The Mother Of All Leakages: How to Simulate Noisy Leakages via Bounded Leakage (Almost) for Free

Gianluca Brian
Sapienza University of Rome
Italy

Antonio Faonio
EURECOM
France

Maciej Obremski
National University of Singapore
Singapore

João L. Ribeiro
Carnegie Mellon University
USA

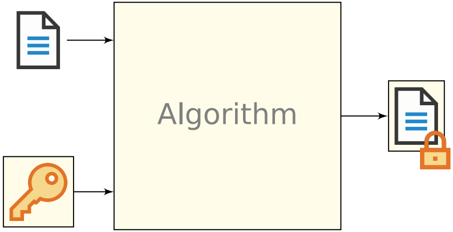
Mark Simkin
Aarhus University
Denmark

Maciej Skórski
University of Luxembourg
Luxembourg

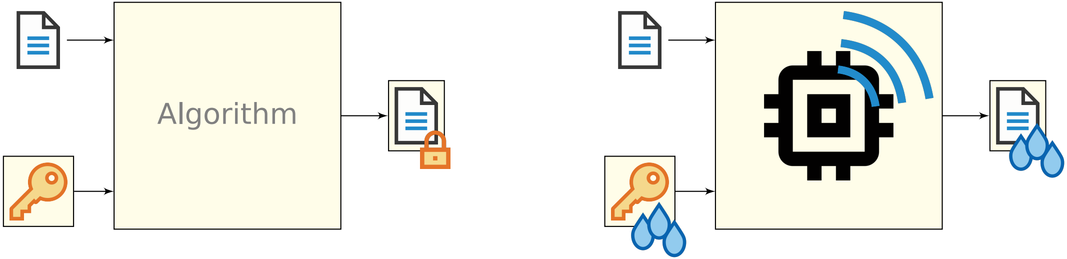
Daniele Venturi
Sapienza University of Rome
Italy

Eurocrypt 2021
Zagreb, Croatia

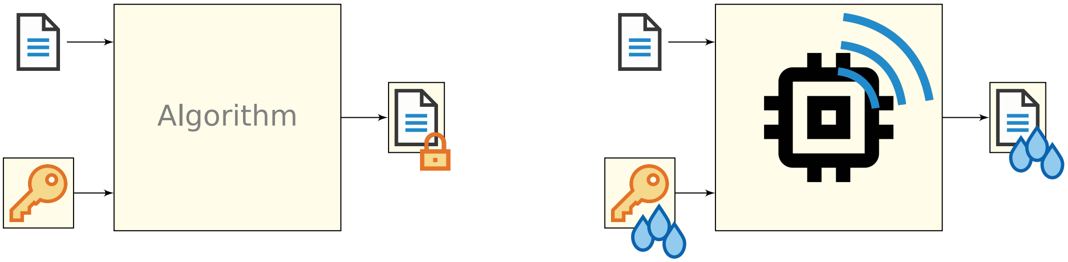
Leakage



Leakage

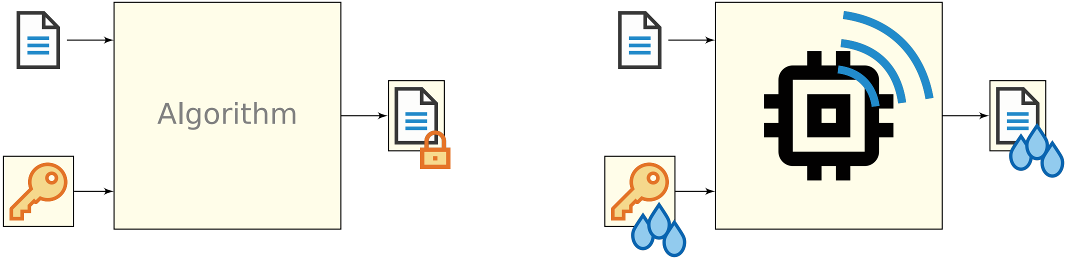


Leakage



Definition

Given a random variable $X \leftarrow \mathcal{X}$, a leakage function is defined as $f : \mathcal{X} \rightarrow \mathcal{Z}$, where $\mathcal{Z} \subseteq \{0,1\}^*$.
The random variable $Z \leftarrow \mathcal{Z}$ such that $Z = f(X)$ is the *leakage* from X.



Definition

Given a random variable $X \leftarrow \mathcal{X}$, a leakage function is defined as $f : \mathcal{X} \rightarrow \mathcal{Z}$, where $\mathcal{Z} \subseteq \{0,1\}^*$.
The random variable $Z \leftarrow \mathcal{Z}$ such that $Z = f(X)$ is the *leakage* from X.

What about $f(x) = x$? Not a valid leakage function!

We need some restrictions on the family $\mathcal{F}$ from which f is chosen...

Leakage models

Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^{\ell}$ for some ℓ.

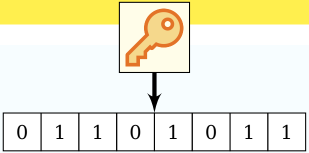
Leakage models

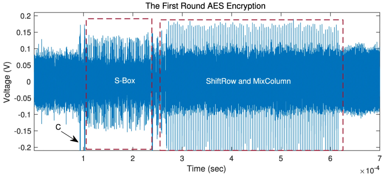
Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^{\ell}$ for some ℓ.

- Simple and versatile.

Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^\ell$ for some ℓ.

- Simple and versatile.
- Not so realistic.



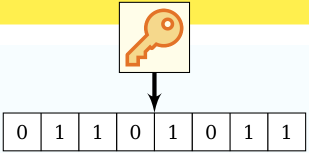


Picture from: *Efficient electro-magnetic analysis of a GPU bitsliced AES implementation [GZC20]*

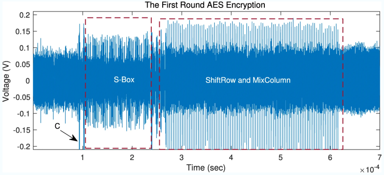
Leakage models

Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^\ell$ for some ℓ.

- Simple and versatile.
- Not so realistic.



Noisy leakage: The output Z of f is large, but contains a small amount of information about X.

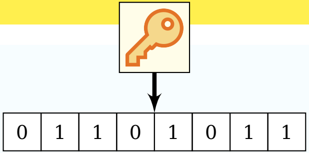


Picture from: *Efficient electro-magnetic analysis of a GPU bitsliced AES implementation [GZC20]*

Leakage models

Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^\ell$ for some ℓ.

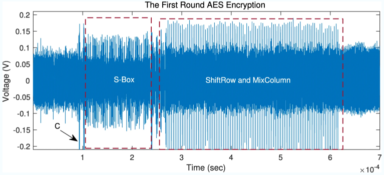
- Simple and versatile.
- Not so realistic.



Noisy leakage: The output Z of f is large, but contains a small amount of information about X.

- **M***in-***E***ntropy-Noisy leakage:* [NS09,NS12]
- **U***niform-Noisy leakage:* [DHLW10]
- **S***tatistical-***D***istance-Noisy leakage:* [DDF14, DDF19]
- **M***utual-***I***nformation-Noisy leakage:* [PGMP19]

And much more...

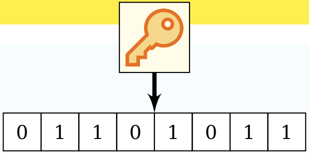


Picture from: *Efficient electro-magnetic analysis of a GPU bitsliced AES implementation [GZC20]*

Leakage models

Bounded leakage: f is such that $\mathcal{Z} \subseteq \{0,1\}^\ell$ for some ℓ.

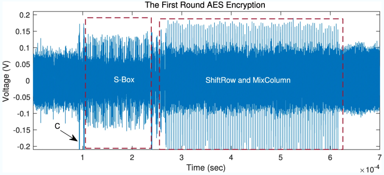
- Simple and versatile.
- Not so realistic.



Noisy leakage: The output Z of f is large, but contains a small amount of information about X.

- **M**_in-_**E**_ntropy-Noisy leakage:_ [NS09,NS12]
- **U**_niform-Noisy leakage:_ [DHLW10]
- **S**_tatistical-_**D**_istance-Noisy leakage:_ [DDF14, DDF19]
- **M**_utual-_**I**_nformation-Noisy leakage:_ [PGMP19]

And much more...

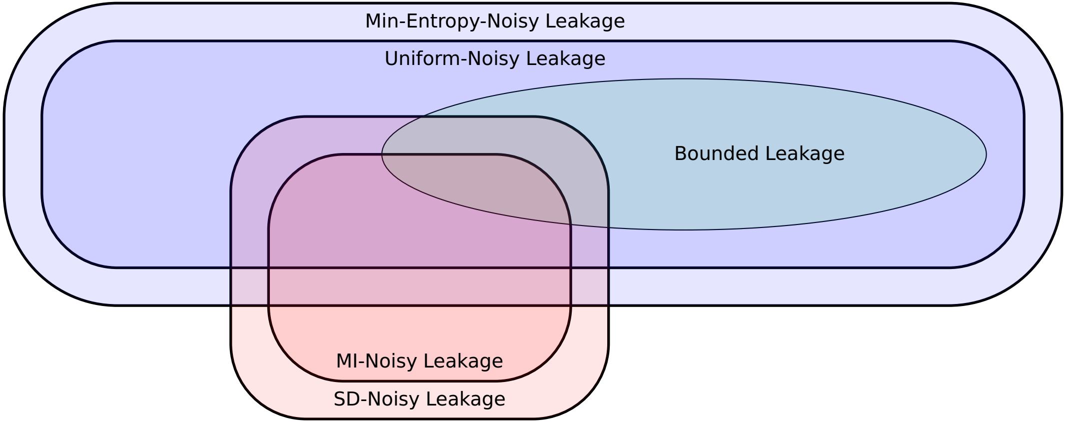


Picture from: *Efficient electro-magnetic analysis of a GPU bitsliced AES implementation [GZC20]*

Separations: we give a full picture of separations between all leakage families.

- *SD-ME Separation:* **SD**-noisy leakage is not contained in **ME**-noisy leakage.
- *SD-MI Separation:* **SD**-noisy leakage and **MI**-noisy leakage are not equivalent.

Relations between leakage models

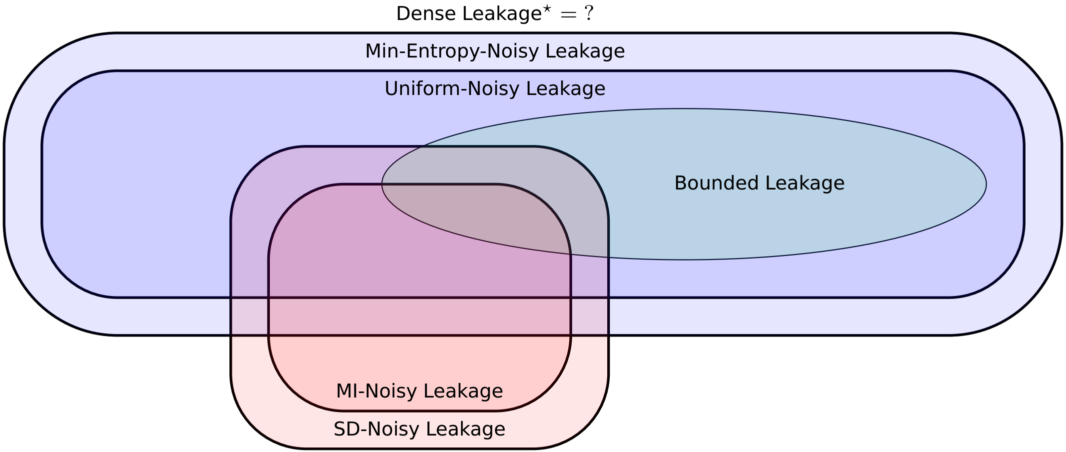


Can we reduce noisy-leakage resilience to bounded-leakage resilience in a general way?

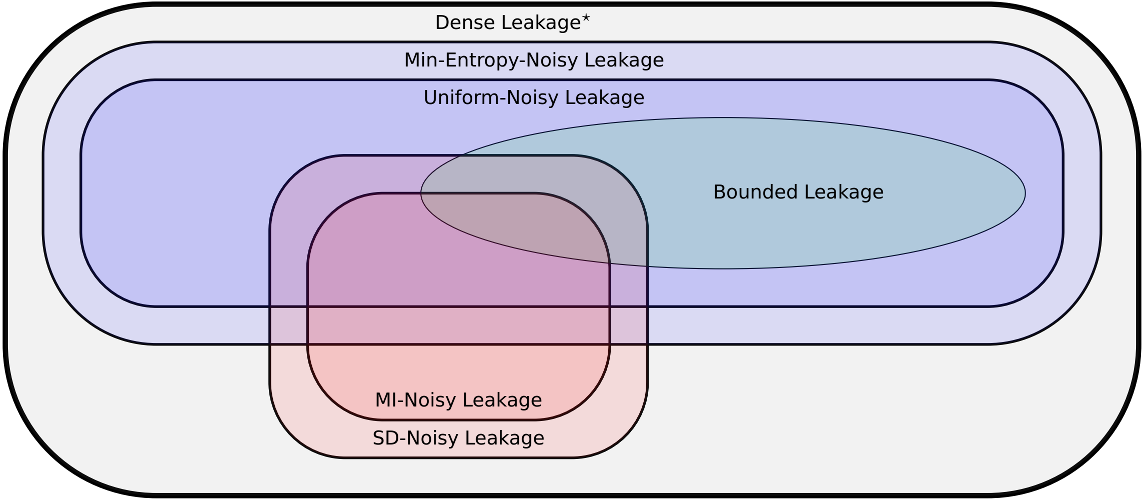
Can we reduce noisy-leakage resilience to bounded-leakage resilience in a general way?

YES!

Relations between leakage models



Relations between leakage models



Simulating dense leakage

Simulation paradigm: we say that $\mathcal{F}(X)$ is ε-simulatable from $\mathcal{G}(X)$ if, for all $f \in \mathcal{F}(X)$, there exists Sim_f such that

$$(X, f(X)) \approx_\varepsilon \left(X, \mathsf{Sim}_f^{\mathsf{Leak}_\mathcal{G}(X,\cdot)}\right).$$

Simulating dense leakage

Simulation paradigm: we say that $\mathcal{F}(X)$ is ε-simulatable from $\mathcal{G}(X)$ if, for all $f \in \mathcal{F}(X)$, there exists Sim_f such that

$$(X, f(X)) \approx_\varepsilon \left(X, \mathsf{Sim}_f^{\mathsf{Leak}_{\mathcal{G}}(X,\cdot)}\right).$$

Theorem: For arbitrary X and for any $\varepsilon \in (0,1]$, the set of dense leakages $\mathsf{Dense}_{p,\gamma,\delta}(X)$ is $(\varepsilon + \varepsilon^{1/4\delta} + \gamma + p)$-simulatable from $\mathsf{Bounded}_\ell(X)$ with

$$\ell = \log(1/\delta) + \log\log(1/\varepsilon) + 2\log\left(\frac{1}{1-\gamma}\right) + 2$$

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.
- We have shown several applications in leakage-resilient cryptography.

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.
- We have shown several applications in leakage-resilient cryptography.

Open problems

- Can we make our simulator efficient for certain families of noisy leakage?

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.
- We have shown several applications in leakage-resilient cryptography.

Open problems

- Can we make our simulator efficient for certain families of noisy leakage?
- Can we extend to multiple queries?

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.
- We have shown several applications in leakage-resilient cryptography.

Open problems

- Can we make our simulator efficient for certain families of noisy leakage?
- Can we extend to multiple queries?

ePrint: 2020/1246

Conclusions

- We introduced the notion of *dense* leakage, which captures many noisy-leakage models.
- We have shown that a single query of *dense* (therefore, *noisy*) leakage can be simulated in the information-theoretic setting using a single query of *bounded* leakage.
- We have shown several applications in leakage-resilient cryptography.

Open problems

- Can we make our simulator efficient for certain families of noisy leakage?
- Can we extend to multiple queries?

ePrint: 2020/1246

Thank You!