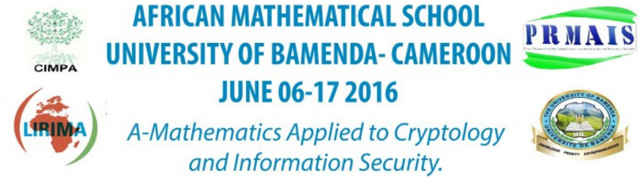
Lattice based Cryptography

Léo Ducas

CWI, Amsterdam, The Netherlands



Outline

Encryption

Problem:

- Two parties **A** and **B** wish to communicate

Encryption

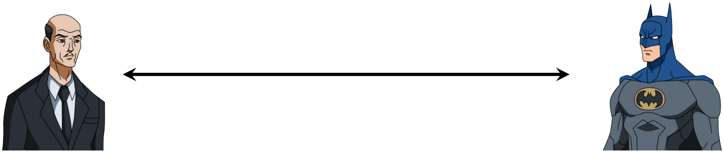
Problem:

- Two parties **A** and **B** wish to communicate

Encryption

Problem:

- Two parties **A** and **B** wish to communicate



Encryption

Problem:

- Two parties **A** and **B** wish to communicate
- An adversary, **J** trying to eavrop

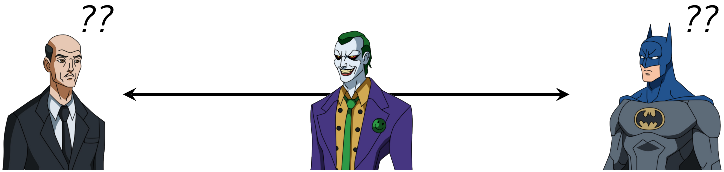
Encryption

Problem:

- Two parties **A** and **B** wish to communicate
- An adversary, **J** trying to eavrop

Problem:

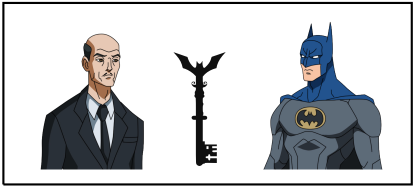
- Two parties **A** and **B** wish to communicate
- An adversary, **J** trying to eavrop
- **A** and **B** want to keep confidentiality



Encryption

Solution : Symmetric cryptography

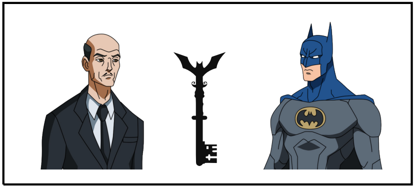
- **A** and **B** agree on a secret key **k** in a close room



Encryption

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room



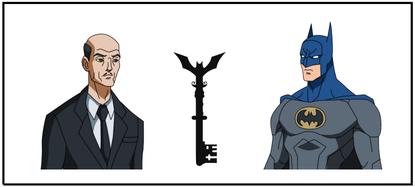
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication

$\boxed{\mathcal{E}}$ $\boxed{\mathcal{D}}$

Encryption

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room

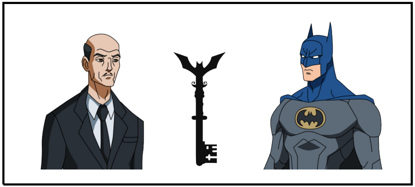


- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication

Encryption

Solution : Symmetric cryptography

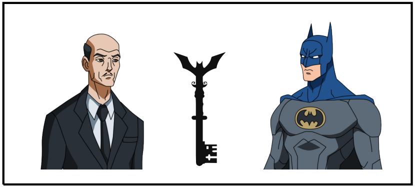
- **A** and **B** agree on a secret key **k** in a close room



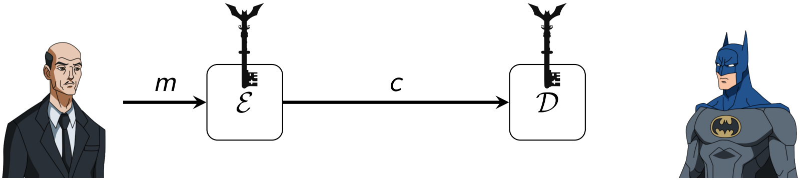
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room



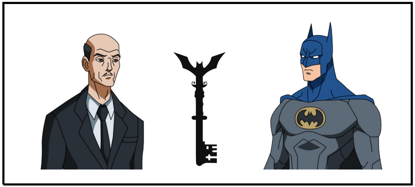
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication



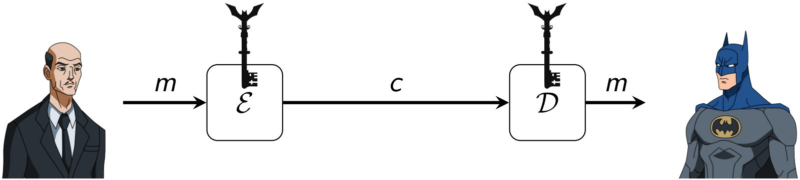
Encryption

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room



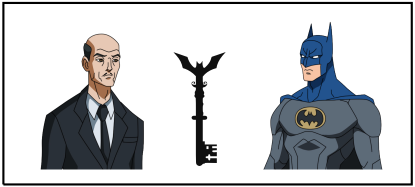
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication



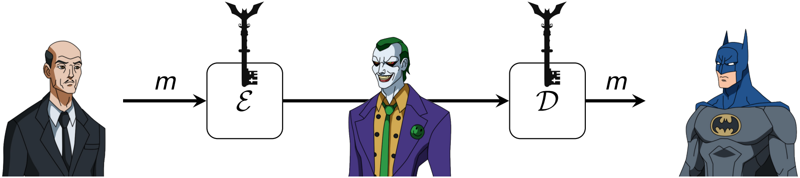
Encryption

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room



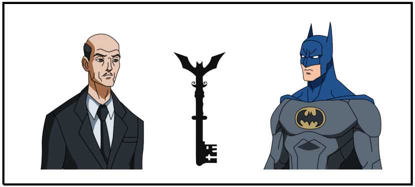
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication



Encryption

Solution : Symmetric cryptography

- **A** and **B** agree on a secret key **k** in a close room

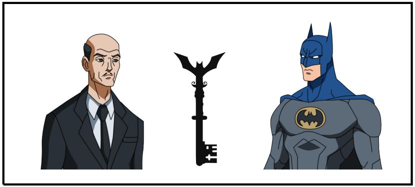


- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication

Encryption

Solution : Symmetric cryptography

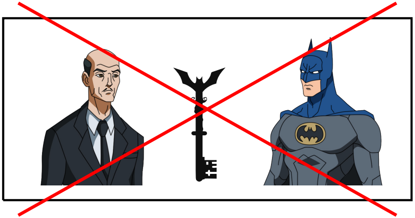
- **A** and **B** agree on a secret key **k** in a close room



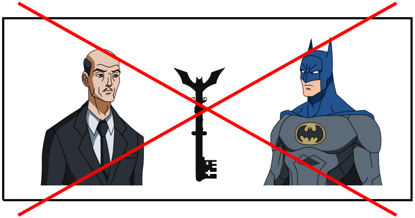
- Latter, **A** and **B** encrypt $\mathcal{E}$ and decrypt $\mathcal{D}$ their communication

Asymmetric cryptography

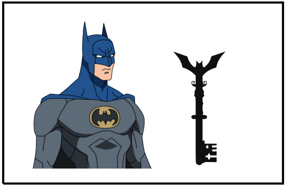
Probleme : Confidentiality without pre-shared key ?



Probleme : Confidentiality without pre-shared key ?

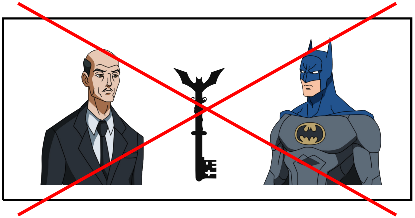


Solution : Make encryption and decryption key different

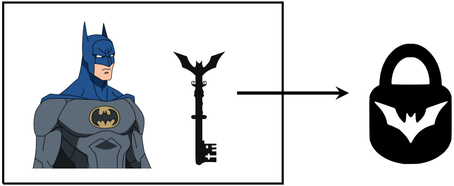


Asymmetric cryptography

Probleme : Confidentiality without pre-shared key ?

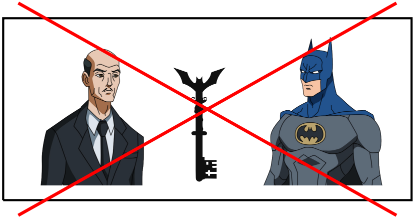


Solution : Make encryption and decryption key different

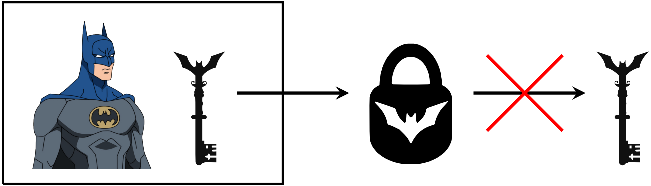


Asymmetric cryptography

Probleme : Confidentiality without pre-shared key ?



Solution : Make encryption and decryption key different

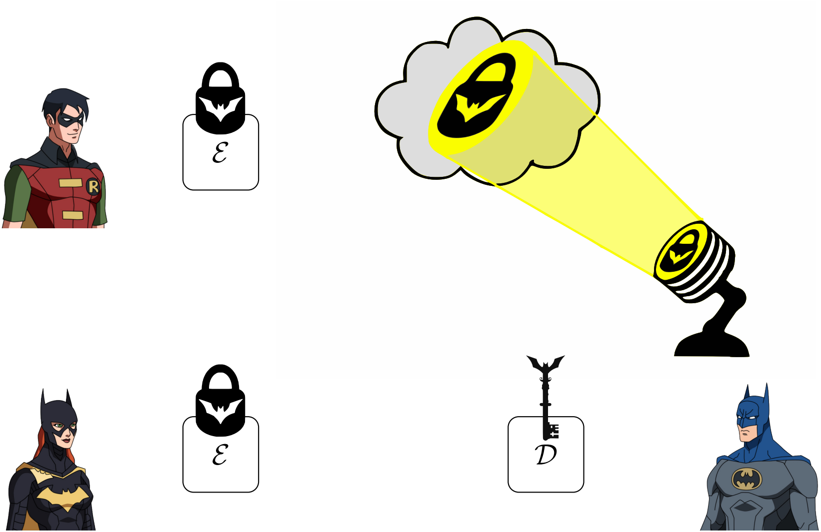


The transformation **private key** → **public key** must be **one-way**.

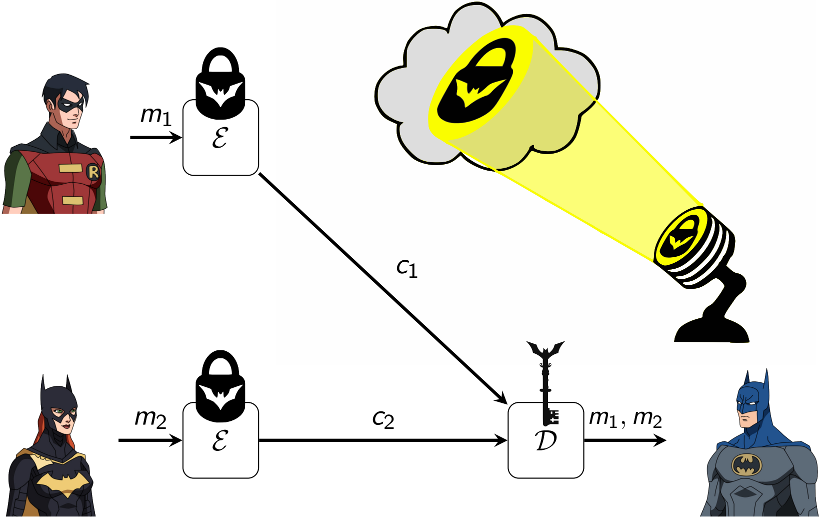
Asymmetric cryptography in action

Asymmetric cryptography in action

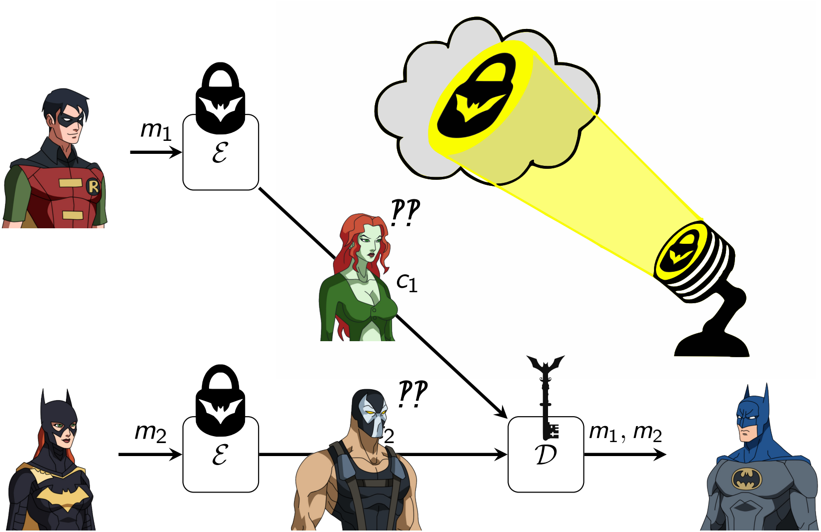
Asymmetric cryptography in action



Asymmetric cryptography in action

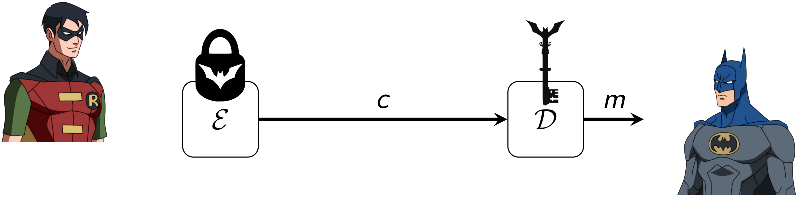


Asymmetric cryptography in action

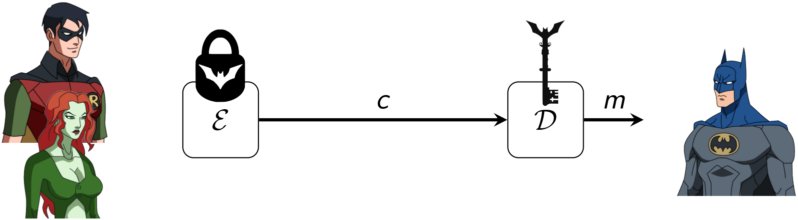


Outline

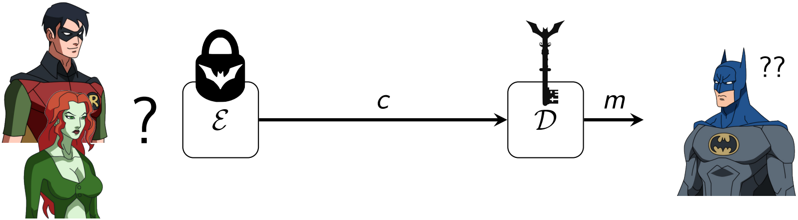
Problem 1: Message authentication



Problem 1: Message authentication

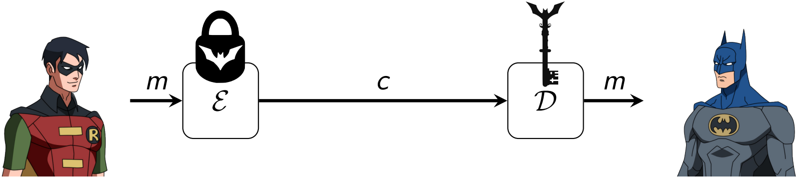


Problem 1: Message authentication

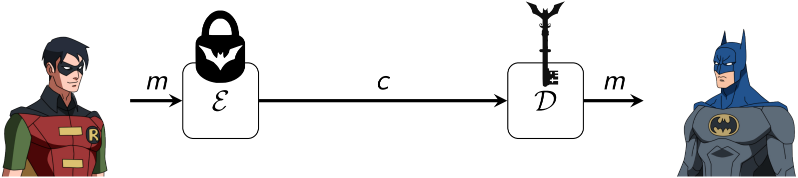


Encryption guarentees confidentiality, but not authenticity:
Poison Ivy can pretend to be Robin

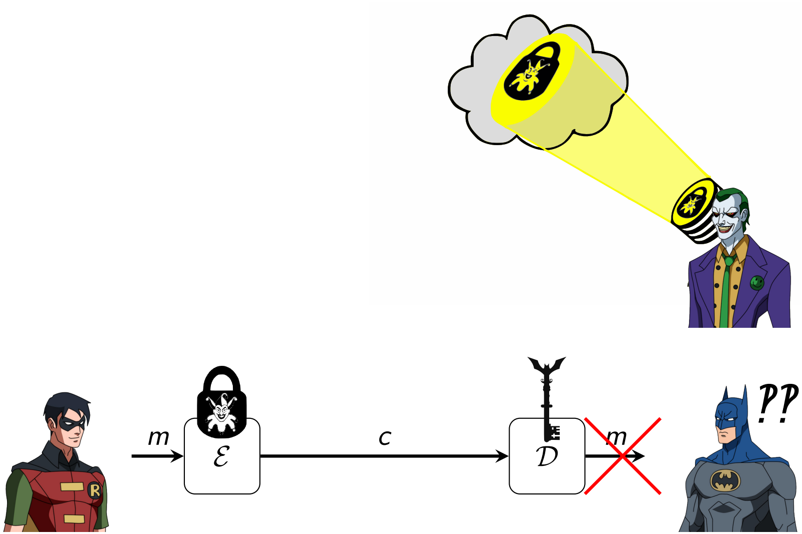
Problem : Key authentication



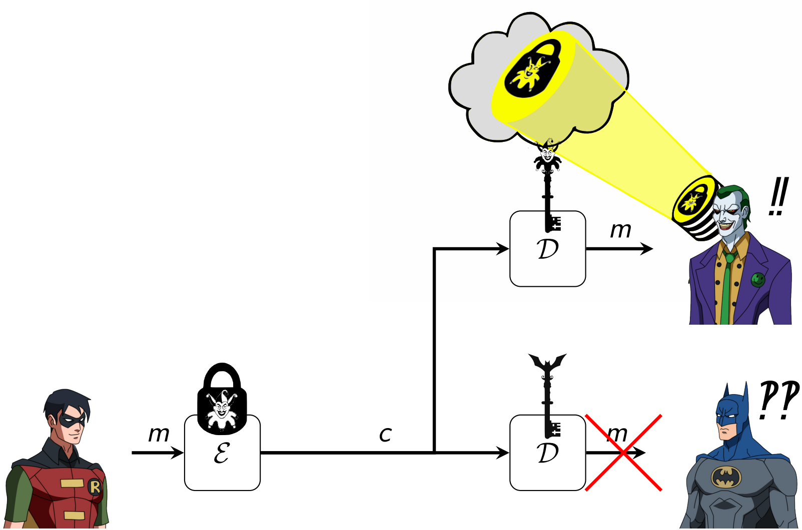
Problem : Key authentication



Problem : Key authentication



Problem : Key authentication



Without authenticity of public key, encryption can be insecure !

Digital signature

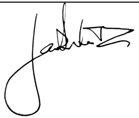
Digital version of signature, or a certificate. Must be

- **impossible to forge**
- **verifiable** by all (using some public key)

Secret key

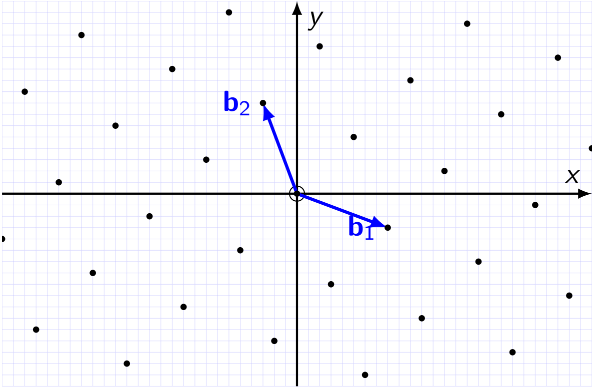
Public key

Signature



Outline

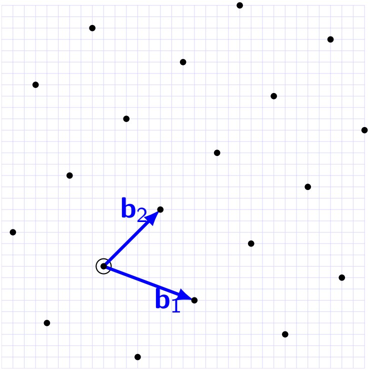
Lattices !



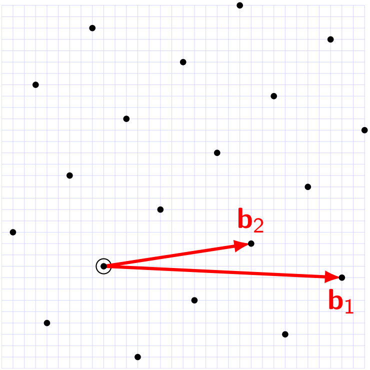
Definition

A lattice L is a discrete subgroup of a finite-dimensional Euclidean vector space.

Bases of a Lattice



Good Basis $\mathbf{G}$ de L



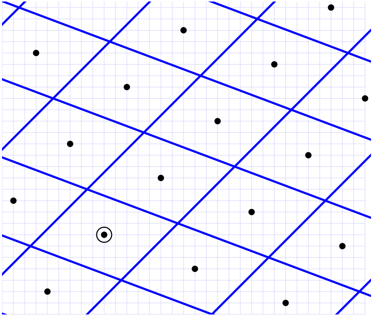
Bad Basis $\mathbf{B}$ de L

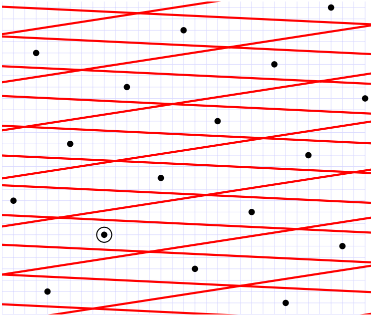
$\mathbf{G} \rightarrow \mathbf{B}$: easy (randomization);

$\mathbf{B} \rightarrow \mathbf{G}$: hard (LLL, BKZ, Lattice Sieve...).

Bases and Fundamental Domains

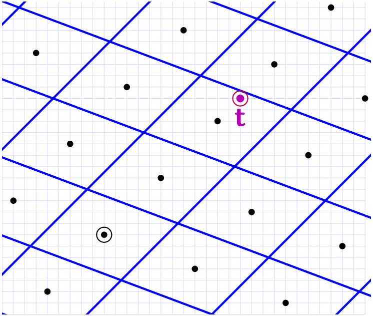
Each Basis defines a **parallelepipedic tiling**.

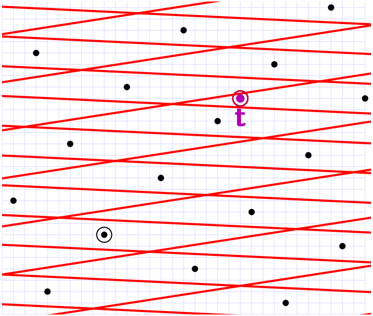




Round'off Algorithm [Lenstra, Babai]:

Each Basis defines a **parallelepipedic tiling**.

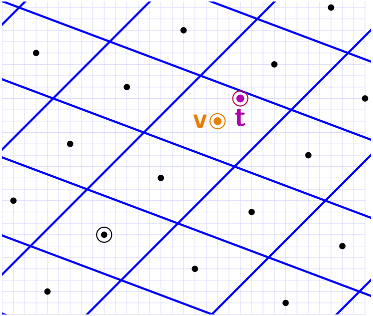


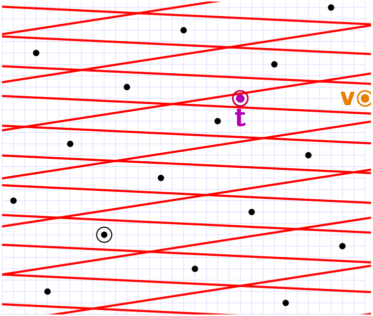


Round'off Algorithm [Lenstra, Babai]:

- Given a target **t**

Each Basis defines a **parallelepipedic tiling**.

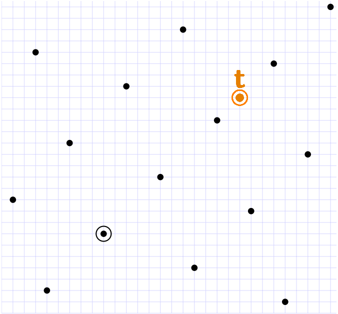




Round'off Algorithm [Lenstra, Babai]:

- Given a target **t**
- Find's **v** $\in L$ at the center the tile.

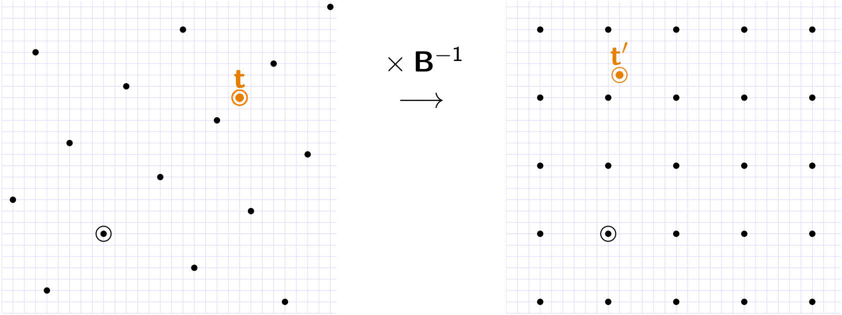
Round'off Algorithm



$\longrightarrow$

Round'off Algorithm [Lenstra,Babai]:

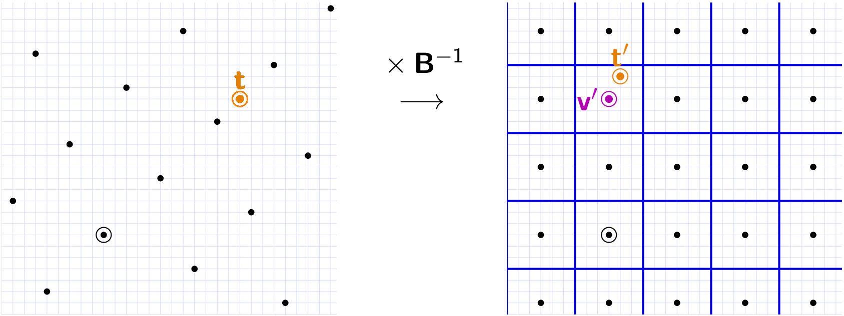
Round'off Algorithm



Round'off Algorithm [Lenstra,Babai]:

- Use $\mathbf{B}$ to switch to the lattice ^{n} $(\times \mathbf{B}^{-1})$

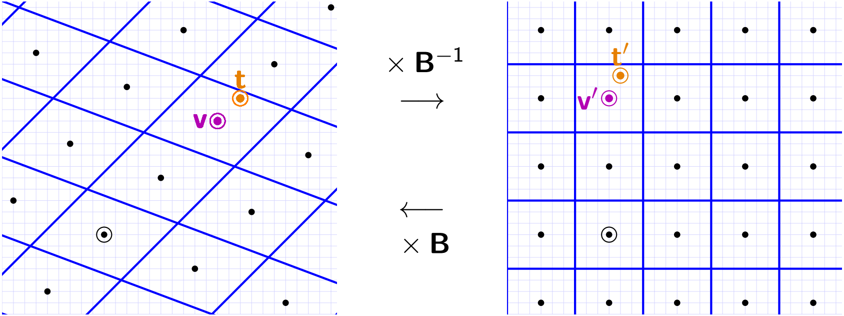
$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t};$$



Round'off Algorithm [Lenstra,Babai]:

- Use $\mathbf{B}$ to switch to the lattice ^{n} $(\times \mathbf{B}^{-1})$
- round each coordinate (square tiling)

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil;$$



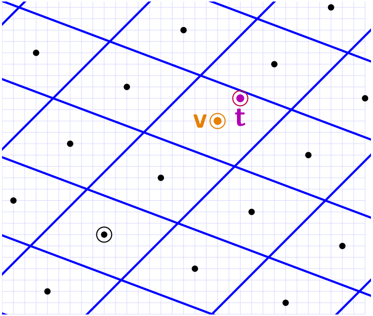
Round'off Algorithm [Lenstra,Babai]:

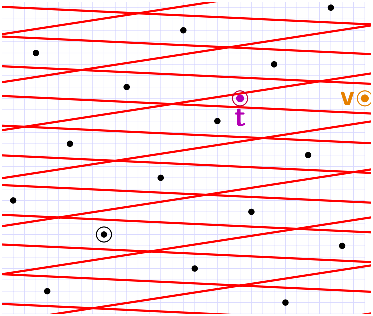
- Use $\mathbf{B}$ to switch to the lattice ^{n} $(\times\mathbf{B}^{-1})$
- round each coordinate (square tiling)
- switch back to L $(\times\mathbf{B})$

$$\mathbf{t}' = \mathbf{B}^{-1}\cdot\mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B}\cdot\mathbf{v}'$$

Finding Close Vectors

Given a good basis **G** the Round'off algorithm allows to solve CVP.
Given only a bad basis **B**, tsolving CVP is a **hard problem**.





Can this somehow be used as a trapdoor ?

Encryption from lattices (simplified)

Using the (second) decoding algorithm, on can recover $\mathbf{v}, \mathbf{e}$ from $\mathbf{w} = \mathbf{v} + \mathbf{e}$ when $\mathbf{e} \in \mathcal{P}(\mathbf{B}^*)$. In particular when:

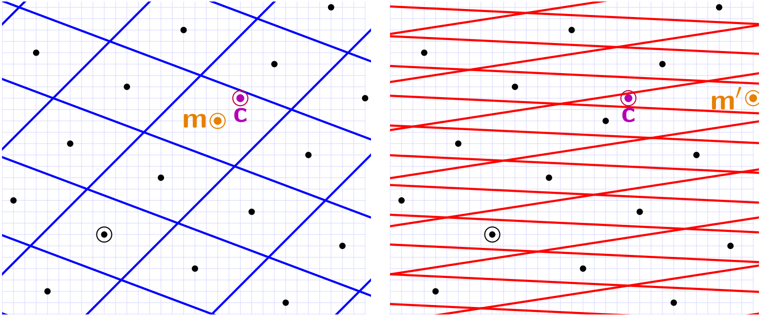
$$\|\mathbf{e}\| \leq \min \|\mathbf{b}_i^*\|$$

Parameter η

- Private key: good basis $\mathbf{G}$ such that $\|\mathbf{g}_i^*\| \geq \eta$
- Public key: bad basis $\mathbf{B}$ such that $\|\mathbf{b}_i^*\| \ll \eta$
- Message : $\mathbf{m} \in \Lambda = \mathcal{L}(\mathbf{B}) = \mathcal{L}(\mathbf{G})$
- Ciphertext : $\mathbf{c} = \mathbf{m} + \mathbf{e}$, for a random error $\mathbf{e}$, $\|\mathbf{e}\| = \eta$
- Decryption : $(\mathbf{m}', \mathbf{e}) = \mathit{decode}(\mathbf{c})$

Encryption from lattices

Decryption : $(\mathbf{m}', \mathbf{e}) = \mathit{decode}(\mathbf{c})$



- With the good basis $\mathbf{G}$, $\mathbf{m}' = \mathbf{m}$
- With the bad basis $\mathbf{B}$, $\mathbf{m}' \neq \mathbf{m}$: decryption fails !

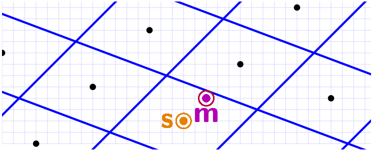
Signatures

Sign

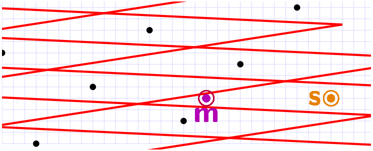
- Hash the message to a random vector **m**.
- apply Round'off with a good basis **G**:
  find **s** $\in L$ proche de **m** .

Vérify

- check that **s** $\in L$ using the bad basis **B**
- and that **m** is close to **s**.



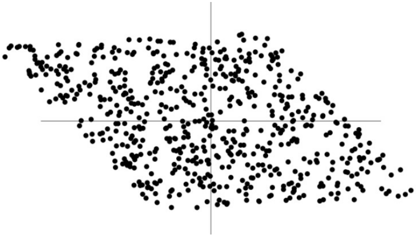
correct signature (close)



Incorrect Signature (far)

A statistical attack [NguReg05,DucNgu12]

The difference $\mathbf{s} - \mathbf{m}$ is always inside the parallelepiped by the good basis G:



Each signatures $(\mathbf{s}, \mathbf{m})$ leaks a bit of information about the secret key G.

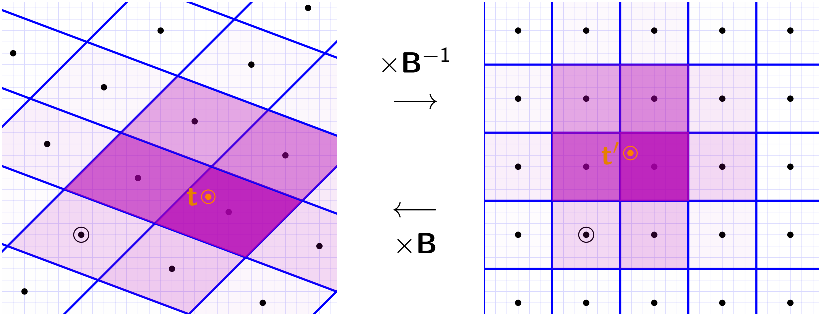
Nguyen et Regev showed how to "learn the parralepiped" using a few signature:

$\Rightarrow$ Total break of original GGH and NTRUSign schemes.

Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

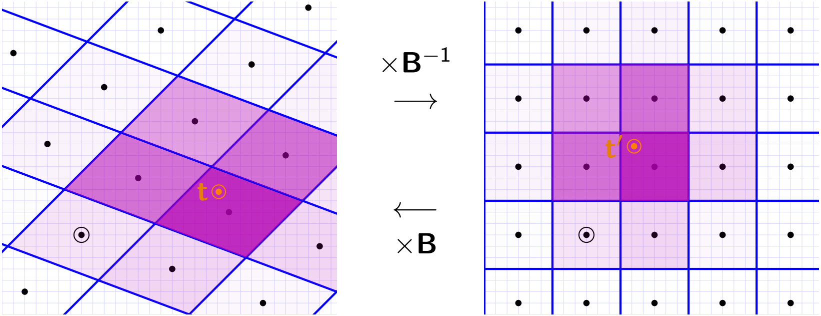
Idea: Hide the parallelepiped by "blurring":



Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

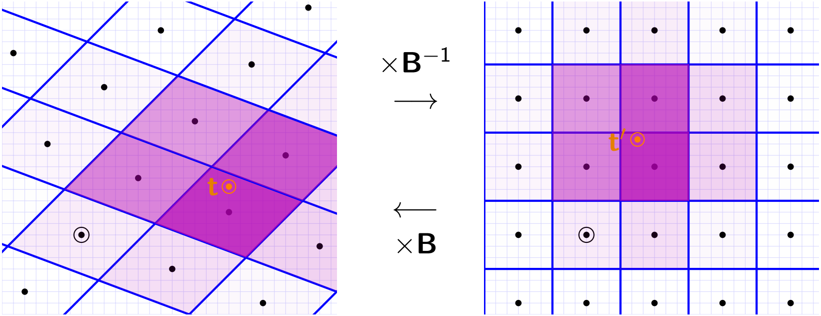
Idea: Hide the parallelepiped by "blurring":



Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

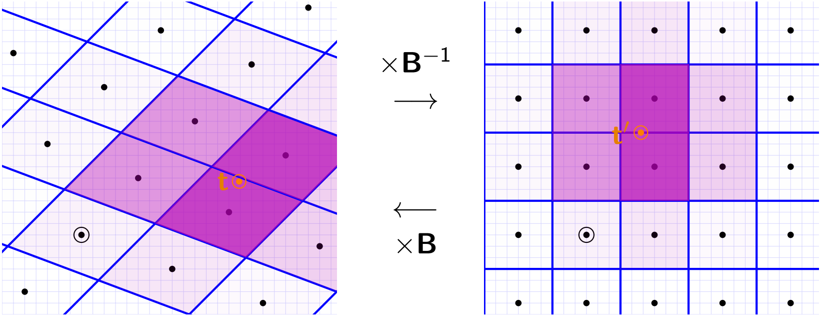
Idea: Hide the parallelepiped by "blurring":



Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

Idea: Hide the parallelepiped by "blurring":

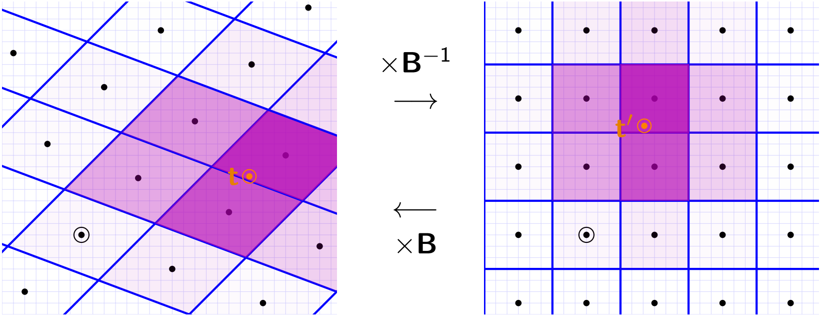


Countermeasures : Randomized Round'off

Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

Idea: Hide the parallelepiped by "blurring":

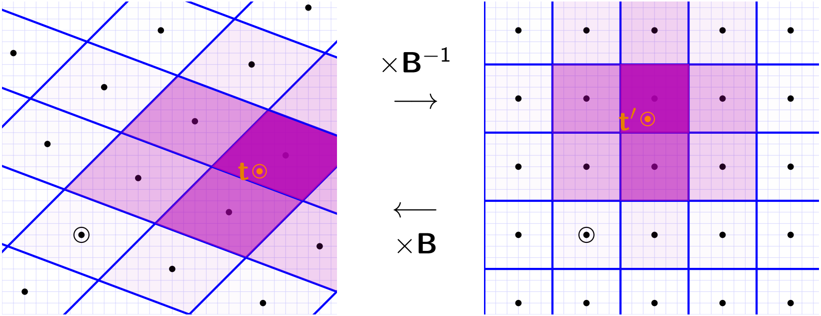


Countermeasures : Randomized Round'off

Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

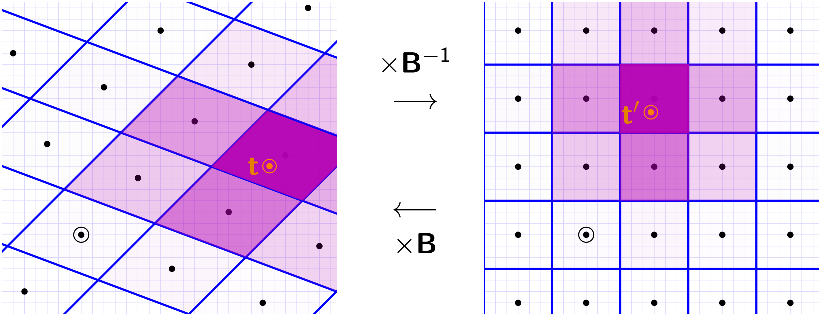
Idea: Hide the parallelepiped by "blurring":



Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

Idea: Hide the parallelepiped by "blurring":

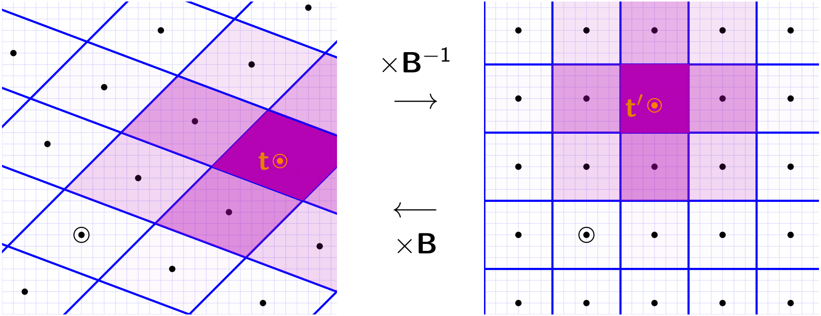


Countermeasures : Randomized Round'off

Round'off:

$$\mathbf{t}' = \mathbf{B}^{-1} \cdot \mathbf{t}; \quad \mathbf{v}' = \lfloor \mathbf{t}' \rceil; \quad \mathbf{v} = \mathbf{B} \cdot \mathbf{v}'$$

Idea: Hide the parallelepiped by "blurring":



Gaussian sampling

Using the appropriate randomized rounding (Gaussian-sampling) the distribution $\mathbf{s} - \mathbf{m}$ can be made Gaussian:

With more effort, the ellipsoid can be transformed into a ball, that leaks no information about the secret basis.

- [Klein 2000, Gentry Peikert Vaikuthanathan 2008]: for a randomization of the Nearest Plane algorithm
- [Peikert 2010] for a randomization of the Round'off algorithm