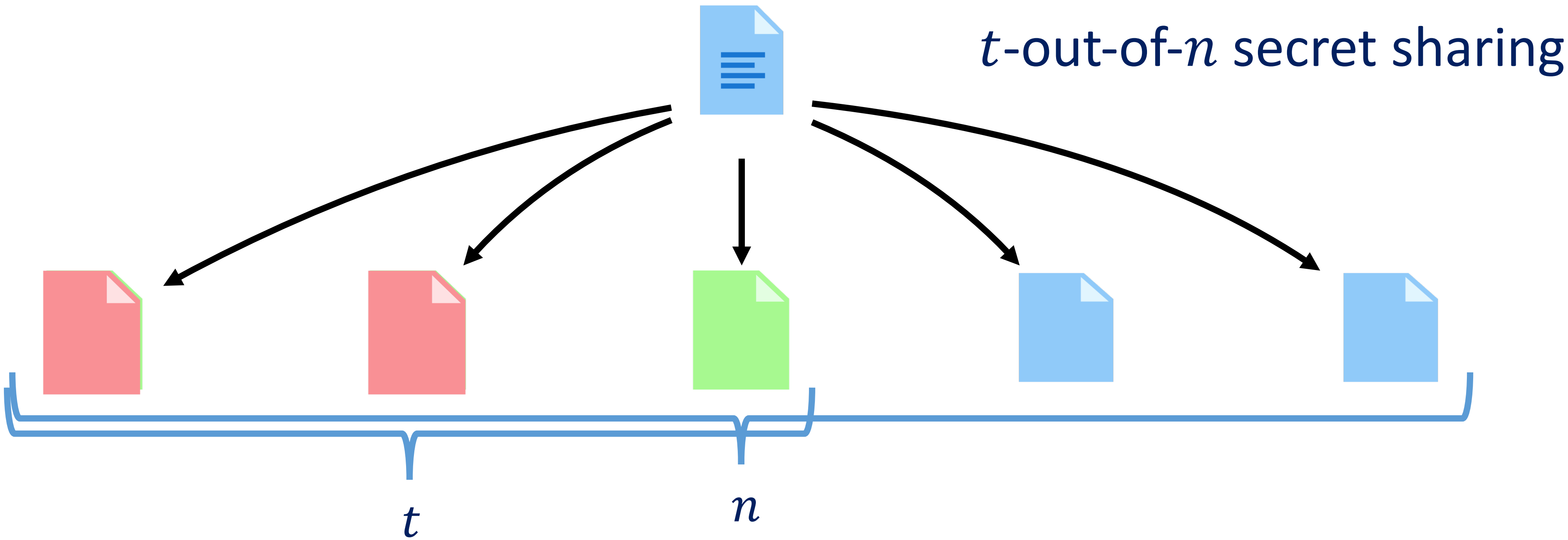
Stronger Lower Bounds for Leakage-Resilient Secret Sharing

Charlotte Hoffmann[1] and Mark Simkin[2]

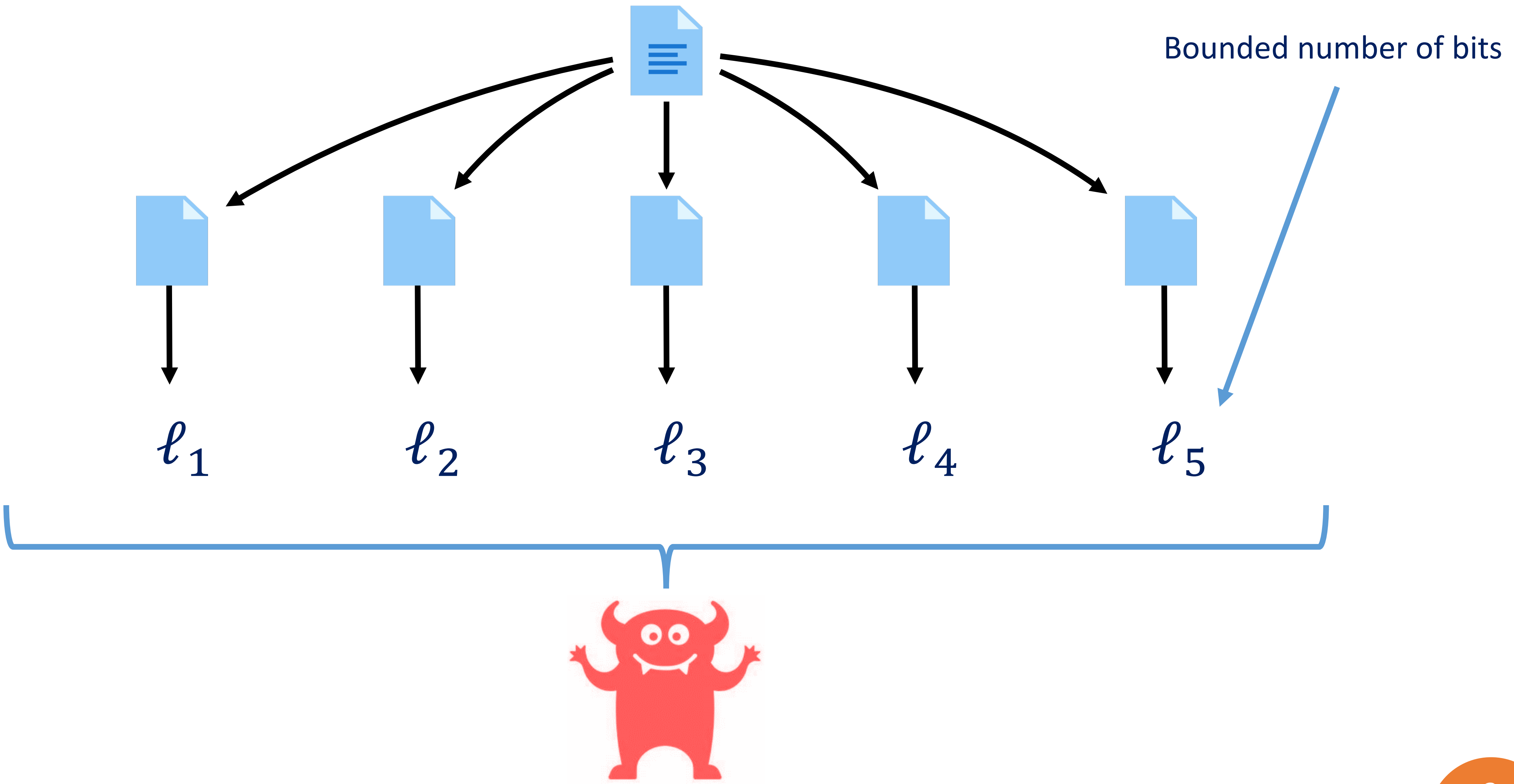
[1]Institute of Science and Technology Austria
[2]Ethereum Foundation

(Threshold) Secret Sharing

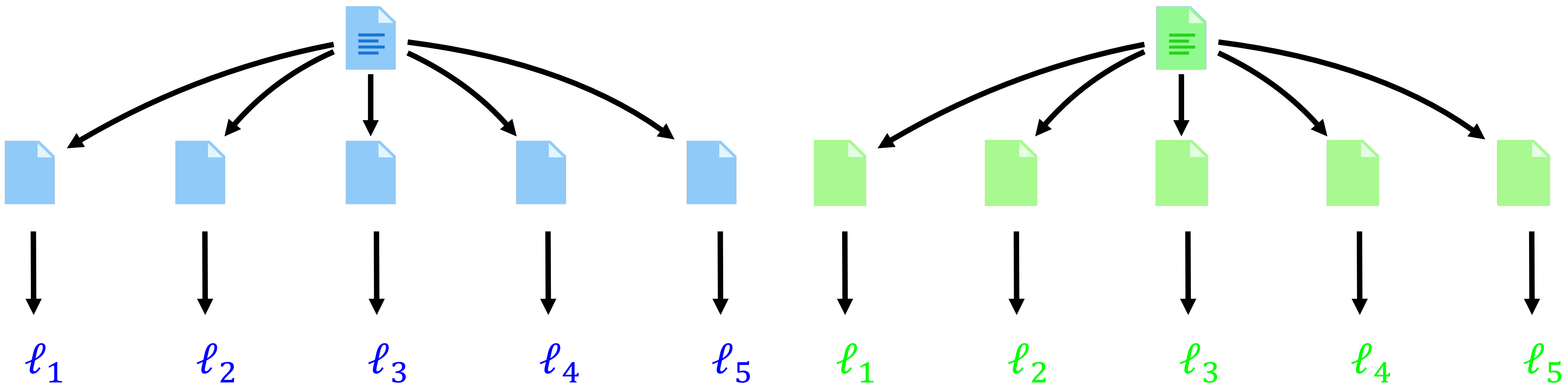


- **Correctness**: any number of shares **above** reconstruction threshold t can reconstruct secret
- **Privacy**: any number of shares **below** reconstruction threshold t learns nothing about secret

Leakage-Resilient Secret Sharing



Leakage-Resilient Secret Sharing - Security



$$(\ell_1, \dots, \ell_n) \approx_\epsilon (\ell_1, \dots, \ell_n)$$

statistically close

[DP07, BGK14, GK18b, GK18a, ADN+19, KMS19, SV19, CKOS21, CKOS22, …]

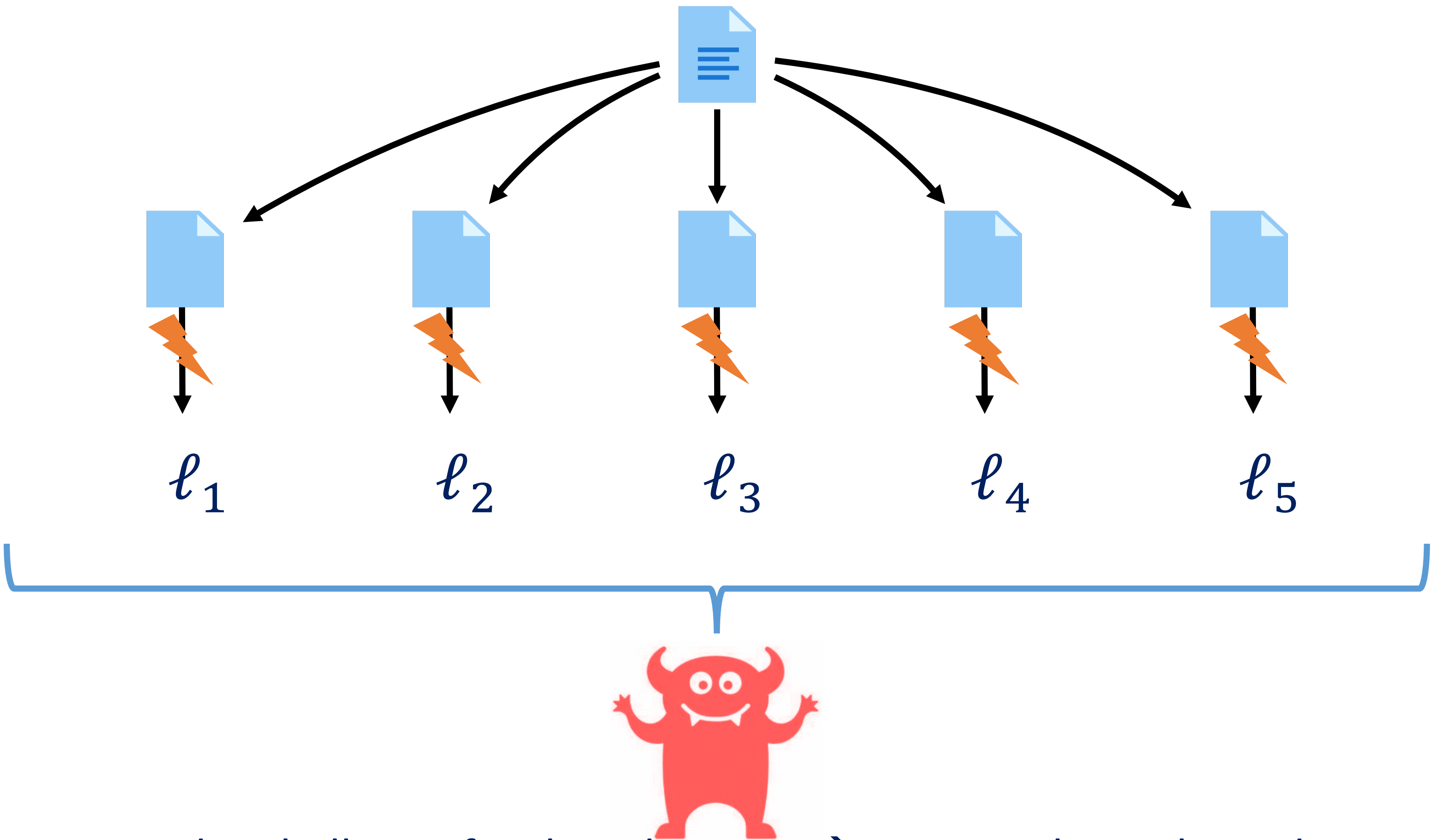
Leakage-Resilience of Shamir's Secret Sharing

- [BDIR18]: t-out-of-n Shamir secret sharing is 1-bit leakage resilient for
$$t > 0.85n$$
- conjecture that this holds for $t > cn$, where c is any constant
- [NS20]: t-out-of-n Shamir secret sharing is **not** 1-bit leakage resilient for
$$t = \frac{cn}{\log n}$$

[BDIR18]: Benhamouda, Degwekar, Ishai, Rabin, Crypto 2018
[NS20]: Nielsen, Simkin, Eurocrypt 2020

Our Contribution

Noisy Leakages

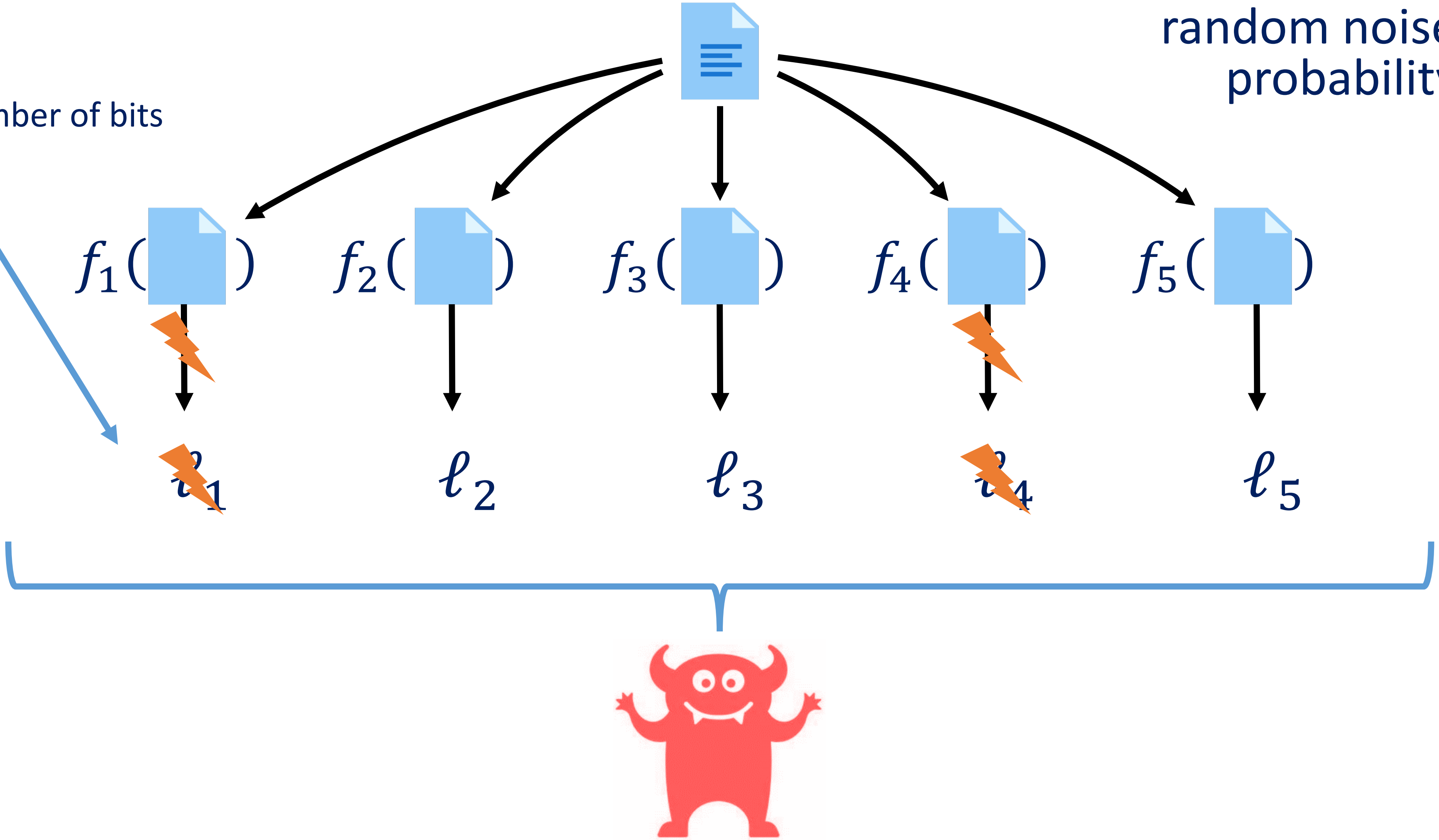


Harder challenge for the adversary → Stronger lower bounds

Noisy Leakages – Our Model

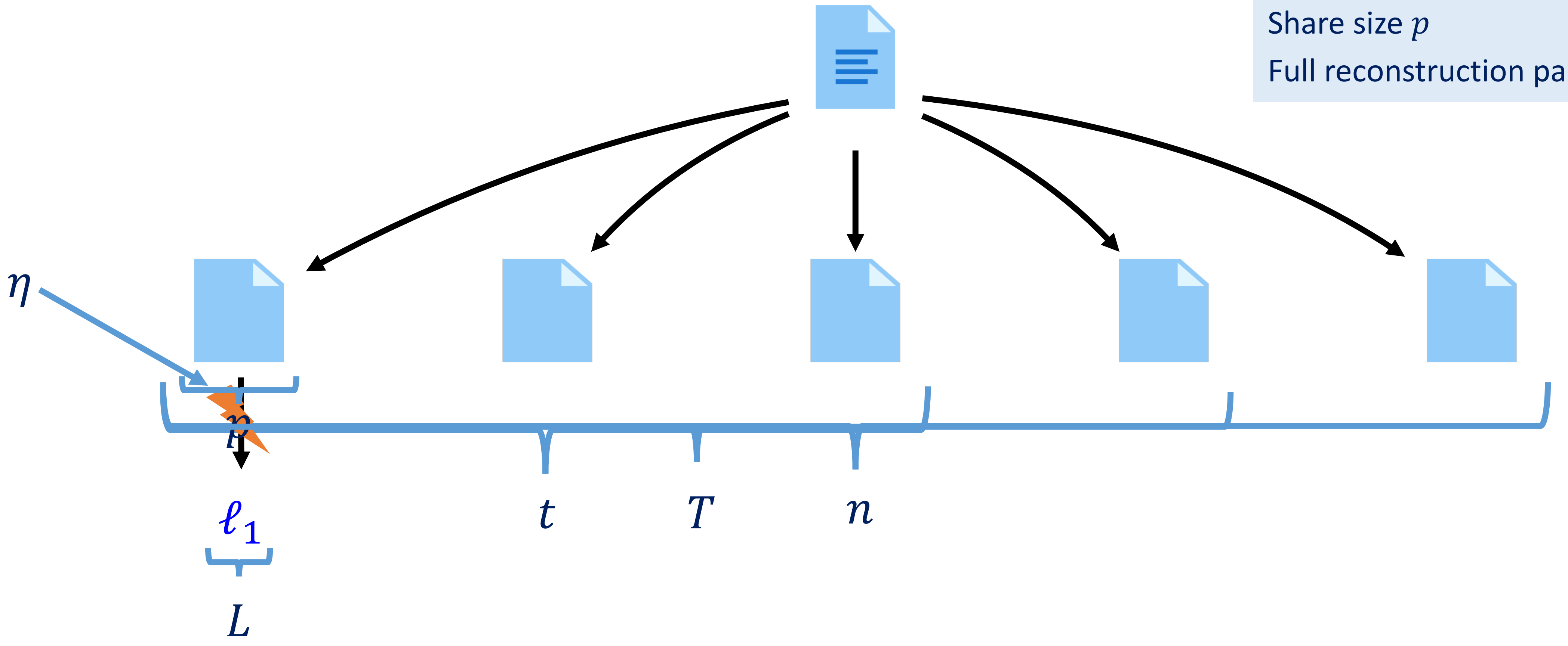
Replace each leakage with uniformly random noise with probability η

Bounded number of bits



Parameters

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T



Our Results – Part 1

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

- For any noisy leakage-resilient secret sharing scheme it holds that

$$p \geq \frac{L(n-t)}{T} - \frac{4n\eta(L + \log 1/\eta) + 1}{T}.$$

- For $\eta \to 0$ obtain noiseless bound from [NS20]: $p \geq \frac{L(n-t)}{T}$.

- For $\eta = 1/64$ obtain $p \geq \frac{L(n-2t)}{2T} - 1$.

Our Results – Part 2

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

- $(\frac{cn}{\log n})$-out-of-n Shamir secret sharing is **not** resilient against **1-bit** leakage, even if a **constant** number of leakages is replaced by random **noise**.

→ Same bound as noiseless case [NS20]

Proof Sketch

Our Results

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

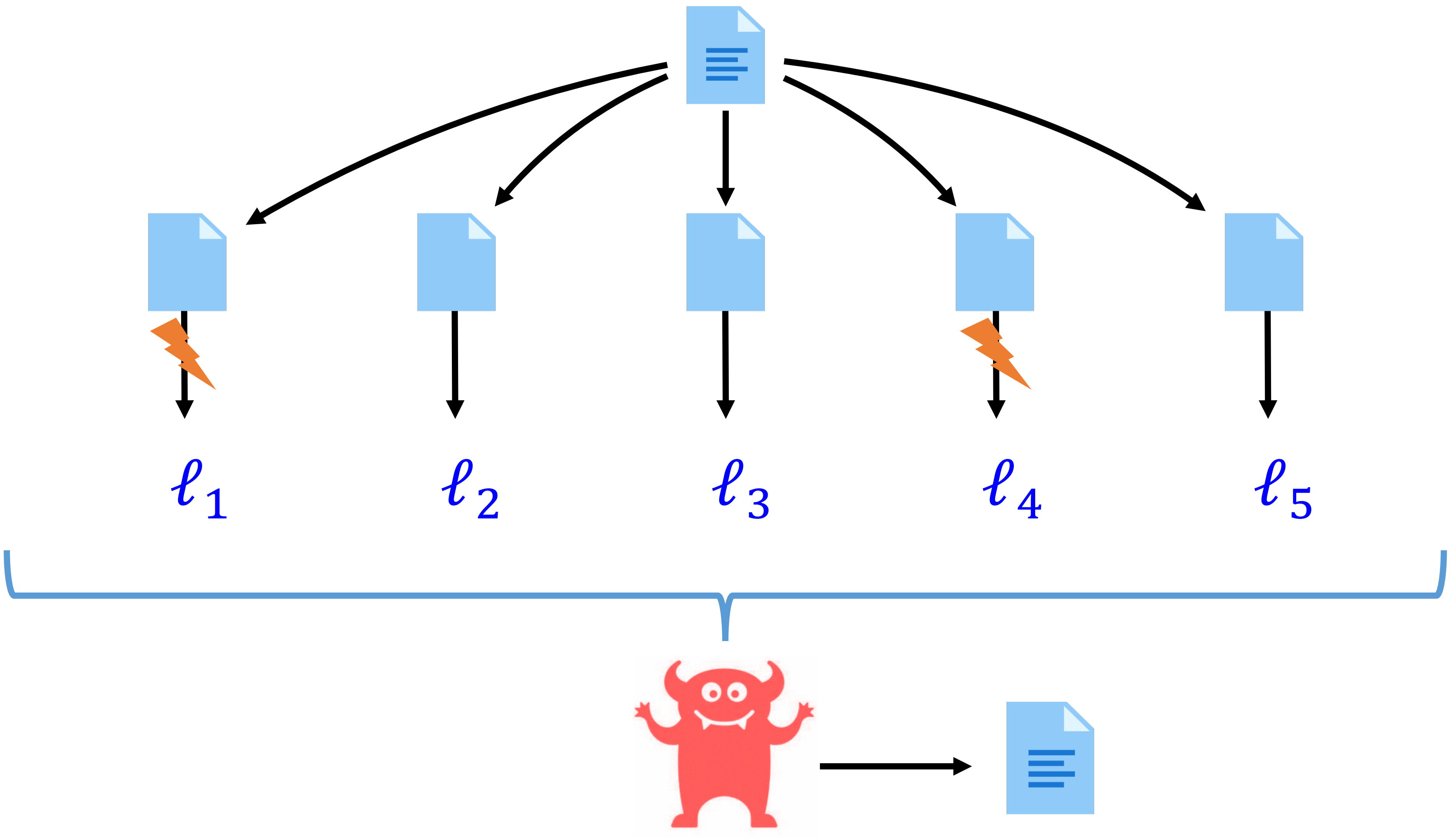
- For any noisy leakage-resilient secret sharing scheme it holds that

$$p \geq \frac{L(n-t)}{T} - \frac{4n\eta(L + \log 1/\eta) + 1}{T}.$$

- $(\frac{cn}{\log n})$-out-of-n Shamir secret sharing is not resilient against 1-bit leakage, even if a constant number of leakages is replaced by random noise.

→ Same bound as noiseless case [NS20]

One-Way Noisy Leakage-Resilience



The Adversary

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

[NS20]

$f_1(\ ) \, f_2(\ ) \, f_3(\ ) \, f_4(\ ) \, f_5(\ )$

Uniform

1. Iterate through all possible secrets and secret sharings and apply functions f_i
2. If only one secret s has a secret sharing that **exactly matches** input, output s.

Probability that any other secret has same leakage

$$\leq 2^{pT-L(n-t+1)}$$

Our work

$f_1(\ ) \qquad f_3(\ ) \, f_4(\ )$

Union bound:

- Fix secrets s_1, s_2.
- Their sharings differ in at least $n-t+1$ shares.
- Probability that sharing produces same leakage: $2^{-L(n-t+1)}$
- Number of possible sharings: 2^{pT}

1. Iterate through all possible secrets and secret sharings and apply functions f_i
2. If only one secret s has a secret sharing that **is close to** input, output s.

Probability that any other leakage is close to input

$$\leq \boxed{\eta^{-4n\eta} 2^{pT}} \boxed{-L(n-t+1-4n\eta)}$$

Number of possible leakage vectors

Probability that sharing produces close leakage

Our Results

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

- For any noisy leakage-resilient secret sharing scheme it holds that

$$p \geq \frac{L(n-t)}{T} - \frac{4n\eta(L+\log 1/\eta)+1}{T}.$$

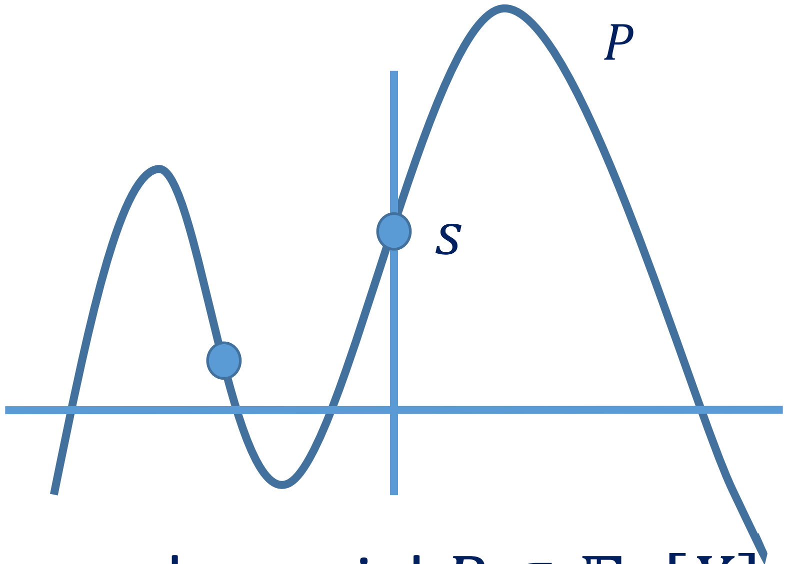
- $(\frac{cn}{\log n})$-out-of-n Shamir secret sharing is not resilient against 1-bit leakage, even if a constant number of leakages is replaced by random noise.

→ Same bound as noiseless case [NS20]

Shamir's Secret Sharing

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

- secret: $s \in \mathbb{F}_q$



- share: point on random polynomial $P \in \mathbb{F}_q[X]$ of degree $t-1$
- t parties can reconstruct s via interpolation
- $t-1$ parties learn nothing about s
- $n = q \rightarrow p = \log n$
- $T = t$

Lower Bound for Shamir's Secret Sharing

Number of parties n

Reconstruction threshold t

Leakage per share L

Noise probability η

Share size p

Full reconstruction parameter T

- For any noisy leakage-resilient secret sharing scheme it holds that

$$p \geq \frac{L(n-t)}{T} - \frac{4n\eta(L + \log 1/\eta) + 1}{T}.$$

- Plug in parameters for $(\frac{cn}{\log n})$-out-of-n Shamir:

$$\boxed{p = \log n}, \boxed{T = t = \frac{cn}{\log n}}, \boxed{L = 1}, \boxed{\eta = \frac{1}{64}}$$

$$\log n \not\geq \frac{3 \log n}{2} - 2$$

Contradiction!

Our Results

Number of parties n
Reconstruction threshold t
Leakage per share L
Noise probability η
Share size p
Full reconstruction parameter T

- For any noisy leakage-resilient secret sharing scheme it holds that

$$p \geq \frac{L(n-t)}{T} - \frac{4n\eta(L + \log 1/\eta) + 1}{T}.$$

- $(\frac{cn}{\log n})$-out-of-n Shamir secret sharing is not resilient against 1-bit leakage, even if a constant number of leakages is replaced by random noise.

→ Same bound as noiseless case [NS20]

Summary

- [BDIR18] conjecture that t-out-of-n Shamir secret sharing is 1-bit leakage resilient for

$$t > cn.$$

- We show that t-out-of-n Shamir secret sharing is **not** 1-bit leakage resilient for

$$t = \frac{cn}{\log n},$$

even if a constant fraction of leakages is replaced by random noise.

- But: Our adversary runs in exponential time.
- Open: Make the attack practical or prove computational leakage-resilience for Shamir secret sharing.

Questions?