Introduction to Side Channel Attacks

Ileana Buhan, March 2024
@ileanabuhan

Radboud University

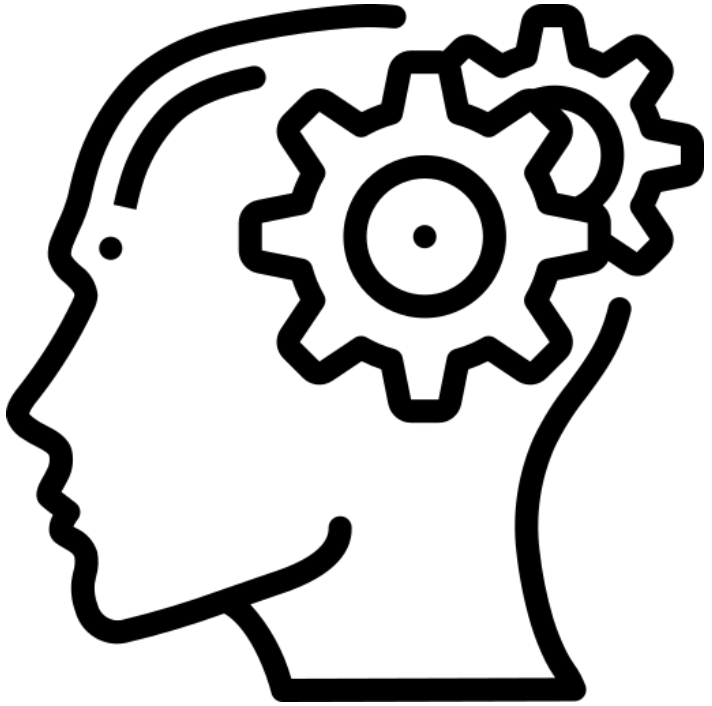
This lecture

1. What is leakage?
2. Simple Power Analysis
3. Differential Power Analysis
4. Countermeasures

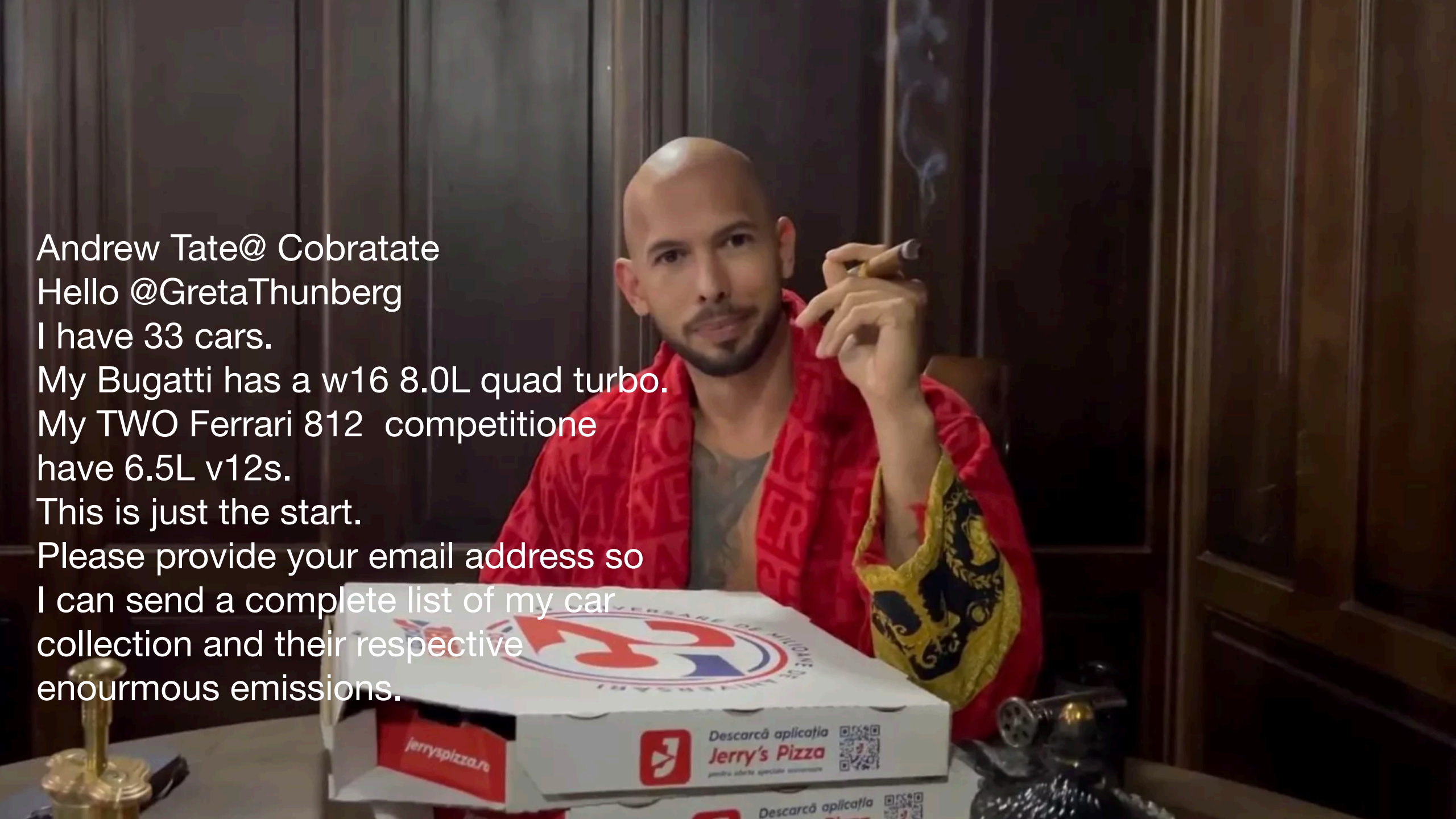
What is leakage?

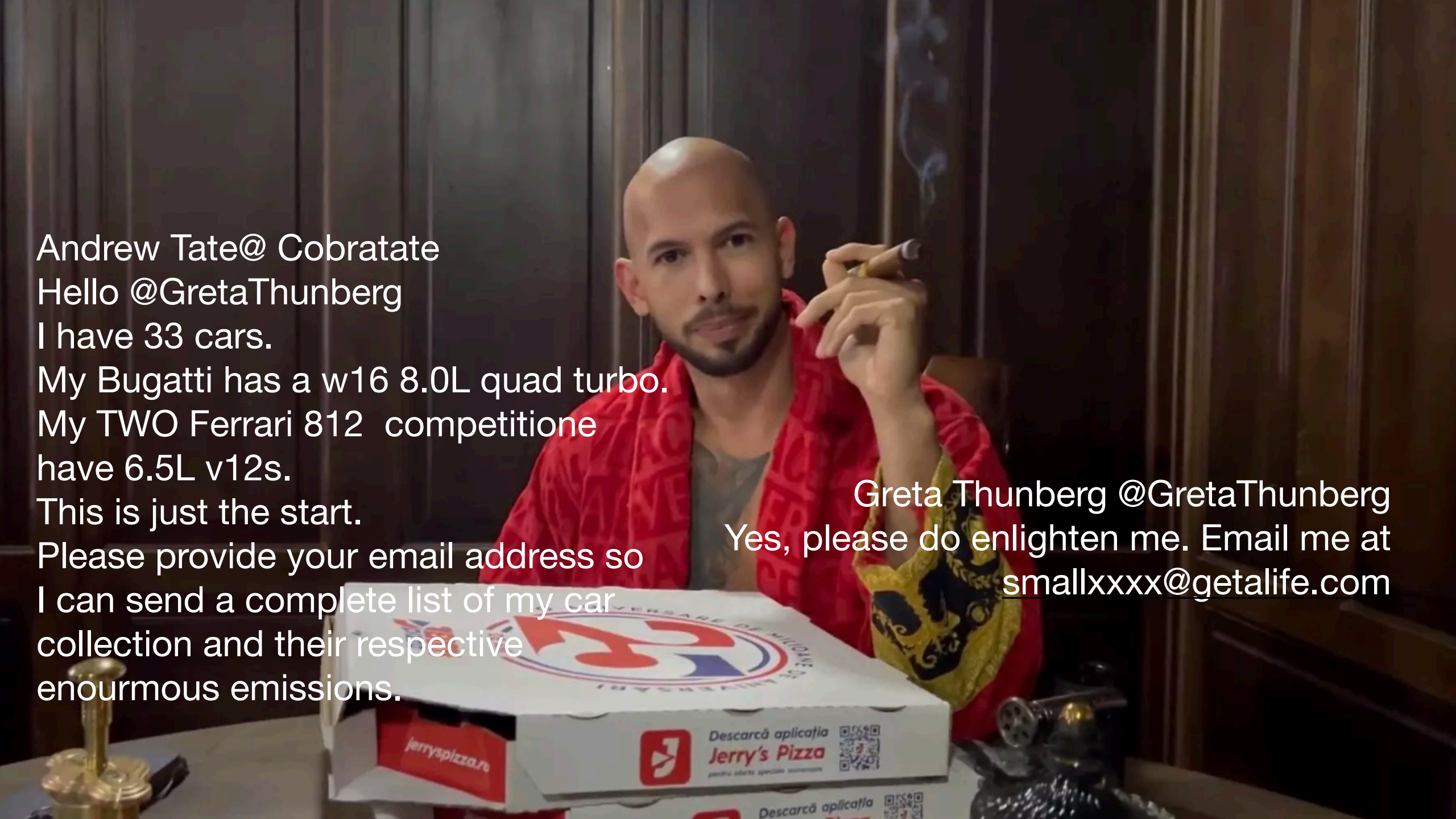
Take a few minutes

What is leakage?




jerryspizza.ro
Descarcă aplicația
Jerry's Pizza


Andrew Tate@ Cobratate
Hello @GretaThunberg
I have 33 cars.
My Bugatti has a w16 8.0L quad turbo.
My TWO Ferrari 812 competitione
have 6.5L v12s.
This is just the start.
Please provide your email address so
I can send a complete list of my car
collection and their respective
enourmous emissions.
jerryspizza.ro
Descarcă aplicația
Jerry's Pizza

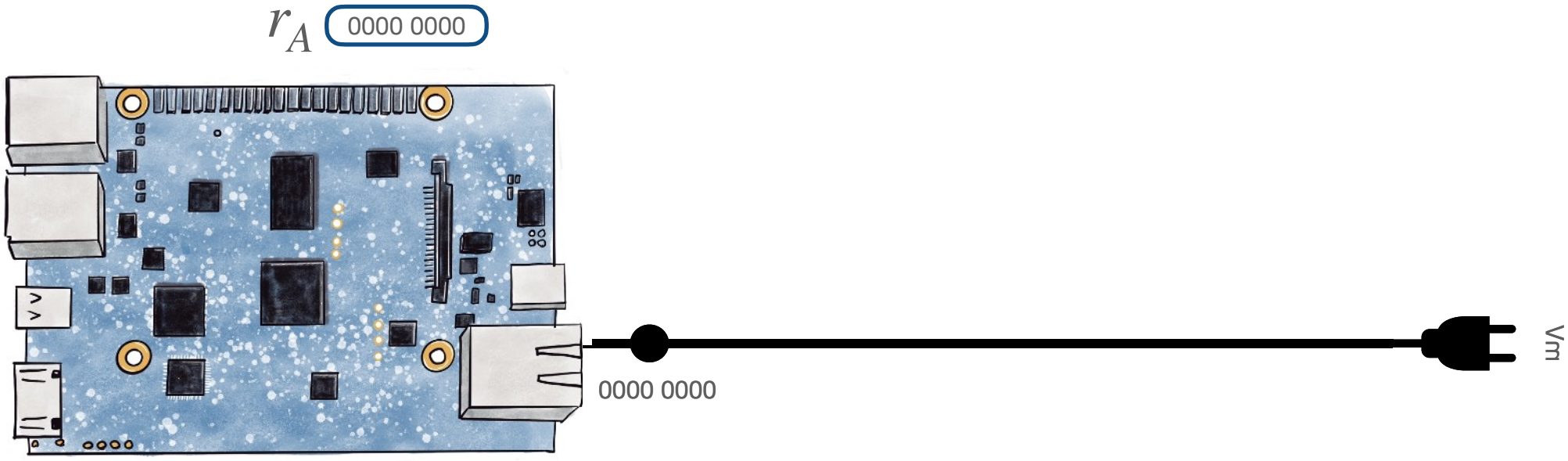


Andrew Tate@ Cobratate
Hello @GretaThunberg
I have 33 cars.
My Bugatti has a w16 8.0L quad turbo.
My TWO Ferrari 812 competitione
have 6.5L v12s.
This is just the start.
Please provide your email address so
I can send a complete list of my car
collection and their respective
enourmous emissions.

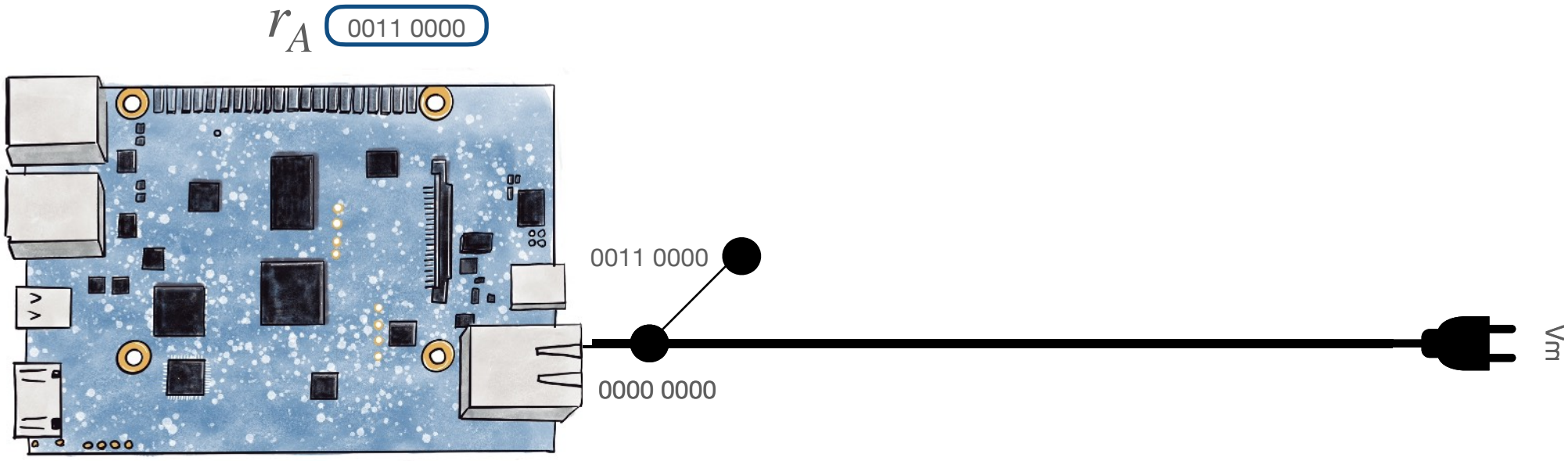
Greta Thunberg @GretaThunberg
Yes, please do enlighten me. Email me at
smallxxxx@getalife.com

Greta Thunberg @GretaThunberg
This is what happens when you dont recycle your pizza boxes

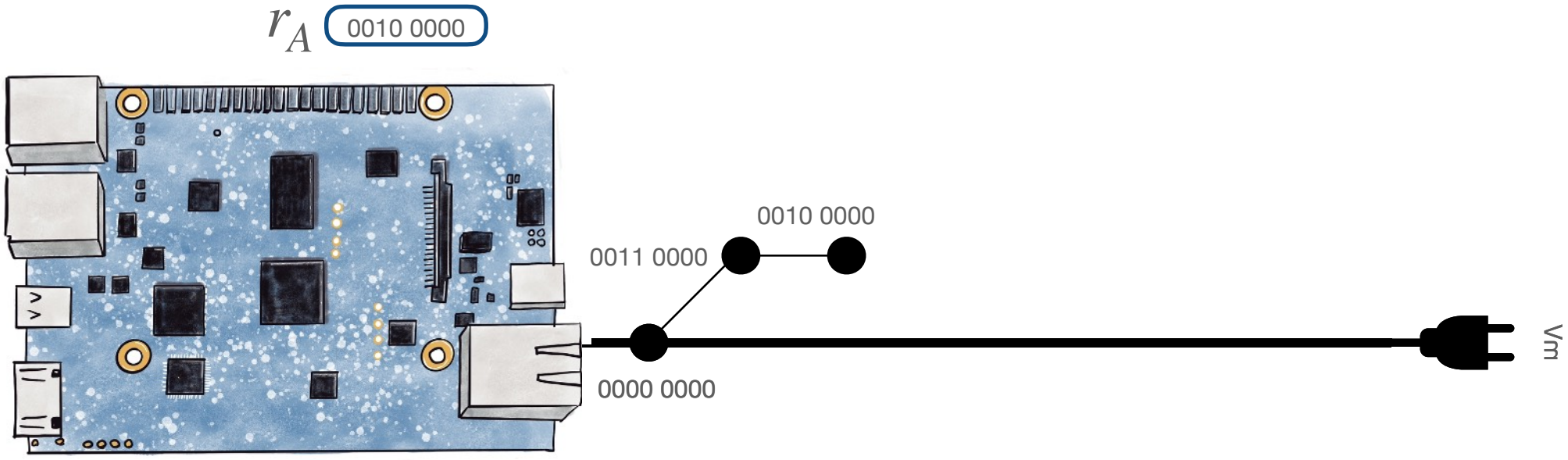
What is leakage for electronic devices?



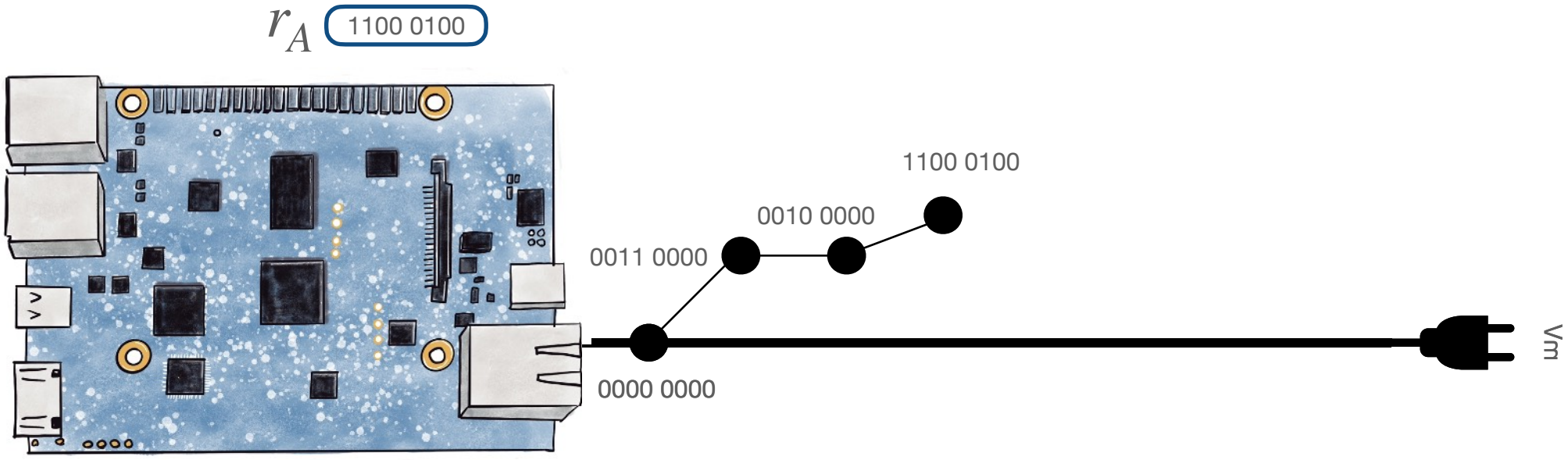
What is leakage for electronic devices?



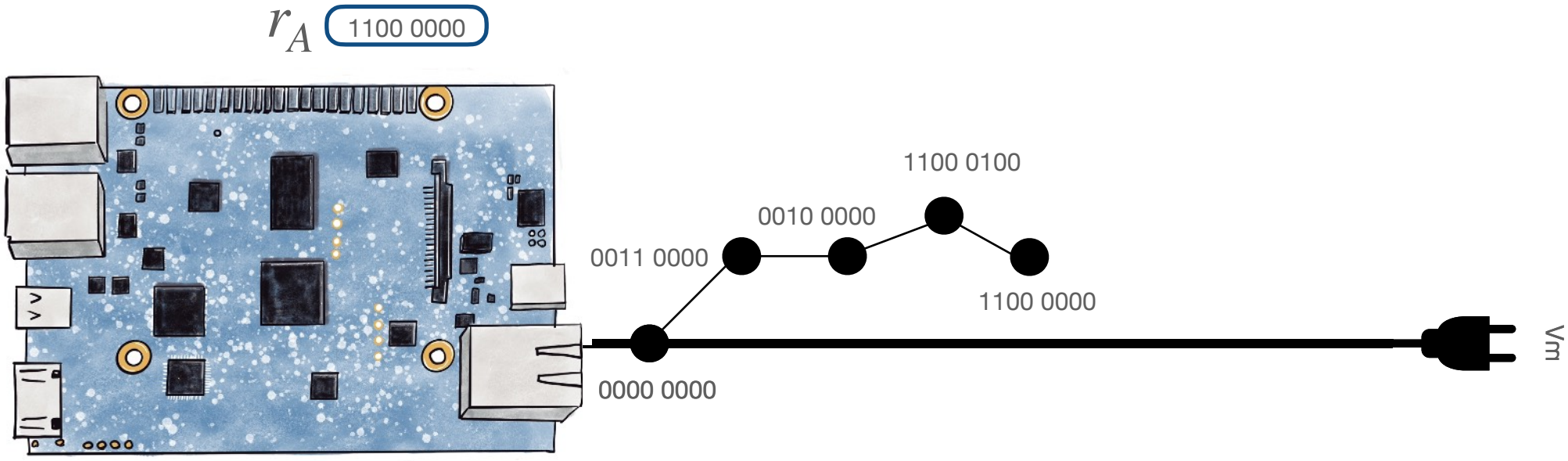
What is leakage for electronic devices?



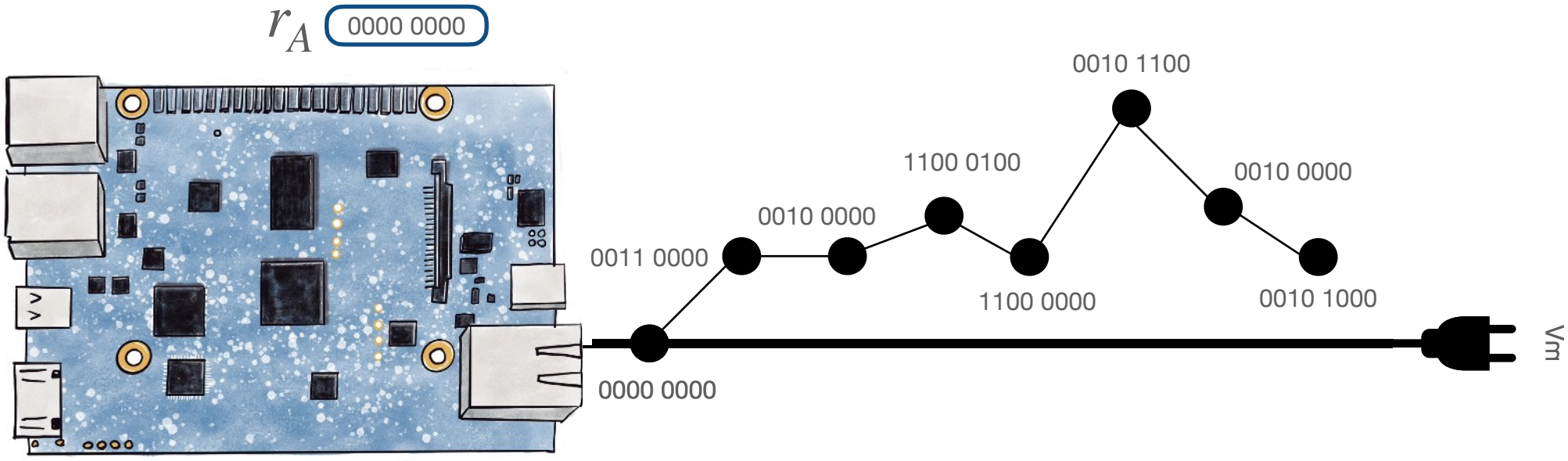
What is leakage for electronic devices?



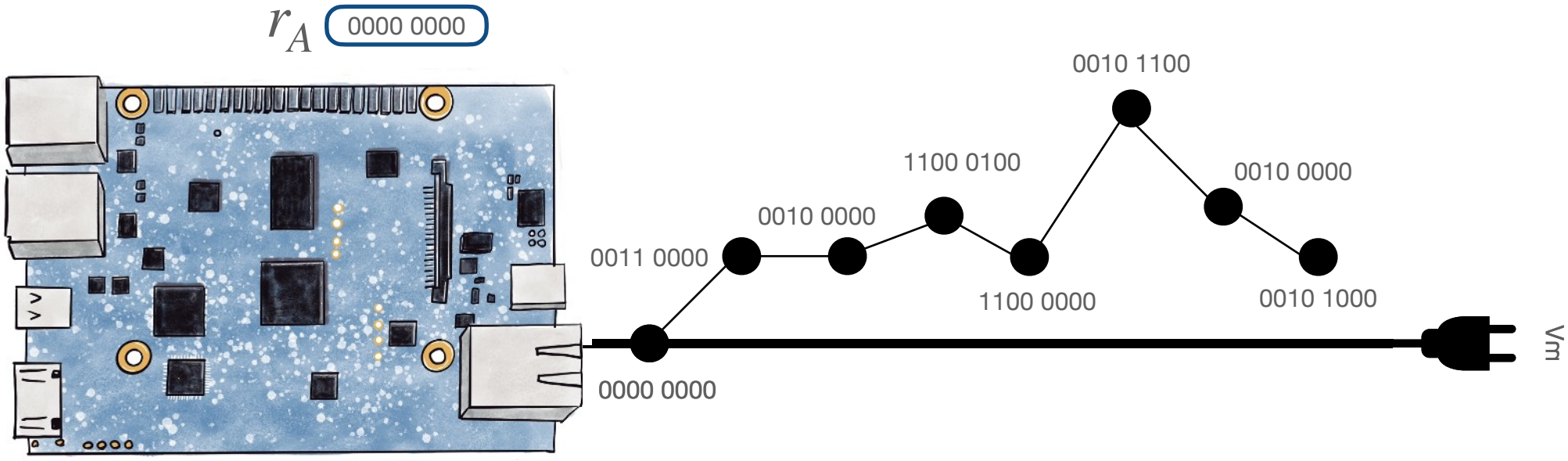
What is leakage for electronic devices?



What is leakage for electronic devices?



What is leakage for electronic devices?



Any observable relation between the value manipulated by the device and a side channel controled by an adversary

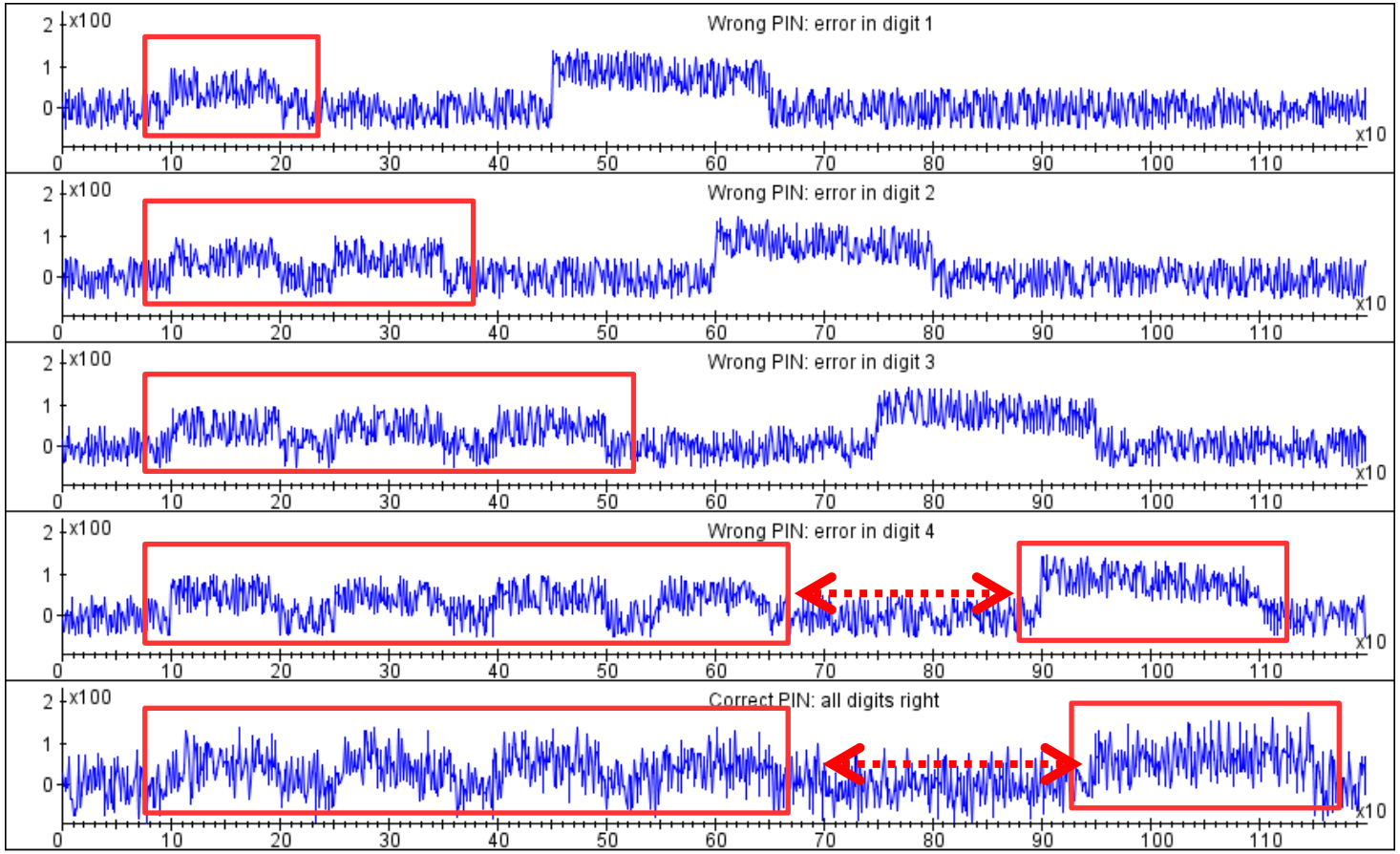
Simple Power Attacks (SPA)

SPA attacks

- Based on one or few measurements

- Used for discovery of data or instruction dependent operations:
  - Symmetric:
    - Number of rounds -> which gives us the key length
    - Memory accesses
  - Asymmetric :
    - The key (ECC/RSA)
    - Implementation details (vannila RSA/RSA-CRT)
    - Key length

PIN verification attempt



????

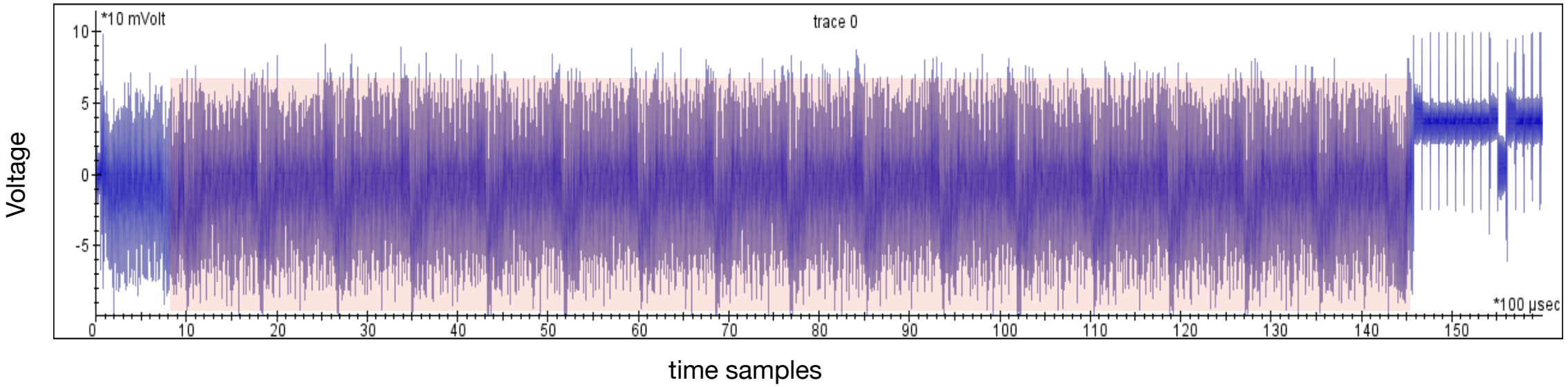
4???

47??

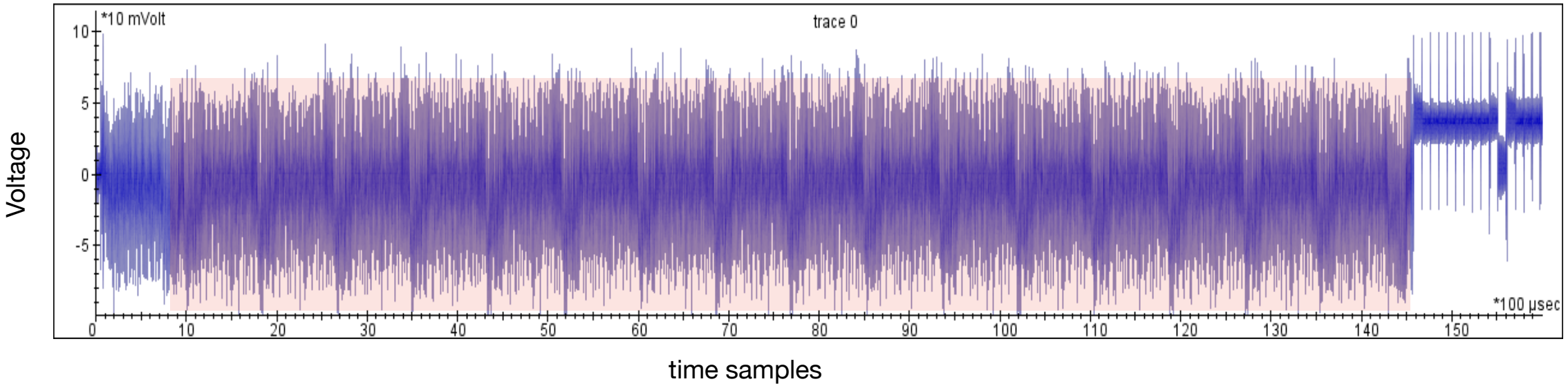
471?

4710

Which algorithm is this?

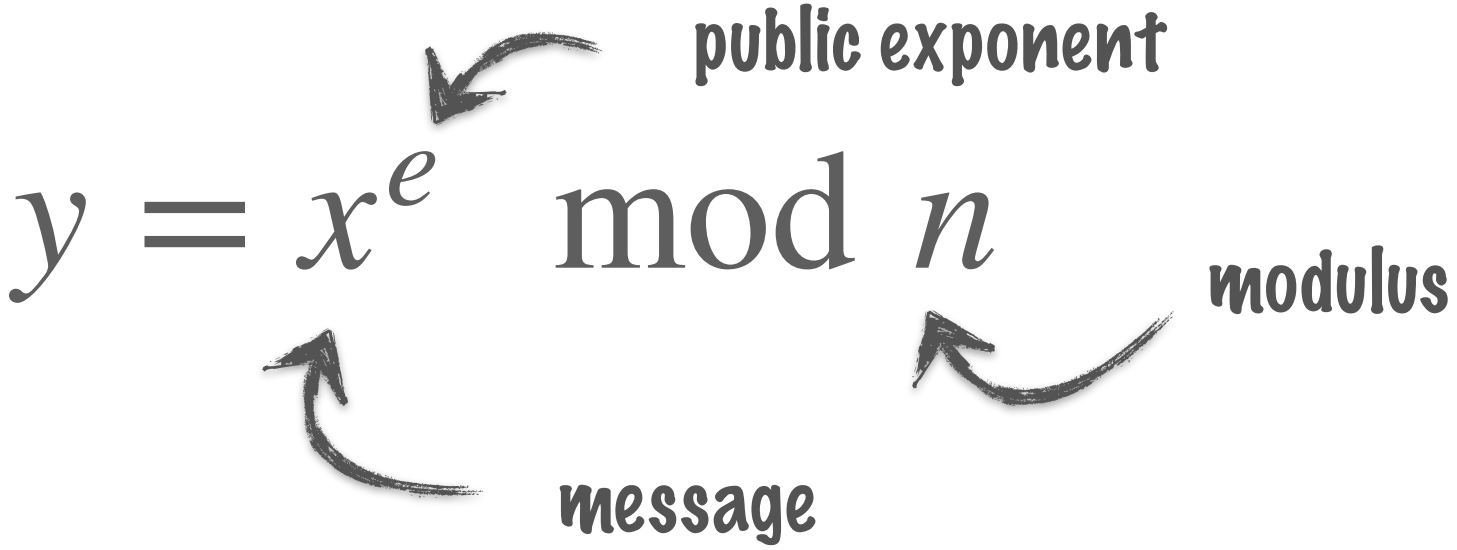


Which algorithm is this?



Answer: DES

RSA exponentiation operation



Implementation of exponentiation operation

Compute $y = x^e \mod n$

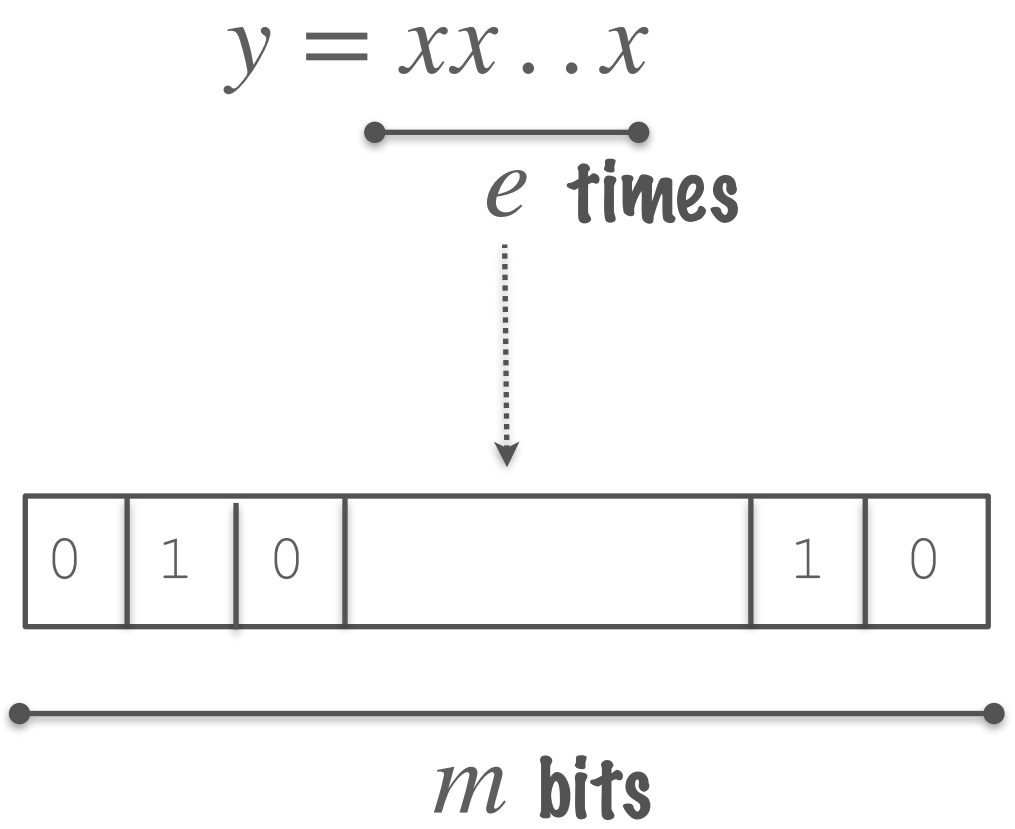
$$y = \underbrace{xx\ldots x}_{e \text{ times}}$$

```
expNaive (x, e, n):
   y=x
   for i=1 to e-1:
      y=yx mod n
return y
```

Implementation of exponentiation operation

Compute $y = x^e \mod n$

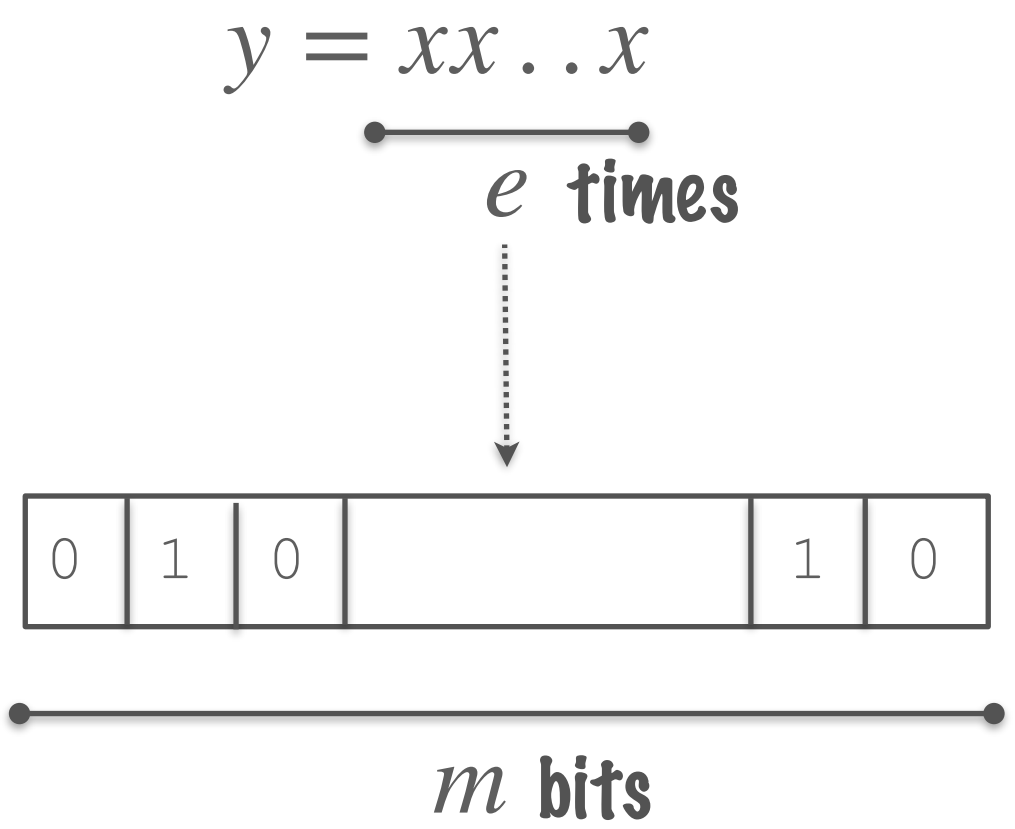
```
expFast (x, e, n):
   y=x
   for i=m-1 to 0:
      y=y*y mod n
      if e_i==1:
         y=y*x mod n
return y
```



Implementation of exponentiation operation

Compute $y = x^e \mod n$

```
expFast (x, e, n):
   y=x
   for i=m-1 to 0:
      y=y*y mod n
      if e_i==1:
         y=y*x mod n
return y
```

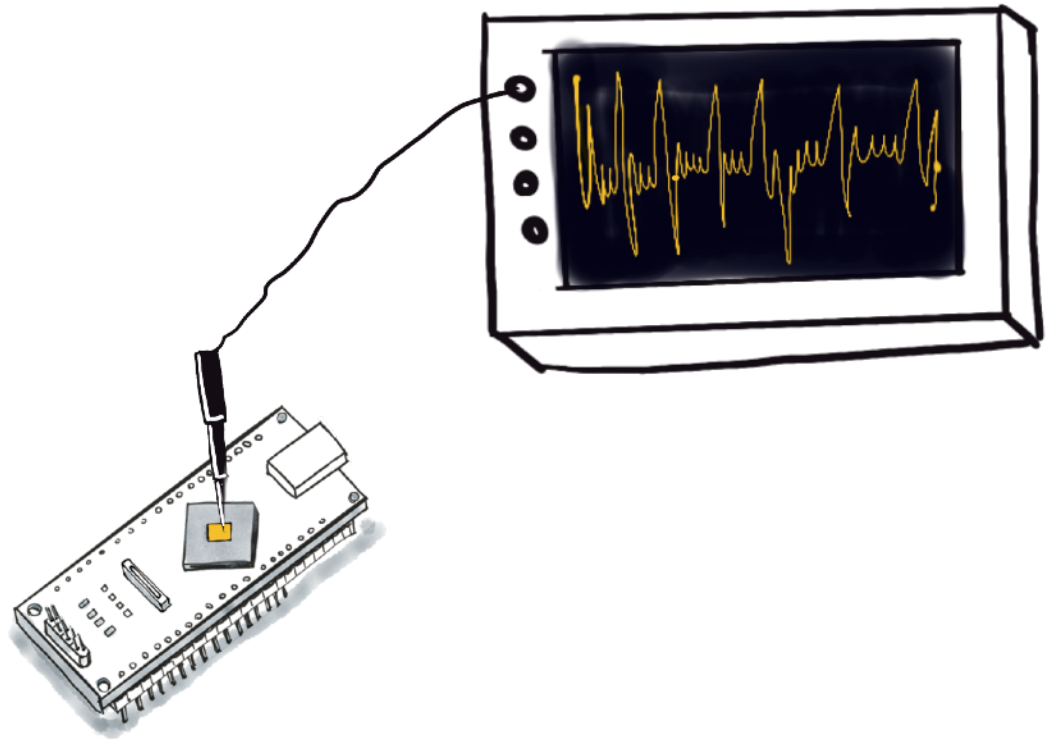


Can you see a potential side-channel?

Implementation of exponentiation operation

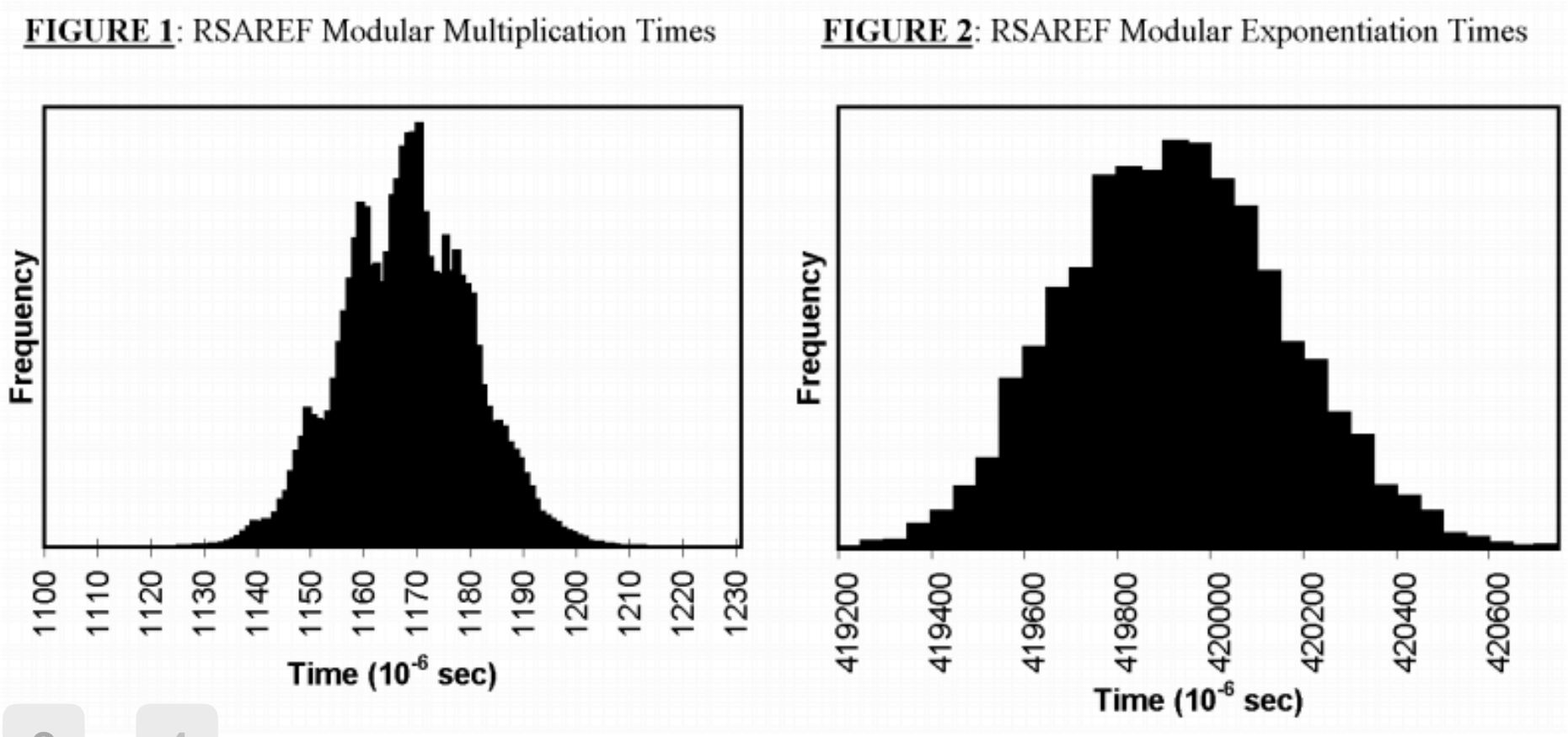
Compute $y = x^d \mod n$

```
expFast (x, d, n):
   y=x
   for i=m-1 to 0:
      y=y*y mod n
      if d_i==1:
         y=y*x mod n
return y
```



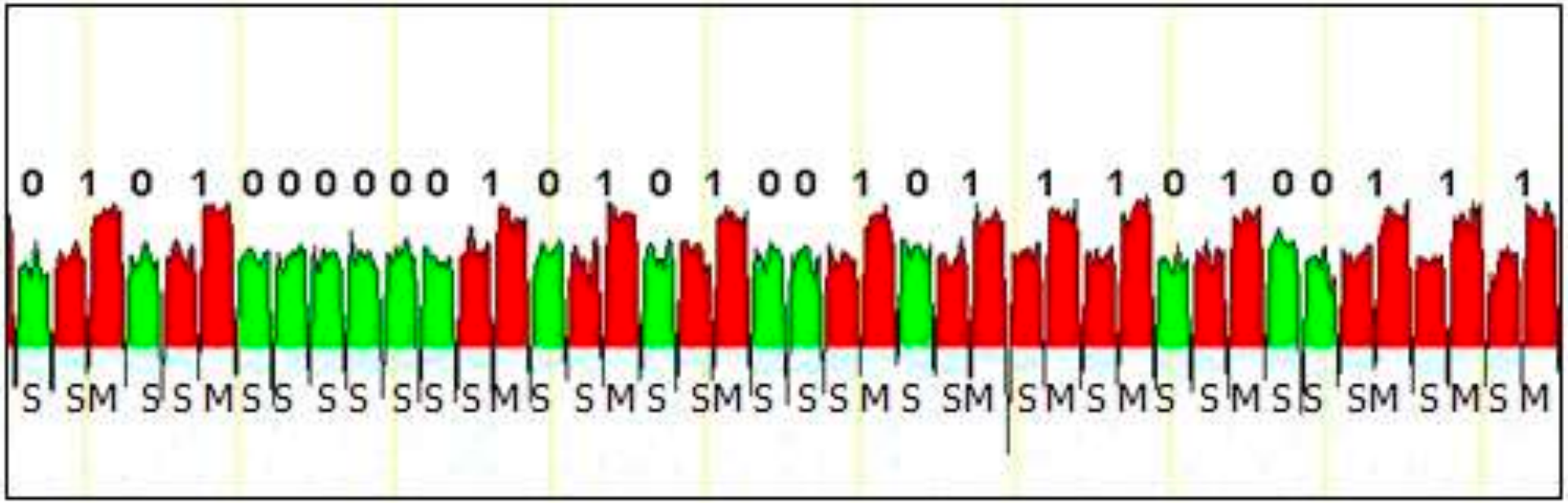
Can you see a potential side-channel?

Is there anything wrong in this picture?



Timing Attacks on Implementations of Die-Hellman, RSA, DSS, and Other Systems, Paul Kocher,1996

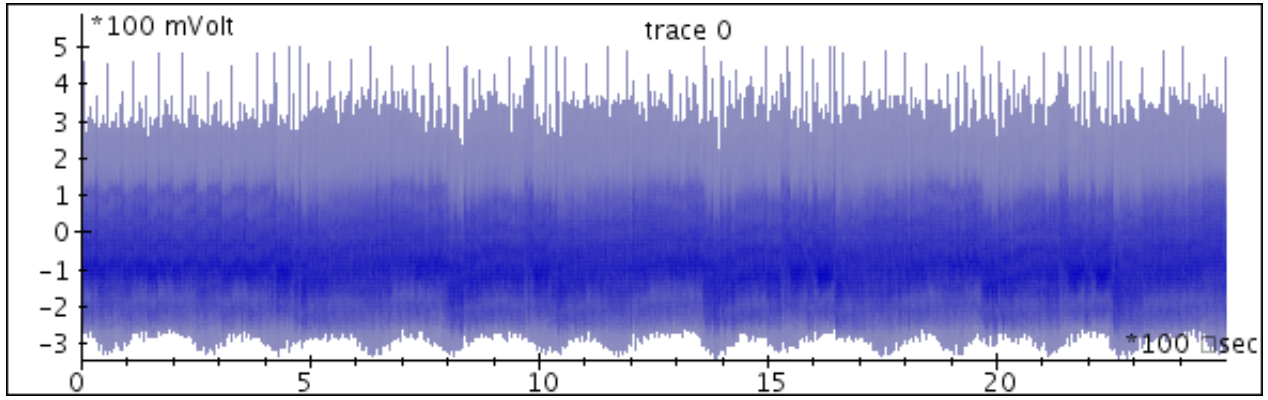
SPA attack of RSA



Source: https://www.eetimes.com/protecting-fpgas-from-power-analysis/#

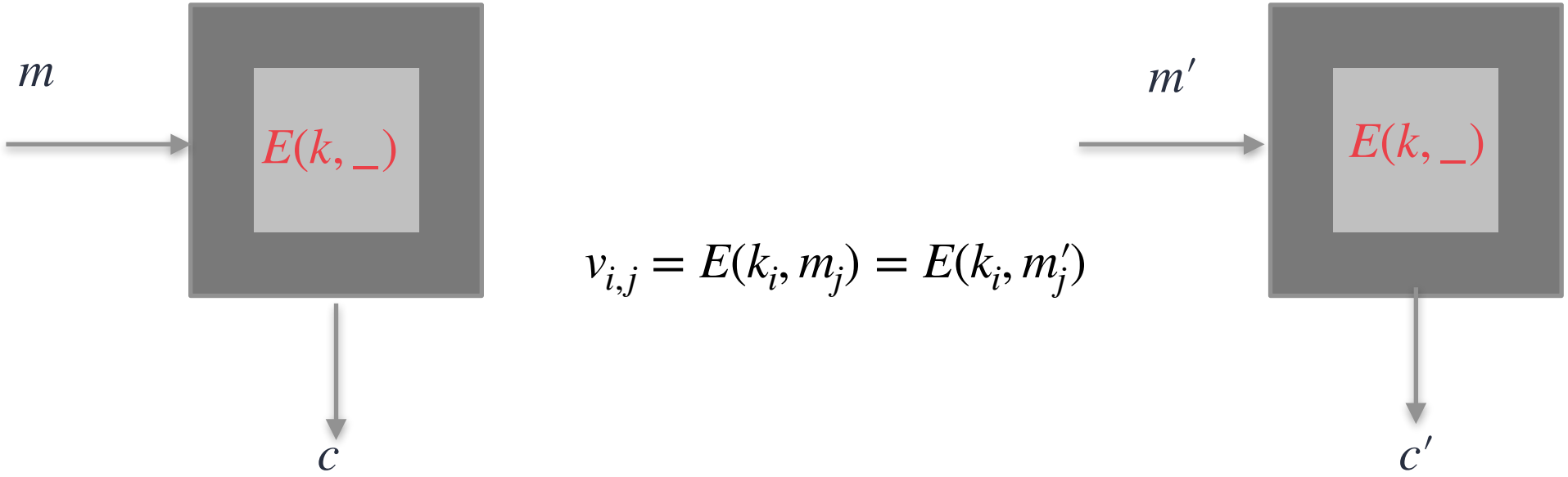
SPA attacks summary

- SPA attacks are not so simple, require detailed knowledge about the implementation



- An advanced option is called collision attacks
- Protecting against RSA means sticking to regularity in computation
- The advanced form of SPA attacks today is called horizontal attacks
- SPA attacks are used to enable more comples physical attacks

Collision attacks



$$v_{i,j} = E(k_i, m_j) = E(k_i, m'_j)$$

Colliding values, reduce the values for the possible keys

DPA attacks

Differential Power/Electromagnetic Analysis

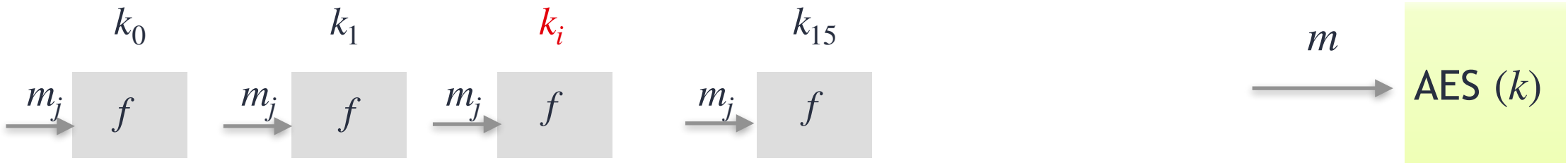
DPA attacks exploit the data dependecy of the power consumption of cryptographic devices. They use a large number of traces to analyze the power consumption at a fixed moment in time as a function of the processed data.

Main steps:

1. Choose the target intermediate value
2. Measure traces, known plaintext/ciphertext
3. Calculate (hypothetical) intermediate values
4. Choose leakage model
5. Recover key using a side channel distinguisher

Power Analysis Attacks, Revealing the Secrets of Smart Cards, Stefan Mangard, Elisabeth Oswald, Thomas Popp, 2007

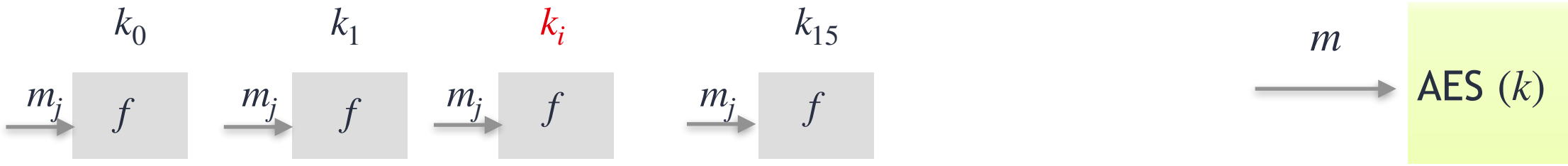
1. Choose the target intermediate value



Intermediate value

$$v_{i,j} = f(k_i, m_j)$$

1. Choose the target intermediate value

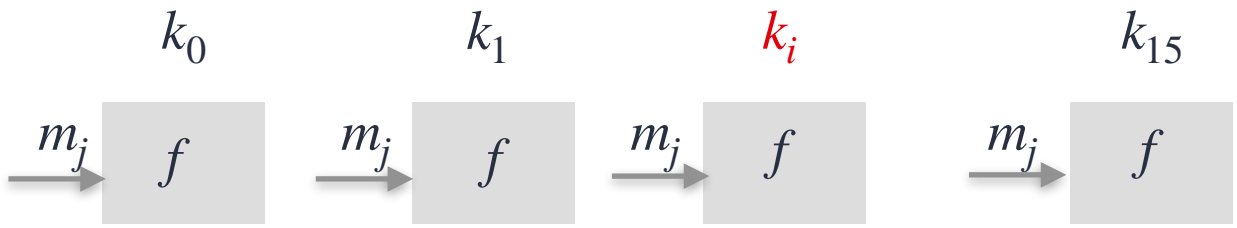


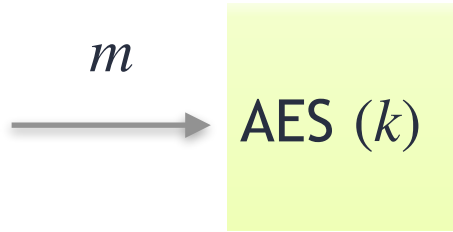
Intermediate value

$$v_{i,j} = f(k_i, m_j)$$

How to choose the target intermediate value?

1. Choose the target intermediate value





Intermediate value

$$v_{i,j} = f(k_i, m_j)$$

How to choose the target intermediate value?

Function of the secret

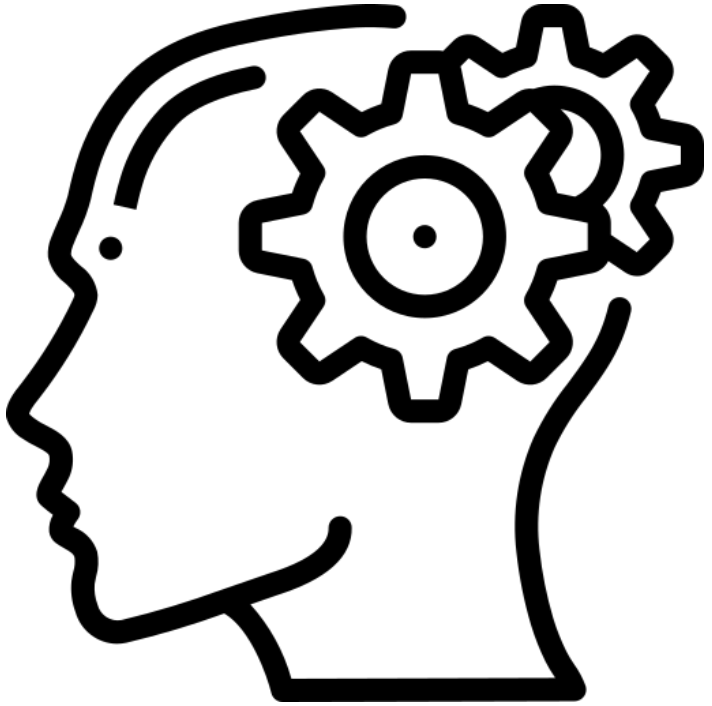
Function of controllable inputs

Function with confusion property

Function with divide and conquer property

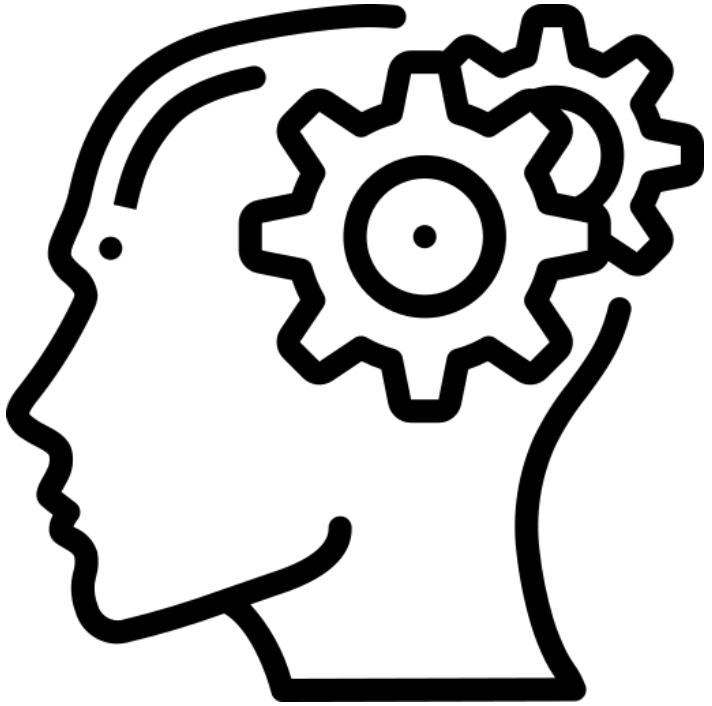
Take a few minutes

What would make a good intermediate value for block ciphers? e.g. AES, DES



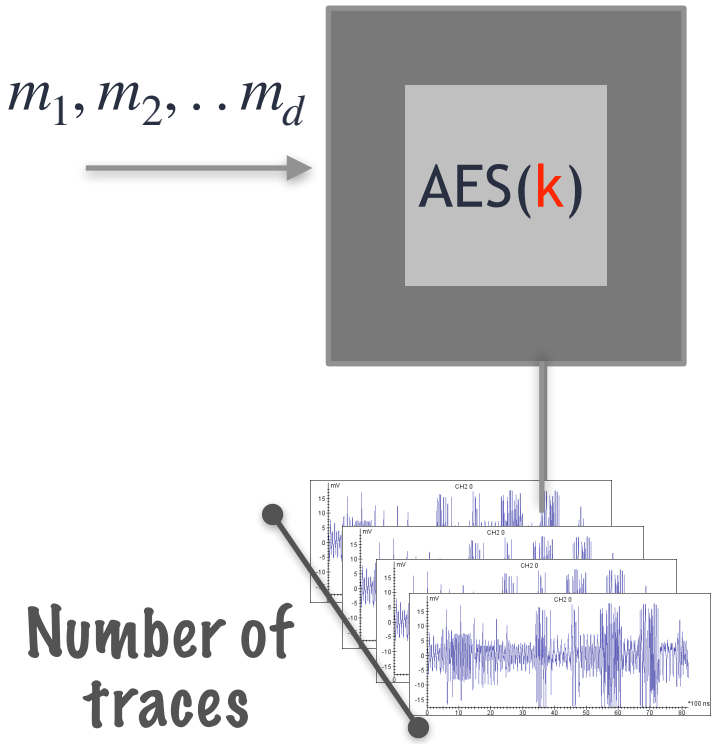
Take a few minutes

What would make a good intermediate value for block ciphers? e.g. AES, DES

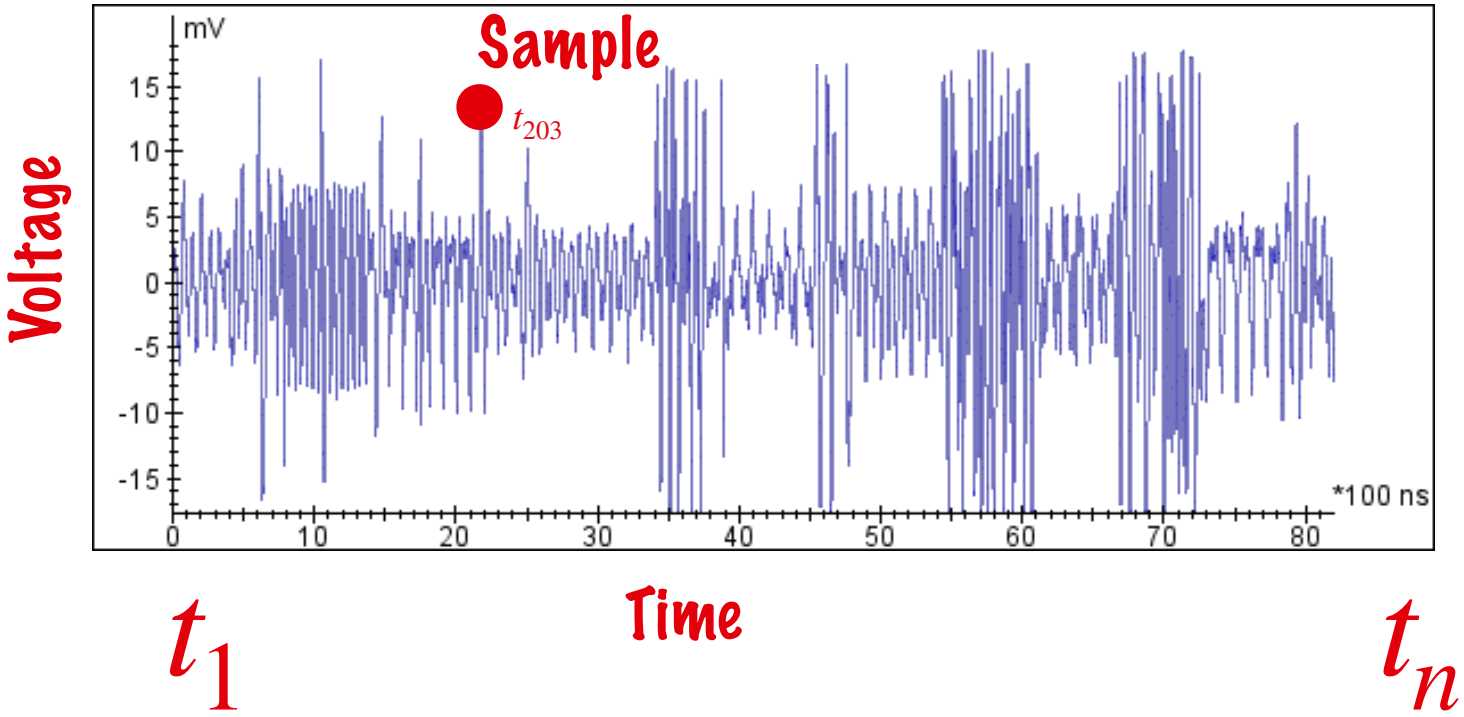


Answer: S-box out, Round-out

2. Measure (power) traces

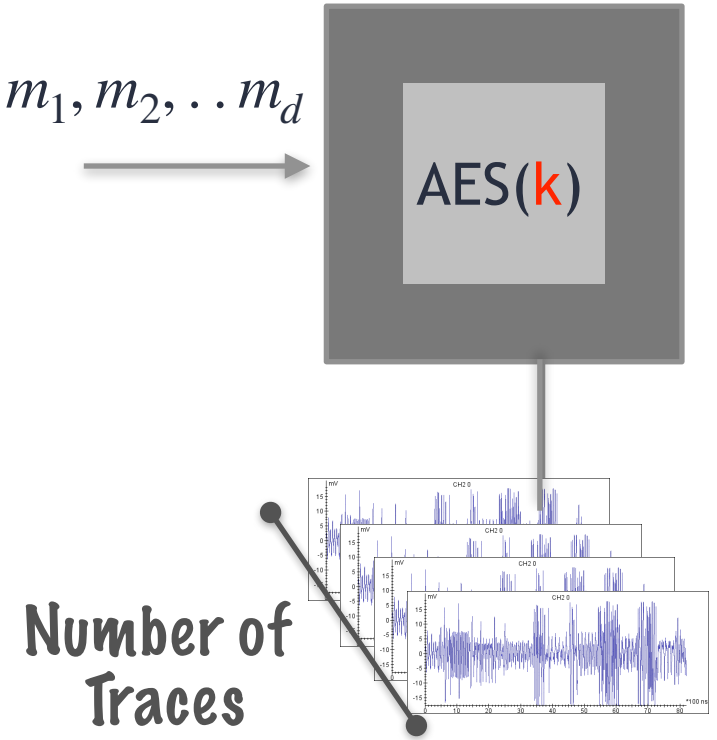


Anatomy of a power trace



It is important that the traces are aligned.

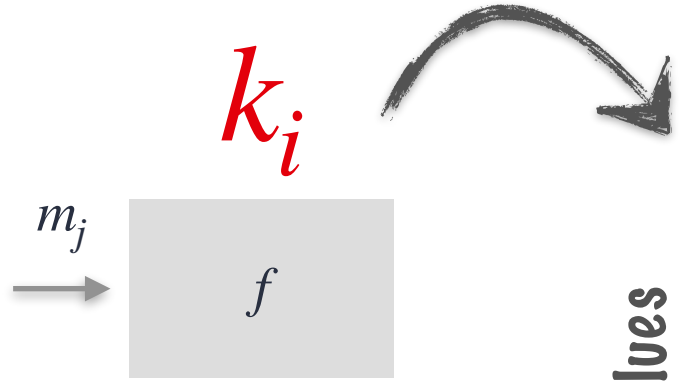
2. Measure (power) traces



m_1	t_1^1	t_2^1		t_n^1	c_1
m_2	t_1^2	t_2^2		t_n^2	c_2
m_d	t_1^d	t_2^d		t_n^d	c_d

It is important that the traces are aligned.

3. Calculate Hypothetical Intermediate Values



$$v_{i,j} = f(k_i, m_j)$$

Possible values

0000 0000
0000 0001
0000 0010

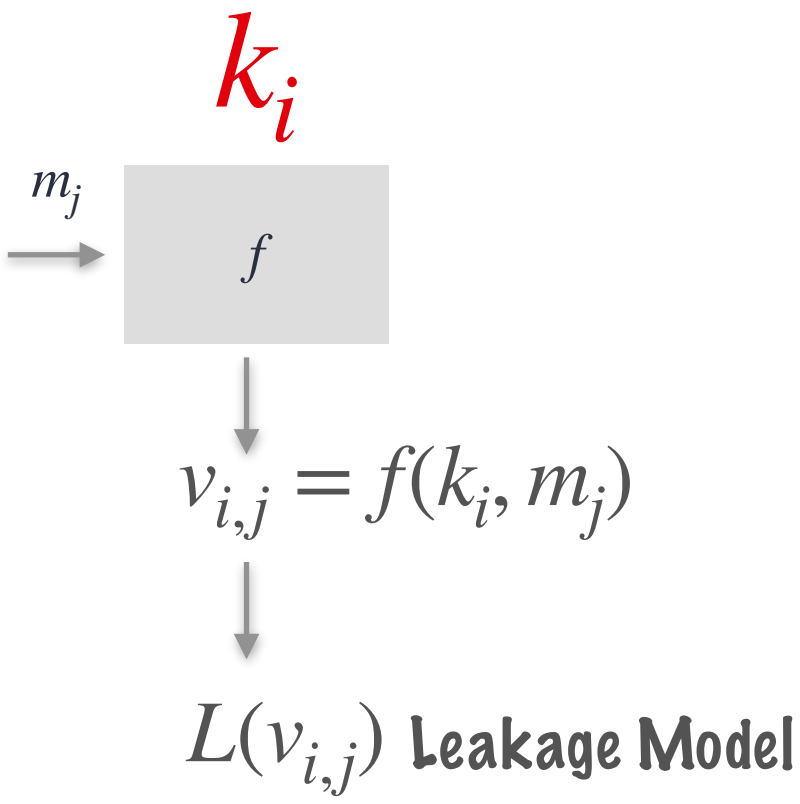
1111 1110
1111 1111

$v_{0,\_} = f(0000\ 0000, m_j)$
$v_{1,\_} = f(0000\ 0001, m_j)$
$v_{2,\_} = f(0000\ 0010, m_j)$

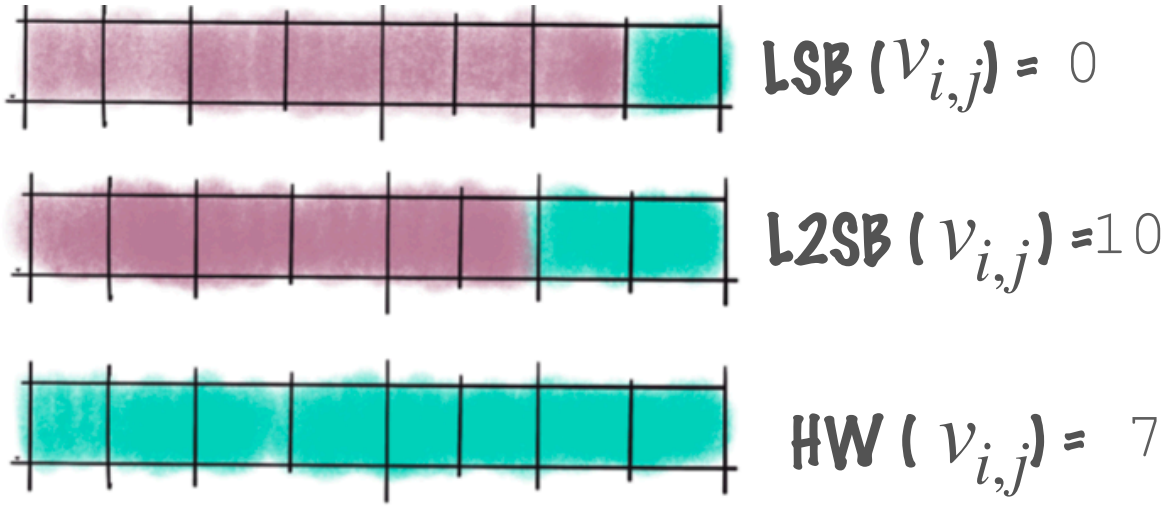
$v_{254,\_} = f(1111\ 1110, m_j)$
$v_{255,\_} = f(1111\ 1111, m_j)$

List of Hypothetical Intermediate Values

4. Map Intermediate Values -> Power Values



$v_{i,j} =$ 1111 1110

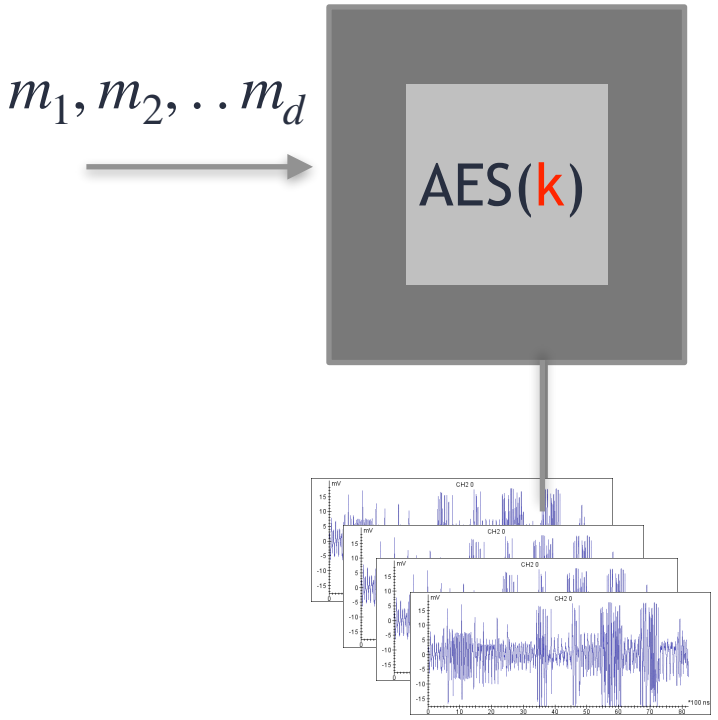


4. Map Intermediate Values -> Power Values

Construct prediction matrix

	k_0	k_1		k_{255}
m_1	$L(v_{0,m_j^1})$	$L(v_{1,m_j^1})$		$L(v_{255,m_j^1})$
m_2	$L(v_{0,m_j^2})$	$L(v_{1,m_j^2})$		$L(v_{255,m_j^2})$
m_d	$L(v_{0,m_j^d})$	$L(v_{1,m_j^d})$		$L(v_{255,m_j^d})$

5. Compare Intermediate Values <-> Power Traces



	k_0	k_1		k_{255}
m_1	$L(v_{0,m_j^1})$	$L(v_{1,m_j^1})$		$L(v_{255,m_j^1})$
m_2	$L(v_{0,m_j^2})$	$L(v_{1,m_j^2})$		$L(v_{255,m_j^2})$
m_d	$L(v_{0,m_j^d})$	$L(v_{1,m_j^d})$		$L(v_{255,m_j^d})$

5. Compare Intermediate Values <-> Power Traces

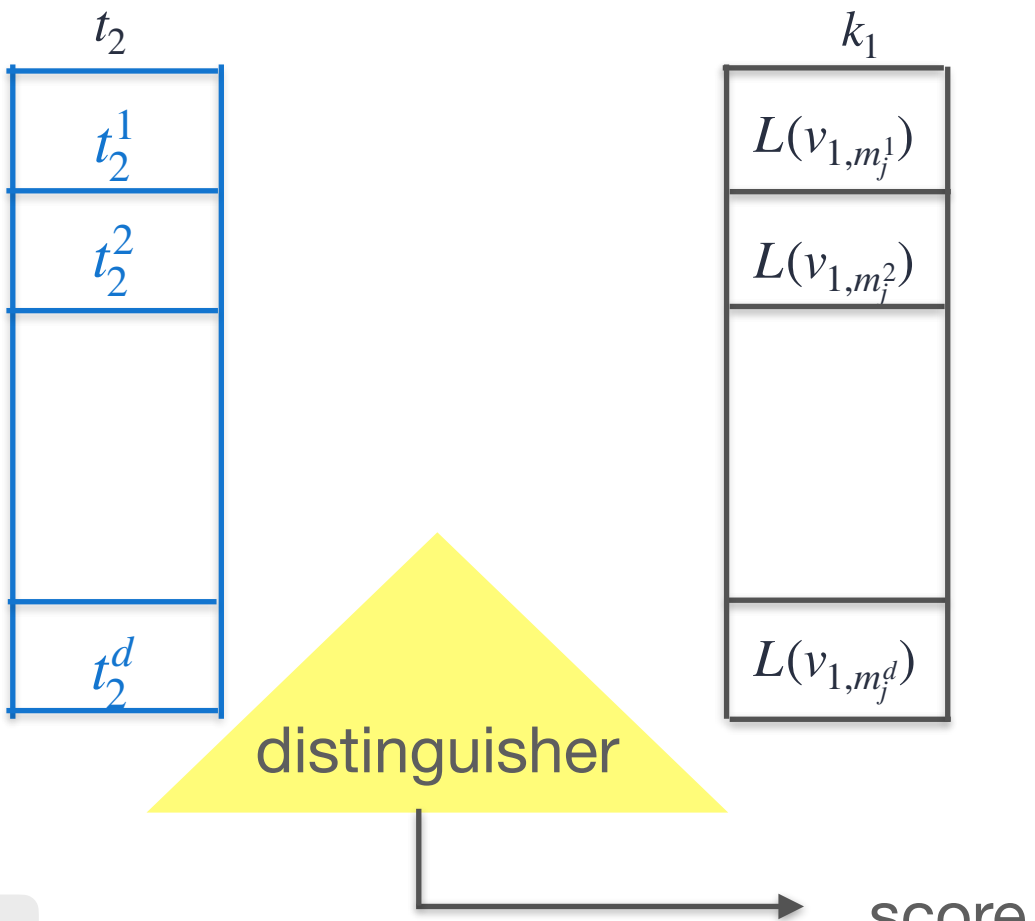
Traces

m_1	t_1^1	t_2^1		t_n^1	c_1
m_2	t_1^2	t_2^2		t_n^2	c_2
m_d	t_1^d	t_2^d		t_n^d	c_d

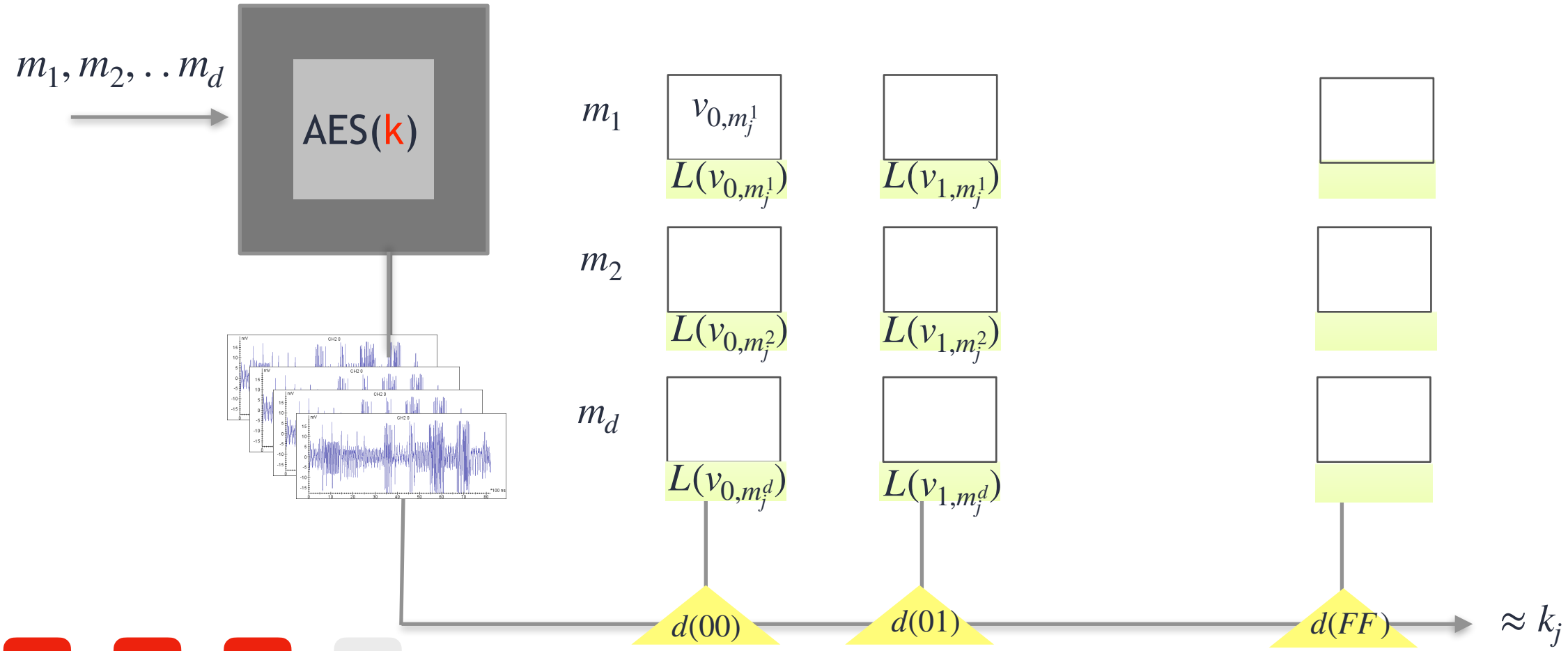
	k_0	k_1		k_{255}
m_1	$L(v_{0,m_j^1})$	$L(v_{1,m_j^1})$		$L(v_{255,m_j^1})$
m_2	$L(v_{0,m_j^2})$	$L(v_{1,m_j^2})$		$L(v_{255,m_j^2})$
m_d	$L(v_{0,m_j^d})$	$L(v_{1,m_j^d})$		$L(v_{255,m_j^d})$

distinguisher

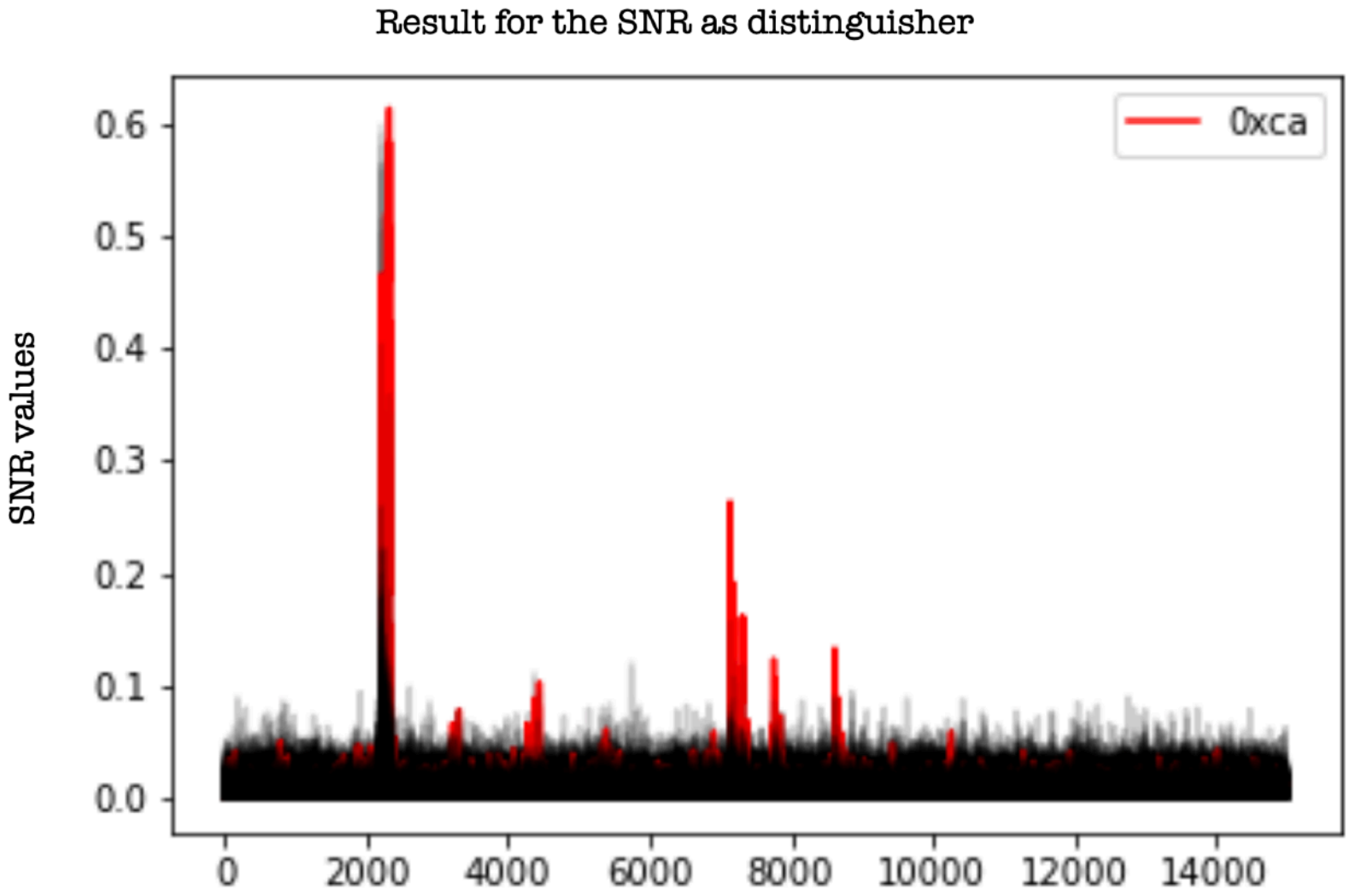
5. Compare Intermediate Values <-> Power Traces



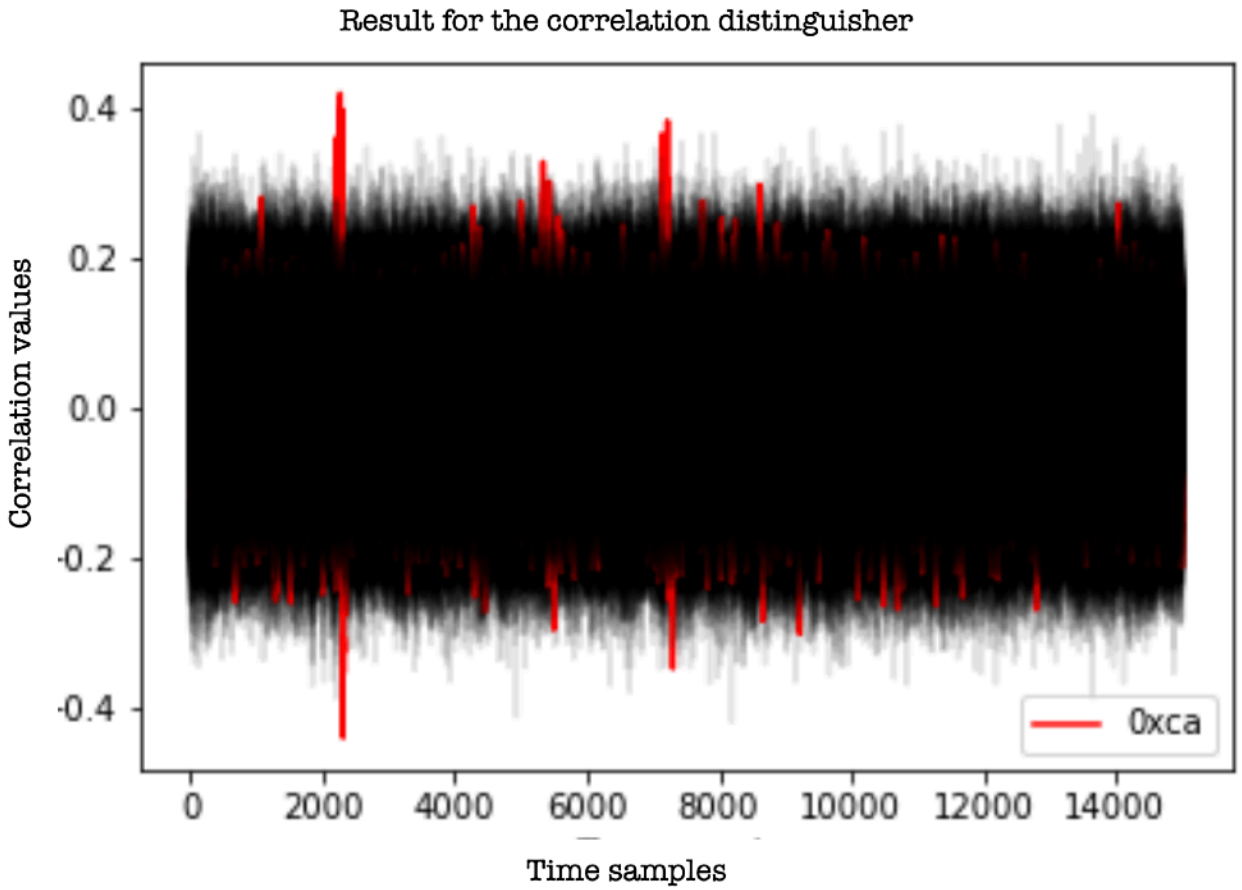
5. Compare Intermediate Values <-> Power Traces



5. Compare Intermediate Values <-> Power Traces



5. Compare Intermediate Values <-> Power Traces



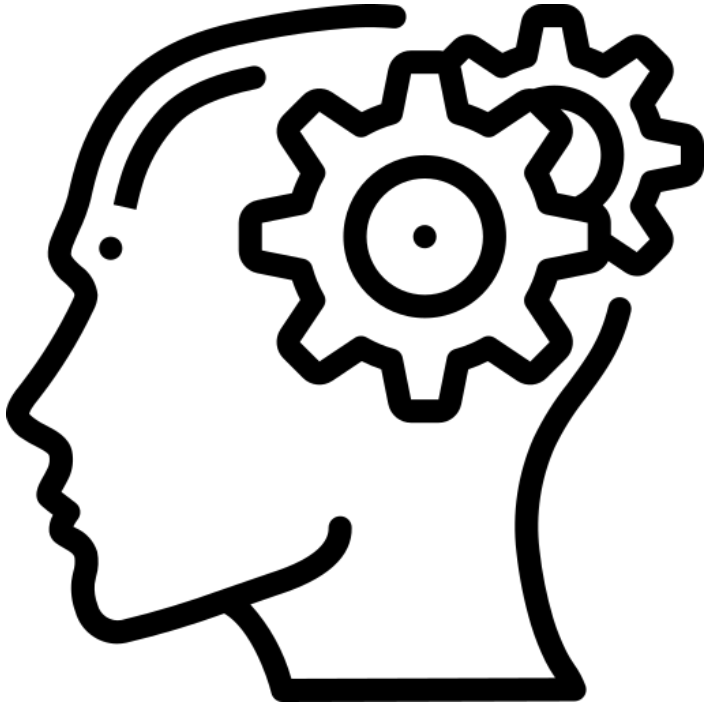
DPA attacks summary

- Choice of leakage model is key to a successfull attack
- Choice of distinguisher:
  - the most powerful is the Correlation Coefficient
  - the most intuitive one is the Difference of Means (DoM)
- DPA vs CPA
- Security order - unprotected implementation - univariate

Countermeasures

Take a few minutes

What would make a good intermediate value for block ciphers? e.g. AES, DES



Answer: S-box out, Round-out

Protection at different levels

Break the link between (actual) intermediate computation values and power consumption

- ➡Transistor-level: special logic styles e.g. WDDL, SABL
- ➡Platform-level: redundancy, adding jitter, noise, . . .
- ➡Program-level: dummy instructions, randomized order, . . .
- ➡Algorithmic level: depends on algebraic operations
- ➡Protocol level: key usage limits, session keys, . . .

The main idea

Masking:

- A random mask is concealing every intermediate value
- The power consumption depends on the masked values and not on the actual values.
- Masking is in principle done on the algorithmic level

Hiding:

- Making power consumption independent of the intermediate values and ofthe operations, uniform or randomized
- Examples: special logic styles, randomization in time domain, lowering SNR

THANK YOU