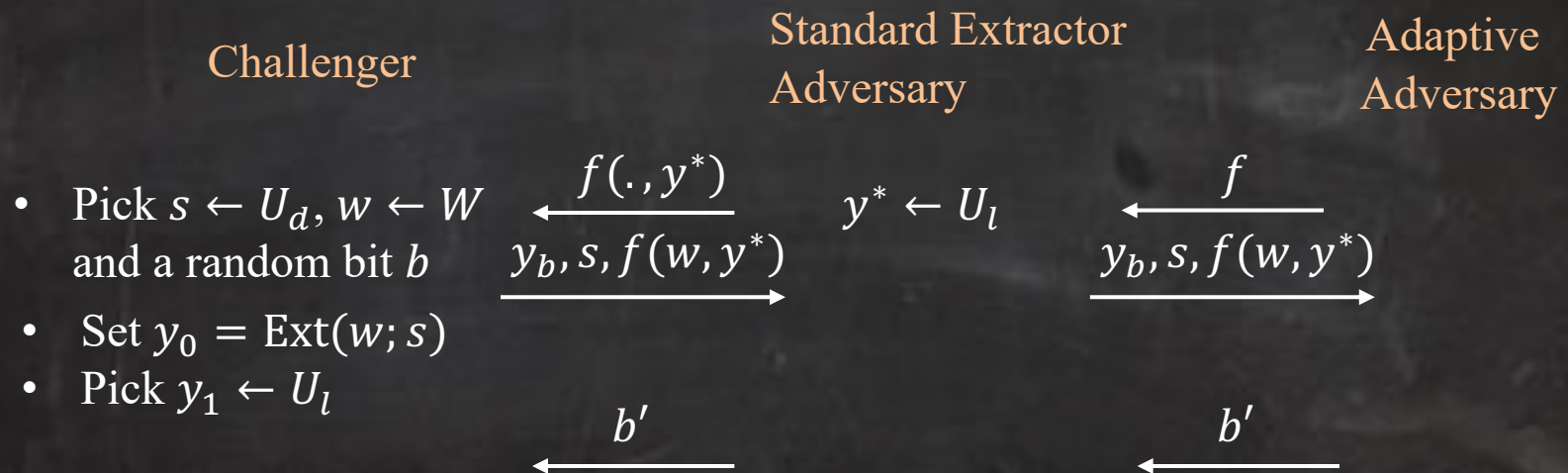
Security: $\Pr[b' = b] = \frac{1}{2} + \epsilon$

Building Blocks

Adaptive Extractors

Theorem: Any average-case extractor is also an adaptive randomness extractor, with a loss in the error.

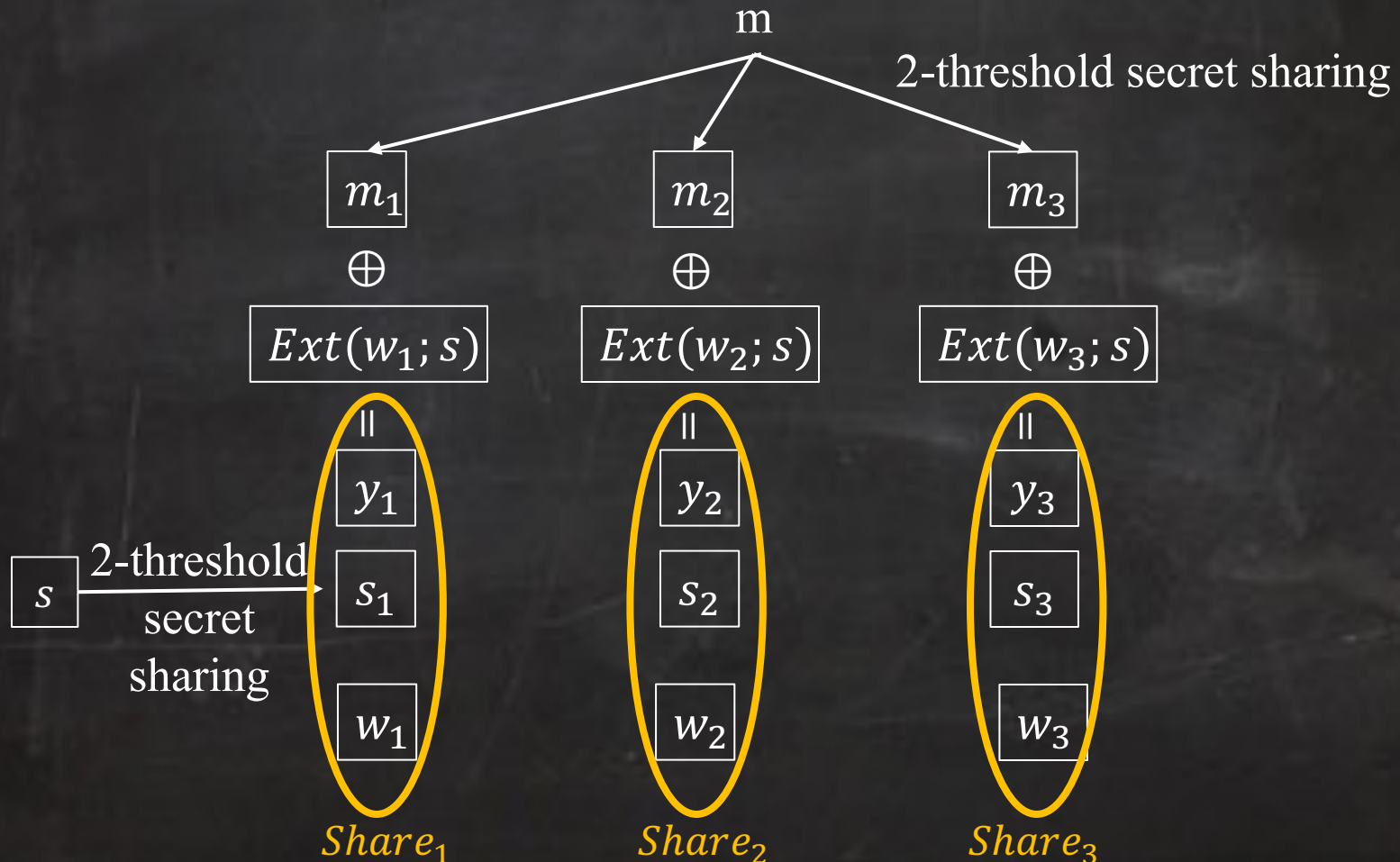
Proof:



If $y^* = y_b$ (which happens with probability $1/2^l$), then all correct evaluations!
 $\therefore$ Adaptive ext error = 2^l . (Standard ext error)

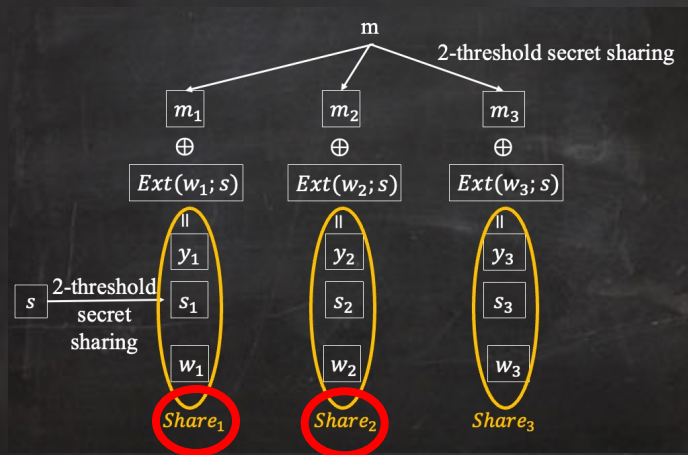
Our Construction

Toy Version (modification of [SV19])



Our Construction

Toy Version (Security?)



μ bits leakage from 1 share

+

1 full share

Use adaptive extractor
security with leakage on w_1

By secret
sharing privacy

- pick s_1 at random.

- f_1 is

- Rep

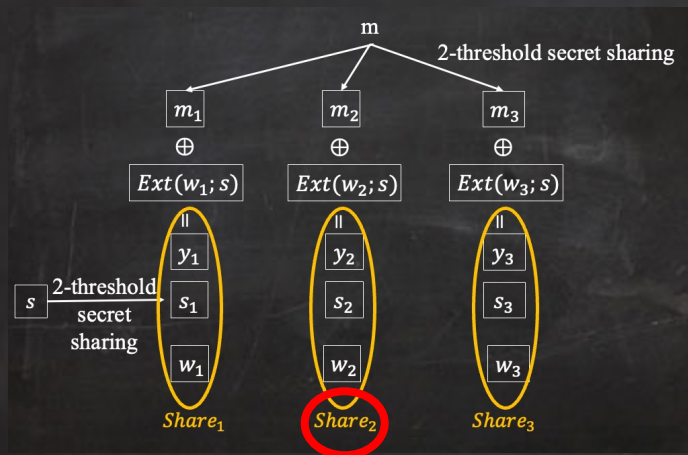
Leakage $f_1(y_1, s_1, w_1)$ is independent of m

factor security,

taking as $f_1(s_1, y_1, w_1)$ adaptive leakage on w_1 .

Our Construction

Toy Version (Security?)



μ bits leakage from 1 share

+

1 full share

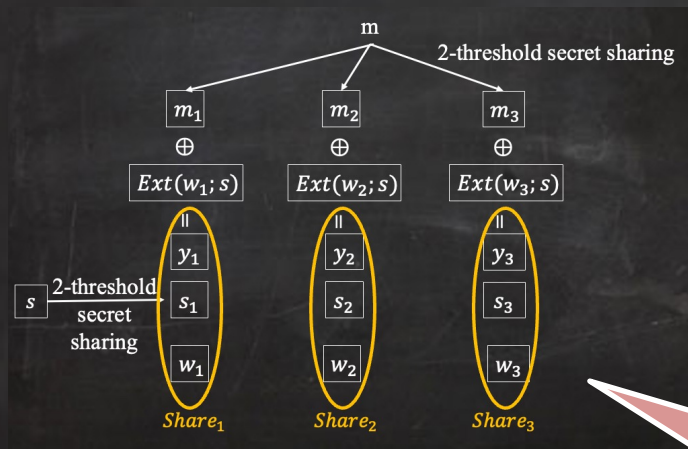
Use privacy of sharing

The 1 full share is also independent of m

m_2 is independent of m .

Our Construction

Toy Version (Security?)



μ bits leakage from $Share_1$

+

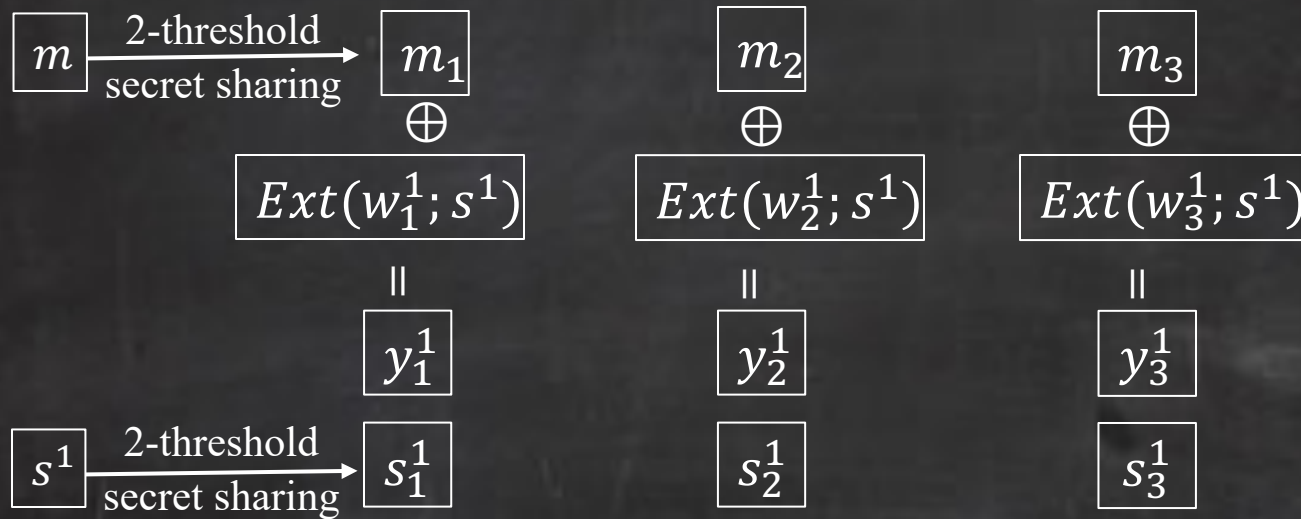
1 full share: $Share_2$

What about adaptive
leakage from $Share_3$?
BREAK!!

$Share_1$ and $Share_3$ depend on s .
Thus, leakage function f_3 depends on s .
Adaptive security fails!!

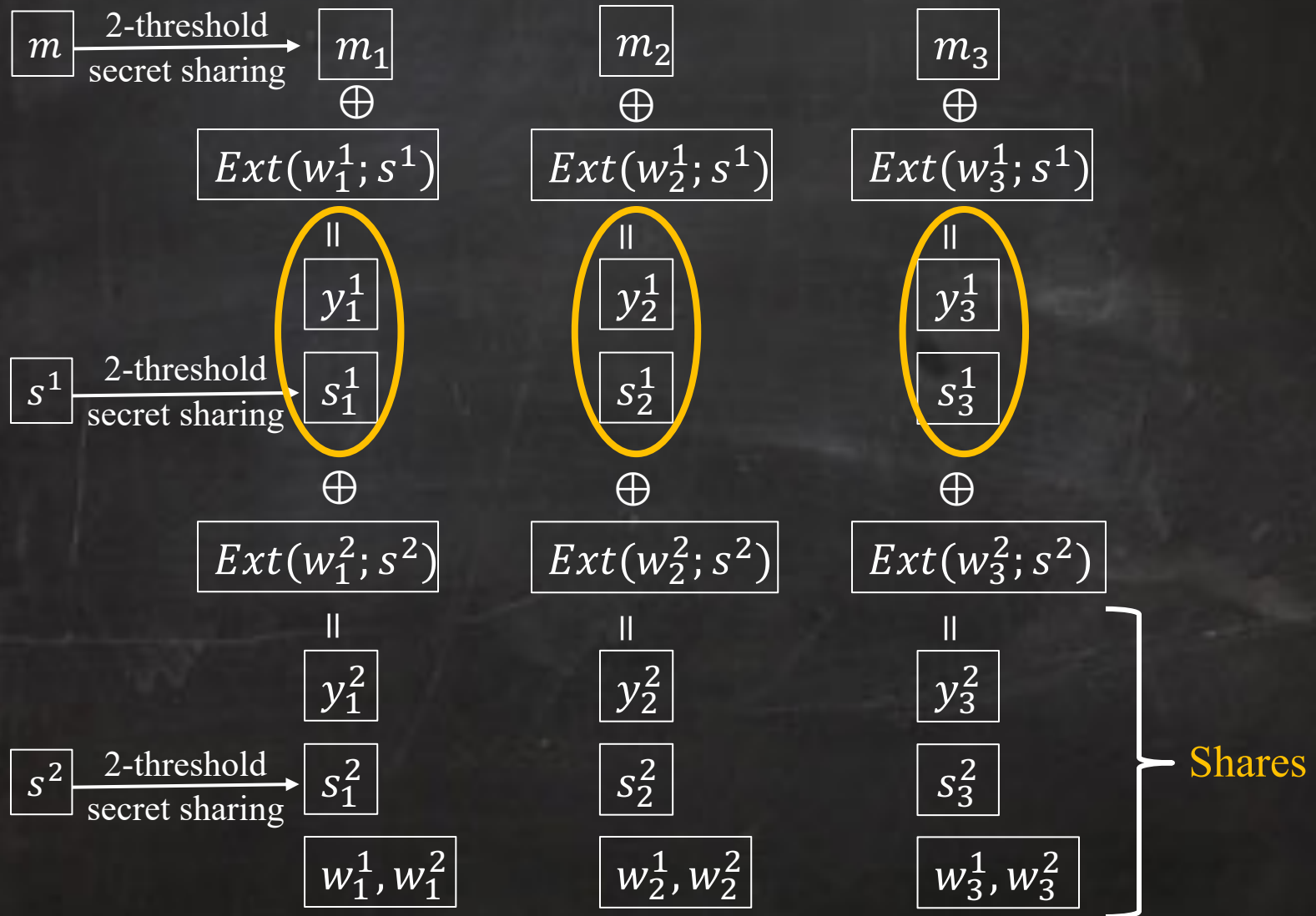
Our Construction

Main Construction Overview



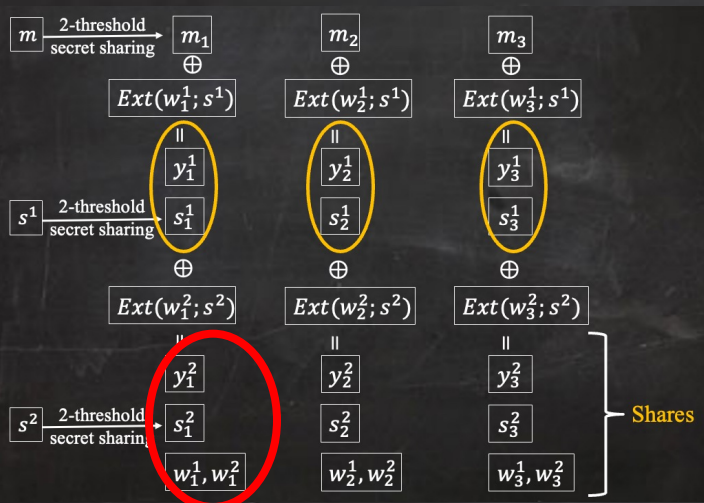
Our Construction

Main Construction Overview



Our Construction

Main Construction: Adaptive Security



μ bits adaptive leakage each from $Share_1$ and $Share_3$

+

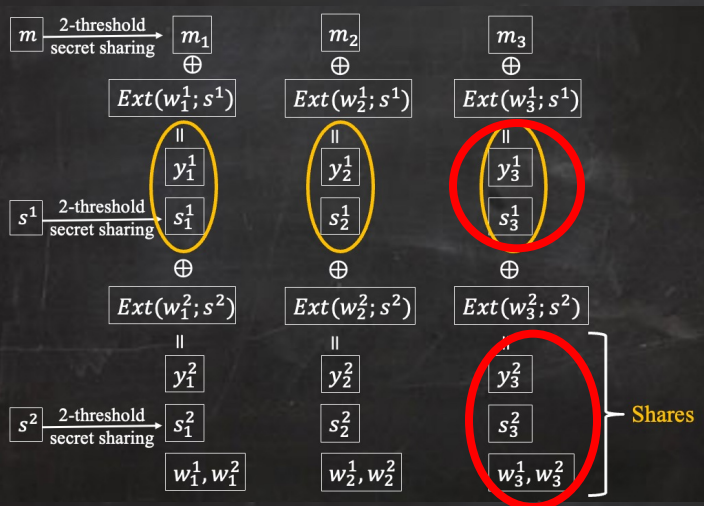
1 full share: $Share_2$

For $Share_1$ and $Share_3$:

- pick y_1^1 and y_3^1 for security to
- A first leakage query independent of m for security to replace y_1^1 and y_3^1 with random.

Our Construction

Main Construction: Adaptive Security



μ bits adaptive leakage each from $Share_1$ and $Share_3$

+

1 full share: $Share_2$

For $Share_1$'s leakage query

- pick y_1^1
- A μ -bit adaptive leakage query for security to replace y_1^1 with random.

First leakage query independent of m_1

For $Share_3$'s leakage query

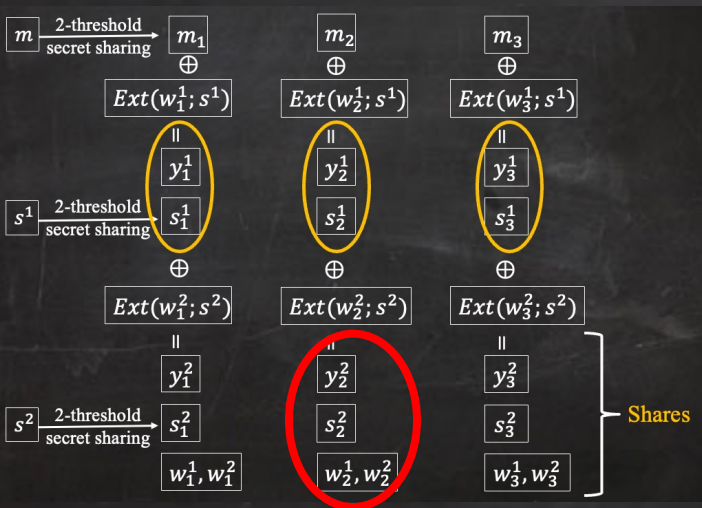
- pick y_3^1
- A μ -bit adaptive leakage query to replace y_3^1 with random.

Second adaptive leakage query independent of m_3

Can't use s^2 's security

Our Construction

Main Construction: Adaptive Security



μ bits adaptive leakage each from $Share_1$ and $Share_3$

+

1 full share: $Share_2$

By

Full share query also independent of m

of m .

First leakage query independent of m_1

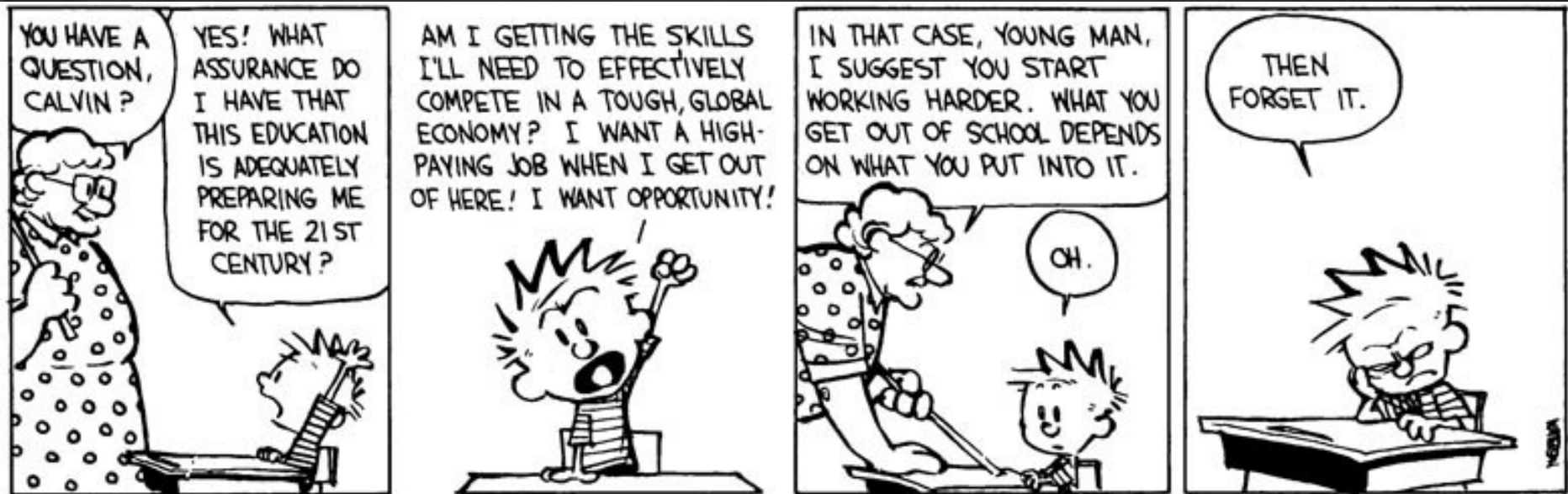
Second adaptive leakage query independent of m_3

For any m, m' , we have $Leak^m \approx Leak^{m'}$.

Summary

- What I showed: adaptive independent scheme with share size: $|y_i^2| + |s_i^2| + |w_i^2| + |w_i^1|$ --- with our adaptive extractors this gives-- $O(|m| + \mu)$.
- Generically, we get same share size for N -parties and threshold t , and for a adaptive joint model!

Paper: <https://eprint.iacr.org/2020/1252>



THANK YOU
Questions?

Thesis Contributions

Leakage Resilient Secret Sharing

TODAY

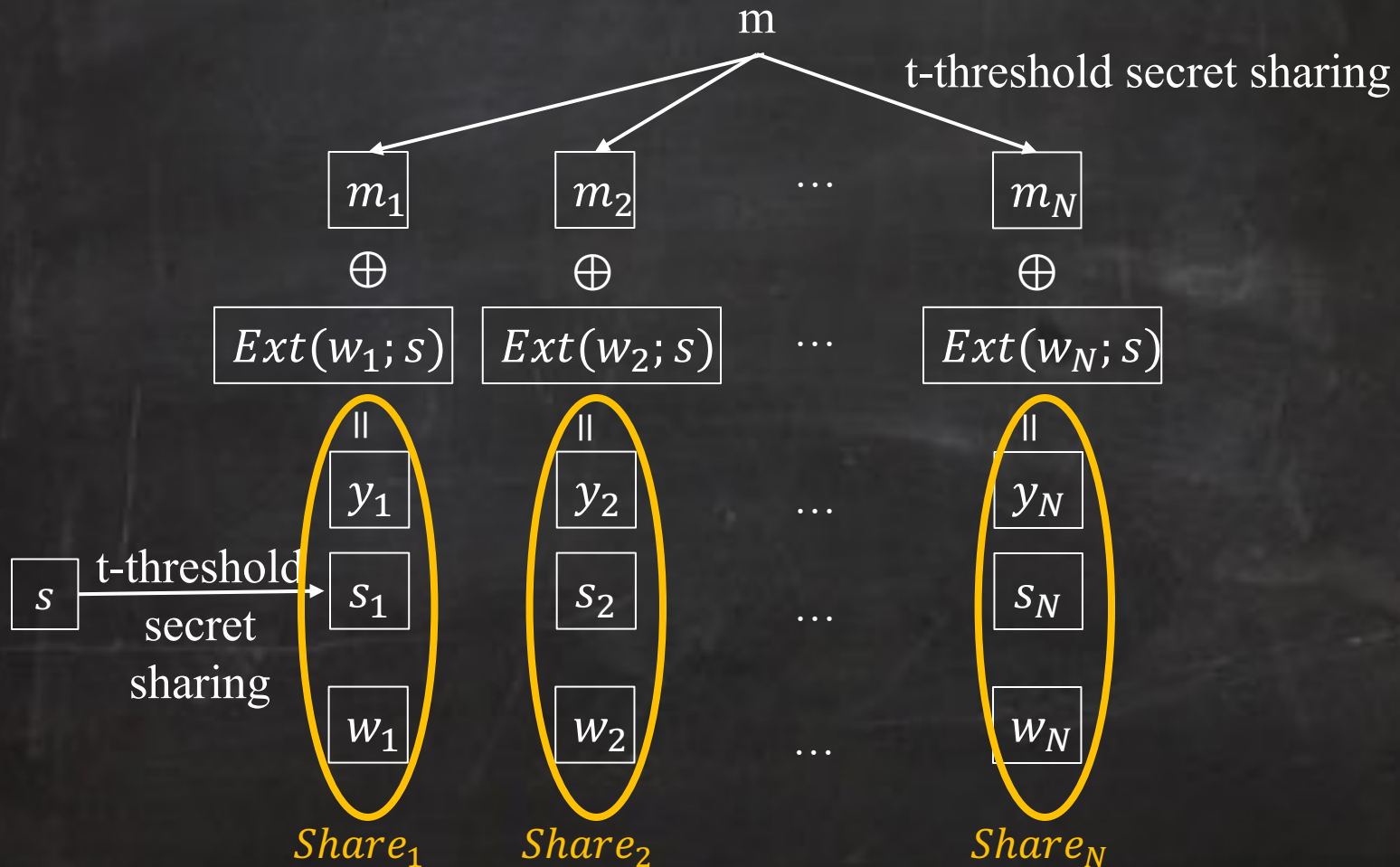
1. Adaptive Extractors and their Application to Leakage Resilient Secret Sharing
Published at: CRYPTO 2021
Joint Work with: Nishanth Chandran, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu
2. Leakage Resilient Secret Sharing with Optimal Share Size.
Under Submission
Joint Work with: Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu
3. Non-malleable Codes
Published at: ECCC
Joint Work with: Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu
4. Simplicity Meets Near-Optimal Rate: Non-malleable Codes and Non-malleable Two-source Extractors via Rate Boosters.
Under Submission
Joint Work with: Divesh Aggarwal, Bhavana Kanukurthi, Sai Lakshmi Bhavana Obbattu, Maciej Obremski

Goal: Optimizing share/code size!

Non-malleable Codes

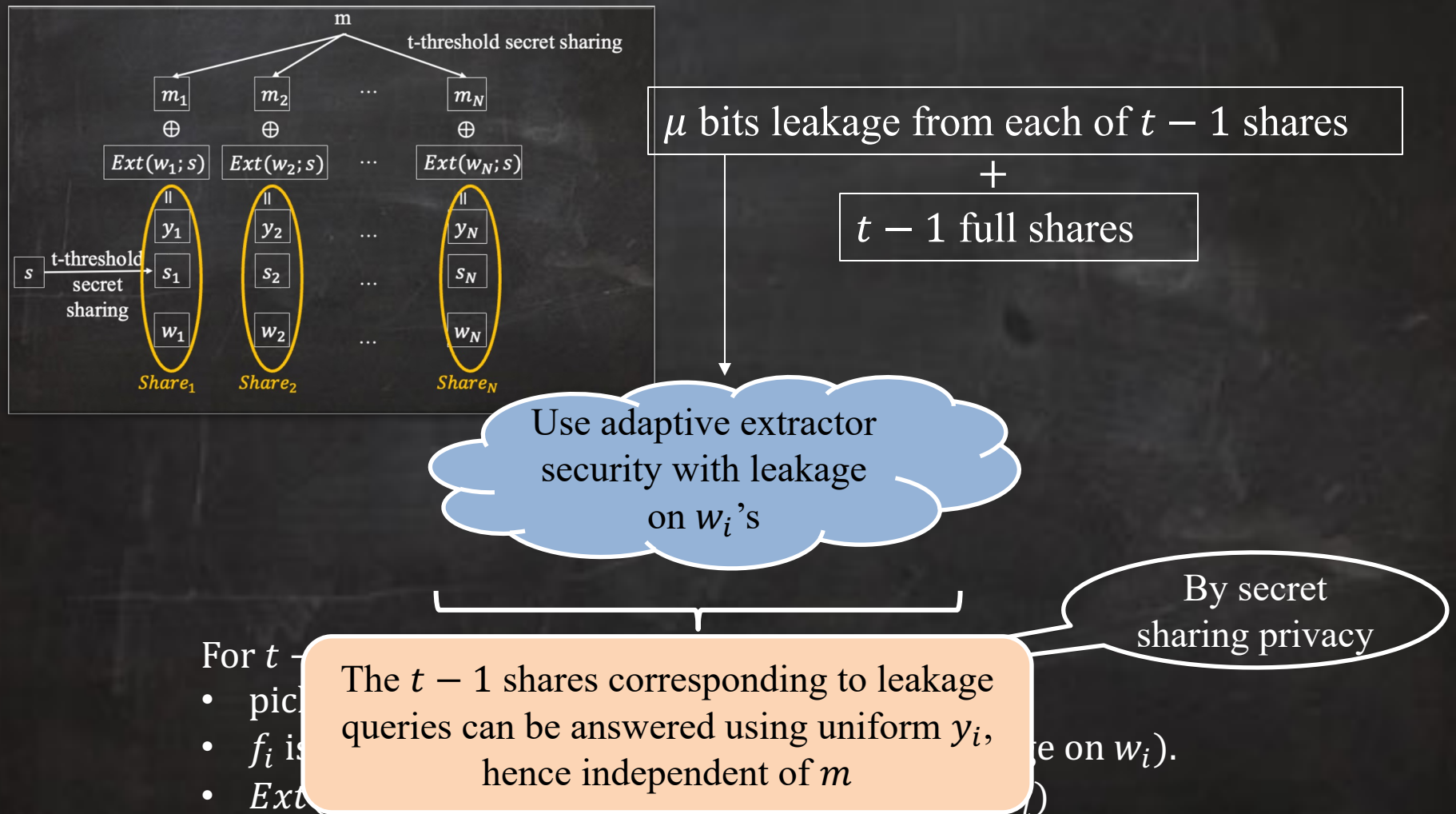
Our Construction

Toy Version (modification of [SV19])



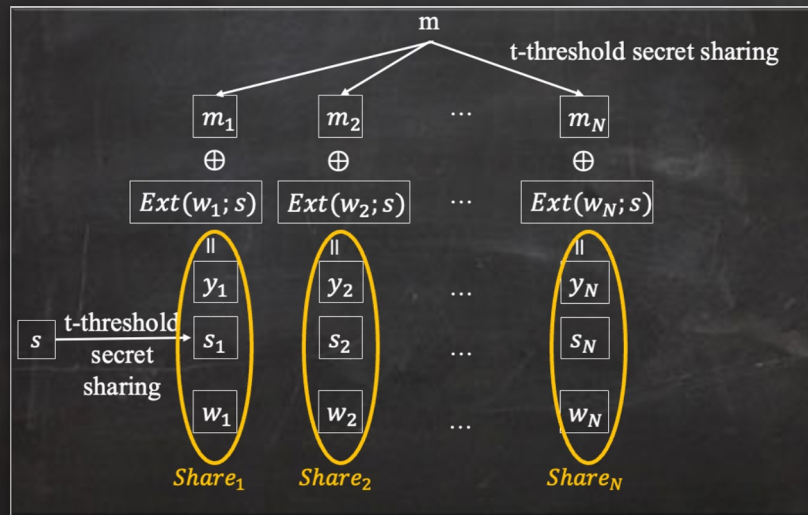
Our Construction

Toy Version (Non-adaptive secure?)



Our Construction

Toy Version (Non-adaptive secure?)



μ bits leakage from each of $t - 1$ shares

+

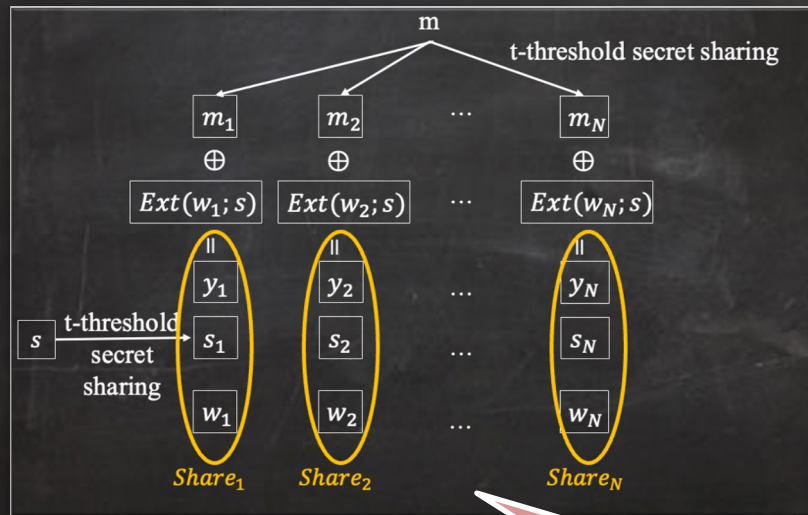
$t - 1$ full shares

The $t - 1$ full shares are also independent of m

These $t - 1$ m_i 's are independent of m .

Our Construction

Toy Version (Non-adaptive secure?)



μ bits leakage from each of $t - 1$ shares

+

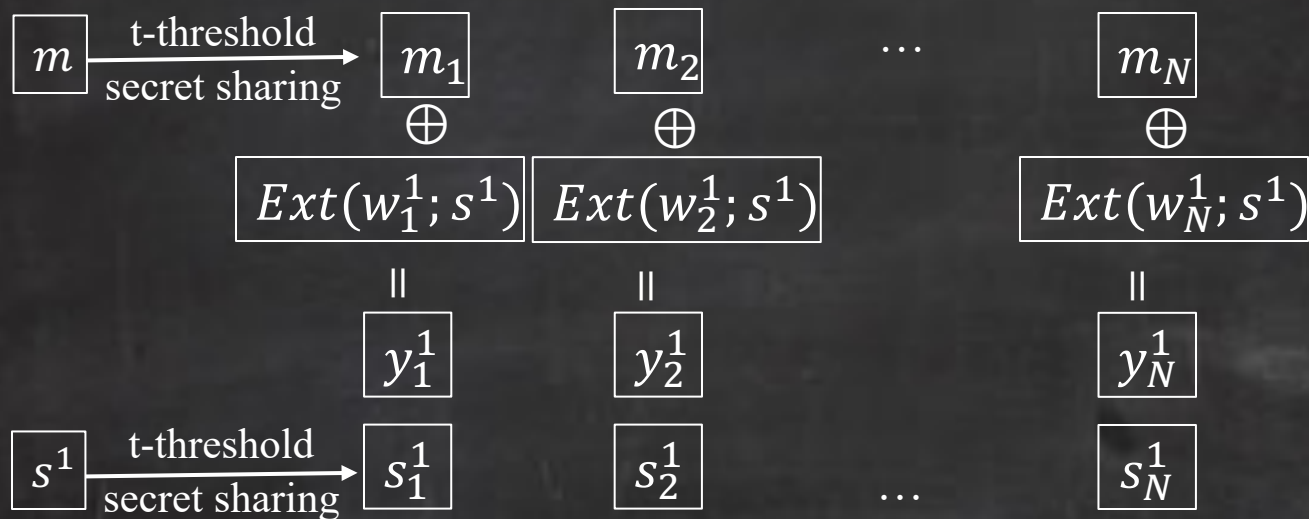
$t - 1$ full shares

What about leakage from
more than $t - 1$ shares?
BREAK!!

$\geq t$ shares depend on s .
Leakage function
depends on s .
Adaptive security fails!!

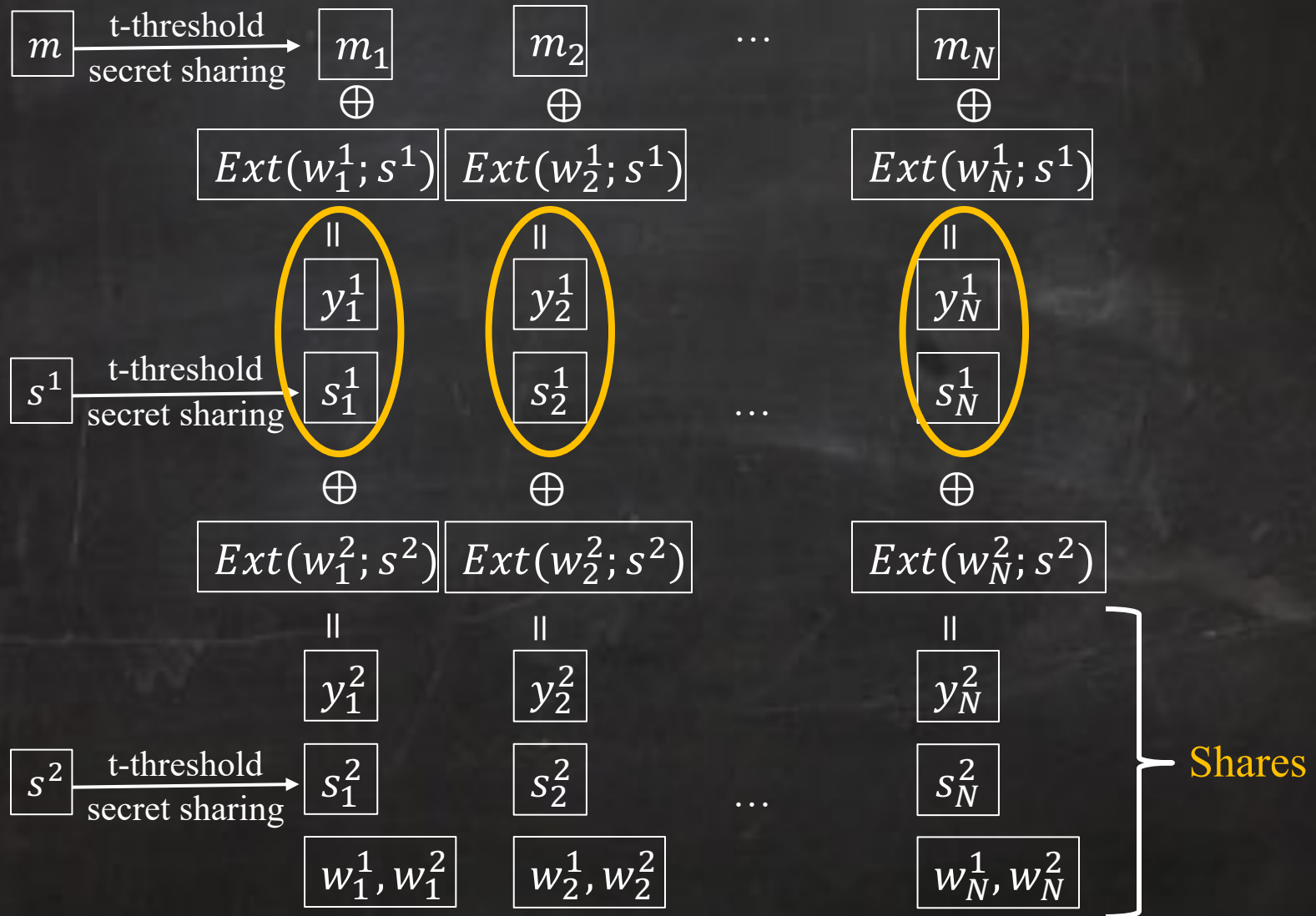
Our Construction

Main Construction Overview



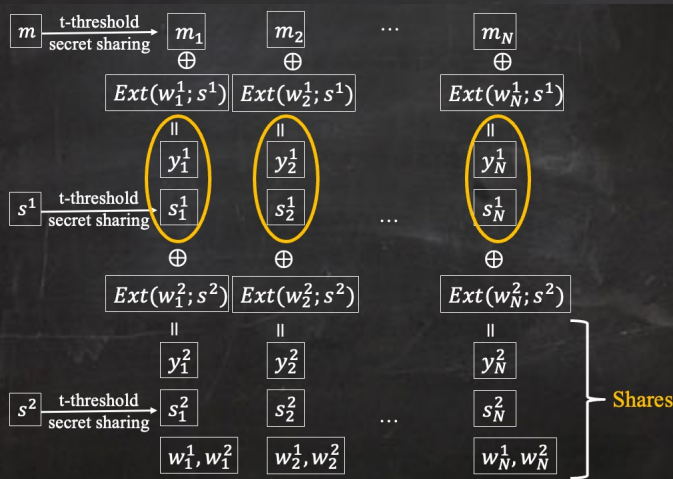
Our Construction

Main Construction: Overview



Our Construction

Main Construction: Adaptive Secure?



For first $t - 1$ adaptive leakage queries:

- pick s^1
- As first $t - 1$ adaptive leakage queries independent of m security of s with uniform random strings.

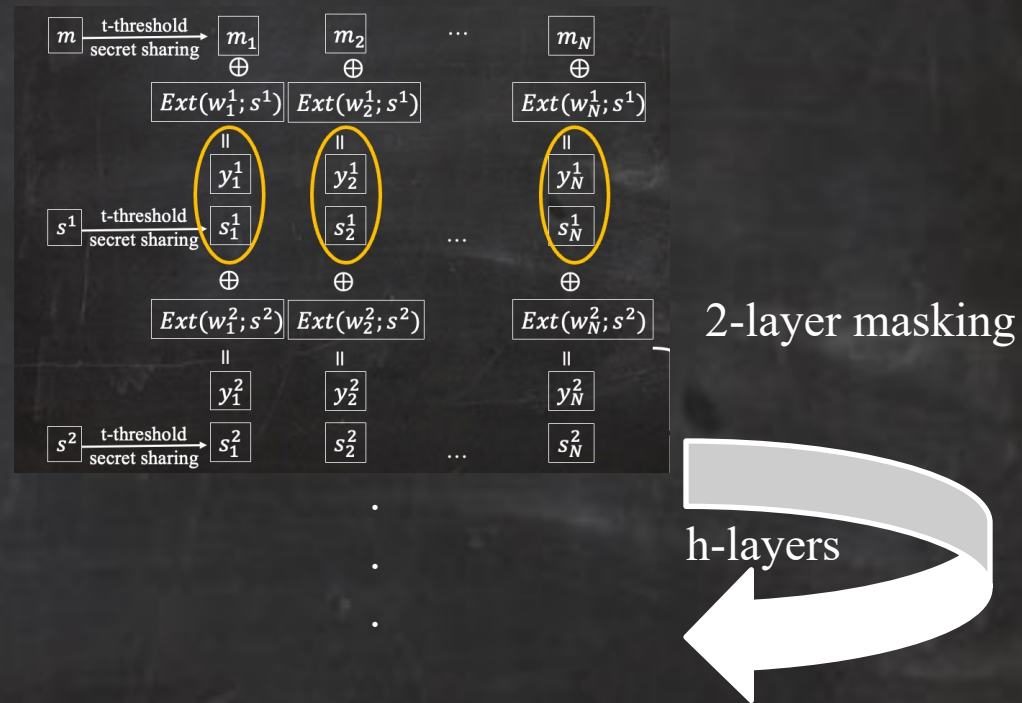
For the next $t - 1$ adaptive leakage queries:

- pick $s^1, s^2, \dots, s^{t-1}$
- As next $t - 1$ adaptive leakage queries independent of m first layer extra random strings.

This 2-layer masking gives:
 μ bit leakage each from $2(t - 1)$ shares adaptively
 +
 $t - 1$ full shares in the end

Our Construction

Main Construction: Extending Security



This h -layer masking gives:
 μ bit leakage each from $h(t - 1)$ shares adaptively
 +
 $t - 1$ full shares in the end