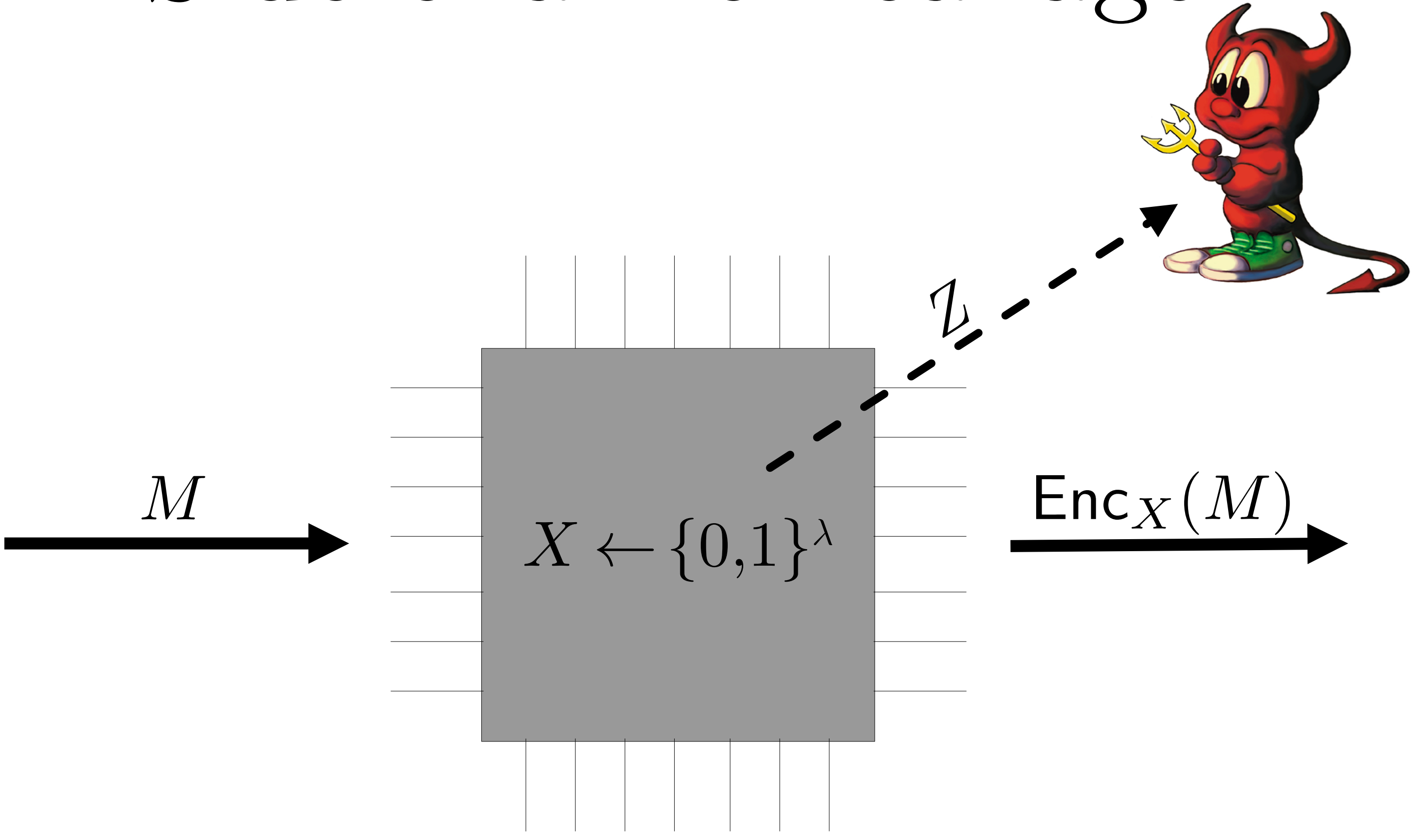
Improved Reductions from Noisy to Bounded and Probing Leakages via Hockey-Stick Divergences

Maciej Obremski	National University of Singapore
João Ribeiro	Univ Nova Lisboa ⟶ Técnico Lisboa
Lawrence Roy	Aarhus University
François-Xavier Standaert	Catholic University of Louvain
Daniele Venturi	Sapienza University of Rome

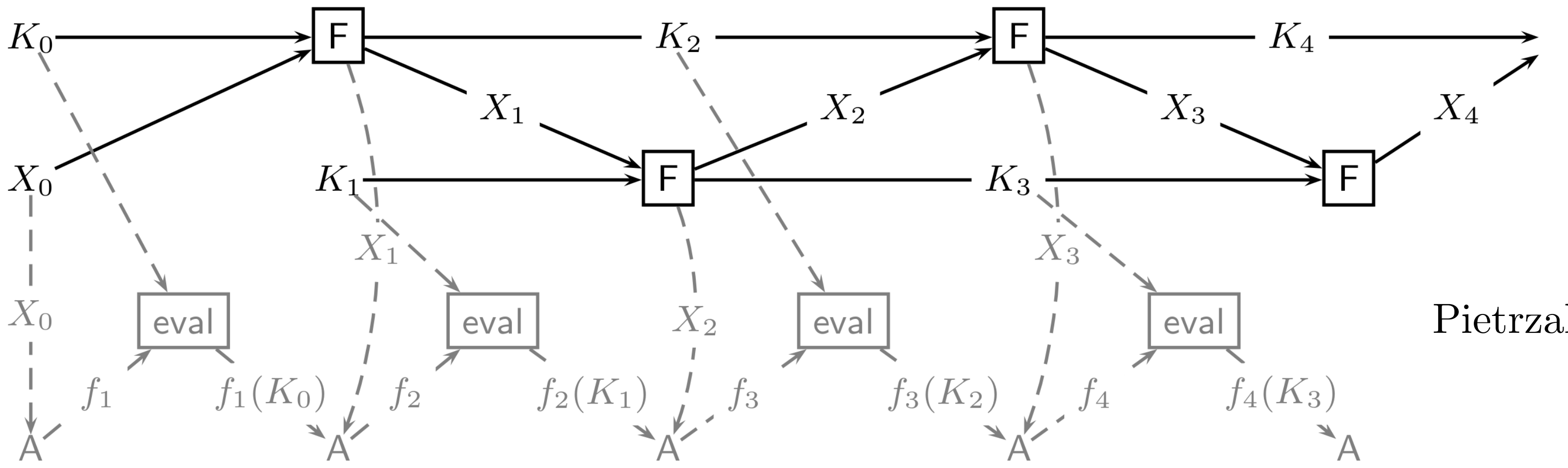
Side-channel leakage



What does Z leak about X?

Primitive-level countermeasures

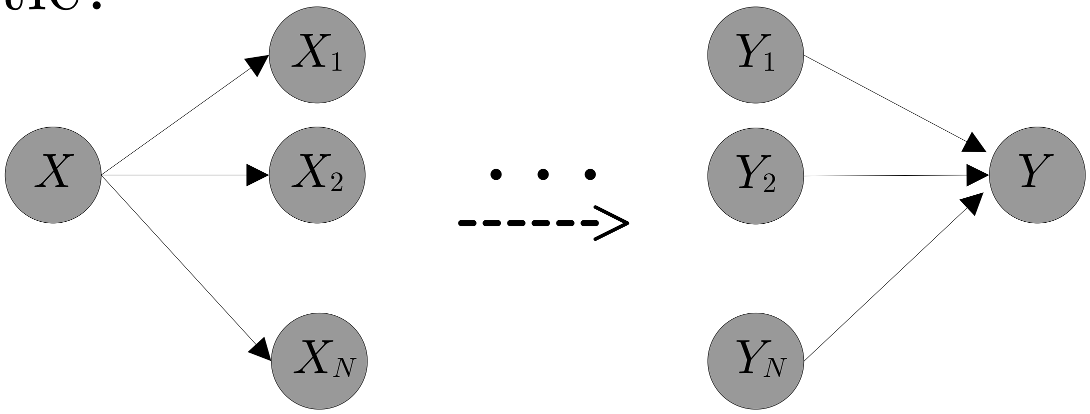
- Leakage resilient cryptography
- Typical simplified model: bounded leakage
  - Realistic?



Pietrzak 2009

Implementation-level countermeasures

- Masking / secret sharing
- Typical simplified model: random probing
  - Realistic?



$$X = \sum_i X_i \qquad \sum_i Y_i = Y$$

Primitive-level countermeasures

ℓ-Bounded leakage model

- Secret $X \leftarrow \mathcal{X}$ is sampled.
- Adversary chooses leakage function $f\colon \mathcal{X} \to \{0,1\}^{\ell}$.
- $Z = f(X)$ is leaked to Adversary

Mother of all leakages
(Brian et al. 2021)

Noisy leakage: randomized function $f\colon \mathcal{X} \to \mathcal{Z}$.

- Real world
  - Secret $X \leftarrow \mathcal{X}$ is sampled.
  - $Z = f(X)$ is leaked to Adversary.
- Simulation
  - Secret $X \leftarrow \mathcal{X}$ is sampled.
  - Simulator chooses bounded leakage function $g\colon \mathcal{X} \to \{0,1\}^{\ell}$.
  - $U = g(X)$ is leaked to Simulator
  - Simulator chooses Z.
  - Z is leaked to adversary.

ϵ = simulation error = distinguishing advantage

Limitations of statistical distance and mutual information

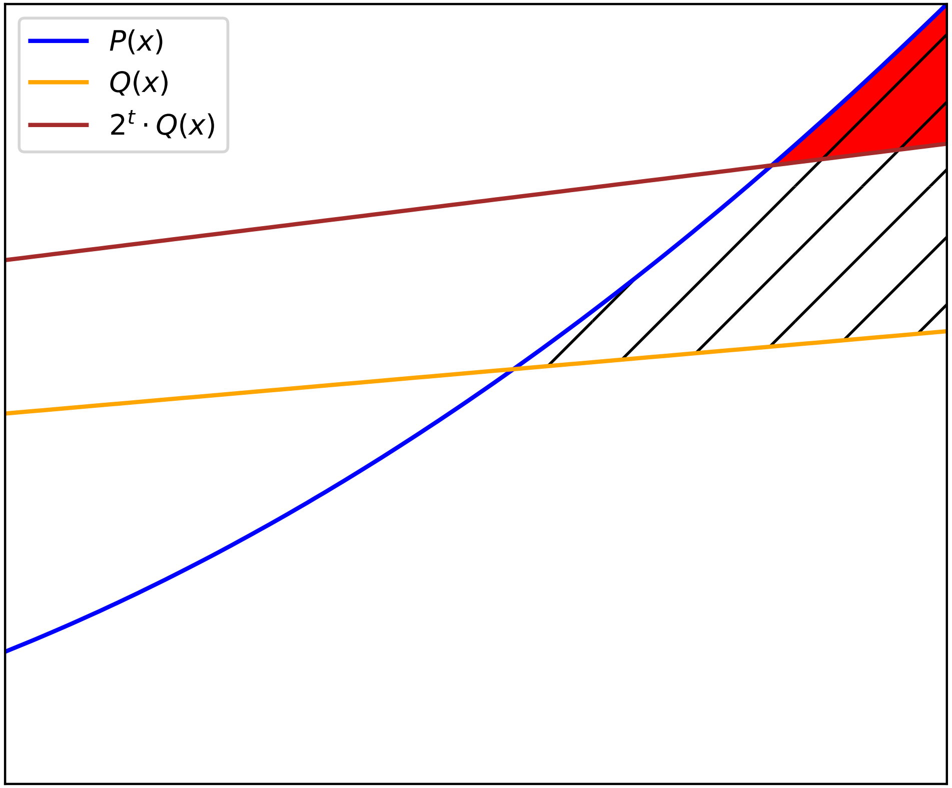
- Some common leakage measures:
  - Statistical distance: $\mathsf{SD}(P_{XZ}, P_X \otimes P_Z)$
  - Mutual information: $I(X;Z)$
- Decrease slowly with noise
- No graceful security degradation
  - Example: leak all of X with probability δ, else leak nothing
  - $\mathsf{SD}(P_{XZ}, P_X \otimes P_Z) \approx \delta$, so simulation from no leakage for $\epsilon \geq \delta$.
  - No security at all with probability δ. Even with $n-1$ bits of bounded leakage we have $\epsilon \geq \delta/2$.

Mother of all leakages
(Brian et al. 2021)

- Dense leakages
  - Simulation from bounded leakage
  - Relations with several other leakage models
- In comparison, we get:
  - Tighter simulator analysis
  - Composition Theorem

Hockey-stick divergence

- $\mathsf{SD}_t(P;Q) = \sup_{\mathcal{S}} \left[P(\mathcal{S}) - 2^t Q(\mathcal{S})\right]$
  $= \sum_x \max\left(0, P(x) - 2^t Q(x)\right)$
- Equivalent to statistical distance when $t = 0$
- Asymmetrical in P vs Q when $t > 0$
- Used in Differential Privacy



(t, δ)-SD-noisy leakage

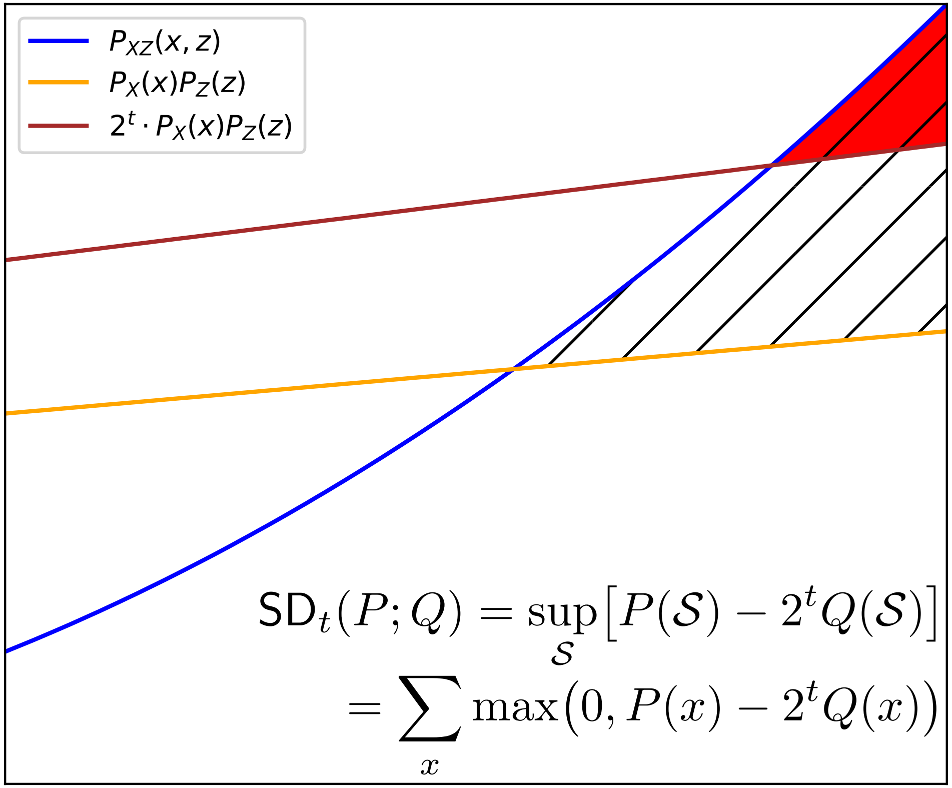
- $Z = f(X)$ has (t, δ)-SD-noisy leakage when

  $$\delta \geq \mathsf{SD}_t(P_{XZ}, P_X \otimes P_Z)$$

- Generalization:
  - (t, δ)-GSD-Noisy leakage:

    $$\delta \geq \mathsf{SD}_t(P_{XZ}, P_X \otimes Q)$$

    for some distribution Q
  - Q "simulates" leakage Z without knowing X



Simulation via bounded leakage

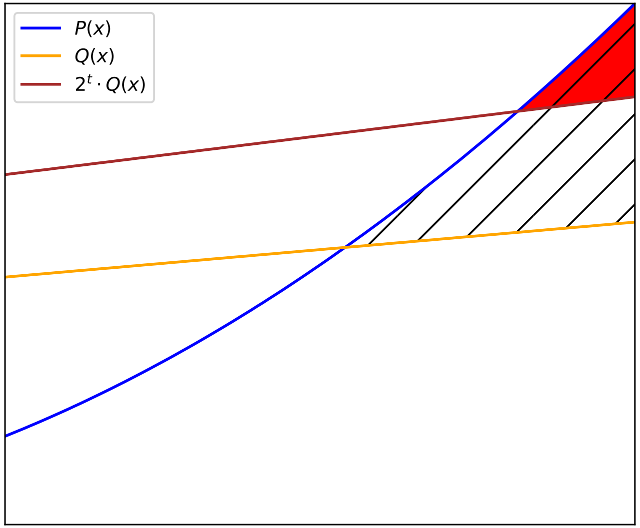
- (t,δ)-GSD-noisy leakage can be simulated from ℓ bits of bounded leakage with simulation error ϵ
  - $\ell = t + \log(\ln(1/\alpha))$
  - $\epsilon = \delta + \alpha$
  - Holds for any $\alpha > 0$

Rejection sampling simulator

- For $i := 0$ to $2^\ell - 1$:
  - Sample $z \leftarrow Q$ (according to random tape R)
  - With probability $\min\left(2^{-t} \cdot \frac{P_{XZ}(x,z)}{P_x(x) \cdot Q(z),1}\right)$:
    - Return i as leakage
  - Return $2^\ell - 1$ as leakage
- Simulator returns z_i, the ith sample of z (according to random tape R)

Rejection sampling simulator

- For $i := 0$ to $2^\ell - 1$:
  - Sample $z \leftarrow Q$ (according to random tape R)
  - With probability $\min\left(2^{-t} \cdot \frac{P_{XZ}(x,z)}{P_x(x) \cdot Q(z)}, 1\right)$:
    - Return i as leakage
  - Return $2^\ell - 1$ as leakage



Simulation error $\delta + \alpha$,
for $\ell = t + \log(\ln(1/\alpha))$

Composition

- Typical leakage occurs multiple times (e.g., once for each round)
- Let Z_1 and Z_2 be conditionally independent $(t_1, \delta_1)/(t_2, \delta_2)$-GSD-noisy leakages from X

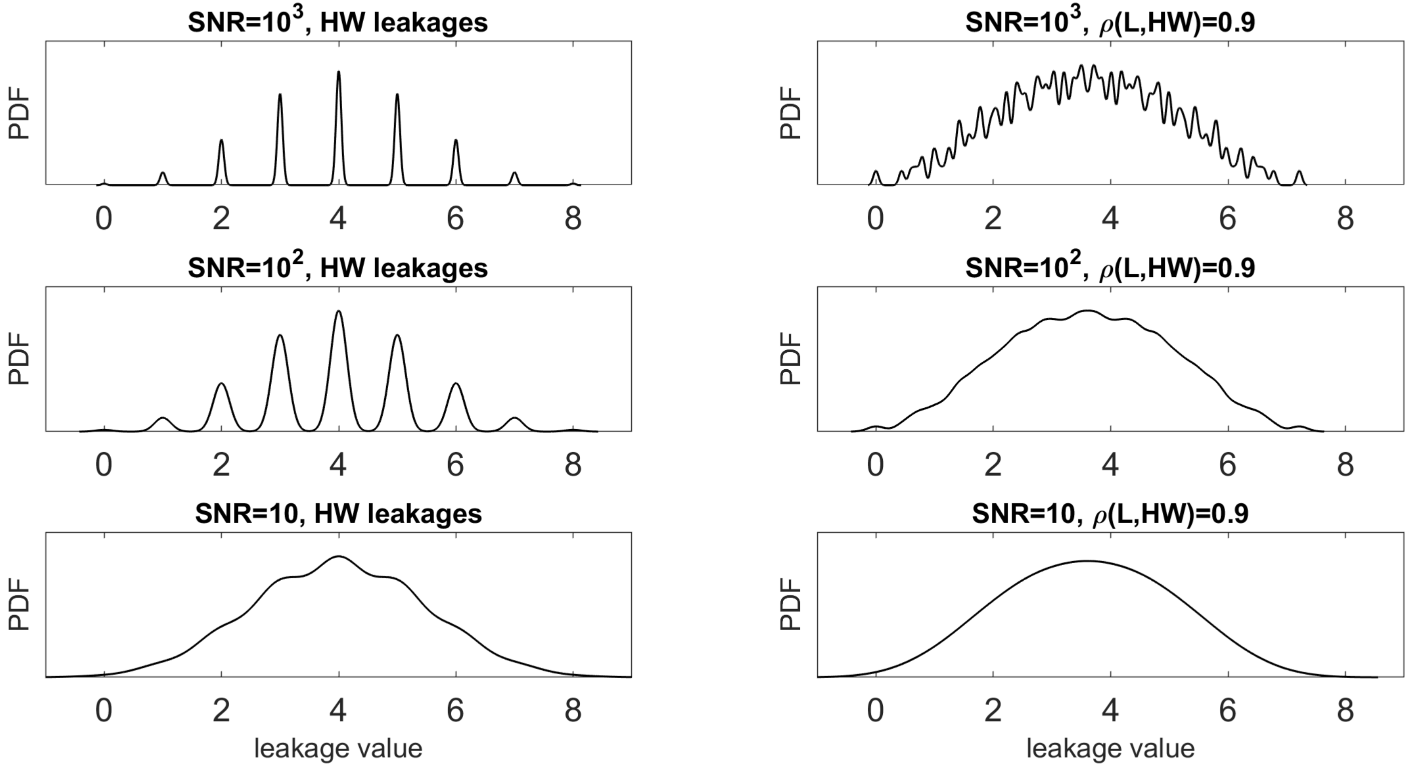
  $\implies (Z_1, Z_2)$ is a $(t_1{+}t_2, \delta_1{+}\delta_2)$-GSD-noisy leakage.
  - Adapted from differential privacy's basic composition theorem (Dwork and Lei 2009)
- Does advanced composition of m leakages work?
  - Yes, but only for small t (e.g. $t < 1/\sqrt{m}$) and a more limited class of leakages.

Parameter computation

- $\mathsf{SD}_t(P;Q) = \sup_{\mathcal{S}} \big[P(\mathcal{S}) - 2^t Q(\mathcal{S})\big]$
- Worst case:
  - $\mathcal{S} = \big\{(x,z) \mid P(x,z) > 2^t Q(x,z)\big\}$
  - Evaluate $P(\mathcal{S}) - 2^t Q(\mathcal{S})$
- For (t,δ)-SD-Noisy Leakage, $\delta = \mathsf{SD}_t(P_{XZ}, P_X \otimes P_Z)$
- For (t,δ)-GSD-Noisy Leakage, $\delta = \mathsf{SD}_t(P_{XZ}, P_X \otimes Q)$
  - Future research: how to choose Q optimally?

Evaluation model

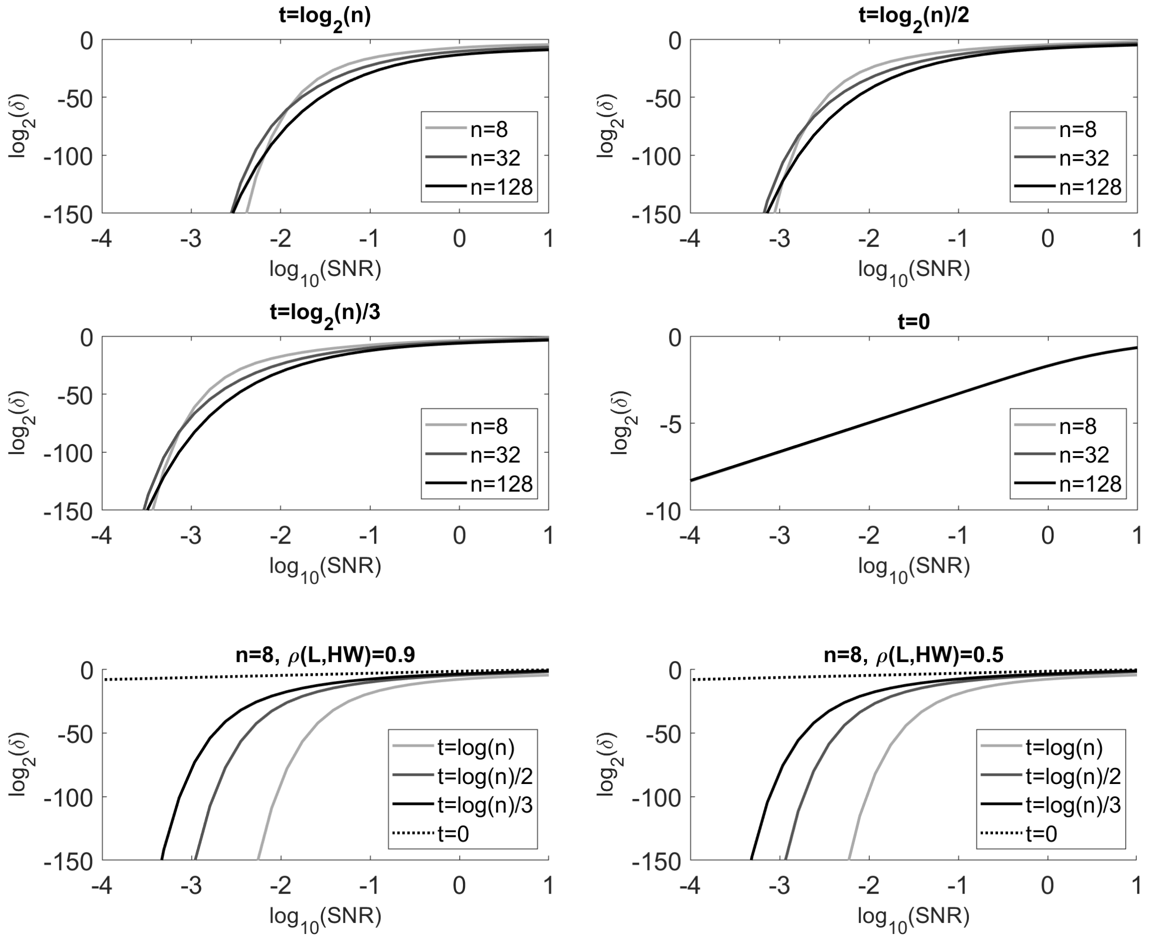
Example leakages:



Gaussian noise + Hamming weight of n-bit secret

Linear function of secret in $\{0,1\}^n$.

Evaluation: SD



Implementation-level countermeasures

Random probing

- Duc et al. 2014
  - p-random probing leakage:
    - Leak $Z = X$ with probability p
    - Else, leak $Z = \perp$
  - Relationship with statistical distance
    - If X is uniform in $\mathcal{X}$ then $p \leq |\mathcal{X}| \cdot \mathsf{SD}_0(P_X \otimes P_Z, P_{XZ})$
    - Note p's dependence on $|\mathcal{X}|$.

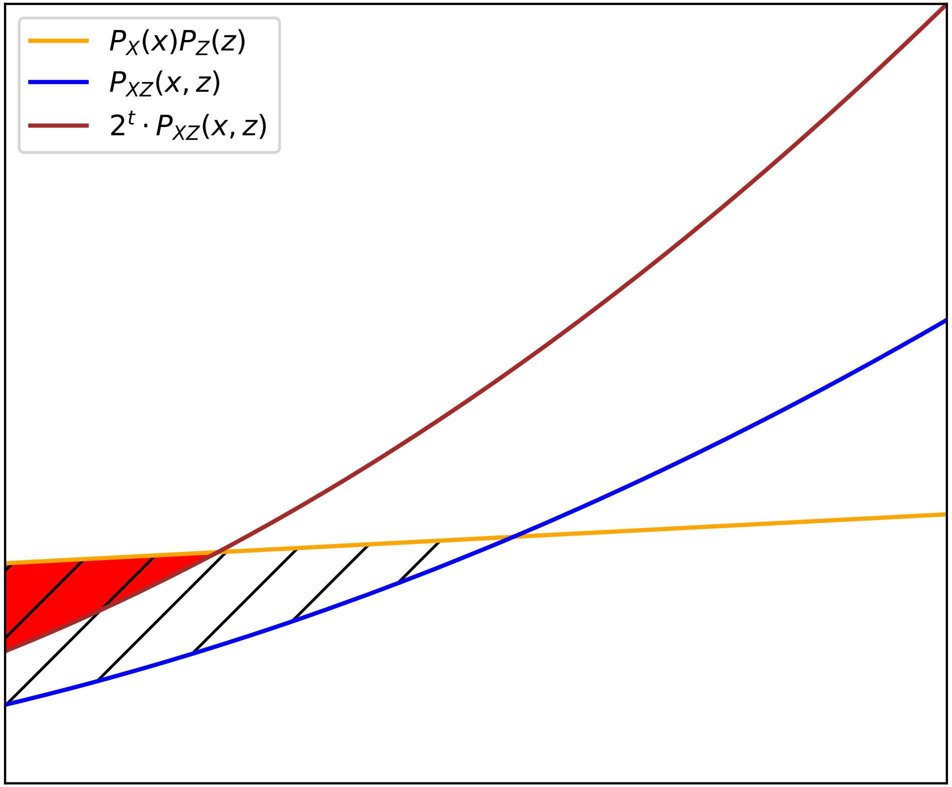
Reverse SD Leakage

- $Z = f(X)$ has (t, δ)-RevSD-noisy leakage when

$$\delta \geq \mathsf{SD}_t(P_X \otimes P_Z, P_{XZ})$$

- Note swap of product and joint distributions

- Has similar generalization to (t, δ)-RevGSD-Noisy leakage



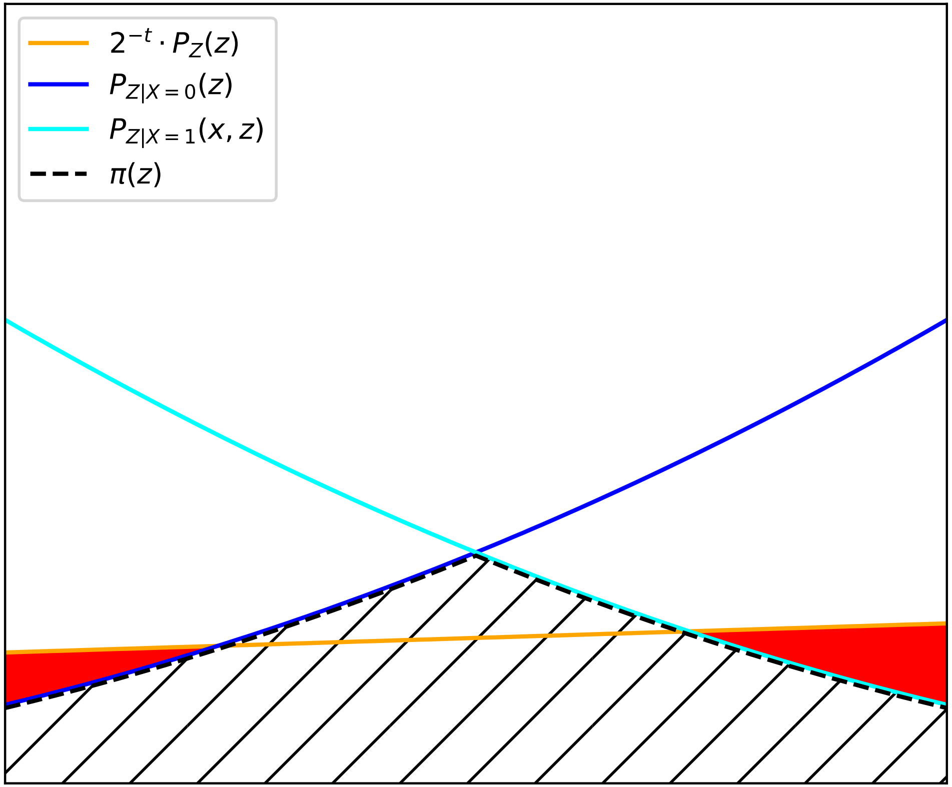
Simulation via Random Probing

- Let X be uniform on $\mathcal{X}$

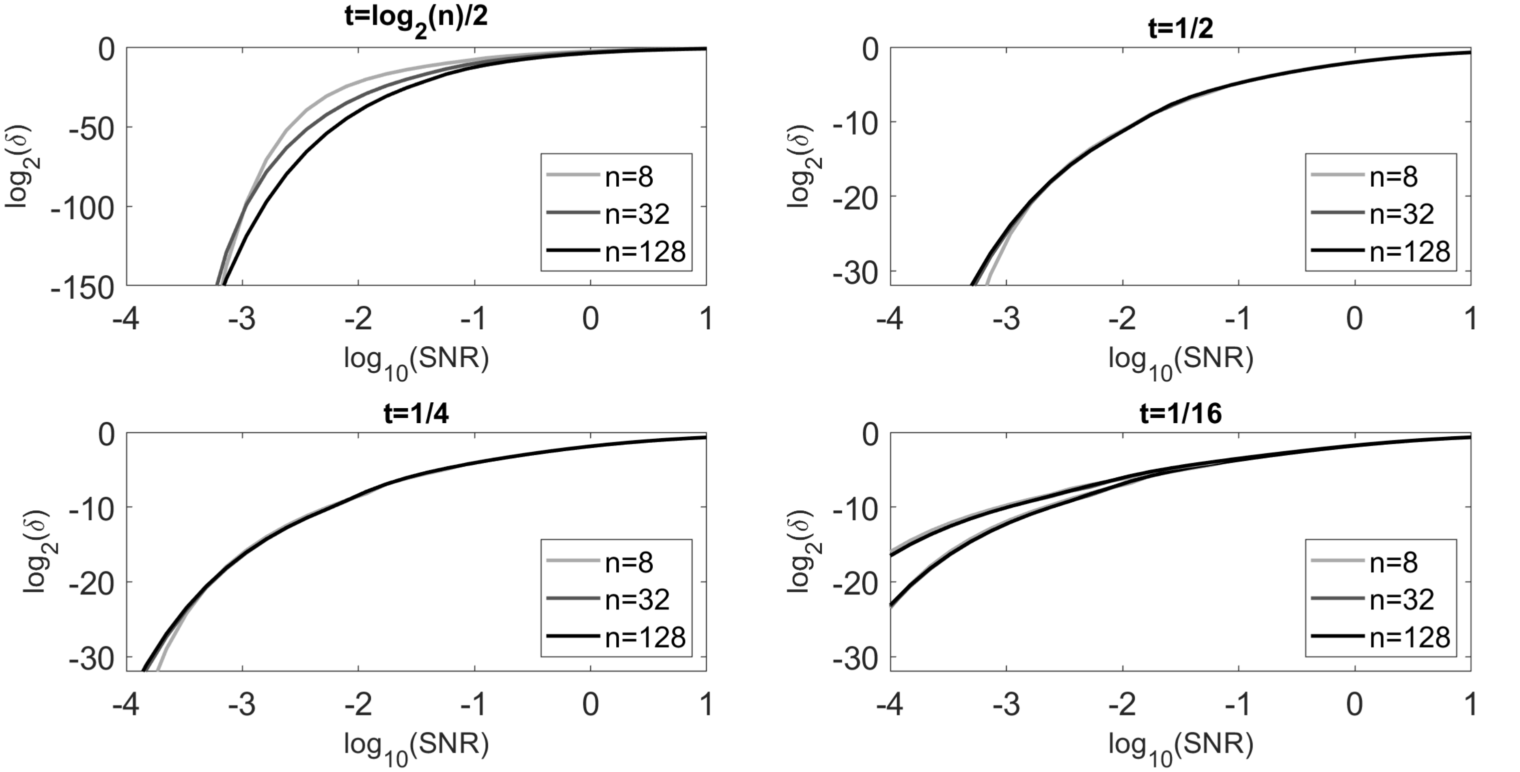
  Let $Z = f(X)$ be a (t,δ)-RevSD-noisy leakage.

$\implies$ Z can be simulated from p-random probing, where

$$p = (1 - 2^{-t}) + 2^{-t}\delta \cdot |\mathcal{X}|$$



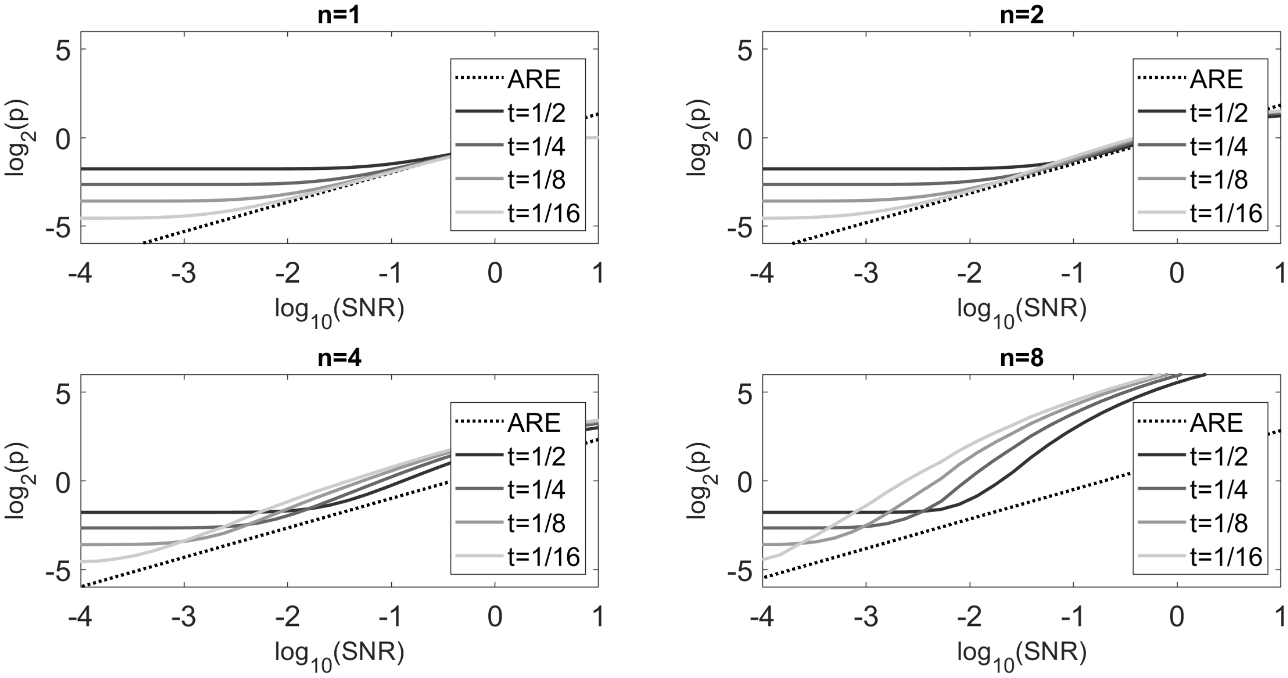
Evaluation: RevSD



The $\delta \cdot |\mathcal{X}|$ term is hidden by rapidly decreasing δ

Evaluation: RevSD

- Comparison with Average Relative Error (ARE) (Prest et al. 2019)



Conclusion

- SD-noisy and RevSD-noisy leakage models
- Reduction to bounded leakage (resp. random probing).
  - This is tight for SD-noisy leakage
  - Provides a bridge between theory and practice
- Composition of SD-noisy leakages
- Evaluation on Hamming weight model
  - Non-trivial concrete bounds