

# Cryptographie à base de réseaux euclidiens

Katharina Boudgoust  
EMSEC

Univ Rennes 1, CNRS, IRISA

3 septembre 2020

# A look on the map - or où me trouver ?

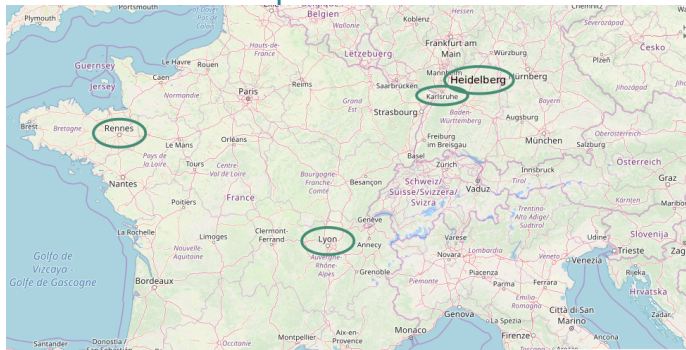


Image: Open Street Map Screen Shot

# Pour savoir plus ...

## EMSEC

## embedded security & cryptography

[Research](#)[Publications](#)[People](#)[Open Positions](#)[Contact](#)

### Presentation

The research team "Embedded Security and Cryptography" (EMSEC) addresses questions related to cryptography, formal methods, and security of hardware and software systems. EMSEC hosts 8 faculty members and researchers from [CNRS](#), [INSA Rennes](#), and [University of Rennes 1](#), and more than 20 PhD students, postdocs, and adjunct members. EMSEC's activities target both the construction of security-preserving mechanisms and the design of



Katharina BOUDGOUST

[Home](#)[Publications](#)[Talks](#)[Teaching](#)[Personal](#)

Since September 2018, I am a Ph.D student in computer science within the [EMSEC](#) team at [IRISA Laboratory](#) in Rennes under the supervision of [Pierre-Alain FOUQUE](#) and [Adeline BOUCLANGI](#).  
From October to December 2019, I visited [Jon STEINFELD](#) at the [Cybersecurity Lab](#) of the [Faculty of Information Technology](#) of the [Monash University](#) in Melbourne, Australia.  
In Mai 2018, I received my master's degree at the [Department of Mathematics](#) at [Karlsruhe Institute of Technology](#). My master thesis [Polyadic groups and applications in cryptography](#) was under  
Prior to this, I received in July 2014 my bachelor's degree at the [Department of Mathematics and Computer Science](#) at [Heidelberg University](#). My bachelor thesis [Die Komplexität von Determinanten](#) of [Ulmar VERNIKOB](#).

#### NEWS

- 20.07.2020: Moved my website to a GitHub page
- 18.04.2020: [Blogpost](#) from Emily Chang added to my reading recommendation list for feminist literature and [Susan Wojcicki](#) to my list of important women in computer science
- 14.04.2020: On Friday, 17th April 2020, I will give an online talk at the [Lecture Cryptography](#)
- 17.02.2020: Participating at the [Lecture Workshop](#) at Simons Institute in Berkeley, US

<https://www.irisa.fr/emsec/>  
<https://katinkabou.github.io/>

# De quoi parlera cette présentation ?

- 1 C'est quoi la cryptographie ?
- 2 C'est quoi un réseau euclidien ?
- 3 Ça veut dire quoi “baser la cryptographie sur quelque chose” ?

# De quoi parlera cette présentation ?

## 1 C'est quoi la cryptographie ?

- Définition
- Symétrique
- Asymétrique

## 2 C'est quoi un réseau euclidien ?

## 3 Ça veut dire quoi “baser la cryptographie sur quelque chose” ?

# Définition

Le mot **cryptographie** se compose des mots en grec ancien kryptos ( $\kappa\rho\upsilon\pi\tau\omega\varsigma$ , caché) et graphein ( $\gamma\rho\alpha\phi\epsilon\iota\nu$ , écrire).

# Définition

Le mot **cryptographie** se compose des mots en grec ancien kryptos ( $\kappa\rho\upsilon\pi\tau\omega\varsigma$ , caché) et graphein ( $\gamma\rho\alpha\phi\epsilon\iota\nu$ , écrire).

Elle a pour objet de protéger des messages en assurant leurs

- **confidentialité**,
- **authenticité** et
- **intégrité**.

# Définition

Le mot **cryptographie** se compose des mots en grec ancien *kryptos* (*κρυπτος*, caché) et *graphein* (*γραφειν*, écrire).

Elle a pour objet de protéger des messages en assurant leurs

- **confidentialité**,
- **authenticité** et
- **intégrité**.

Science (publique) très jeune : née dans les années 1970, avec les publications de Merkle [Mer78], Diffie et Hellman [DH76].



# Définition

Le mot **cryptographie** se compose des mots en grec ancien *kryptos* (*κρυπτος*, caché) et *graphein* (*γραφειν*, écrire).

Elle a pour objet de protéger des messages en assurant leurs

- **confidentialité**,
- **authenticité** et
- **intégrité**.

Science (publique) très jeune : née dans les années 1970, avec les publications de Merkle [Mer78], Diffie et Hellman [DH76].

Fondation de l'IACR (International Association for Cryptologic Research) en 1982.

# La cryptographie symétrique



Images: <https://svgsilh.com/de/ffc107/image/1473654.html>

# La cryptographie symétrique



clé secrète  $k$   
message  $m$



clé secrète  $k$

$$\xrightarrow{c = \text{Enc}(m, k)}$$

$$m' = \text{Dec}(c, k)$$

message chiffré  $c$   
si tout va bien  $m = m'$

Images: <https://svgsilh.com/de/ffc107/image/1473654.html>

# Le chiffre de César

## Le chiffre de César

Chiffrement par **décalage**. Chaque lettre est décalée par  $k$ , où  $k$  est une lettre de l'alphabète.

**Clé:** A  $\rightarrow$  pas de décalage

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

devient

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Texte en clair: INTRODUCTION

Texte chiffré: INTRODUCTION

# Le chiffre de César

## Le chiffre de César

Chiffrement par **décalage**. Chaque lettre est décalée par  $k$ , où  $k$  est une lettre de l'alphabète.

**Clé:** B  $\rightarrow$  décalage par une position

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

devient

B C D E F G H I J K L M N O P Q R S T U V W X Y Z A

Texte en clair: INTRODUCTION

Texte chiffré: JOUSPEVDUJPO

# Le chiffre de César

## Le chiffre de César

Chiffrement par **décalage**. Chaque lettre est décalée par  $k$ , où  $k$  est une lettre de l'alphabète.

**Clé:** U  $\rightarrow$  décalage par 20 positions

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

devient

U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

Texte en clair: INTRODUCTION

Texte chiffré: CHNLIXOWNCIH

# Le chiffre de César

## Le chiffre de César

Chiffrement par **décalage**. Chaque lettre est décalée par  $k$ , où  $k$  est une lettre de l'alphabète.

**Clé:** U  $\rightarrow$  décalage par 20 positions

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

devient

U V W X Y Z A B C D E F G H I J K L M N O P Q R S T

Texte en clair: INTRODUCTION

Texte chiffré: CHNLIXOWNCIH

Casser par **brute-force** ( $\hat{=}$  essayer toutes les 26 possibilités)

# La cryptographie asymétrique





# La cryptographie asymétrique



message  $m$



clé secrète  $sk$   
clé publique  $pk$

$$\xrightarrow{c = \text{Enc}(m, pk)}$$

$$m' = \text{Dec}(c, sk)$$

message chiffré  $c$

si tout va bien  $m = m'$

# La cryptographie asymétrique



message  $m$



clé secrète  $sk$   
clé publique  $pk$

$$c = \text{Enc}(m, pk)$$



$$m' = \text{Dec}(c, sk)$$

message chiffré  $c$

si tout va bien  $m = m'$

**pas d'échange de clé nécessaire !**

# Cryptosystème de ElGamal

Paramètres: groupe cyclique  $G = \langle g \rangle$  de l'ordre  $q$  ( $h^q = 1 \forall h \in G$ )



message  $m \in G$

$r \leftarrow \{0, \dots, q-1\}$

$$c = (c_1, c_2) = (g^r, m \cdot pk^r)$$

$\longrightarrow$



sk =  $x \leftarrow \{0, \dots, q-1\}$

pk =  $g^x$

$$m' = c_2 \cdot (c_1^x)^{-1}$$

# Cryptosystème de ElGamal

Paramètres: groupe cyclique  $G = \langle g \rangle$  de l'ordre  $q$  ( $h^q = 1 \forall h \in G$ )



message  $m \in G$

$r \leftarrow \{0, \dots, q-1\}$



sk =  $x \leftarrow \{0, \dots, q-1\}$

pk =  $g^x$

$$c = (c_1, c_2) = (g^r, m \cdot \text{pk}^r) \longrightarrow$$

$$m' = c_2 \cdot (c_1^x)^{-1}$$

Correcte ?

$$\begin{aligned} m' &= c_2 \cdot (c_1^x)^{-1} = m \cdot \text{pk}^r \cdot ((g^r)^x)^{-1} \\ &= m \cdot (g^x)^r \cdot g^{-rx} = m \cdot g^{xr} \cdot g^{-xr} = m. \end{aligned}$$

# La crypto dans la vie quotidienne

Pourquoi on s'intéresse à la cryptographie ?

Signal, PGP, Passport européen, TLS, ...



Images: wikipedia.org et pixaby.com

# La crypto dans la vie quotidienne

Pourquoi on s'intéresse à la cryptographie ?

Plus de buzz words : Clouds, Blockchain, ...



Mais retournons vers les maths :-)

Images: [publicdomainpictures.net](https://publicdomainpictures.net) et [pixaby.com](https://pixaby.com)

# De quoi parlera cette présentation ?

- 1 C'est quoi la cryptographie ?
- 2 C'est quoi un réseau euclidien ?
  - Définition
  - Le déterminant d'un réseau
  - Problèmes difficiles
- 3 Ça veut dire quoi “baser la cryptographie sur quelque chose” ?

# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$



# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$

L'exemple le plus simple:  $n = 1$ ,  $B = (1)$  et  $\Lambda(B) = \mathbb{Z}$ .

# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$

L'exemple le plus simple:  $n = 1$ ,  $B = (1)$  et  $\Lambda(B) = \mathbb{Z}$ .

Un autre exemple simple:  $n = 1$ ,  $B = (3)$  et  $\Lambda(B) = 3\mathbb{Z}$ .

# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$

L'exemple le plus simple:  $n = 1$ ,  $B = (1)$  et  $\Lambda(B) = \mathbb{Z}$ .

Un autre exemple simple:  $n = 1$ ,  $B = (3)$  et  $\Lambda(B) = 3\mathbb{Z}$ .

On ajoute une dimension:  $n = 2$ ,  $B = ((0, 1), (1, 0))$  et  $\Lambda(B) = \mathbb{Z}^2$ .

# Définition réseau euclidien

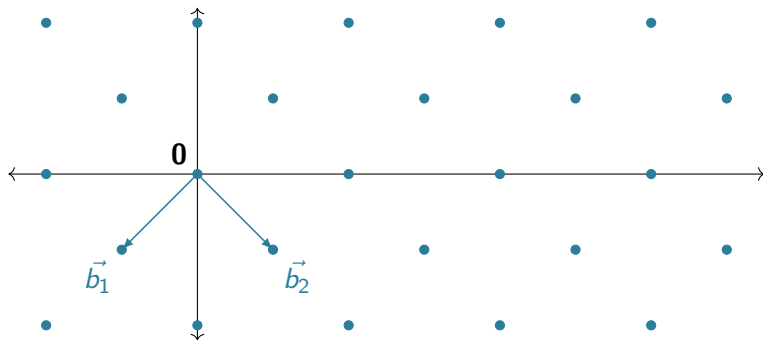
Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$

# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

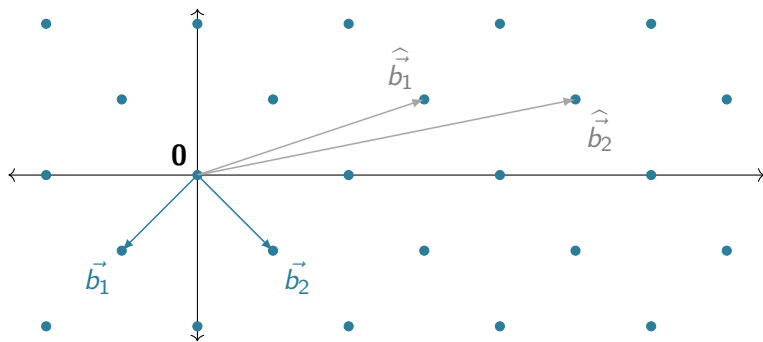
$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$



# Définition réseau euclidien

Un **réseau euclidien**  $\Lambda$  de **dimension**  $n$  est l'ensemble des combinaisons linéaires à coefficients entiers de  $n$  vecteurs de base indépendants  $B = (\vec{b}_1, \dots, \vec{b}_n)$  de l'espace vectoriel  $\mathbb{R}^n$ ,

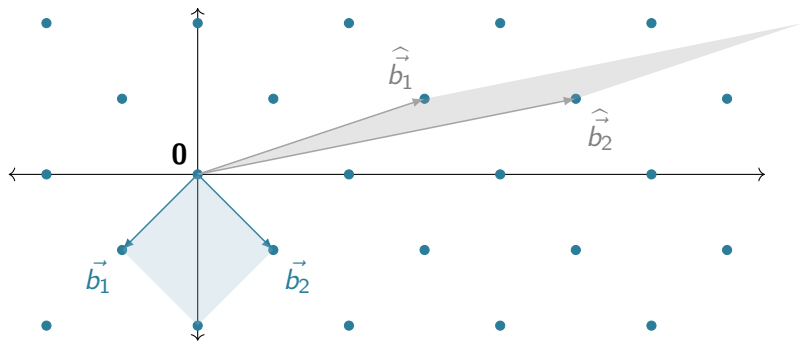
$$\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}.$$



# Propriétés des réseaux euclidiens

Un invariant d'un réseau euclidien  $\Lambda(B) = \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid a_i \in \mathbb{Z} \right\}$  est son **déterminant**

$$\det(\Lambda) = \text{vol} \left\{ \sum_{i=1}^n a_i \cdot \vec{b}_i \mid 0 \leq a_i < 1 \right\}.$$



# Deux problèmes difficiles 1/2

Soit  $\Lambda(B)$  un réseaux avec une base  $B$ . Le **minimum**<sup>1</sup> de  $\Lambda(B)$  est défini par  $\lambda_1(\Lambda(B)) = \min_{\vec{v} \in \Lambda(B) \setminus \{\vec{0}\}} \|\vec{v}\|$ .

---

<sup>1</sup>Il faut fixer la norme, par ex. la norme euclidienne/norme du supremum



## Deux problèmes difficiles 1/2

Soit  $\Lambda(B)$  un réseau avec une base  $B$ . Le **minimum**<sup>1</sup> de  $\Lambda(B)$  est défini par  $\lambda_1(\Lambda(B)) = \min_{\vec{v} \in \Lambda(B) \setminus \{\vec{0}\}} \|\vec{v}\|$ .

### Problem (Shortest Vector Problem)

*Étant donnée une base  $B$ , trouver  $\vec{v} \in \Lambda(B)$  non nul tel que  $\lambda_1(\Lambda(B)) = \|\vec{v}\|$ .*

---

<sup>1</sup>Il faut fixer la norme, par ex. la norme euclidienne/norme du supremum

## Deux problèmes difficiles 1/2

Soit  $\Lambda(B)$  un réseau avec une base  $B$ . Le **minimum**<sup>1</sup> de  $\Lambda(B)$  est défini par  $\lambda_1(\Lambda(B)) = \min_{\vec{v} \in \Lambda(B) \setminus \{\vec{0}\}} \|\vec{v}\|$ .

### Problem (Shortest Vector Problem)

*Étant donnée une base  $B$ , trouver  $\vec{v} \in \Lambda(B)$  non nul tel que  $\lambda_1(\Lambda(B)) = \|\vec{v}\|$ .*

### Problem (Closest Vector Problem)

*Étant donnée une base  $B$  et un vecteur  $\vec{t} \in \mathbb{R}^n$ , trouver  $\vec{v} \in \Lambda(B)$  qui minimise  $\|\vec{v} - \vec{t}\|$ .*

---

<sup>1</sup>Il faut fixer la norme, par ex. la norme euclidienne/norme du supremum

## Deux problèmes difficiles 1/2

Soit  $\Lambda(B)$  un réseau avec une base  $B$ . Le **minimum**<sup>1</sup> de  $\Lambda(B)$  est défini par  $\lambda_1(\Lambda(B)) = \min_{\vec{v} \in \Lambda(B) \setminus \{\vec{0}\}} \|\vec{v}\|$ .

### Problem (Shortest Vector Problem)

*Étant donnée une base  $B$ , trouver  $\vec{v} \in \Lambda(B)$  non nul tel que  $\lambda_1(\Lambda(B)) = \|\vec{v}\|$ .*

SVP est une instance de CVP avec  $\vec{t} = \vec{0}$  et la restriction que  $\vec{v} \neq \vec{0}$ .

### Problem (Closest Vector Problem)

*Étant donnée une base  $B$  et un vecteur  $\vec{t} \in \mathbb{R}^n$ , trouver  $\vec{v} \in \Lambda(B)$  qui minimise  $\|\vec{v} - \vec{t}\|$ .*

---

<sup>1</sup>Il faut fixer la norme, par ex. la norme euclidienne/norme du supremum

# Deux problèmes difficiles 1/2

Soit  $\Lambda(B)$  un réseau avec une base  $B$ . Le **minimum**<sup>1</sup> de  $\Lambda(B)$  est défini par  $\lambda_1(\Lambda(B)) = \min_{\vec{v} \in \Lambda(B) \setminus \{\vec{0}\}} \|\vec{v}\|$ .

## Problem (Shortest Vector Problem)

*Étant donnée une base  $B$ , trouver  $\vec{v} \in \Lambda(B)$  non nul tel que  $\lambda_1(\Lambda(B)) = \|\vec{v}\|$ .*

SVP est une instance de CVP avec  $\vec{t} = \vec{0}$  et la restriction que  $\vec{v} \neq \vec{0}$ .

## Problem (Closest Vector Problem)

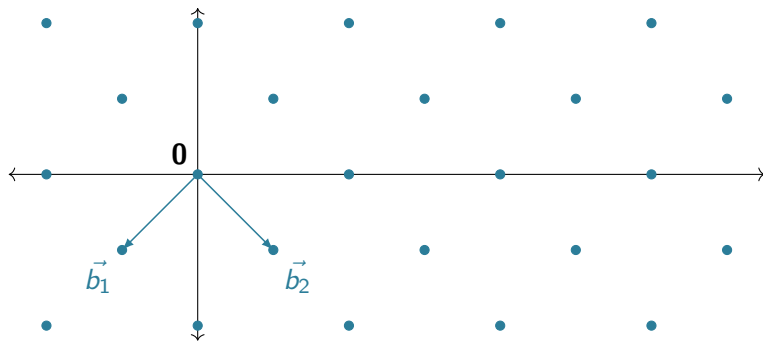
*Étant donnée une base  $B$  et un vecteur  $\vec{t} \in \mathbb{R}^n$ , trouver  $\vec{v} \in \Lambda(B)$  qui minimise  $\|\vec{v} - \vec{t}\|$ .*

Les deux problèmes sont NP-difficile ( $\hat{=}$  très difficile, à préciser).

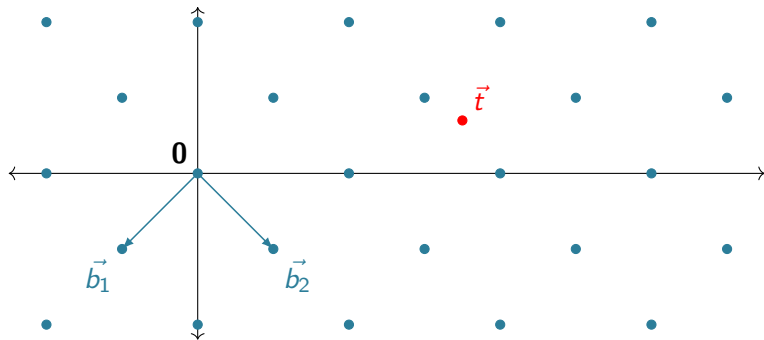
---

<sup>1</sup>Il faut fixer la norme, par ex. la norme euclidienne/norme du supremum

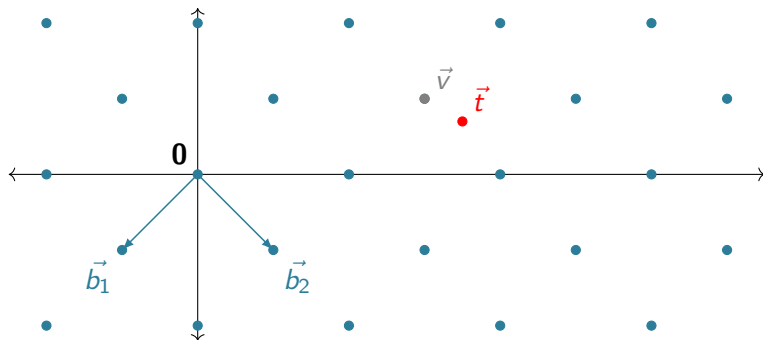
## Deux problèmes difficiles 2/2



## Deux problèmes difficiles 2/2



## Deux problèmes difficiles 2/2



# De quoi parlera cette présentation ?

- 1 C'est quoi la cryptographie ?
- 2 C'est quoi un réseau euclidien ?
- 3 Ça veut dire quoi “baser la cryptographie sur quelque chose” ?
  - Une réduction
  - Hypothèse de Diffie et Hellman
  - Contexte actuel



# Une réduction

Étant donnés deux problèmes,  $A$  et  $B$ .

## Definition (informel)

Une **réduction** est un moyen de convertir un problème  $A$  en un autre problème  $B$  de telle sorte qu'une solution au problème  $B$  peut être utilisée pour résoudre le problème  $A$ .

# Une réduction

Étant donnés deux problèmes,  $A$  et  $B$ .

## Definition (informel)

Une **réduction** est un moyen de convertir un problème  $A$  en un autre problème  $B$  de telle sorte qu'une solution au problème  $B$  peut être utilisée pour résoudre le problème  $A$ .

On note  $A \leq B$  ou  $A \rightarrow B$ .

# Une réduction

Étant donnés deux problèmes,  $A$  et  $B$ .

## Definition (informel)

Une **réduction** est un moyen de convertir un problème  $A$  en un autre problème  $B$  de telle sorte qu'une solution au problème  $B$  peut être utilisée pour résoudre le problème  $A$ .

On note  $A \leq B$  ou  $A \rightarrow B$ .

La difficulté du problème  $A$  **induit** la difficulté de  $B$ .

Autrement dit, la difficulté du problème  $B$  **est basée** sur la difficulté du problème  $A$ .

# Une réduction simple

## Exemple

Nous savons additionner, soustraire et diviser par 2.

Problème  $A \triangleq$  la multiplication

Problème  $B \triangleq$  élever au carré.

# Une réduction simple

## Exemple

Nous savons additionner, soustraire et diviser par 2.

Problème  $A \hat{=}$  la multiplication

Problème  $B \hat{=}$  élever au carré.

Problème  $A$  peut être réduit au problème  $B$  :

$$a \cdot b = \frac{(a + b)^2 - a^2 - b^2}{2}$$

# Une réduction simple

## Exemple

Nous savons additionner, soustraire et diviser par 2.

Problème  $A \hat{=}$  la multiplication

Problème  $B \hat{=}$  élever au carré.

Problème  $A$  peut être réduit au problème  $B$  :

$$a \cdot b = \frac{(a + b)^2 - a^2 - b^2}{2}$$

En sens inverse, problème  $B$  peut être réduit au problème  $A$  :

$$a^2 = a \cdot a$$

# Une réduction simple

## Exemple

Nous savons additionner, soustraire et diviser par 2.

Problème  $A \hat{=}$  la multiplication

Problème  $B \hat{=}$  élever au carré.

Problème  $A$  peut être réduit au problème  $B$  :

$$a \cdot b = \frac{(a + b)^2 - a^2 - b^2}{2}$$

En sens inverse, problème  $B$  peut être réduit au problème  $A$  :

$$a^2 = a \cdot a$$

$A \rightarrow B$  et  $B \rightarrow A$ , alors  $A \leftrightarrow B$ .

# Cryptosystème de ElGamal

Paramètres: groupe cyclique  $G = \langle g \rangle$  de l'ordre  $q$



$$m \in G, r \leftarrow \{0, \dots, q-1\}$$



$$\text{sk} = x, \quad \text{pk} = g^x$$

$$c = (c_1, c_2) = (g^r, m \cdot \text{pk}^r)$$

$\xrightarrow{\hspace{2cm}}$

L'hypothèse décisionnelle de Diffie-Hellman (DDH):

$$(g^a, g^b, g^{ab}) \approx (g^a, g^b, g^d)$$

Elle induit la difficulté de distinguer

$$(\text{pk}, g^r, m \cdot \text{pk}^r) \approx (\text{pk}, g^r, m \cdot g^d)$$



# Contexte actuel

- **Compétition post-quantique du NIST<sup>2</sup>**  
Processus de standardisation, lancé 02/2016,  
07/2020 : 7 candidats au troisième tour, dont 5 basé sur les réseaux

---

<sup>2</sup>National Institute of Standards and Technology

# Contexte actuel

- **Compétition post-quantique du NIST<sup>2</sup>**  
Processus de standardisation, lancé 02/2016,  
07/2020 : 7 candidats au troisième tour, dont 5 basé sur les réseaux
- **Recommandation à lire : [Pei16]**  
Enquête sur une décennie de cryptographie à base de réseaux

---

<sup>2</sup>National Institute of Standards and Technology

# Contexte actuel

- **Compétition post-quantique du NIST<sup>2</sup>**  
Processus de standardisation, lancé 02/2016,  
07/2020 : 7 candidats au troisième tour, dont 5 basé sur les réseaux
- **Recommandation à lire : [Pei16]**  
Enquête sur une décennie de cryptographie à base de réseaux
- **Mon sujet : variantes structurées**  
Efficacité versus sécurité
- **On se revoit au deuxième semestre**  
dans le cours Crypto

---

<sup>2</sup>National Institute of Standards and Technology

# Questions ?



Images: <https://pxhere.com/en/photo/1369232>

# Références



Diffie, Whitfield and Hellman, Martin. (1976)

On homomorphisms onto finite groups

**IEEE transactions on Information Theory** 22.6 644–654



Merkle, Ralph C. (1978)

Secure communications over insecure channels

**Communications of the ACM** 21(4) 294–299



Peikert, Chris. (2016)

A Decade of Lattice Cryptography

**Foundations and Trends in Theoretical Computer Science** 10(4) 283–424