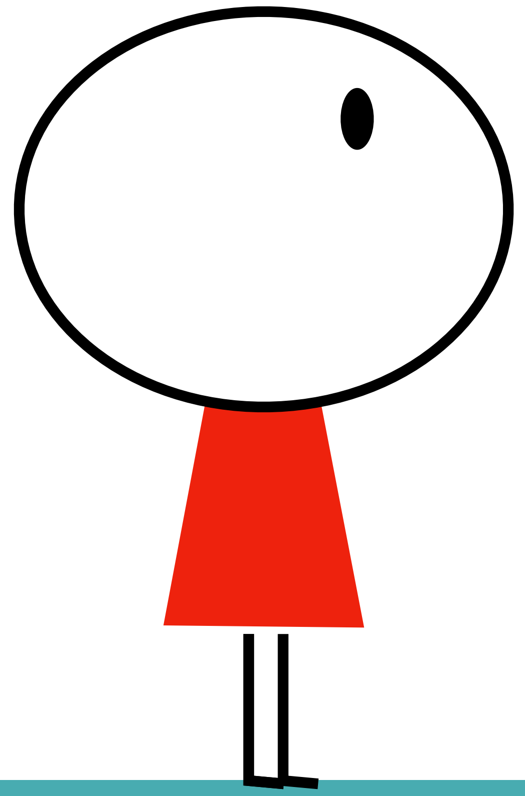
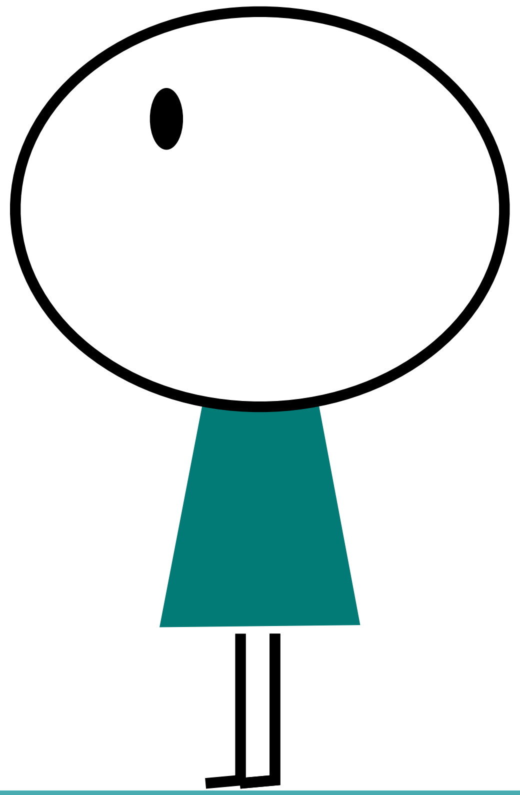
Lattice-based crypto

Overview of attack techniques and countermeasures





Mélissa Rossi

Lattices and hard problems

A lattice Λ is an additive subgroup generated by n linearly independent vectors of $\mathbb{R}^n$.

A lattice Λ is an additive subgroup generated by n linearly independent vectors of $\mathbb{R}^n$.

Lattices and hard problems

Given a lattice Λ

Find the vector $\mathbf{v}$ that has the smallest nonzero norm

Short Vector Problem (SVP)

Lattices and hard problems

« Linear system solving with noise »

Given the pair $\left(\mathbf{A} \in \mathbb{Z}_q^{m\times n}, \mathbf{b} = \mathbf{A}\mathbf{z}+\mathbf{e} \in \mathbb{Z}_q^m\right)$ where

$\mathbf{A}$ is sampled uniformly at random

$\mathbf{e}$ and $\mathbf{z}$ are sampled following a small distribution χ

Find $\mathbf{z}$ $\quad \mathbf{s} = \begin{bmatrix}\mathbf{z}\\ \mathbf{e}\end{bmatrix}$

Learning With Errors (LWE)

Lattice-based algorithms

Signature schemes

Public key encryption schemes

1. Strong hardness properties
2. Simple designs (but complex analysis)
3. Concrete candidates schemes
   NIST round 2: 12 out of 26 candidates
   NIST round 3: 5 out of 7 candidates
   NIST first standards: at least 2
   NIST round 4: ?

LWE-based public key encryption in a nutshell

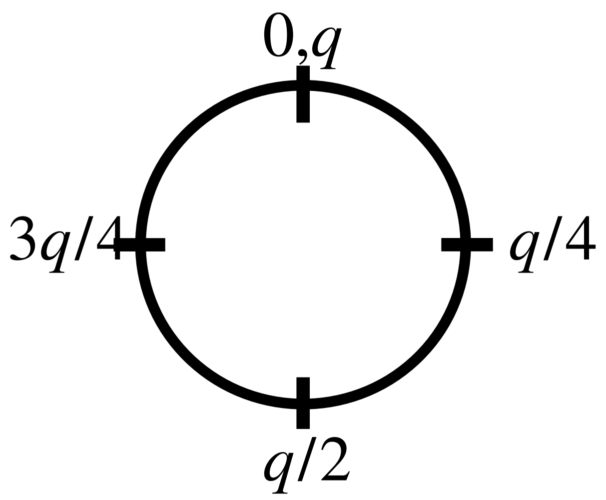
- J. Ding, X. Xie and X. Lin EUROCRYPT'14
- C. Peikert PQCRYPTO'14
- J. W. Bos, C. Costello, M. Naehrig and D. Stebila S&P'15
- E. Alkim, L. Ducas, T. Pöppelmann and P. Schwabe USENIX'16

$(\mathbf{A}, \mathbf{b})$ ←

$\left(\mathbf{A}, \mathbf{b} = \mathbf{A}\mathbf{z}+\mathbf{e}\right)$

$$\mathbf{b}' = \mathbf{A}^T\mathbf{z}'+\mathbf{e}'$$

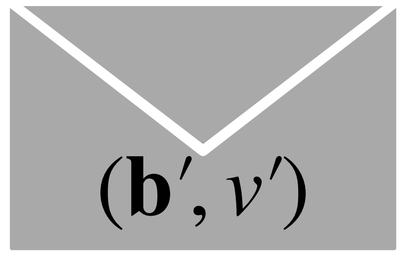
$$v' = \mathbf{b}^T\mathbf{z}'+\mathbf{e}''+\frac{q}{2}m$$



message

1-bit encryption

→



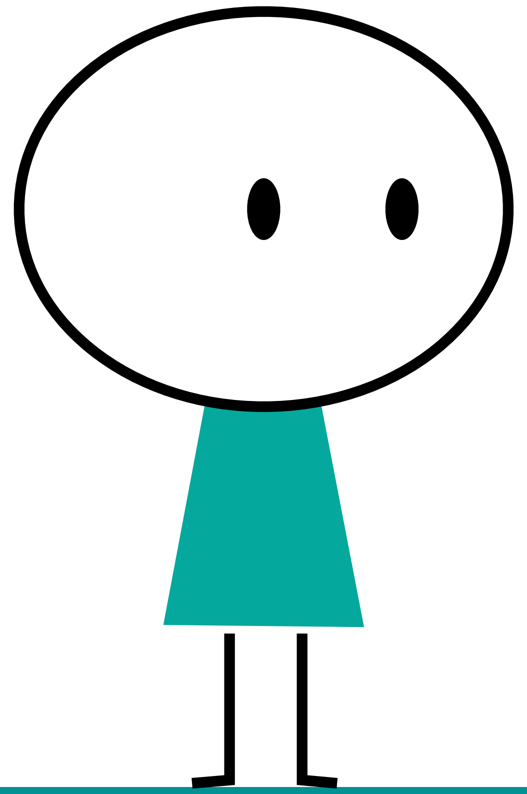
$$m' = \left\lfloor \frac{2}{q}\left(v' - \mathbf{z}^T\mathbf{b}'\right) \right\rceil$$

$$m' \approx m + \underbrace{\left\lfloor \frac{2}{q}\left(\mathbf{e}^T\mathbf{z}'+\mathbf{e}''-\mathbf{z}^T\mathbf{e}'\right) \right\rceil}_{}$$

message

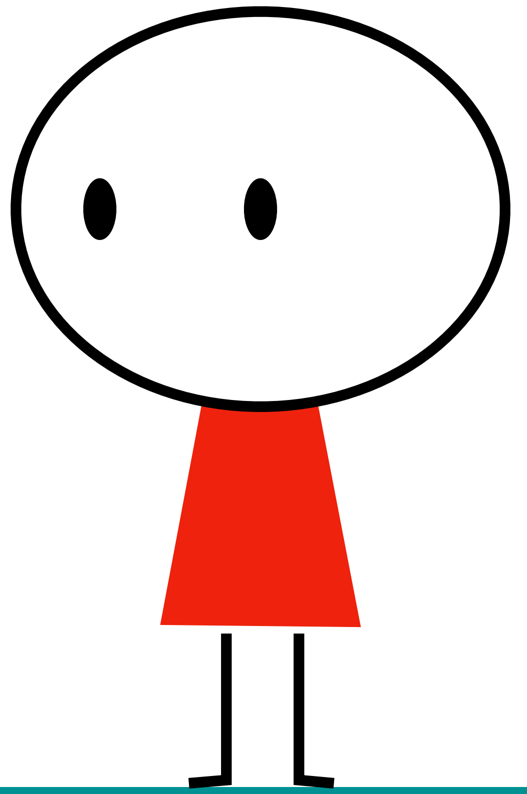
1-bit decryption

Noise smaller than $1/2$



High level idea behind

Crystals-Kyber, Frodo, Saber and NewHope



A Fiat-Shamir with aborts signature in a nutshell

- V. Lyubashevsky EUROCRYPT'12
- L. Ducas, A. Durmus, T. Lepoint and V. Lyubashevsky CRYPTO'13
- S. Bai and D. Galbraith CT-RSA'14

Short Integer Solution (SIS)

$$\left(\mathbf{A}, \mathbf{t} = \mathbf{A}\mathbf{s} \bmod q\right)$$

$(\mathbf{A}, \mathbf{t})$

message $(\mathbf{z}, c)$

Signature algorithm:

message

1: **do**

2: $\quad \mathbf{y} \xleftarrow{\$} Y$

3: $\quad c \leftarrow H(\mathbf{A}\mathbf{y}, m)$

4: $\quad \mathbf{z} \leftarrow c \cdot \mathbf{s} + \mathbf{y}$

5: **while** Rejected($\mathbf{z}$)

6: **return** $(\mathbf{z}, c)$

Verification:

1: $\mathbf{r} \leftarrow \mathbf{A} \cdot \mathbf{z} - \mathbf{t} \cdot c$

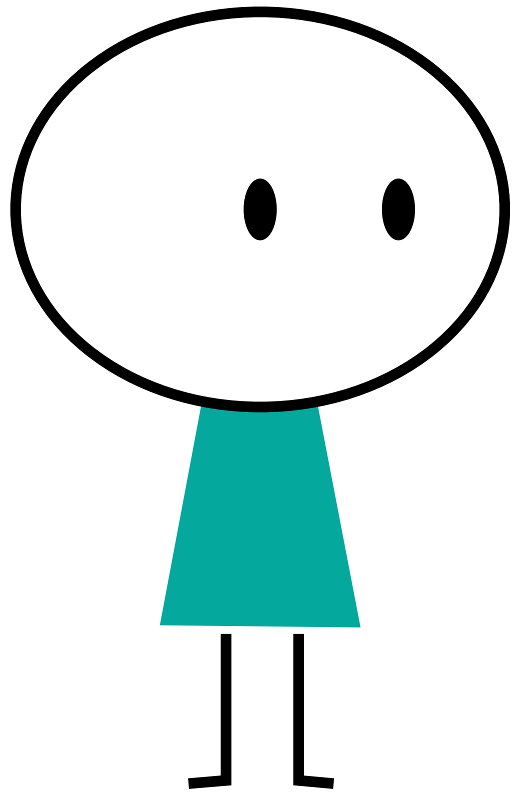
2: $c' \leftarrow H(\mathbf{r}, m)$

3: if $c' = c$ and $\mathbf{z}$ is small enough:

4: $\quad$ return Valid

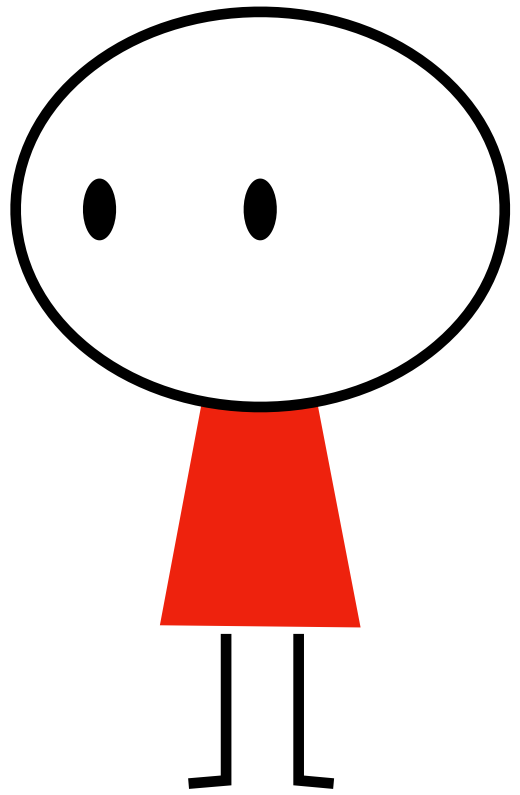
5: else:

6: $\quad$ return Invalid



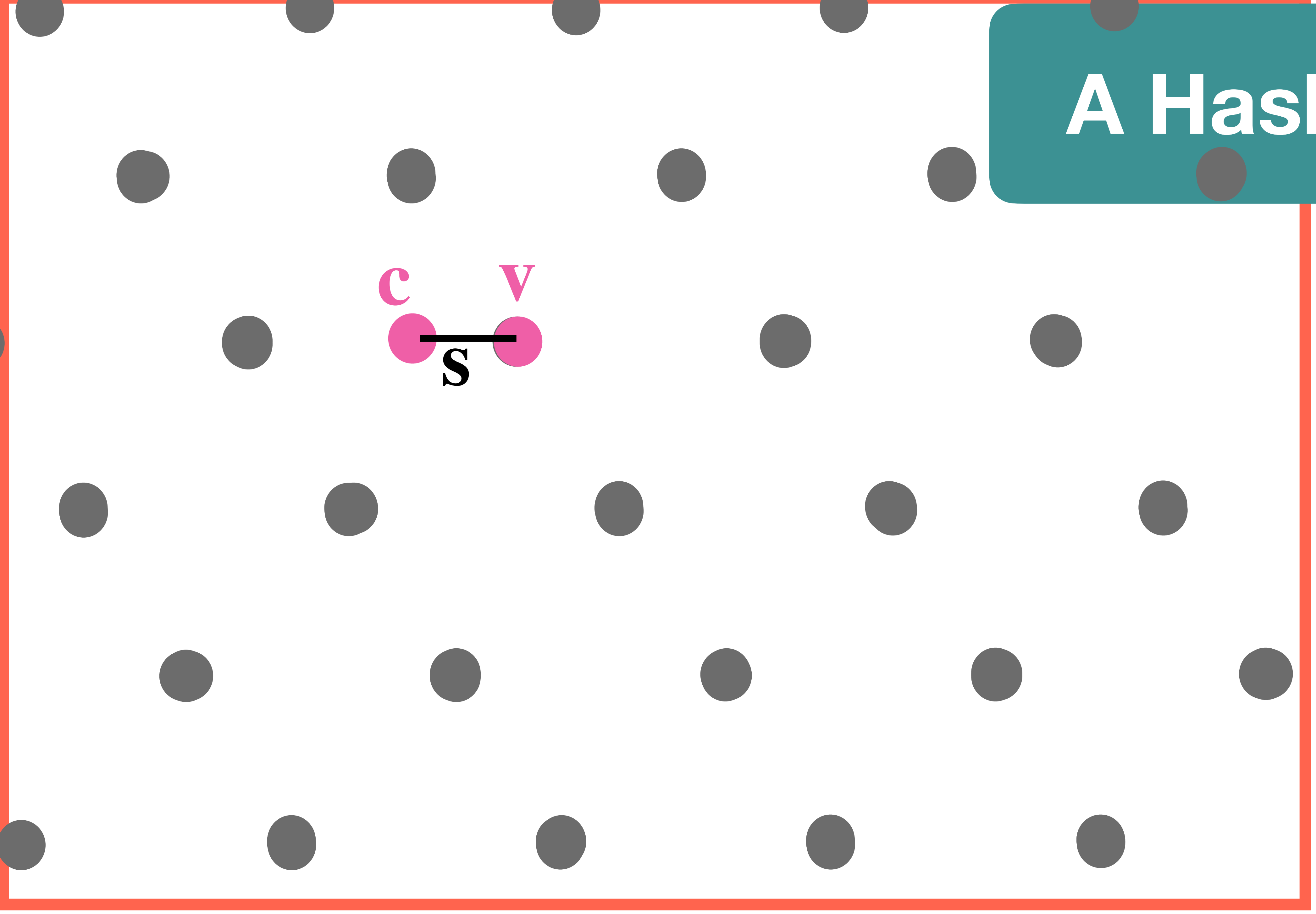
High level idea behind

Crystals-Dilithium, BLISS, GLP, BG



A Hash and sign in a nutshell

‣ C.Gentry, C. Peikert and V. Vaikuntanathan STOC'08



$\mathbf{A}$

Generate matrices $\mathbf{A}$, $\mathbf{B}$ such that

$$\begin{cases} \mathbf{B}\mathbf{A} = \mathbf{0} \\ \mathbf{B} \text{ has small coefficients} \end{cases}$$

message $\mathbf{s}$

Signature algorithm:

message

1: compute $\mathbf{c}$ such that $\mathbf{c}\mathbf{A} = H(m)$

2: $\mathbf{v} \leftarrow$ a vector in $\Lambda(\mathbf{B})$ close to $\mathbf{c}$

3: return $\mathbf{s} \leftarrow \mathbf{c} - \mathbf{v}$

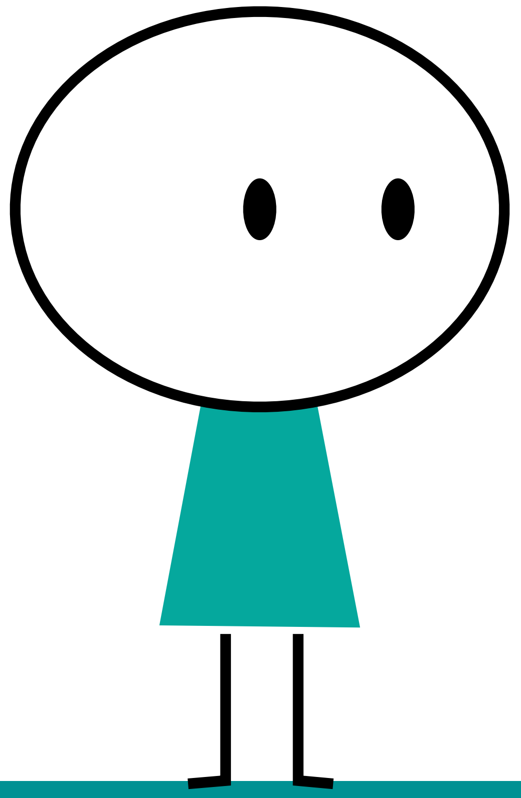
Verification:

1: if $\mathbf{s}$ is short and $\mathbf{s}\mathbf{A} = H(m)$

2: return Valid

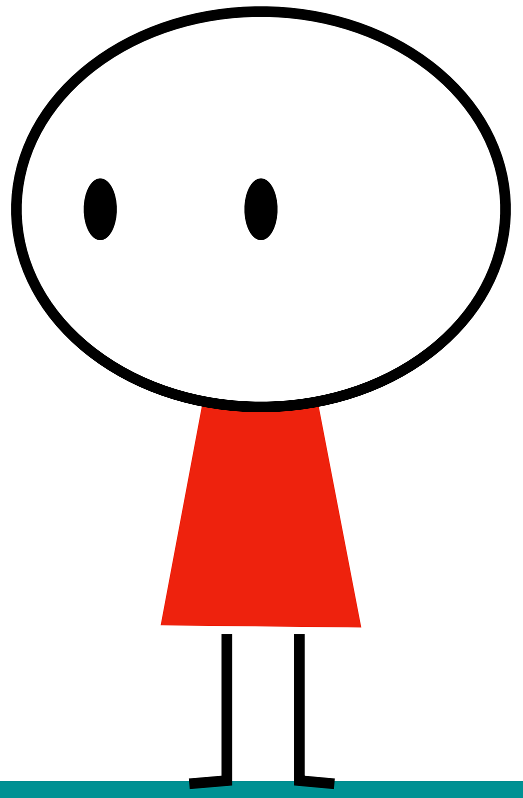
3: else:

4: return Invalid



High level idea behind

GPV, Falcon, Mitaka



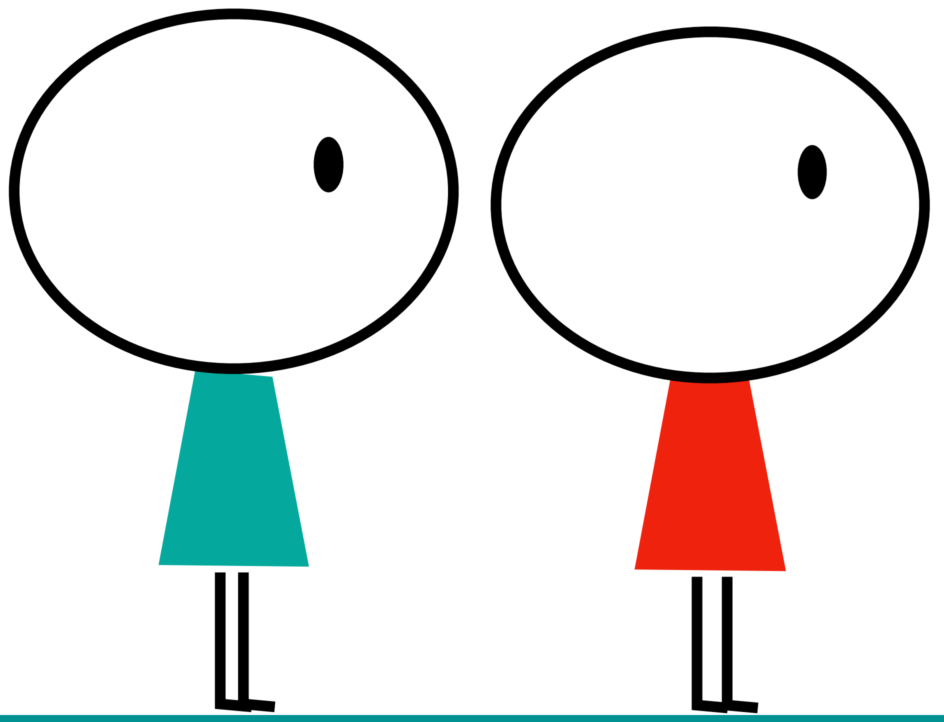
Lattice-based algorithms

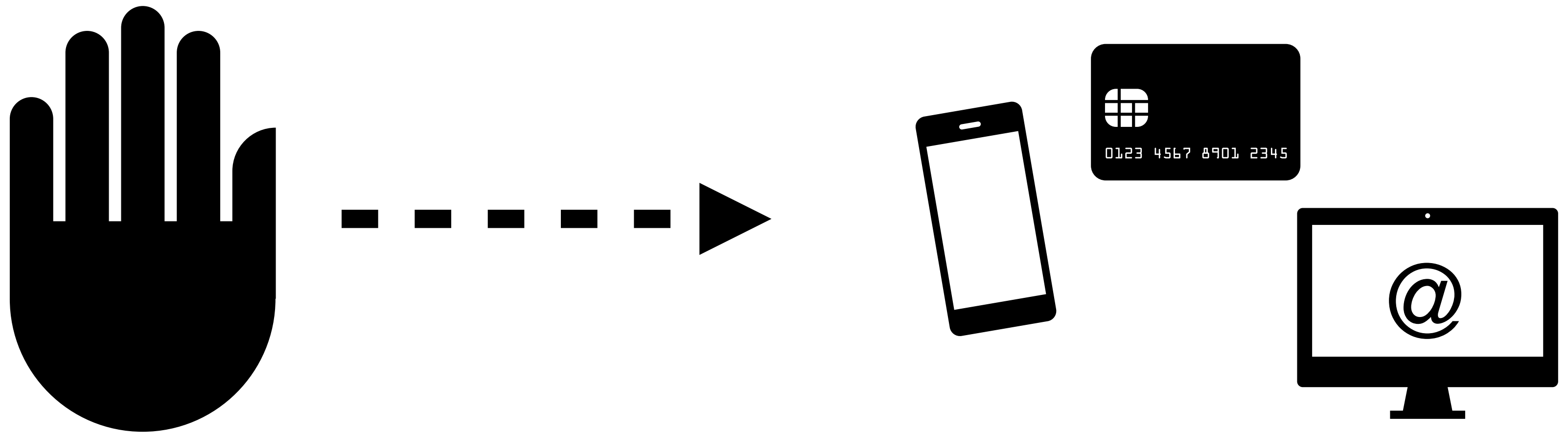
Signature schemes

Public key encryption schemes

Are you secure for real-world development ?

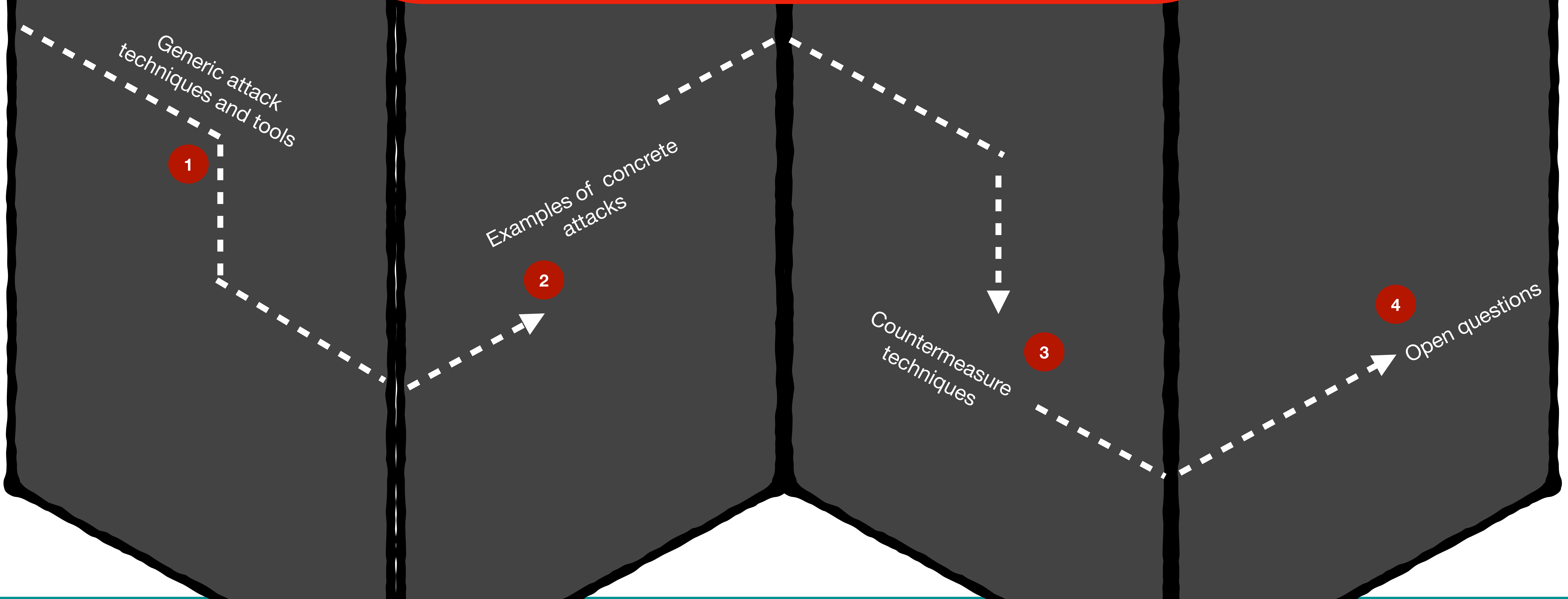
Are you timing resistant ?
Are you secure against physical attacks?
Are you misuse resistant ?
Are you decryption-failure resistant?
… by how much ?

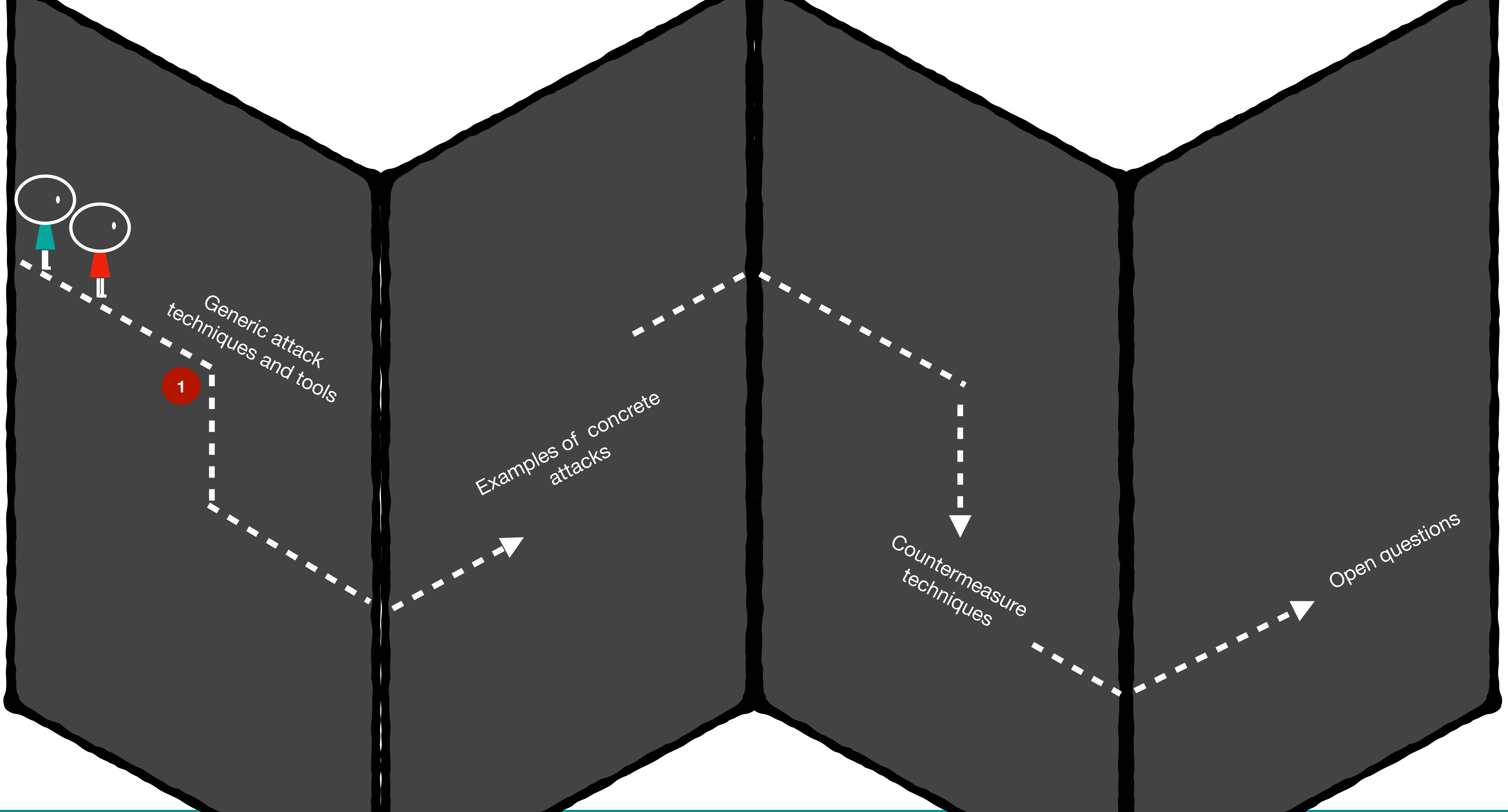




Disclaimer

Due to time limit, we will not go into much details during this overview. But, the purpose of C2 days is exchanging, so feel free to come and ask for details.




Generic attack techniques and tools
1
Examples of concrete attacks
Countermeasure techniques
Open questions

Primal attack to assess the mathematical security

LWE $\mapsto$ SVP $\mapsto$ Lattice reduction

« Linear system solving with noise »

Given the pair $\left(\mathbf{A} \in \mathbb{Z}_q^{m \times n}, \mathbf{b} = \mathbf{A}\mathbf{z} + \mathbf{e} \in \mathbb{Z}_q^m\right)$ where

$\mathbf{A}$ is sampled uniformly at random

$\mathbf{e}$ and $\mathbf{z}$ are sampled following a small distribution χ

Find $\mathbf{z}$

Learning With Errors (LWE)

Kannan's embedding:

The vector $\left[\mathbf{e}^T, \mathbf{z}^T, 1\right]$ is a short vector of the lattice $\Lambda(\mathbf{B})$ where

$$\mathbf{B} = \begin{bmatrix} q\mathbf{I_m} & 0 & 0 \\ -\mathbf{A} & -\mathbf{I_n} & 0 \\ \mathbf{b} & 0 & 1 \end{bmatrix}$$

More precisely, $\Lambda(\mathbf{B}) = \left\{(\mathbf{x}^T, \mathbf{y}^T, w) \text{ such that } \mathbf{x} + \mathbf{A}\mathbf{y} - w\mathbf{b} = \mathbf{0} \bmod q\right\}$

Given a lattice $\Lambda(B)$

Find the vector $\mathbf{v}$ that has the smallest nonzero norm

Short Vector Problem (SVP)

Lattice Reduction (LLL, BKZ)

Tools to assess the mathematical security (primal attack)

Quantifying security: **Cost** of the best known attack against the underlying lattice hard problem for specific parameters e.g. 2^{128}

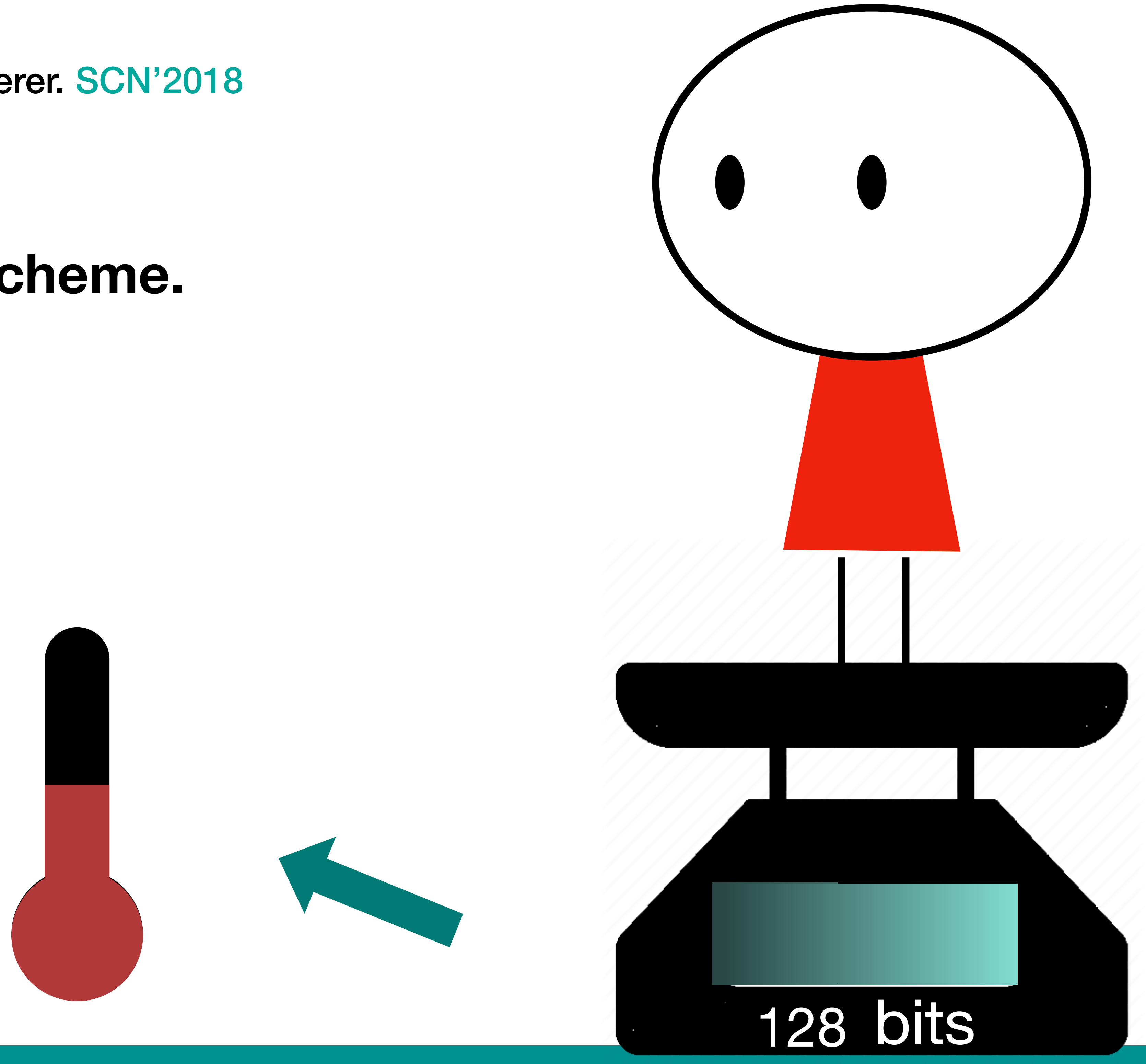
LWE $\mapsto$ SVP $\mapsto$ Lattice reduction
block-size of BKZ $\mapsto$ cost models $\mapsto$ bit security

- E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe. USENIX'2016
- M. R Albrecht, F. Göpfert, F. Virdia, and T. Wunderer. ASIACRYPT'2017
- M. R. Albrecht, B. R. Curtis, A. Deo, A. Davidson, R. Player, E. W. Postlethwaite, F. Virdia, and T. Wunderer. SCN'2018

- **LWE estimator: Tool to compute the bit security of any LWE-NTRU-based scheme.**

- **Leaky LWE estimator: Tool to include partial side information in the scale.**
  - D. Dachman-Soled, L. Ducas, H. Gong and M. Rossi. CRYPTO'2020.

Side information
Partial information on the secret (side-channel, timing attacks, constraints on the design…)



LeakyLWE Estimator : including hints before lattice reduction

$$\text{LWE} \xrightarrow{\text{Kannan}} \text{DBDD}_{\Lambda_0,\boldsymbol{\Sigma}_0,\mu_0}$$

$$\downarrow \text{Hint}$$

$$\text{DBDD}_{\Lambda_1,\boldsymbol{\Sigma}_1,\mu_1}$$

$$\vdots$$

$$\downarrow \text{Hint}$$

$$\text{DBDD}_{\Lambda_n,\boldsymbol{\Sigma}_n,\mu_n} \xrightarrow[\text{Homogenize \& Isotropize}]{} \text{SVP} \longrightarrow \text{Lattice Reduction}$$

Perfect hints

$\mathbf{v}, l \in \mathbb{Z}$ such that $\langle \mathbf{s}, \mathbf{v} \rangle = l$

Modular hints

$\mathbf{v}, l, k \in \mathbb{Z}$ such that $\langle \mathbf{s}, \mathbf{v} \rangle = l \mod k$

Approximate hints

$\mathbf{v}, l \in \mathbb{Z}$ such that $\langle \mathbf{s}, \mathbf{v} \rangle \approx l$

Side-channel applications basic example

Secret coefficient $s_i \in \{-5,\ldots,5\}$ (represented by a signed 16-bits integer)

After a power analysis, attacker learns the hamming weight of s_0, say
HW(s_0) $= 2 \longrightarrow s_0 \in \{3,\ 5\}$.

To hints

1. a modular hint: $\langle \mathbf{s}, \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \rangle = 1 \mod 2$,

2. an approximate hint: $\langle \mathbf{s}, \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \rangle \approx 4$, with variance 1.

Tool Demonstration

Another attack: the hidden parallelepiped attack

- P. Nguyen, O. Regev Eurocrypt'2006
- L. Ducas, P. Nguyen Asiacrypt'2012

Generate matrices $\mathbf{A}, \mathbf{B}$ such that

$$\begin{cases} \mathbf{B}\mathbf{A} = \mathbf{0} \\ \mathbf{B} \text{ has small coefficients} \end{cases}$$

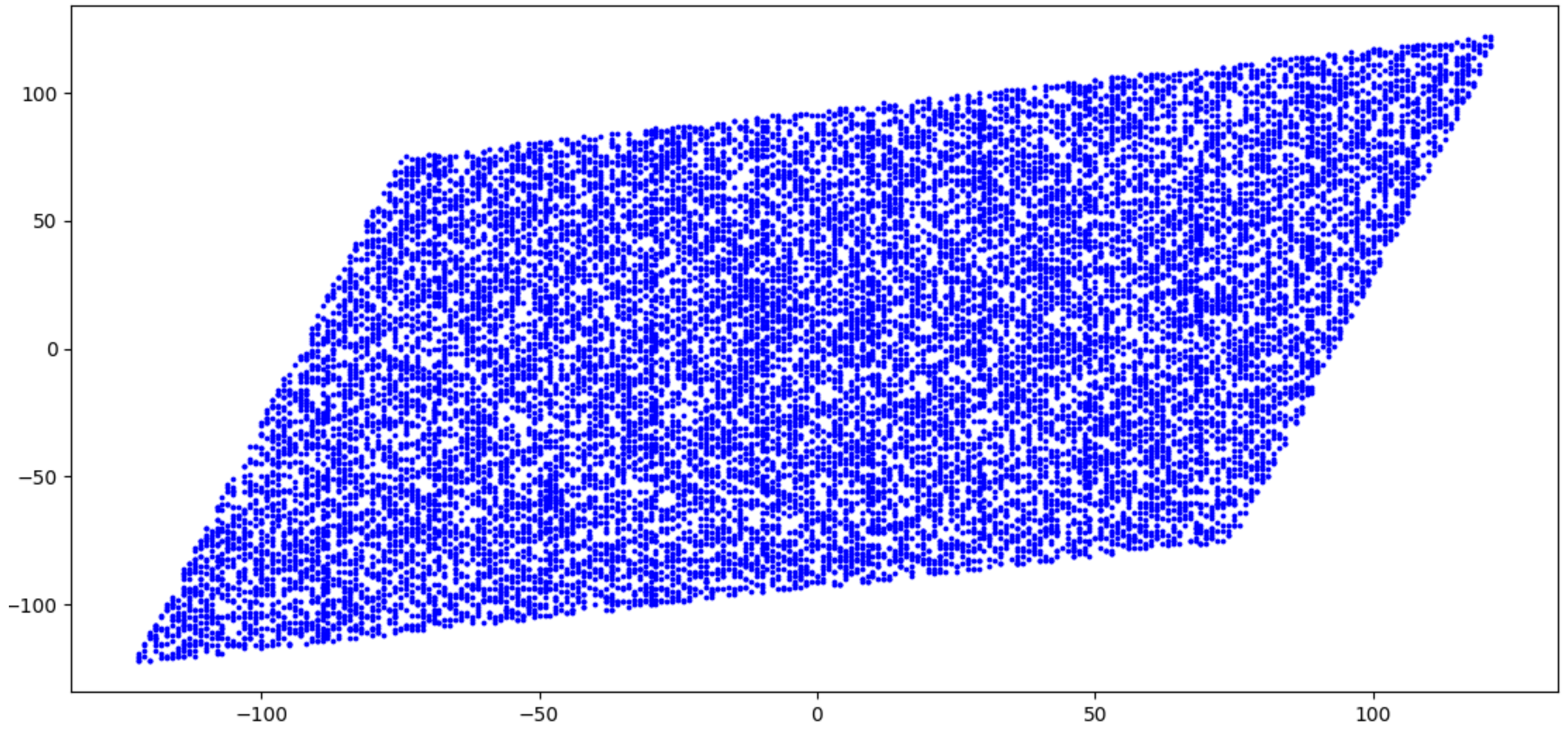
Signature algorithm:

1: compute $\mathbf{c}$ such that $\mathbf{c}\mathbf{A} = H(m)$
2: $\mathbf{v} \leftarrow$ a vector in $\Lambda(\mathbf{B})$ close to $\mathbf{c}$
3: return $\mathbf{s} \leftarrow \mathbf{c} - \mathbf{v}$

Babai's reduction: take **the** closest vector.

!

HPP attack: with enough signatures, we can « see » the private basis



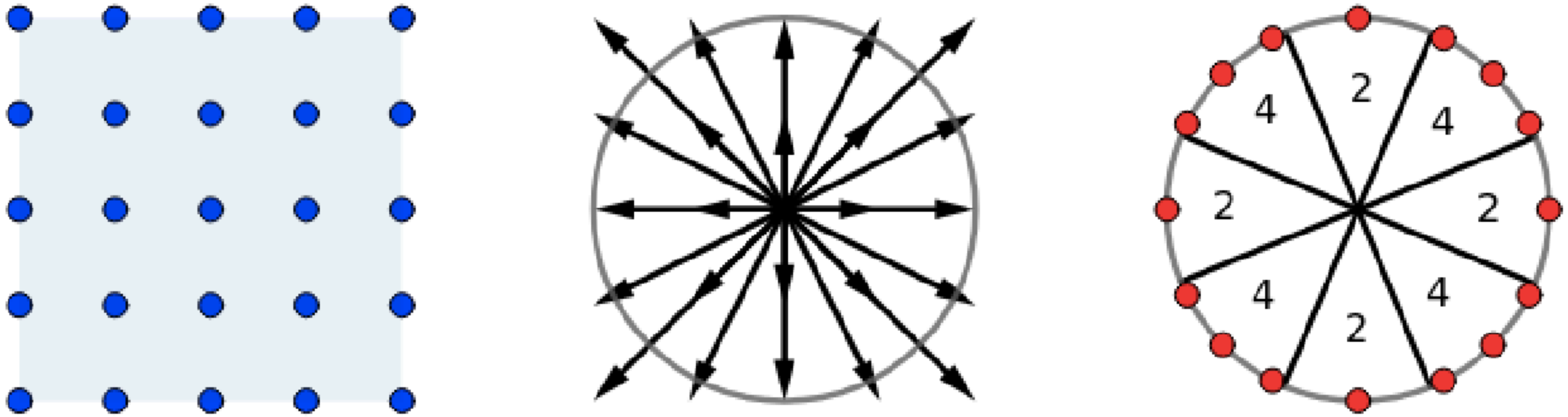
Distribution of signatures

Hidden parallelepiped attack: how to recover the basis?

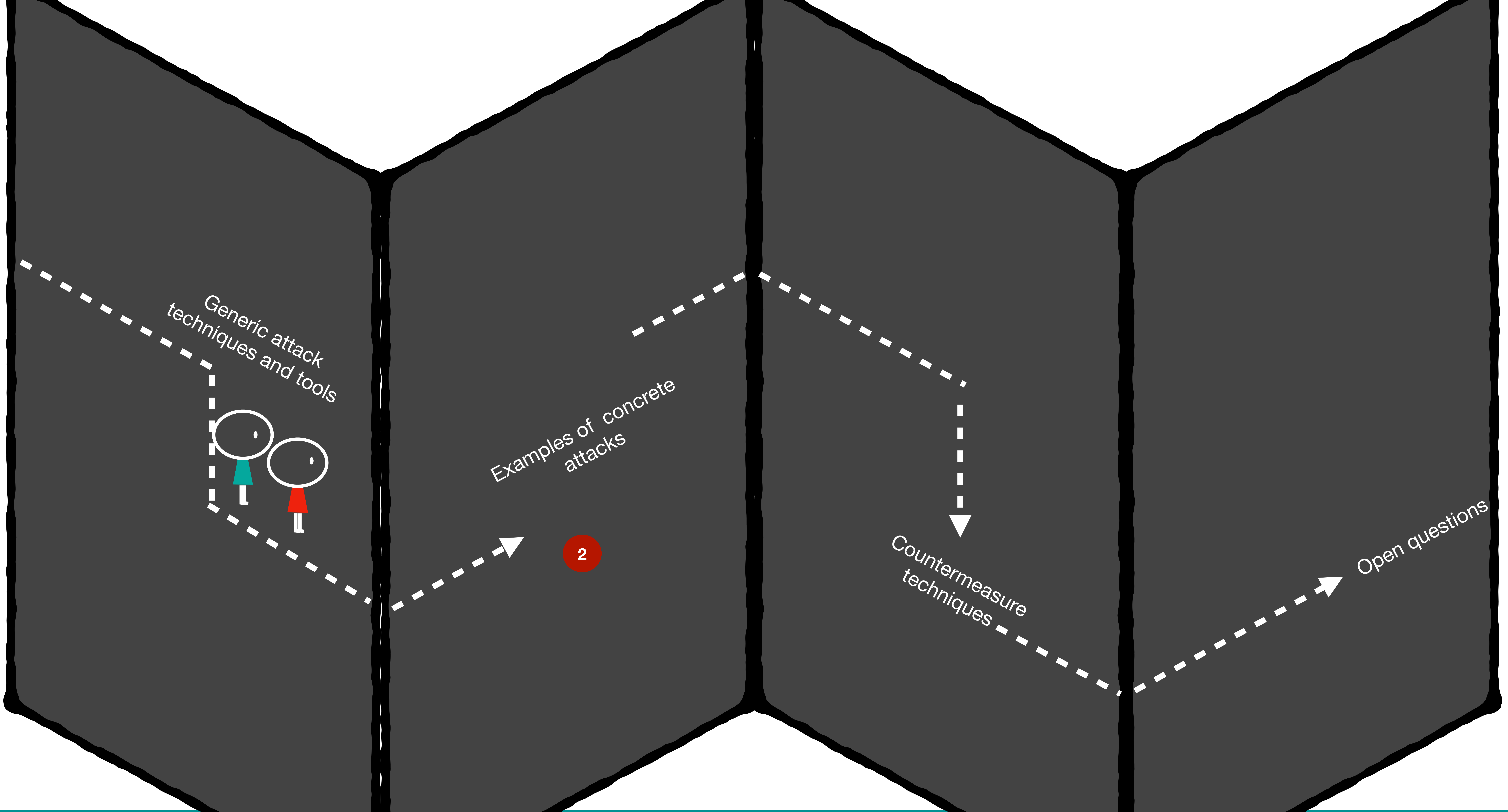
Even if we see the basis in 2D, recovering the basis is tricky.

- First, we morph the problem into a **hidden hypercube problem** (Cholesky decomposition of the covariance matrix)
- Second, we note that the fourth moment over the unit sphere is minimized in the corners.

$$\boxed{\text{mom}_4(w) = \text{Exp}_{u \in U}\left[\langle u, w\rangle^4\right]}$$



Thus, we can perform a **gradient descent** to recover the corners and then the basis.


Generic attack techniques and tools
Examples of concrete attacks
2
Countermeasure techniques
Open questions

Timing attacks

<u>Timing attack:</u> the attacker knows the time that the algorithm takes e.g. the number of iterations.

In lattice-based schemes, we always to sample small coefficients.

Gaussians are often used for two reasons:

Performance

Security reductions

It implies computing transcendental functions $\exp(\,.\,)$ and $\cosh(\,.\,)$ → Hard to compute efficiently in constant time!

Many timing attacks
targeting Gaussian distributions in lattice-based signature schemes

- L. Groot Bruinderink, A. Hülsing, T. Lange, and Y. Yarom. CHES'2016
- T. Espitau, P.-A. Fouque, B. Gérard, M. Tibouchi. SAC'2016
- P. Pessl, L. Groot Bruinderink, and Y. Yarom. ACM-CCS'2017
- T. Espitau, P.-A. Fouque, B. Gérard and M. Tibouchi. ACM-CCS'2017
- J. Bootle, C. Delaplace, T. Espitau, P.-A. Fouque and M. Tibouchi. ASIACRYPT'2018
- G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi and M. Tibouchi. ACM-CCS'2019
- P.-A. Fouque, P. Kirchner,,M. Tibouchi, A. Wallet, and Y. Yu. EUROCRYPT'2020

An example presented in the next slide →

An example of timing attack on BLISS signature scheme

$$\frac{1}{\cosh(x)} = \frac{\exp(-|x|)}{1/2 + 1/2\exp(-2|x|)}$$

Sampling a Bernoulli with parameter cosh(x) :$\mathscr{B}_{1/\cosh(x)}$

1: $x \leftarrow |x|$
2: $a \leftarrow \mathscr{B}_{\exp(-x)}$
3: $b \leftarrow \mathscr{B}_{1/2}$
4: $c \leftarrow \mathscr{B}_{\exp(-x)}$
5: **if** $\bar{a} \wedge (b \vee c)$ **then restart**
6: **return** a

Even if every Bernoulli sampling is constant time, there is still **timing attack!**

➡ Probability of going from step 5 to step 6:

$$\begin{aligned}\mathbb{P}(\overline{\bar{a} \wedge (b \vee c)}) &= 1 - \mathbb{P}(\bar{a}) \cdot \mathbb{P}(b \vee c) \\ &= 1 - (1 - \mathbb{P}(a)) \cdot (1 - \mathbb{P}(\bar{b} \wedge \bar{c})) \\ &= 1 - (1 - \exp(-x))\left(1 - \frac{1 - \exp(-x)}{2}\right) \\ &= \frac{1 + \exp(-2x)}{2}\end{aligned}$$

Depends on the input!

Correctness

The distribution of a is indeed $\mathscr{B}_{1/\cosh(x)}$.

- L. Ducas, A. Durmus, T. Lepoint and V. Lyubashevsky CRYPTO'13

Idea of the attack

Actually $x = -|\langle z, \mathbf{S}c\rangle|$

We select the signatures (z, c) that end up in **one iteration.**

It means that $\dfrac{1 + \exp(-2|\langle z, \mathbf{S}c\rangle|)}{2}$ is large.

Then, $|\langle z, \mathbf{S}c\rangle|$ is close to 0.

➡ Can be solved with a phase retrieval algorithm (machine learning).

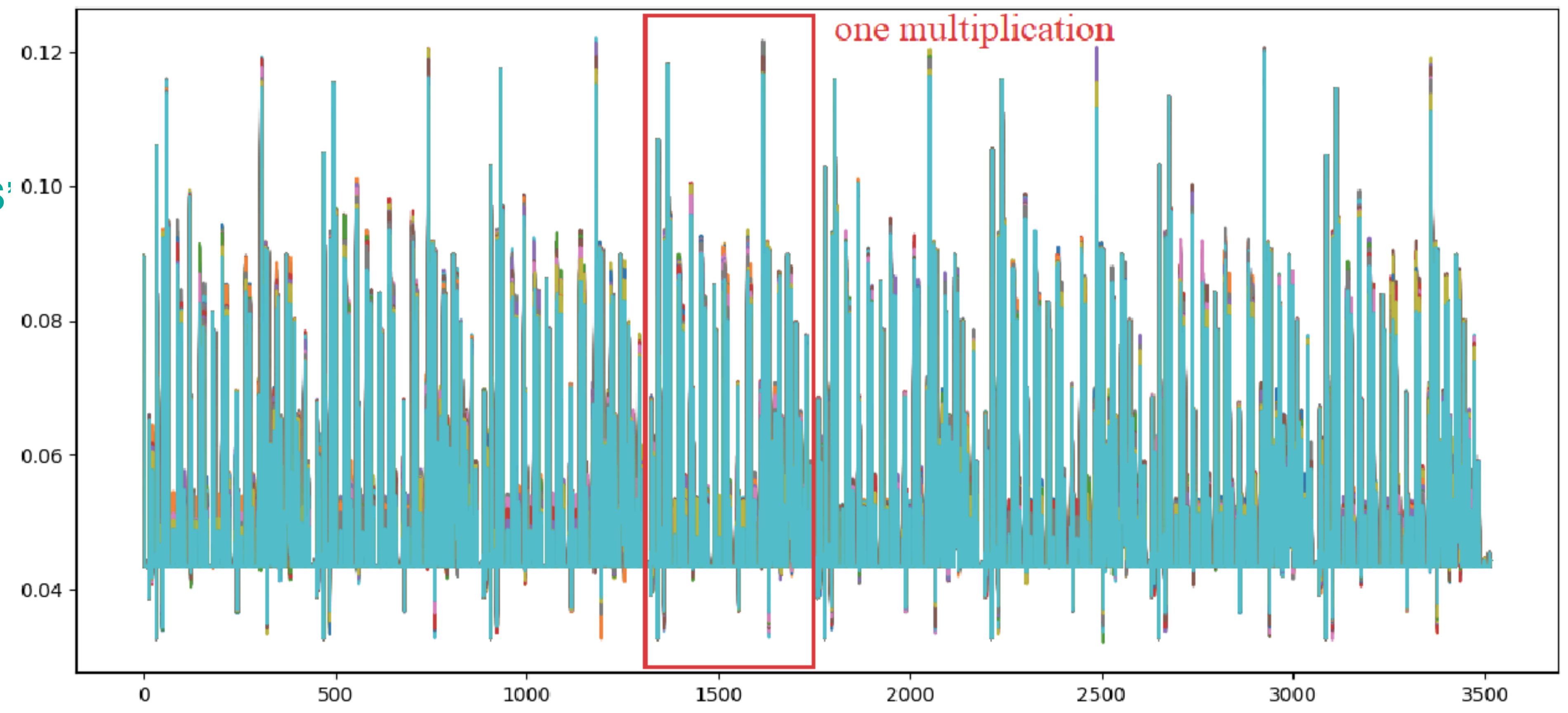
Power consumption attacks

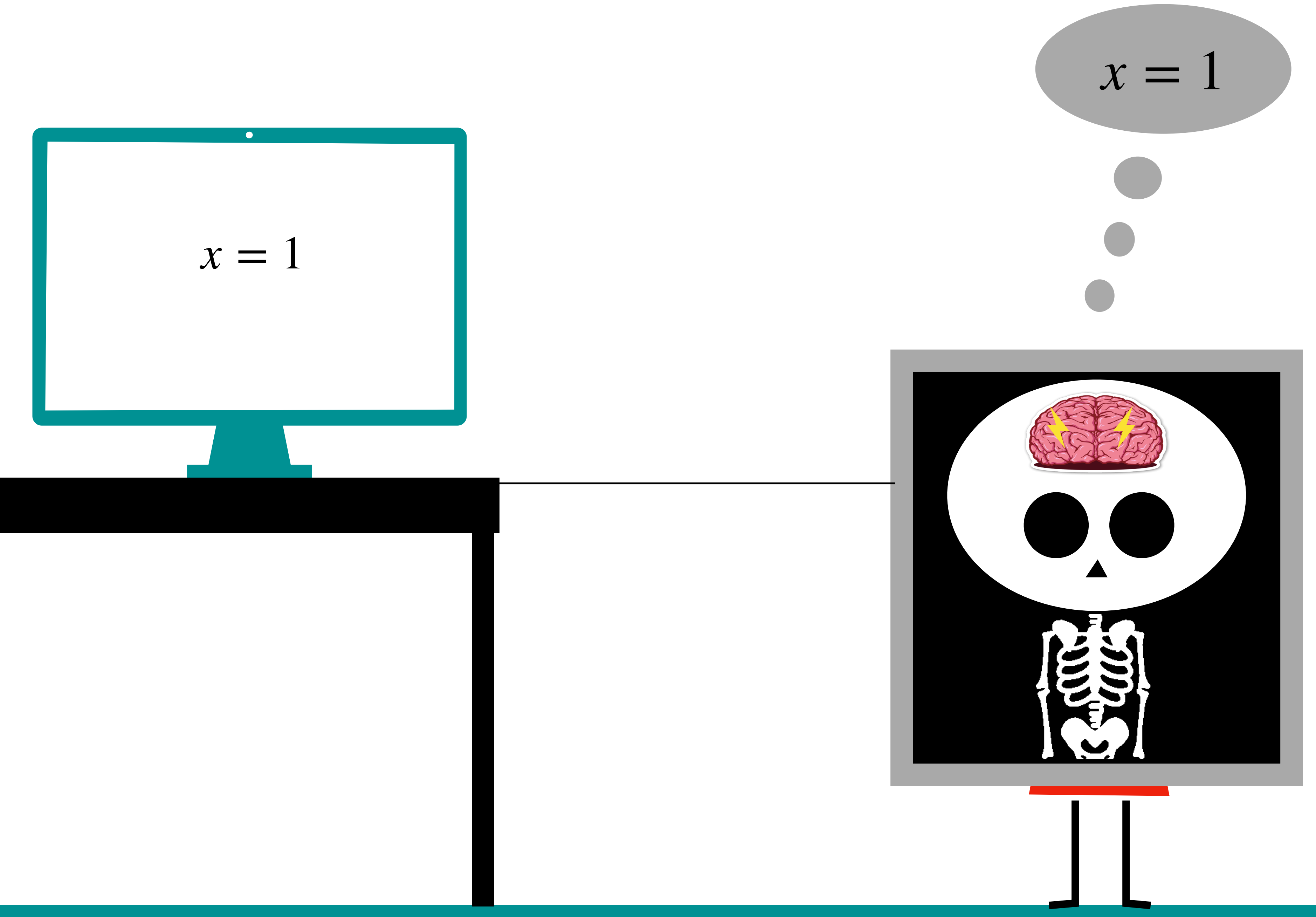
Power consumption attack: the attacker knows the power consumption of the device executing the algorithm. He has access to « traces ».

Many attacks as well

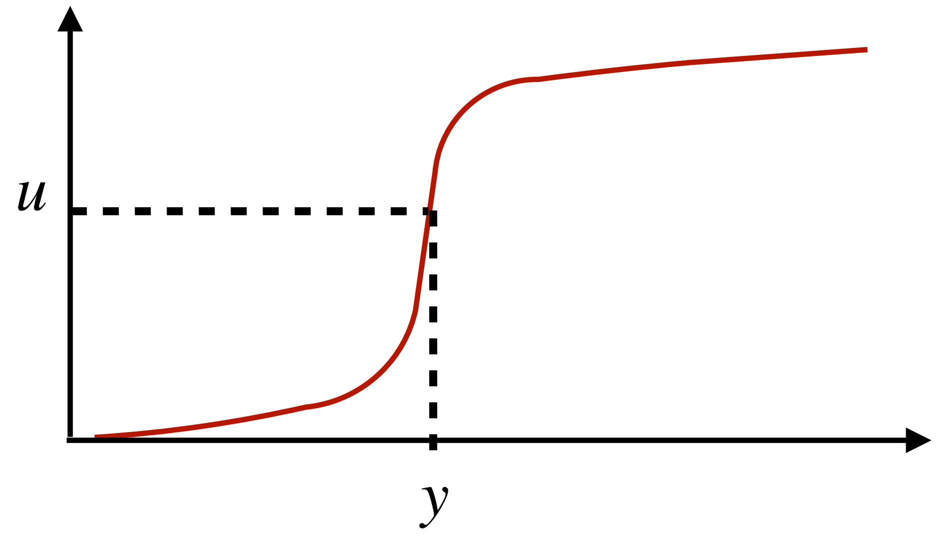
- R. Primas, P. Pessl, S. Magnard. CHES'2017
- S. Bhasin, J.-P. D'Anvers, D. Heinz, T. Pöppelmann, M. Van Beirendonck. TCHES'2021
- B.-Y Sim, J. Kwon, J. Lee, I.-J. Kim, T. Lee, J. Han, H. Yoon, J. Choo, D.-G. Han. IEEE-ACESS
- B.-Y. Sim, A. Park. eprint'2021
- P. Ravi, S. Sinha Roy, A. Chattopadhyay, S. Bhasin. CHES'2020
- E. Karabulut, A. Aysu. DAC'2021
- M. Guerreau, A. Martinellli, T. Ricosset, M. Rossi. TCHES'2022

An example presented in the next slides





Usual suspects:
- multiplication with the secret: $\mathbf{A}\mathbf{s}$
- NTT
- message encoding
- Fujisaki-Okamoto transform
- Internal distributions
- Cumulative Distribution Tables



Falcon signature scheme

Signature algorithm:

1: compute $\mathbf{c}$ such that $\mathbf{cA} = H(m)$

2: $\mathbf{v} \leftarrow$ a vector in $\Lambda(\mathbf{B})$ close to $\mathbf{c}$

3: return $\mathbf{s} \leftarrow \mathbf{c} - \mathbf{v}$

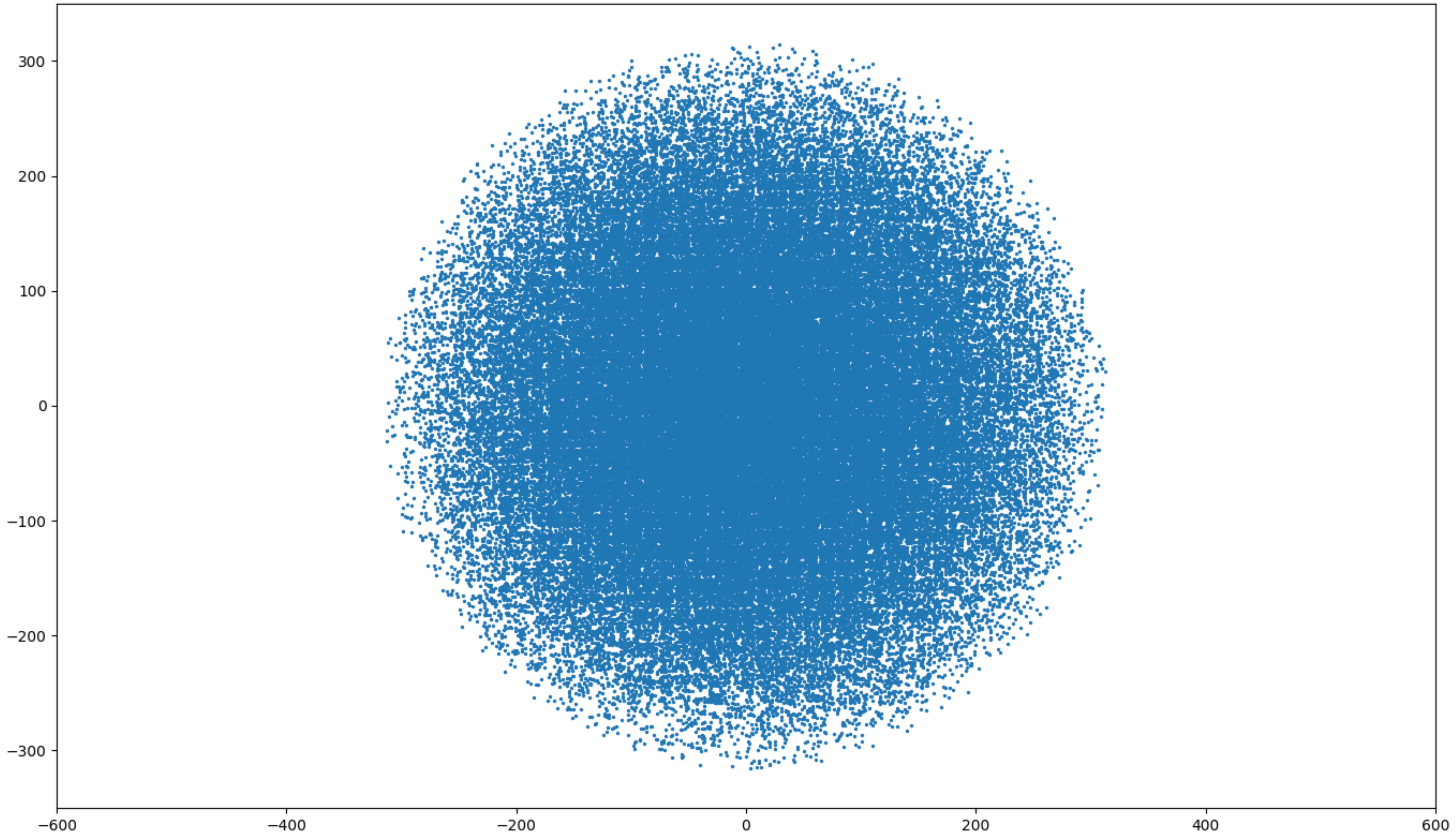
To avoid the hidden parallelepiped attack!

Take **a close** vector but not the closest.

Take the closest vector

Add a Gaussian random shift z_0

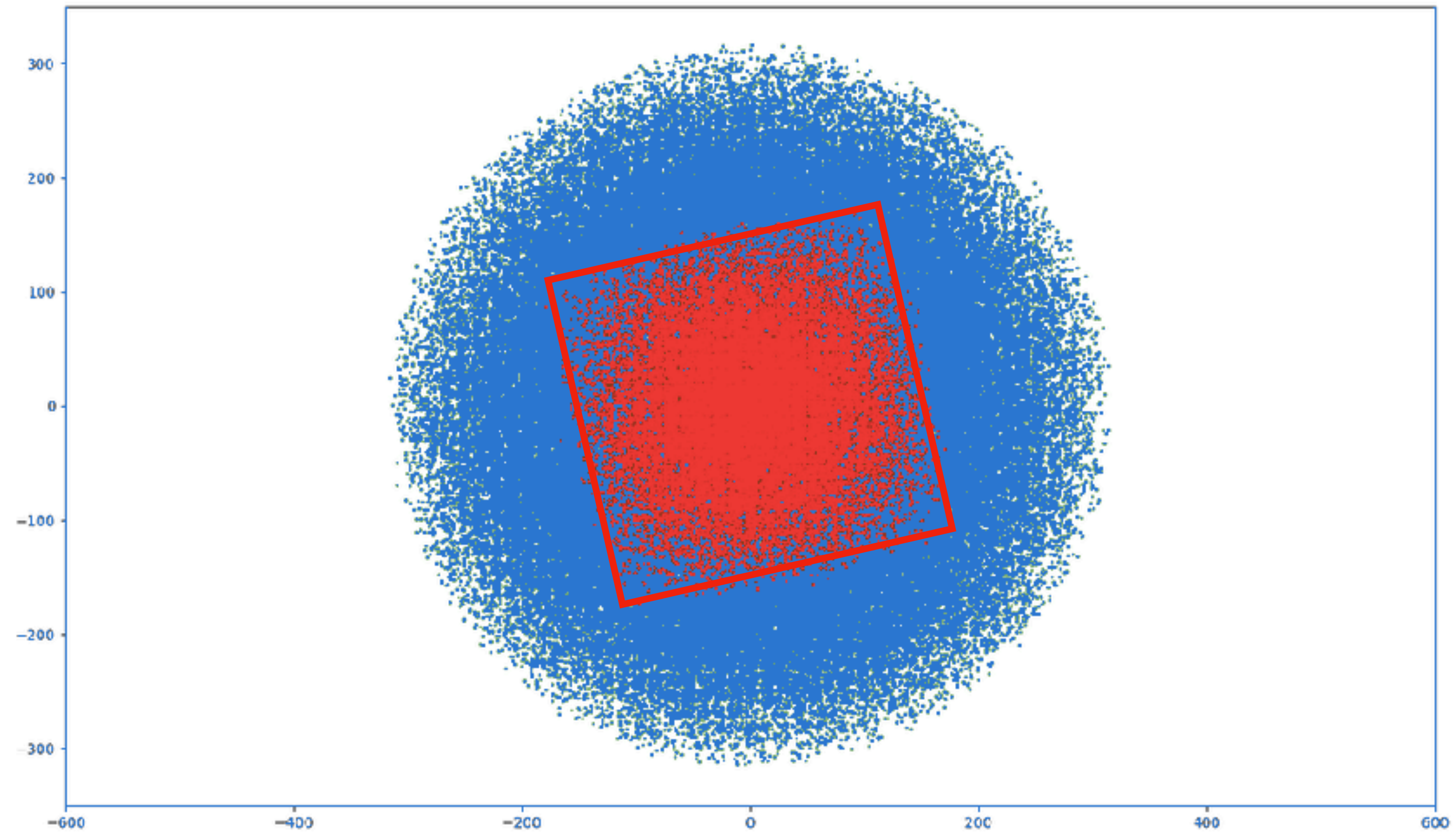
The distribution of signatures is then independent from the secret basis $\mathbf{B}$



Intuition of the power analysis attack of Falcon

Intuition of the attack

If we select the inputs such that the **Gaussian shift** is zero, we can apply the HPP attack.



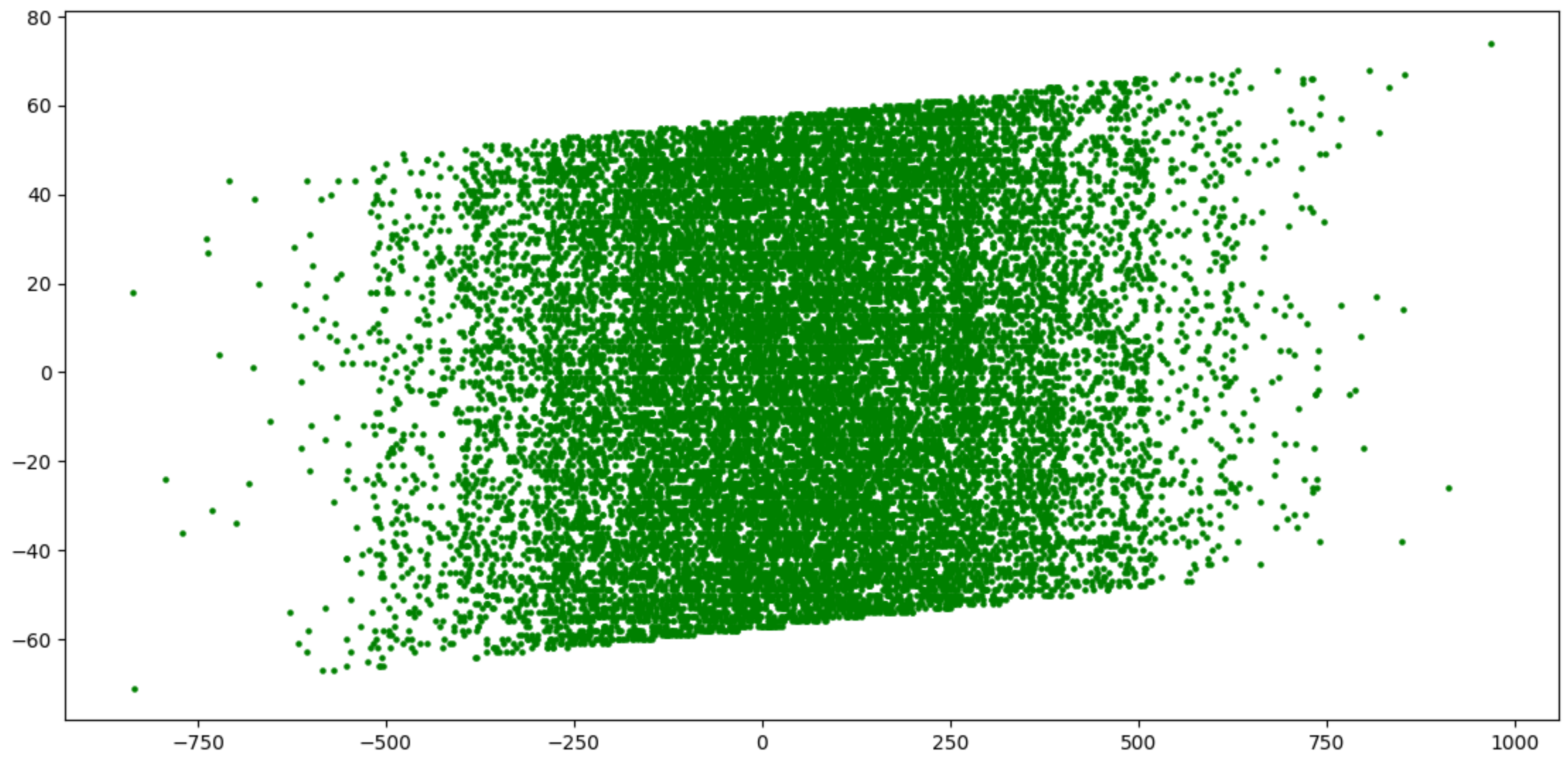
Non shifted signatures in red

What about high dimensions? There is a negligible amount of zero-shift in *all* 512 dimensions.

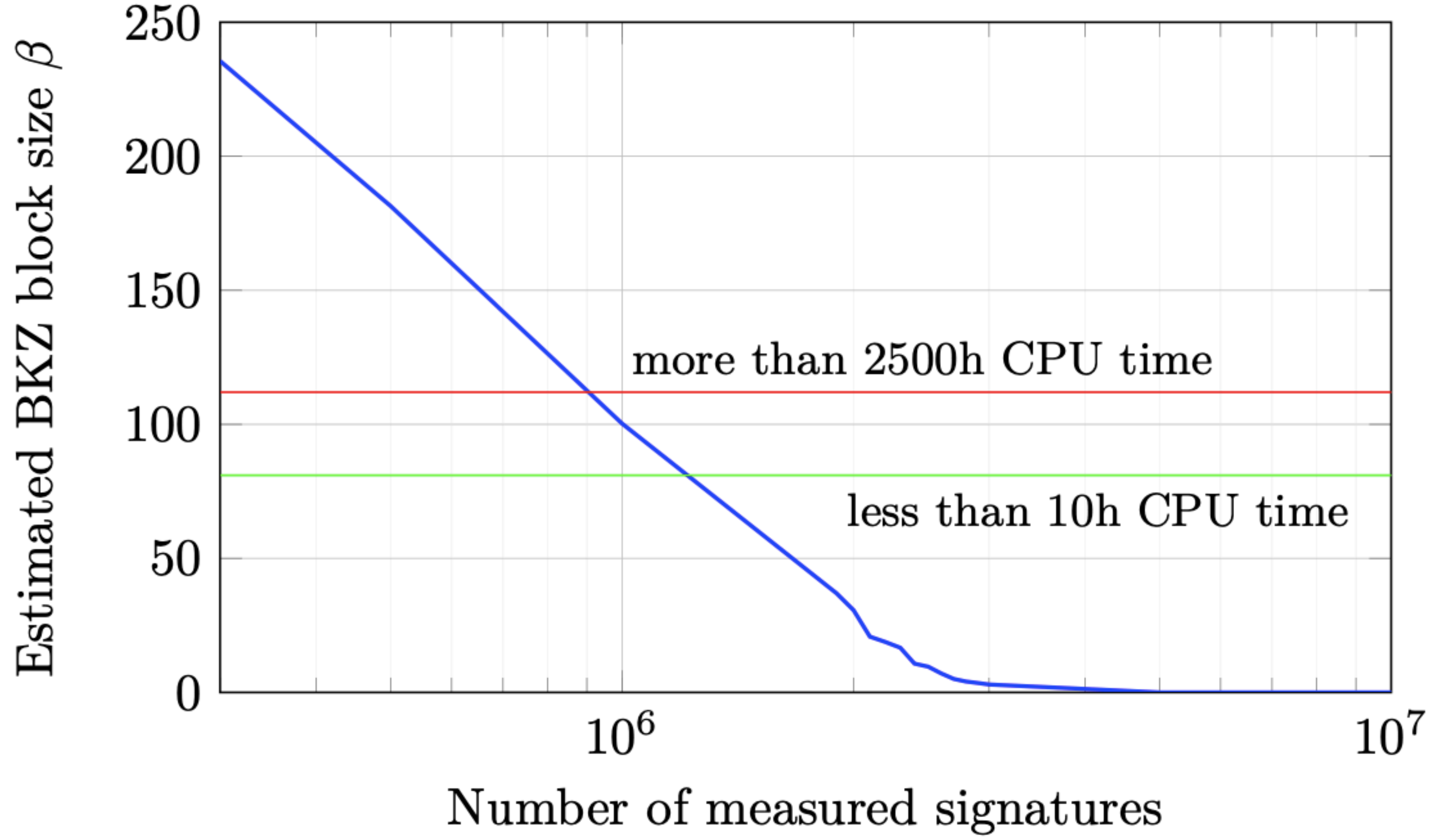
Single trace power analysis of Falcon

We focus on one dimension.
A **single trace analysis** can provide the information: shift $= 0$ or $\neq 0$.

Signatures for which shift $= 0$ in the first coordinate



Performance of the attack



➡ It is possible to apply **a partial HPP.**

We recover one vector of the basis, this is enough to **recover the full basis** thanks to the structure of the private key.

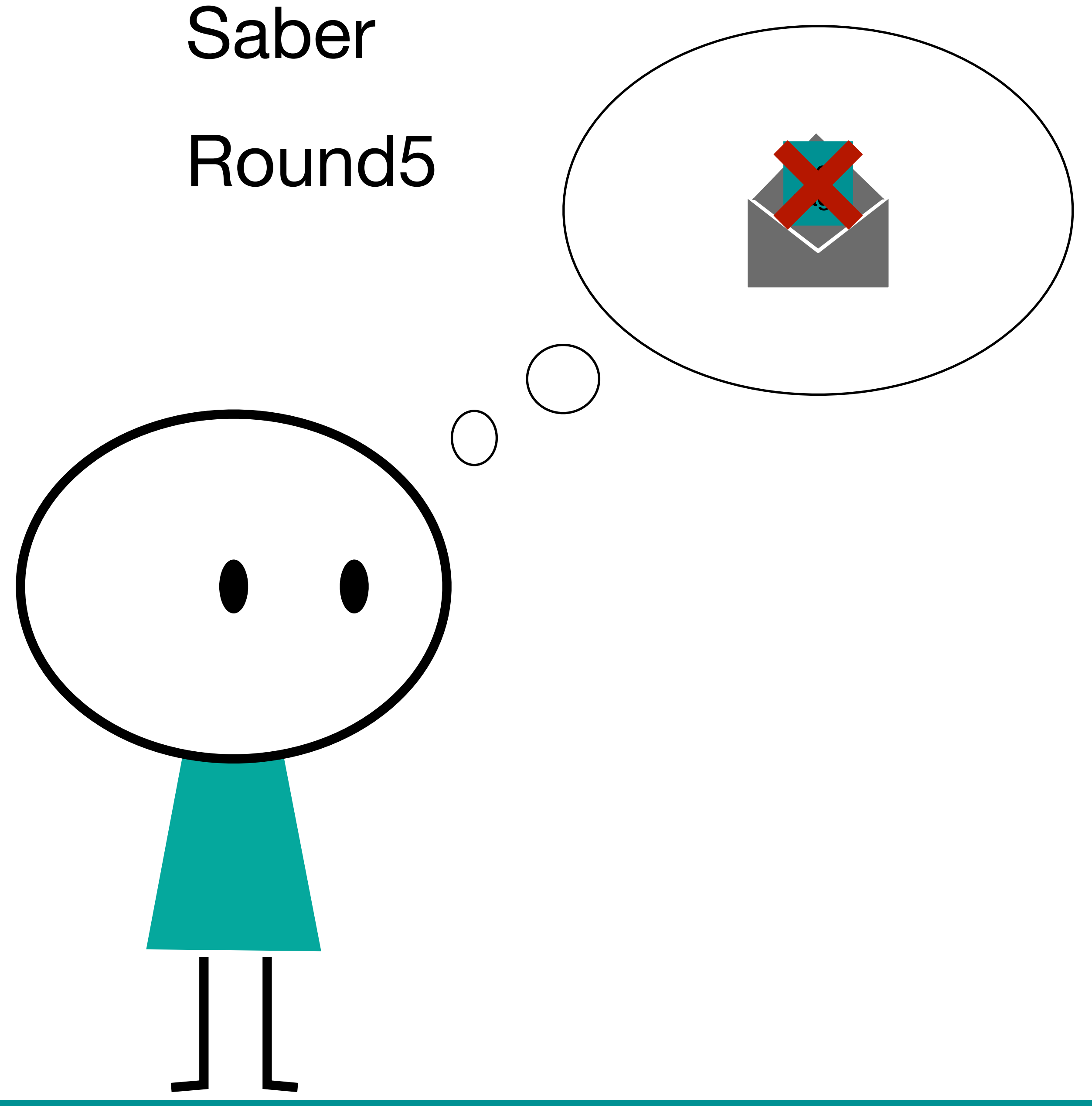
Decryption failure attacks

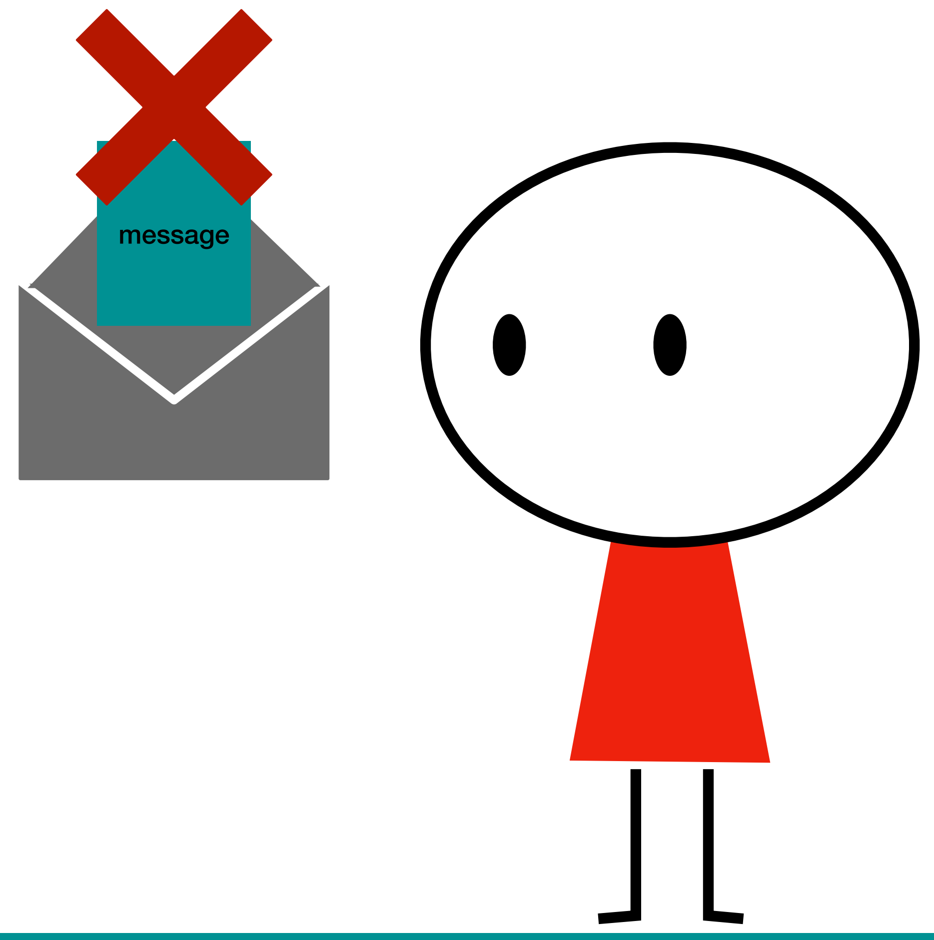
➡ Failure probability for a honest user

0	NTRU, NTRU Prime
2^{-216}	NewHope
2^{-206}	Three Bears
2^{-199}	FrodoKEM
2^{-164}	Kyber
2^{-142}	LAC
2^{-136}	Saber
2^{-117}	Round5

Extremely unlikely for honest users

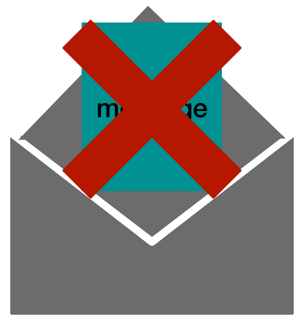
➡ But knowing that a ciphertext has triggered a failure: is it a problem?





What information do we gain from a decryption failure ?

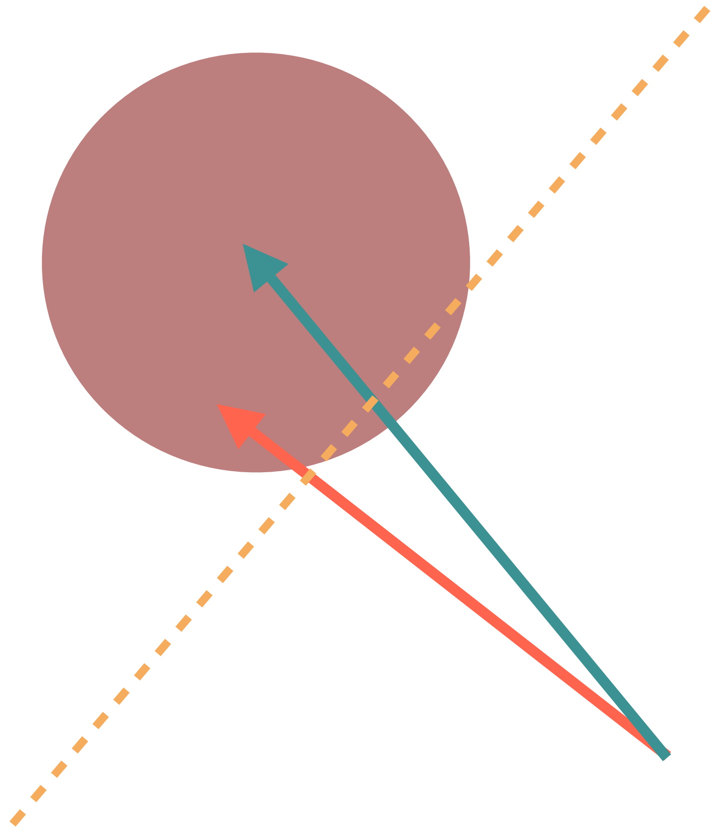
Recall that $m' \approx m + \left\lfloor \frac{2}{q}\left(\mathbf{e}^T\mathbf{z}' + \mathbf{e}'' - \mathbf{z}^T\mathbf{e}'\right) \right\rceil$

 $\iff \left\lfloor \frac{2}{q}\left(\mathbf{e}^T\mathbf{z}' + \mathbf{e}'' - \mathbf{z}^T\mathbf{e}'\right) \right\rceil \geq \frac{1}{2}$

 $: \left| \mathbf{s}^T \mathbf{w} \right| \geq \frac{q}{4}$

 $: \mathbf{s}^T \mathbf{w} \geq \frac{q}{4}$

 $: \mathbf{s} \approx k \cdot \mathbf{w}$ $\quad (\mathbf{s} = k \cdot \mathbf{w} + \epsilon)$



Approximate hint with LeakyLWEestimator

k and the standard deviation of ϵ depend on
- the standard deviation of $\mathbf{w}$
- the norm of $\mathbf{s}$, $\approx \sqrt{n}\sigma$
- the parameter q

- J.-P. D'Anvers, Q. Guo, T. Johansson, A. Nilsson, F. Vercauteren, and I. Verbauwhede. PKC'19
- Dachman-Soled, L. Ducas, H. Gong and M. Rossi. CRYPTO'2020.

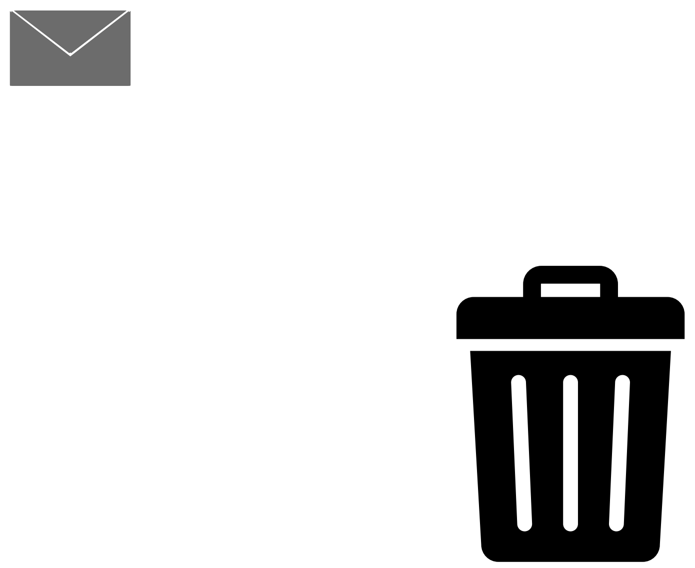
A generic decryption failure attack

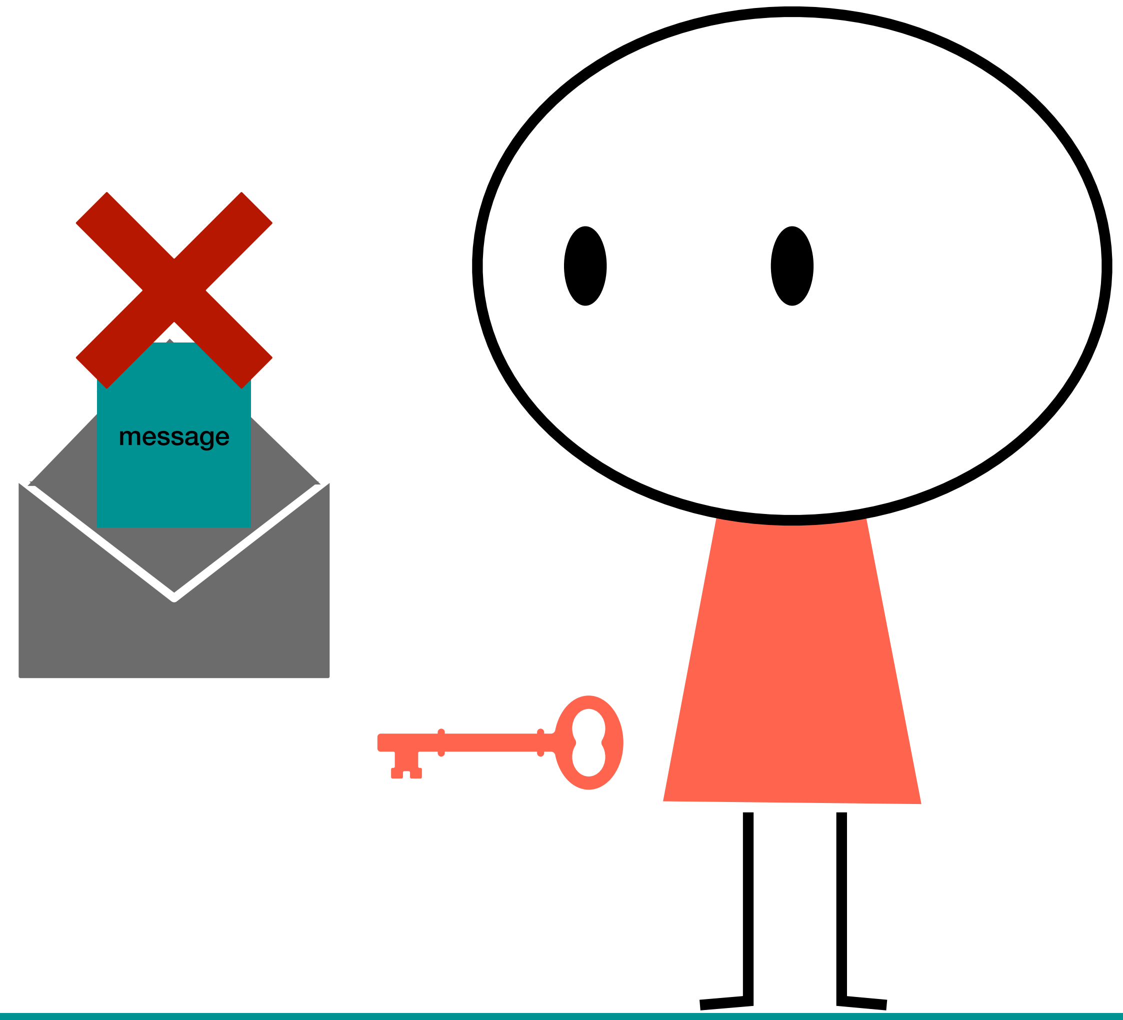
- J.-P. D'Anvers, Q. Guo, T. Johansson, A. Nilsson, F. Vercauteren, and I. Verbauwhede. PKC'19

1. **Failure Boosting :** Heavy quantum precomputation to select « weak » and submit them to decryption

2. Any provides some information on $\mathbf{z}, \mathbf{e}$

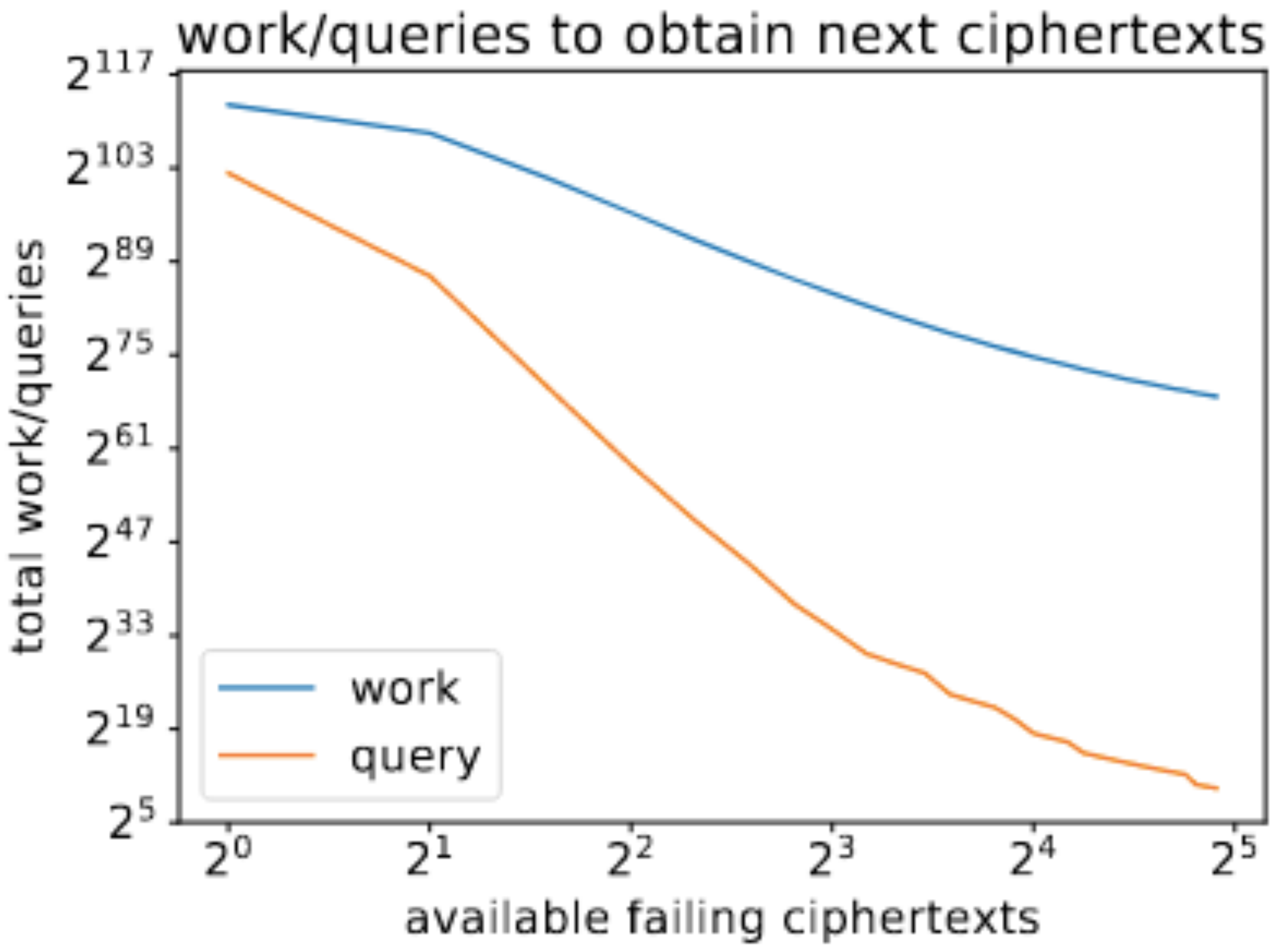
Found a weak ciphertext !





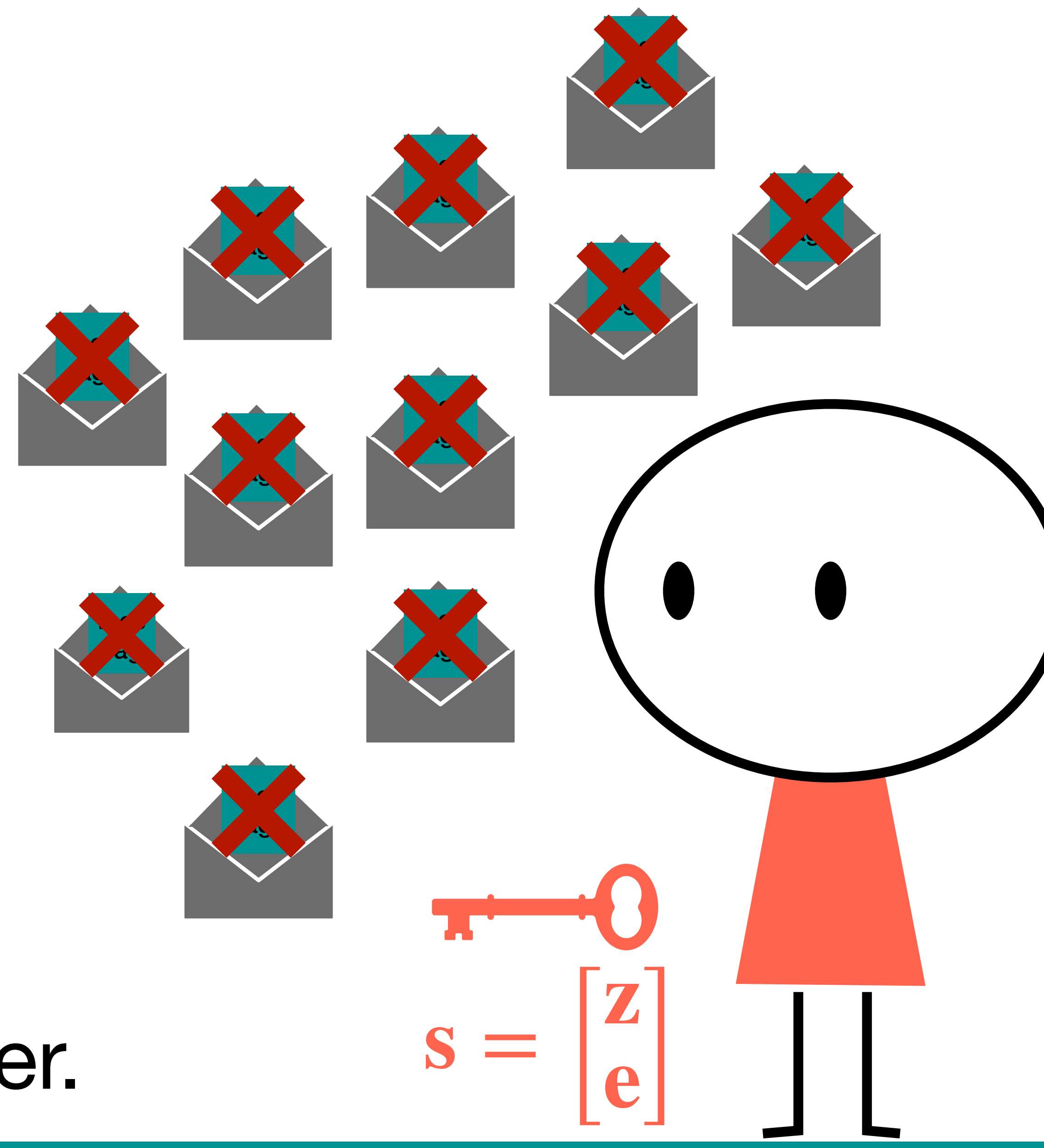
Improvement: directional failure boosting attack

Geometric criterion for selecting new failures

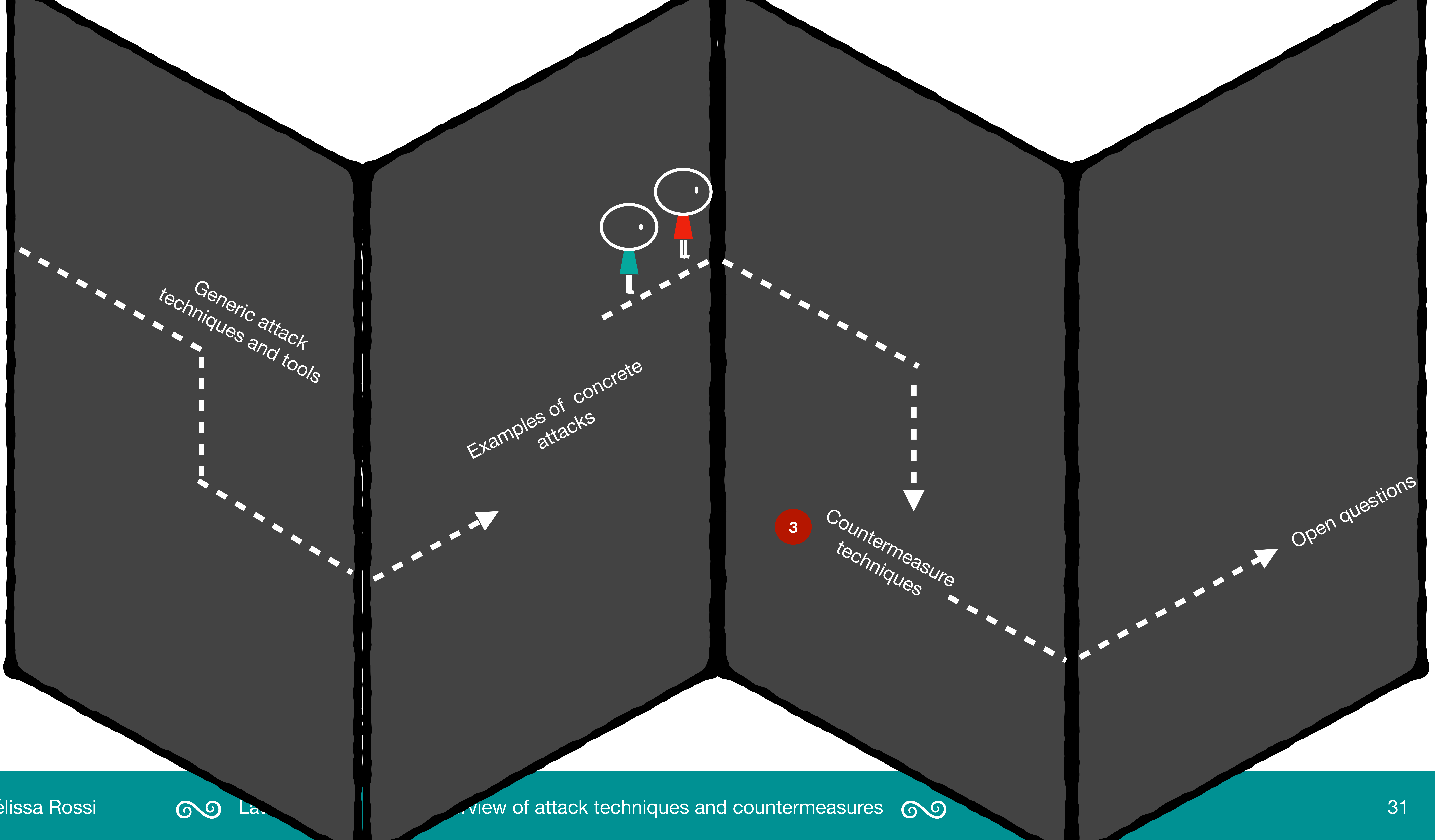


The cost is **dominated** by the search of the first failure

- ***(One) failure is not an option:***
  Bootstrapping the search for failures in lattice-based encryption schemes. EUROCRYPT'2020. J.-P. D'Anvers, M. Rossi and F. Virdia.



Once one failure happen  the selection of the subsequent  is easier.


Generic attack techniques and tools
Examples of concrete attacks
3
Countermeasure techniques
Open questions

How to remove the attack entry points

The entry points include:

- ✦ computer-science unfriendly distributions like Gaussians.
- ✦ secret-dependent internal distributions.
- ✦ numerous operations with the secret.
- ✦ nonzero failure probability.

Here are some countermeasure techniques:

- For fixing the distributions:
  1. Renyi divergence arguments
  2. Polynomial approximations
- In a generic way:
  3. Masking techniques adapted for lattices

1) Rényi divergence arguments

- S. Bai, A. Langlois, T. Lepoint, D. Stehlé, R. Steinfeld ASIACRYPT'15
- T. Prest ASIACRYPT'17

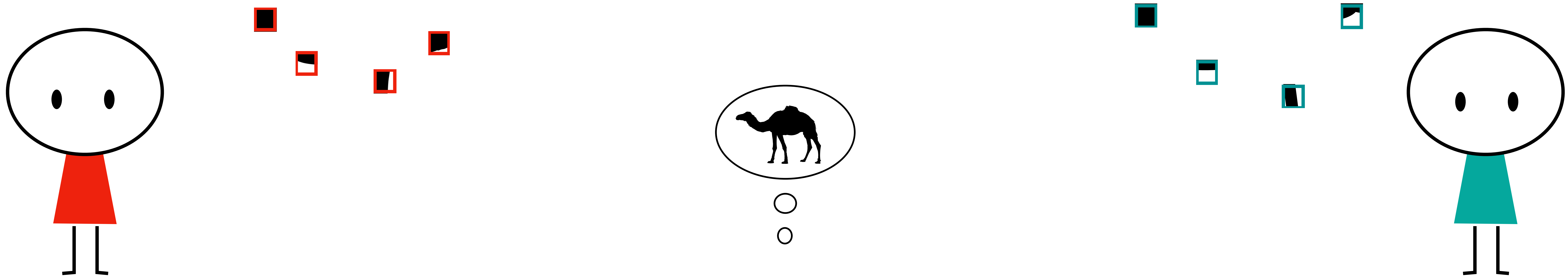
Distributions may be approximated/simplified because of the limited number of queries

Take two cryptographic schemes
- One with distribution $\mathscr{D}$
- One with an approximate distribution $\mathscr{D}'$ with the same support

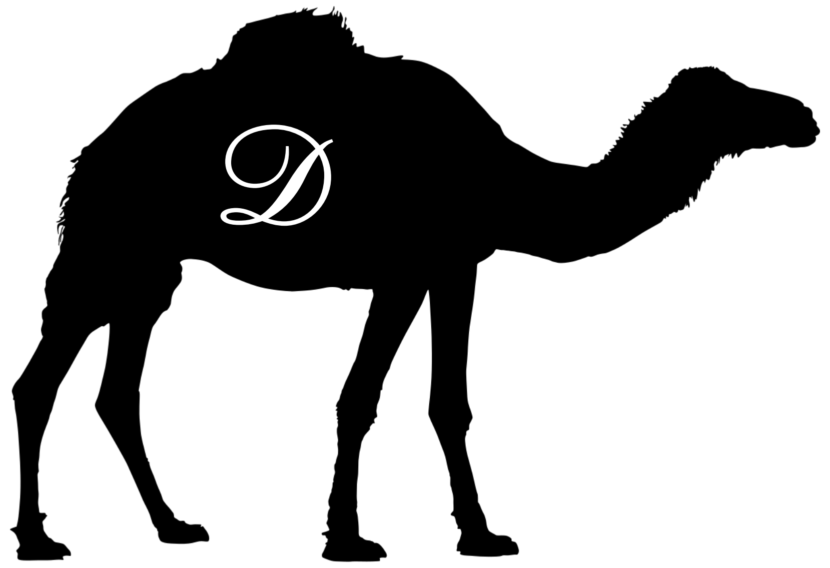
Suppose that :

1. $\mathscr{D}$ and $\mathscr{D}'$ are close enough : $\left\| 1 - \dfrac{\mathscr{D}'}{\mathscr{D}} \right\|_\infty \leq 2^{-K}$
2. the number of sample queries is bounded

Then, the **bit security will remain almost the same.**



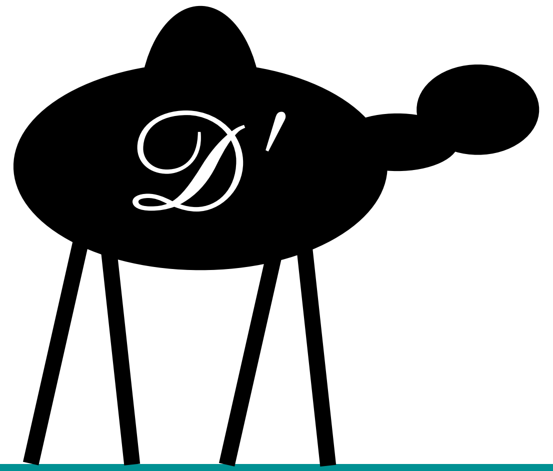
2) Polynomial approximation for Gaussians



Transcendental function

Polynomial approximation

Degree d polynomial in $\mathbb{Z}[x]$ with small coefficients



- **Taylor expansion** $\mathscr{D}'(x) = \mathscr{D}(0) + \mathscr{D}^{(1)}(0) \cdot x + \cdots + \frac{\mathscr{D}^{(d)}(0)}{d!} \cdot x^d$
- **Padé approximants** (rational function approximation)
  - T. Prest ASIACRYPT'17

  Two polynomials, higher degrees $\mathscr{D}'(x) = \frac{P(x)}{Q(x)}$
- **Minimax computations** : Sollya software package
  - N. Brisebarre and S. Chevillard IEEE'07
  - S. Chevillard, M. Joldes and C. Q. Lauter ICMS'10
  - R. Zhao, R. Steinfeld and A. Sakzad IEEE'19

  Floating point arithmetics $$\mathscr{D}' = \arg \min_{\deg(P) \leq d} \left(\sup_{x \in I} \left(1 - \frac{P(x)}{\mathscr{D}(x)} \right) \right)$$
- **Projections with respect to the Sobolev Norm**
  - *GALACTICS [...]* ACM-CCS'2019. G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi and M. Tibouchi.

$$\|f\|_\infty \leq \sqrt{2} \cdot \|f\|_S$$

Examples of application of such tools

Falcon Performance penalty factor : $+50\ \%$

- J. Howe, T. Prest, T. Ricosset and M. Rossi. PQ-CRYPTO'2020.
- *T. Pornin https://falcon-sign.info/falcon-impl-20190802.pdf*

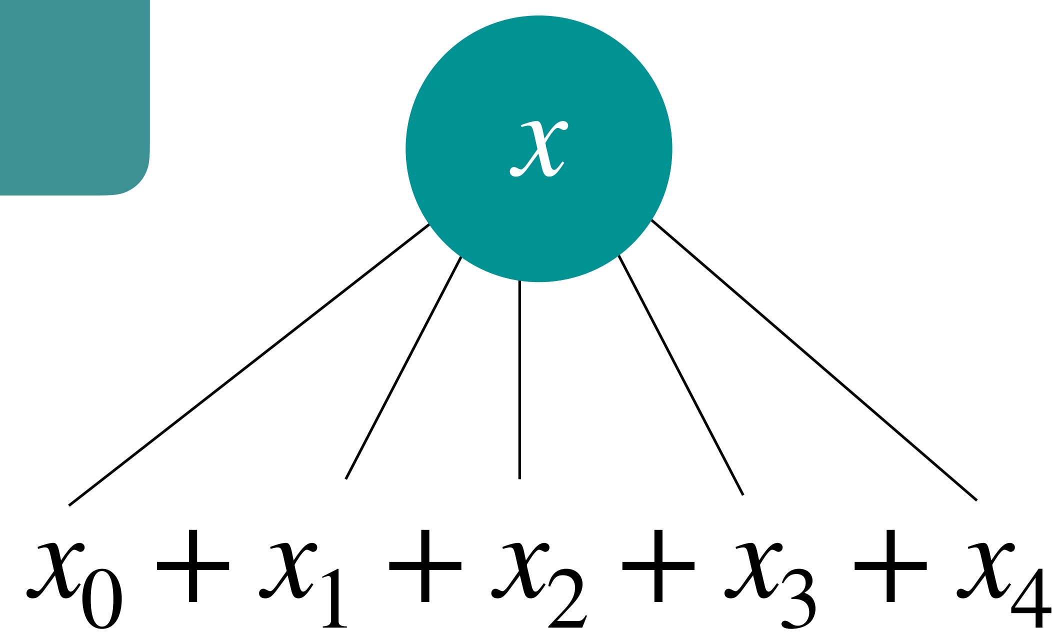
BLISS Performance penalty factor : $+13\ \%$

- G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi and M. Tibouchi. ACM-CCS'2019.

Masking lattice-based schemes

Designs for the multiplication of two shared values

- L. Goubin and J. Patarin CHES'1999
- S. Chari, C. Jutla, J. Rao and P. Rohatgi CRYPTO'1999

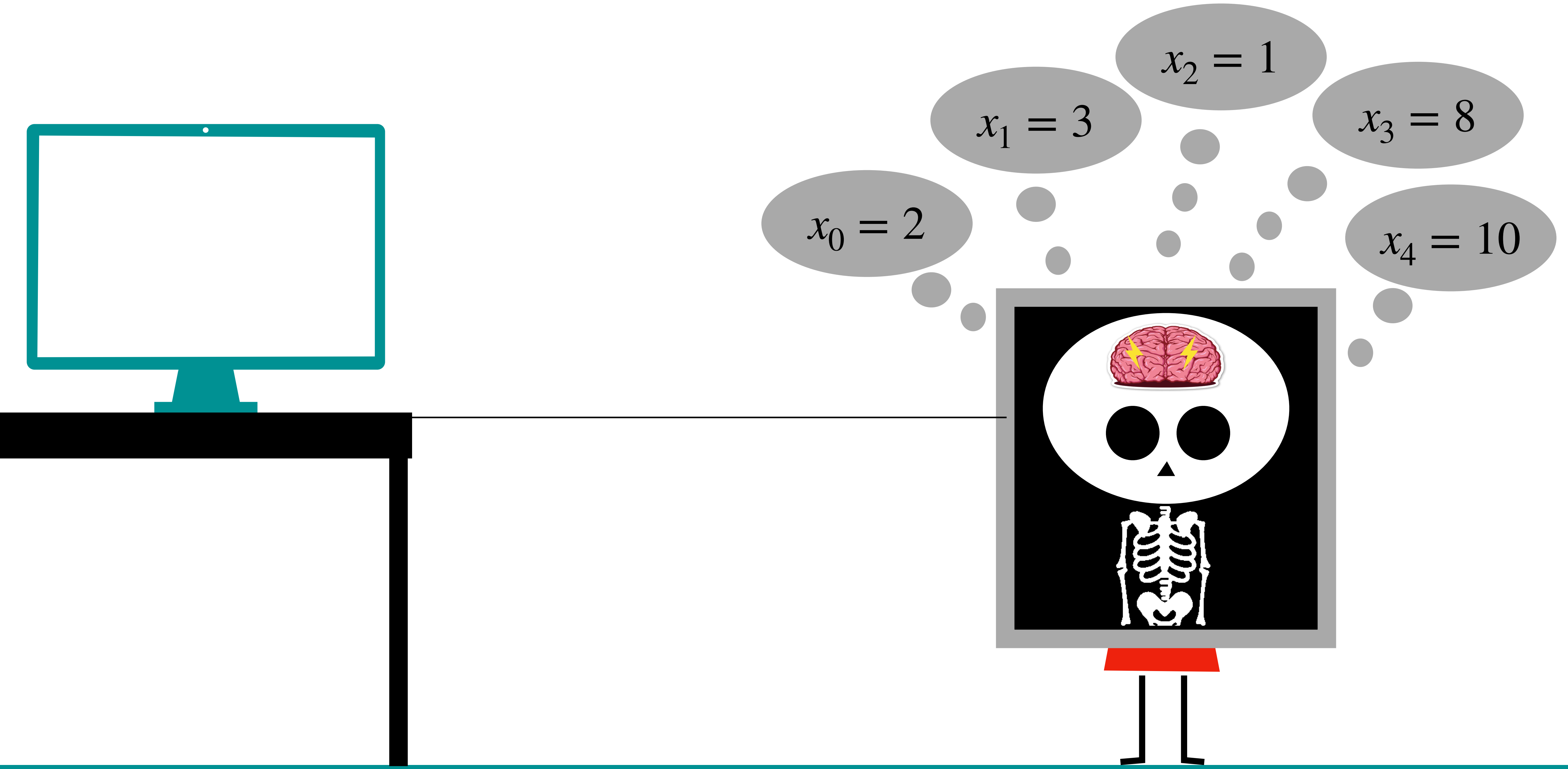


Each share looks random.

The only way to recover x is to know all of them.

Masking order : $d = 4$.

➡ Increase of the noise: Highly complicates the dependancies between the secret and the measurement



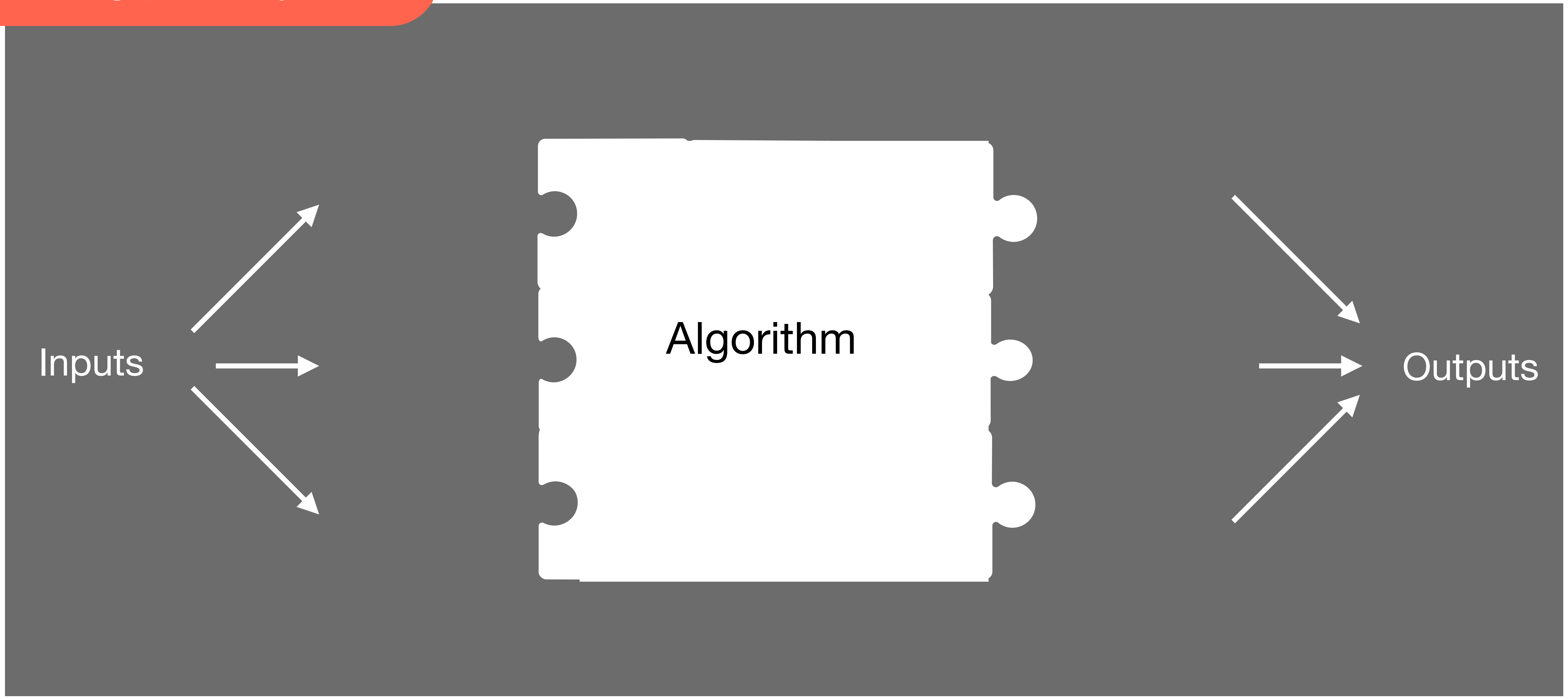
The real secret value is

$$x = 2 + 3 + 1 + 8 + 10$$
$$= 24$$

Masking lattice-based schemes

- Y. Ishai, A. Sahai and D. Wagner CRYPTO'2003
- G. Barthe, S. Belaıd, F. Dupressoir, P.-A. Fouque, B. Grégoire, P.-Y. Strub, and R. Zucchini. ACM-CCS'2016

Masking proof system



Proofs of masking for each gadget
+
Composition proofs

Masking for lattice-based cryptography

Need for lattice adapted gadgets

- Uniform random generation
- Gaussian generation
- Rejection sampling

Signature-adapted security property

Non-interference with public outputs

Examples of overhead on the number of cycles for qTesla signature scheme

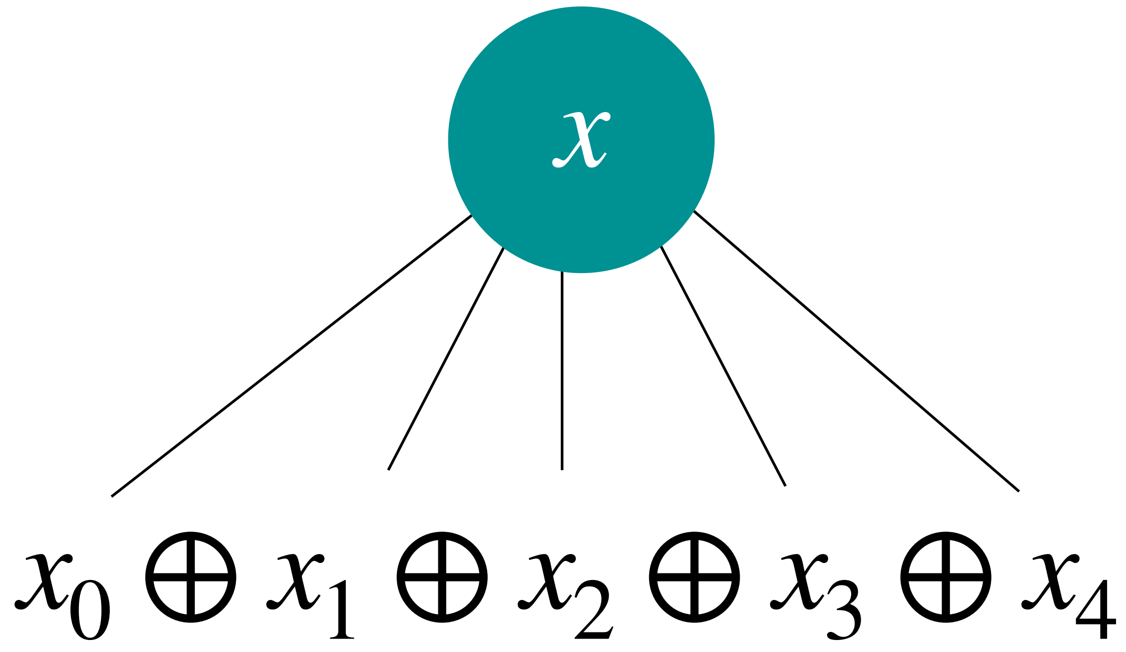
Unmasked	Order 1	Order 2	Order 3	Order 4
1	$\times 4$	$\times 21$	$\times 37$	$\times 60$

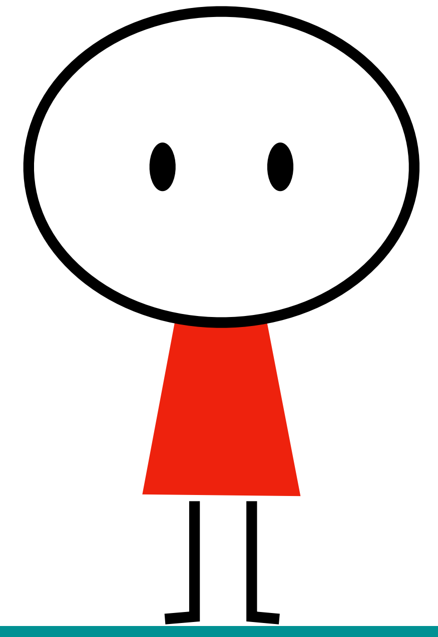
- F. Gérard and M. Rossi. CARDIS'2019.

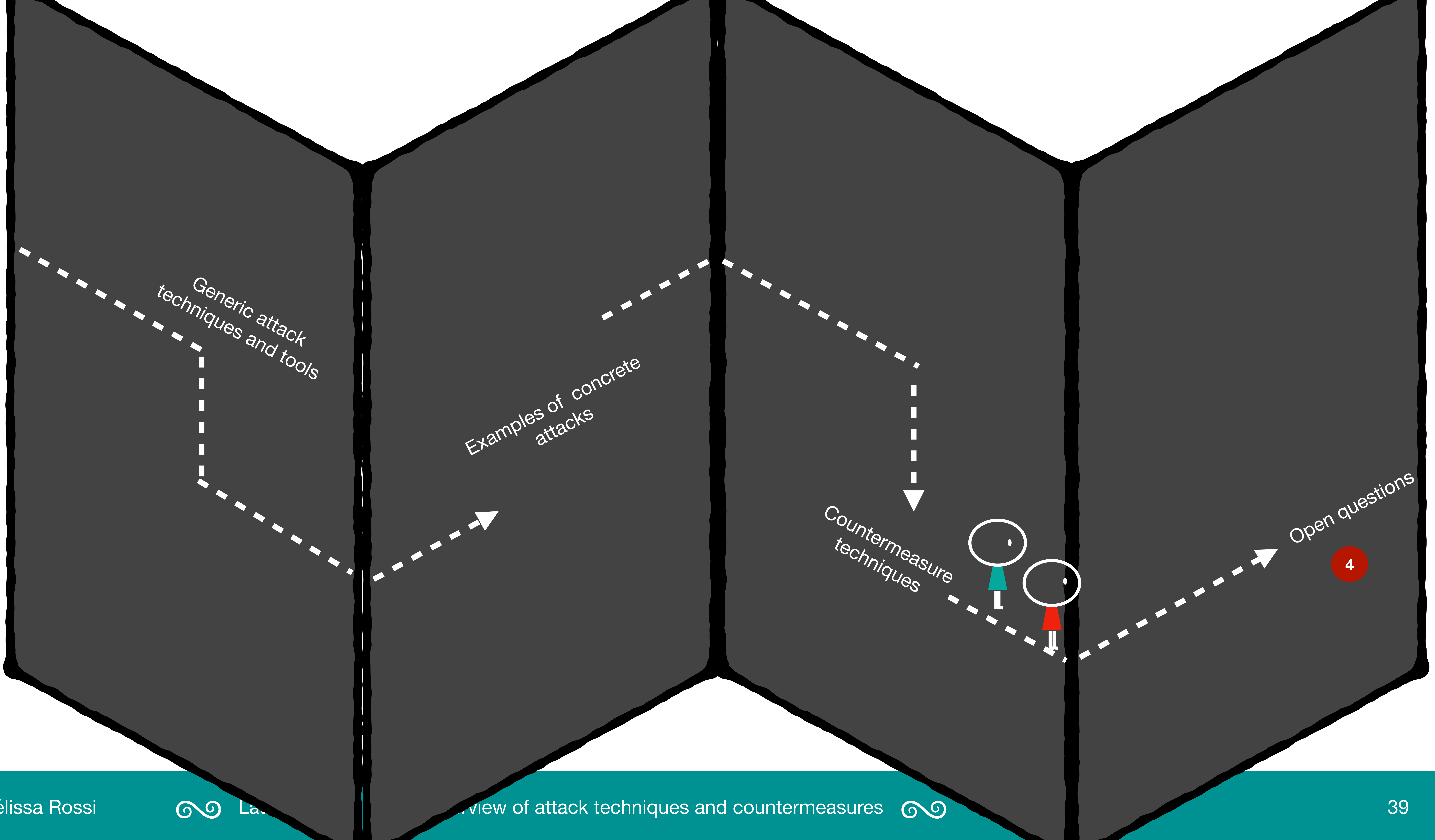
- G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, B. Grégoire, M. Rossi and M. Tibouchi. EUROCRYPT'2017.
- G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi and M. Tibouchi. ACM-CCS'2019.
- T. Espitau, P.-A. Fouque, F. Gérard, M. Rossi, A. Takahashi, M. Tibouchi, A. Wallet, Y. Yu EUROCRYPT'2022

The constructions must use mask conversions

- J.-S. Coron, J. Großschädl and P. K. Vadnala CHES'2014
- J.-S. Coron, J. Großschädl, M. Tibouchi, and P. K. Vadnala FSE'2015
- J.-S. Coron CHES'2017






Generic attack techniques and tools
Examples of concrete attacks
Countermeasure techniques
Open questions
4

Open problems

Masking friendly design

The designs contain many « masking unfriendly » features: Gaussian distributions, uniform small distributions, comparison of sensitive values, rejection, prime modulus…

➡ Schemes designs that minimize the masking overhead at a cost of less efficient unmasked version.

Fujisaki-Okamoto transform

This transform is needed because it protects against active attacks (IND-CCA2 security) but it highly increases the attack surface and introduces new attack entry points.

➡ Is re-encryption (or similar tests) inevitable?
➡ Is it possible to design a fully protected generic Fujisaki-Okamoto transform?

Other entry points

➡ Are lattice-based schemes fault-resilient?

Blackbox attacks

➡ Cryptanalysis of ideal lattices

Des questions?

FRANCE CYBERSECURITY
CHALLENGE

➡ du **vendredi 29 avril 2022 à 14h jusqu'au dimanche 8 mai 2022 à 18h**.

➡ moins de 25 ans? Vous pouvez être sélectionnés pour l'équipe de France

➡ Plus d'infos sur : https://www.ssi.gouv.fr/agence/cybersecurite/france-cybersecurity-challenge-2022/