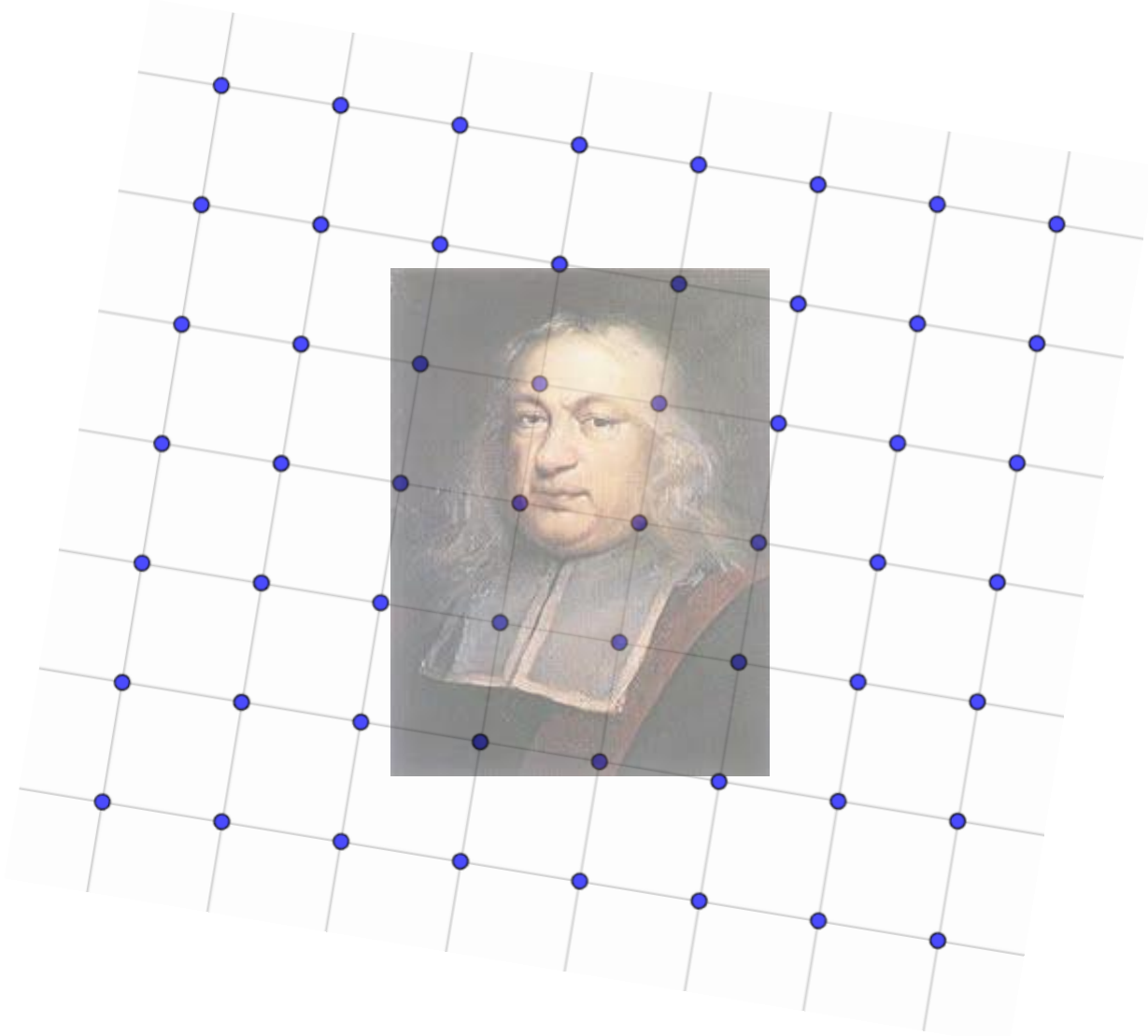


Réseaux : de Fermat à la cryptographie post-quantique

Séminaire de mathématiques de Ginette
mardi 24 janvier 2023

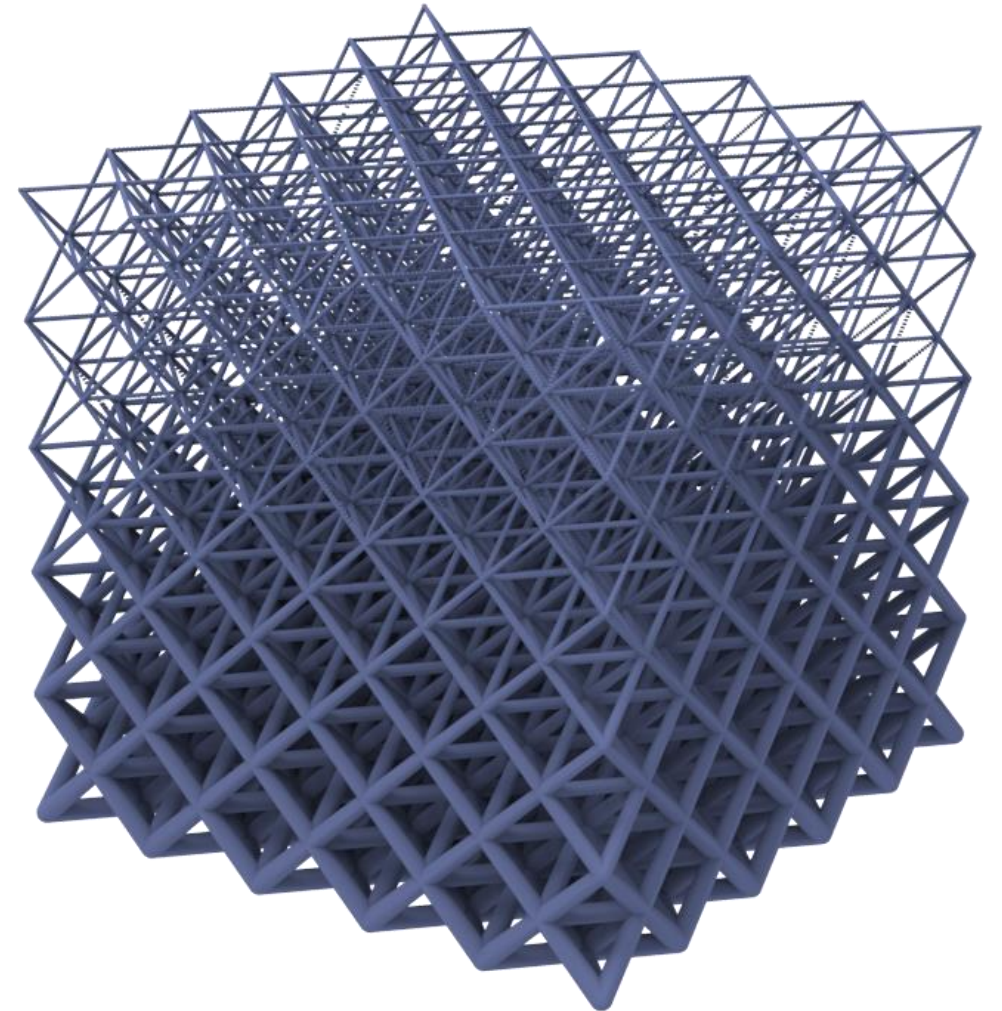
Henry Bambury (MPSI2 16-17/MP*1 17-18)
henry.bambury@ens.fr



C'est quoi un réseau ?

Les deux carrés de Fermat

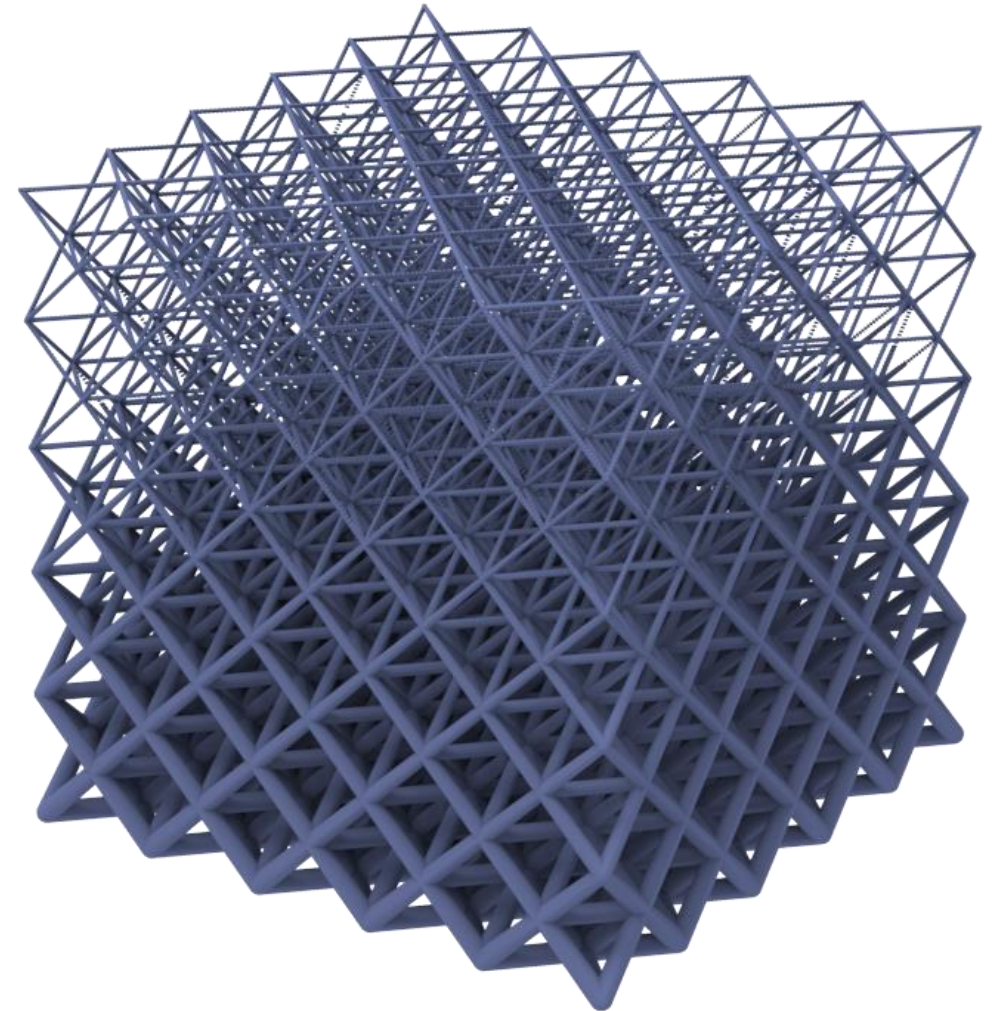
Application en cryptographie moderne



C'est quoi un réseau ?

Les deux carrés de Fermat

Application en cryptographie moderne



Réseaux : définition et premières propriétés

Soit $B = (b_1, \dots, b_n)$ une famille libre de \mathbb{R}^n .

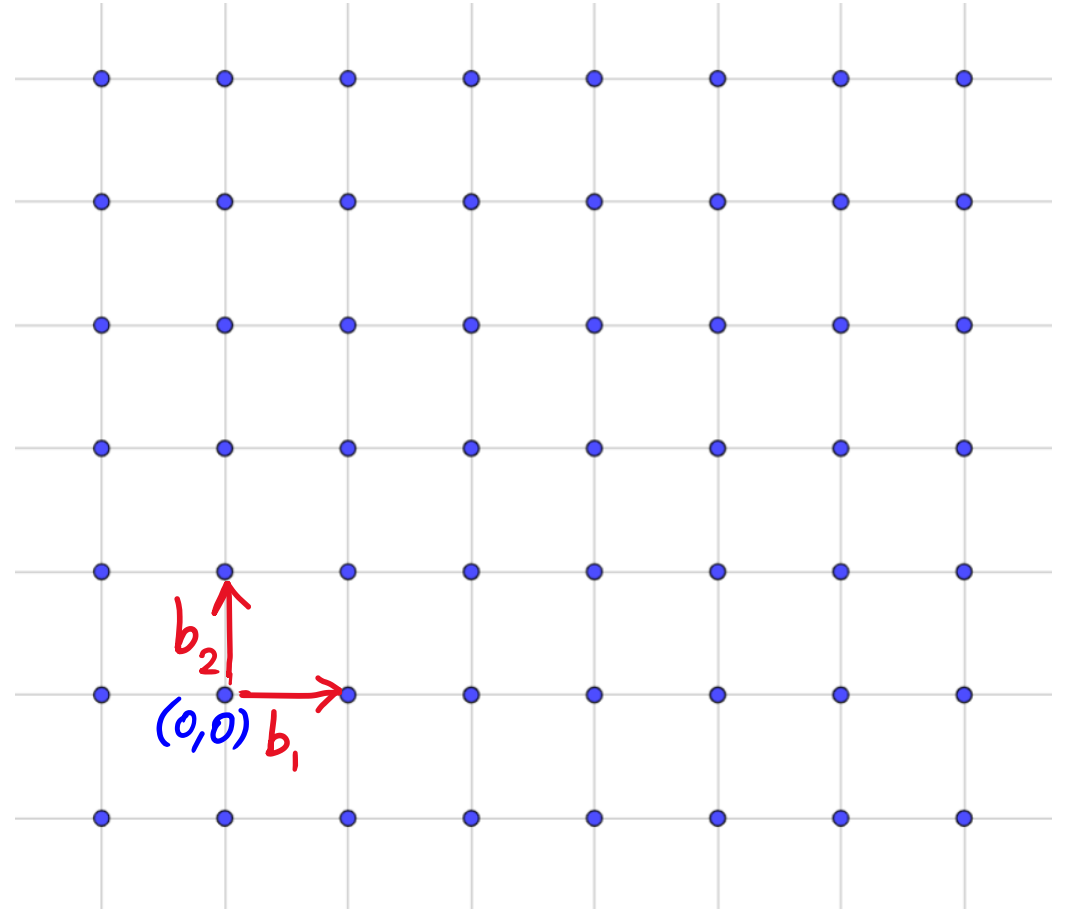
Définition (Réseau) :

$$\mathcal{L}(B) := \left\{ \sum_{i=1}^n x_i b_i \mid (x_1, \dots, x_n) \in \mathbb{Z}^n \right\}$$

Réseaux : définition et premières propriétés

$$\mathcal{L}(B) := \left\{ \sum_{i=1}^n x_i b_i \mid (x_1, \dots, x_n) \in \mathbb{Z}^n \right\}$$

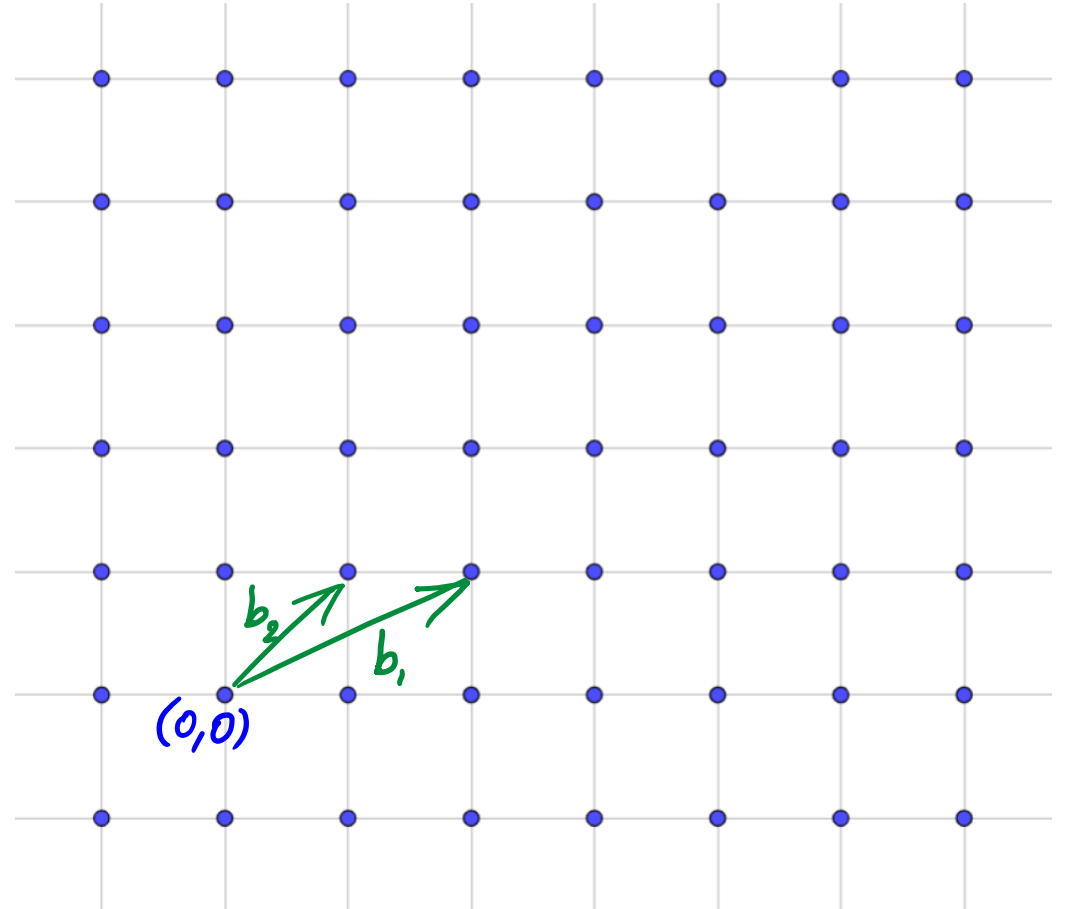
$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



Réseaux : définition et premières propriétés

$$\mathcal{L}(B) := \left\{ \sum_{i=1}^n x_i b_i \mid (x_1, \dots, x_n) \in \mathbb{Z}^n \right\}$$

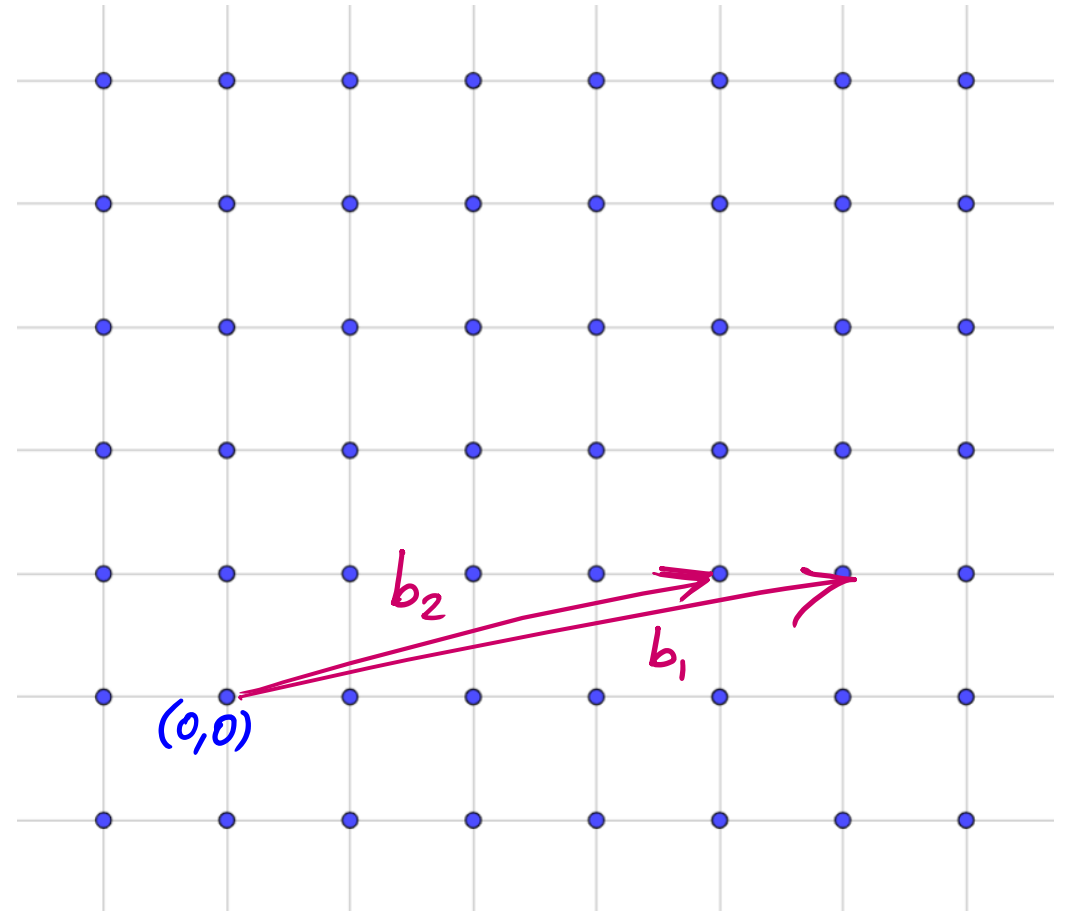
$$B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$



Réseaux : définition et premières propriétés

$$\mathcal{L}(B) := \left\{ \sum_{i=1}^n x_i b_i \mid (x_1, \dots, x_n) \in \mathbb{Z}^n \right\}$$

$$B = \begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}$$



Réseaux : définition et premières propriétés

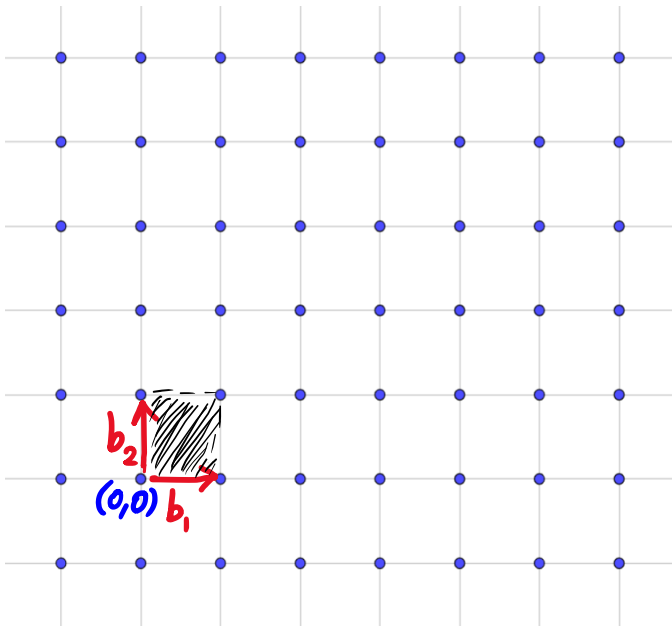
Proposition (Bases d'un réseau) :

$$\mathcal{L}(B) = \mathcal{L}(C) \Leftrightarrow \exists U \in \text{GL}_n(\mathbb{Z}) : B = CU$$

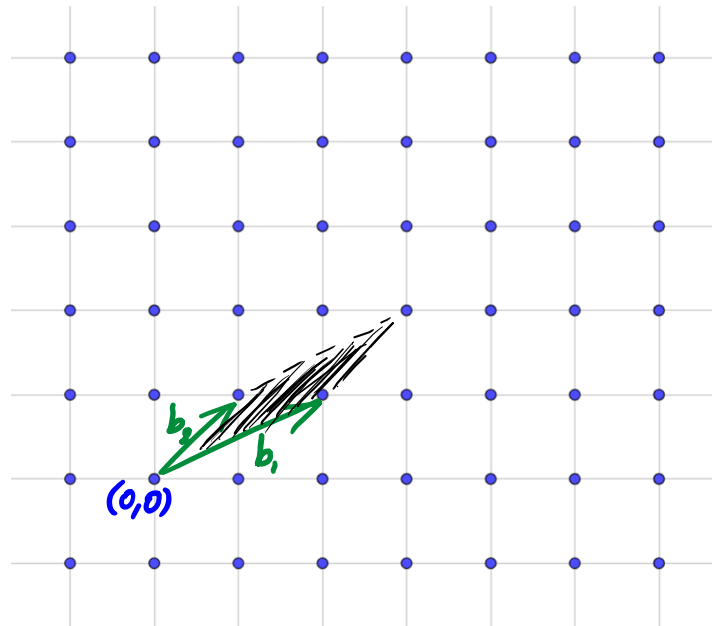
Définition (Volume) :

$$\text{Vol}(\mathcal{L}(B)) = |\det(B)|$$

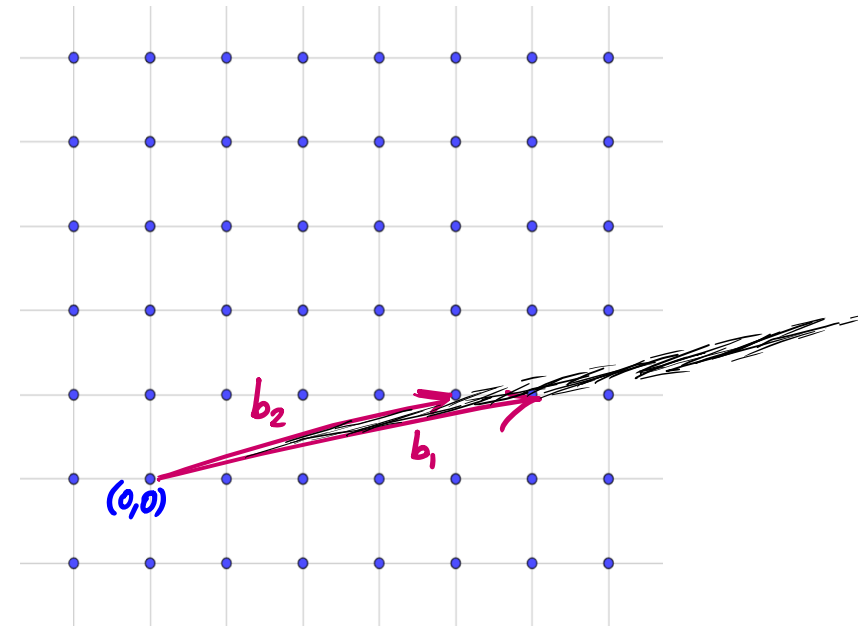
Réseaux : définition et premières propriétés



$$B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



$$B = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$

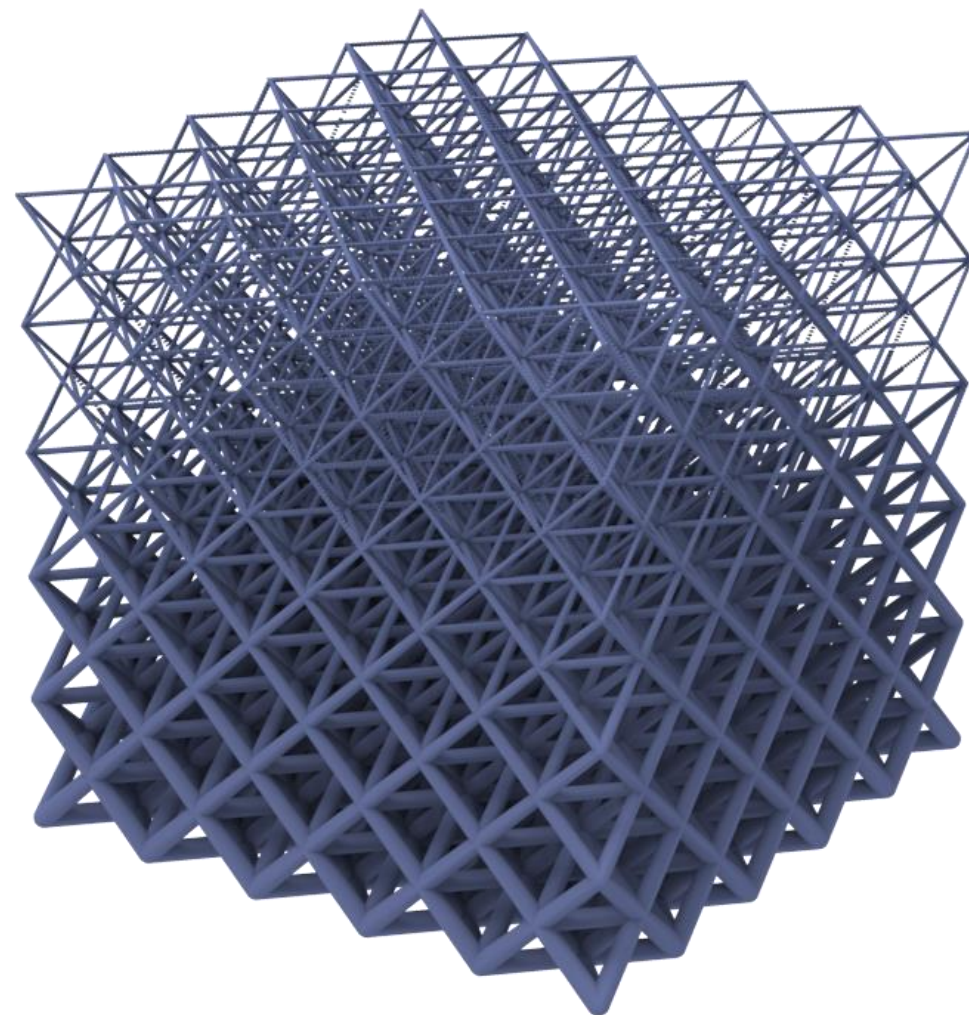


$$B = \begin{pmatrix} 5 & 4 \\ 1 & 1 \end{pmatrix}$$

C'est quoi un réseau ?

Les deux carrés de Fermat

Application en cryptographie moderne



Le théorème des deux carrés de Fermat

Théorème :

Soit p un nombre premier impair.

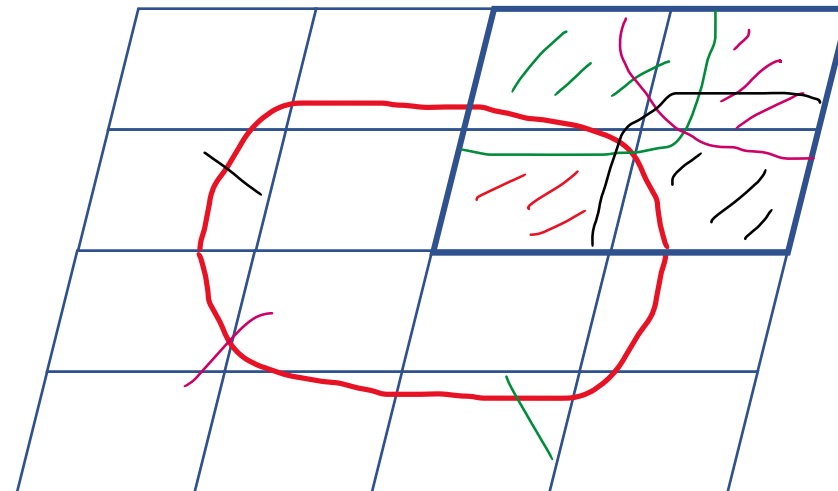
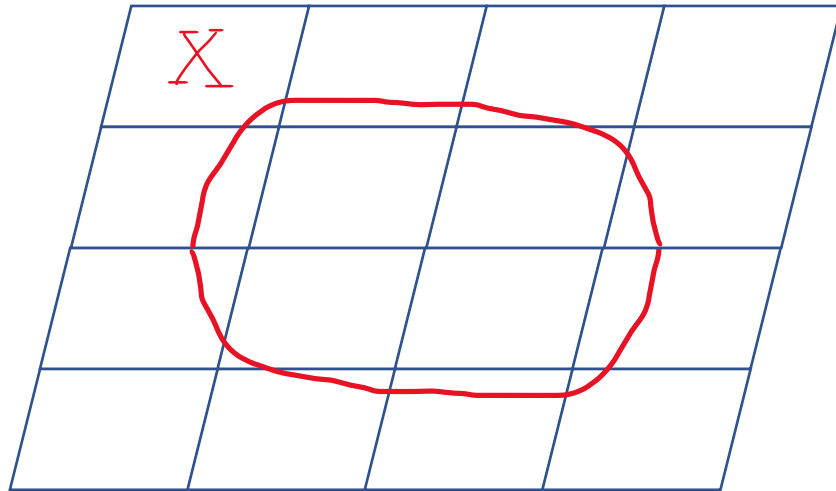
$$p \equiv 1 \pmod{4} \Leftrightarrow \exists (a, b) \in \mathbb{Z}^2 : p = a^2 + b^2$$

Le théorème des deux carrés de Fermat : preuve

Lemme (Minkowski) :

Soit \mathcal{L} un réseau de rang 2 et $X \subset \mathbb{R}^2$ convexe et symétrique en 0. Alors

$$\mathcal{A}(X) > 4\text{Vol}(\mathcal{L}) \Rightarrow X \cap \mathcal{L} \neq \{0\}$$



Le théorème des deux carrés de Fermat : preuve

| Trouver $q \in \mathbb{Z}$ tel que $q^2 \equiv -1 \pmod{p}$.

| Considérer $\mathcal{L}(b_1, b_2)$ où $b_1 = \begin{pmatrix} 1 \\ q \end{pmatrix}$ et $b_2 = \begin{pmatrix} 0 \\ p \end{pmatrix}$.

| Conclure grâce au résultat de Minkowski.



Le théorème des quatre carrés de Lagrange

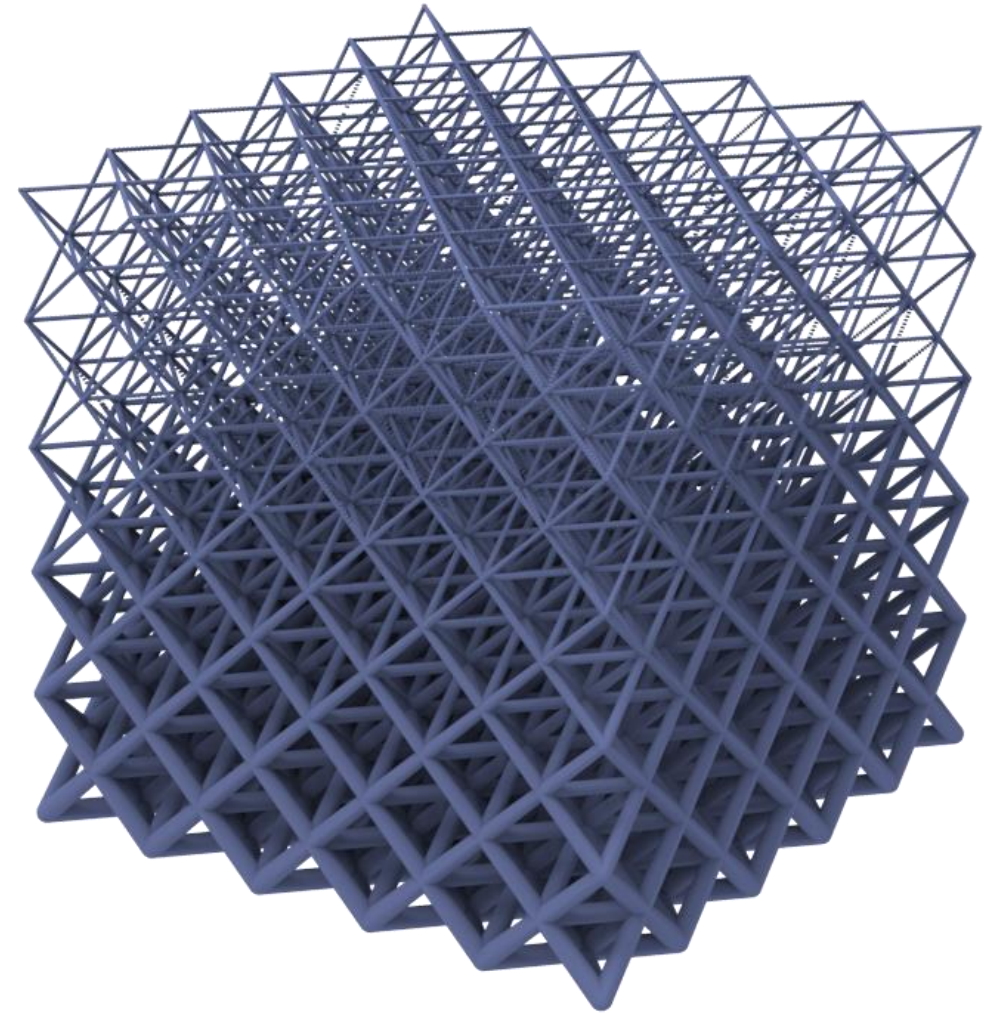
Théorème :

Tout entier positif peut se décomposer
en une somme de quatre carrés d'entiers.

C'est quoi un réseau ?

Les deux carrés de Fermat



Application en cryptographie moderne



Une rapide histoire de la cryptologie

A horizontal timeline with a blue arrow pointing right, marking key milestones in cryptography. Hand-drawn red annotations and images are placed above and below the timeline.

- 3900**: A scroll is shown above the timeline. A red thought bubble contains a simple cipher: A → B, B → C, C → D.
- 100**: A cartoon of a man in a red cape and white tunic, looking thoughtful with his hand on his chin.
- 800**: Arabic script is shown above the timeline, representing early cryptographic methods.
- 1570**: A red thought bubble shows two stick figures with crowns facing each other, with a double-headed arrow between them and a key above the arrow.
- 1919**: A photograph of a mechanical cipher machine (likely a rotor machine) is shown above the timeline.
- 1942**: A red thought bubble shows a laptop computer.

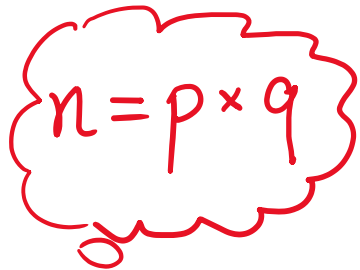


Une rapide histoire de la cryptologie



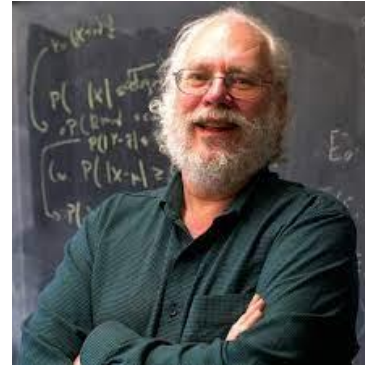
Diffie Hellman

1976*



1977

(...)



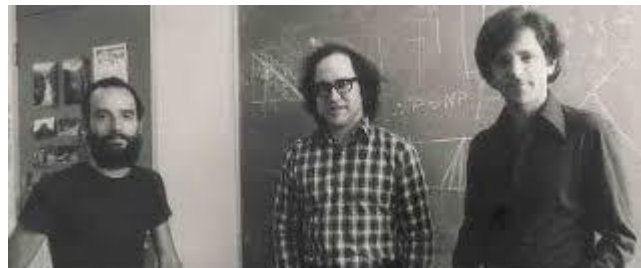
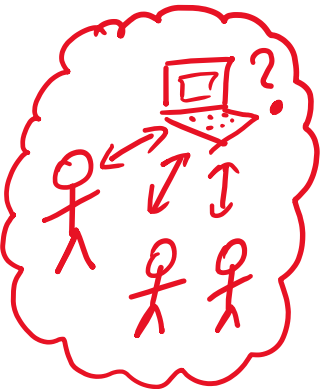
1994



2006

NIST

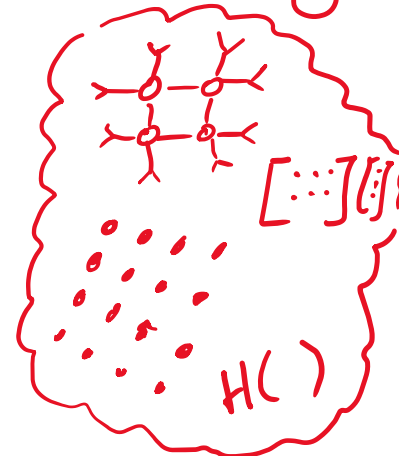
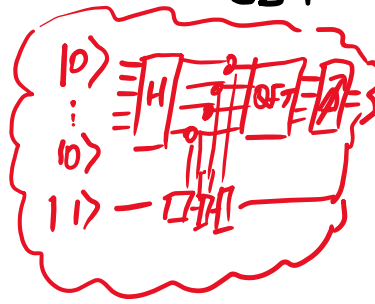
2017 +



R

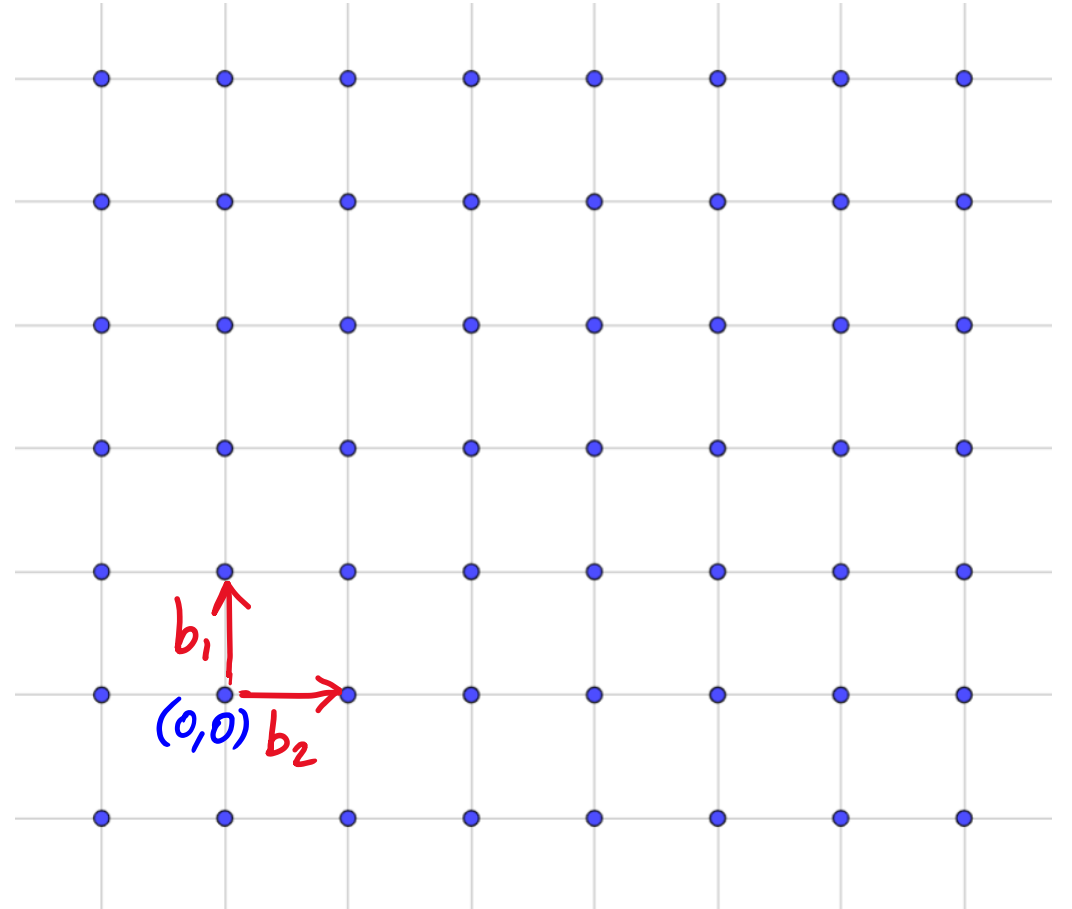
S

A



Cryptographie à base de réseaux Euclidiens

$$\mathcal{L} = \left\{ \sum_{i=1}^n a_i b_i \mid (a_1, \dots, a_n) \in \mathbb{Z}^n \right\}$$

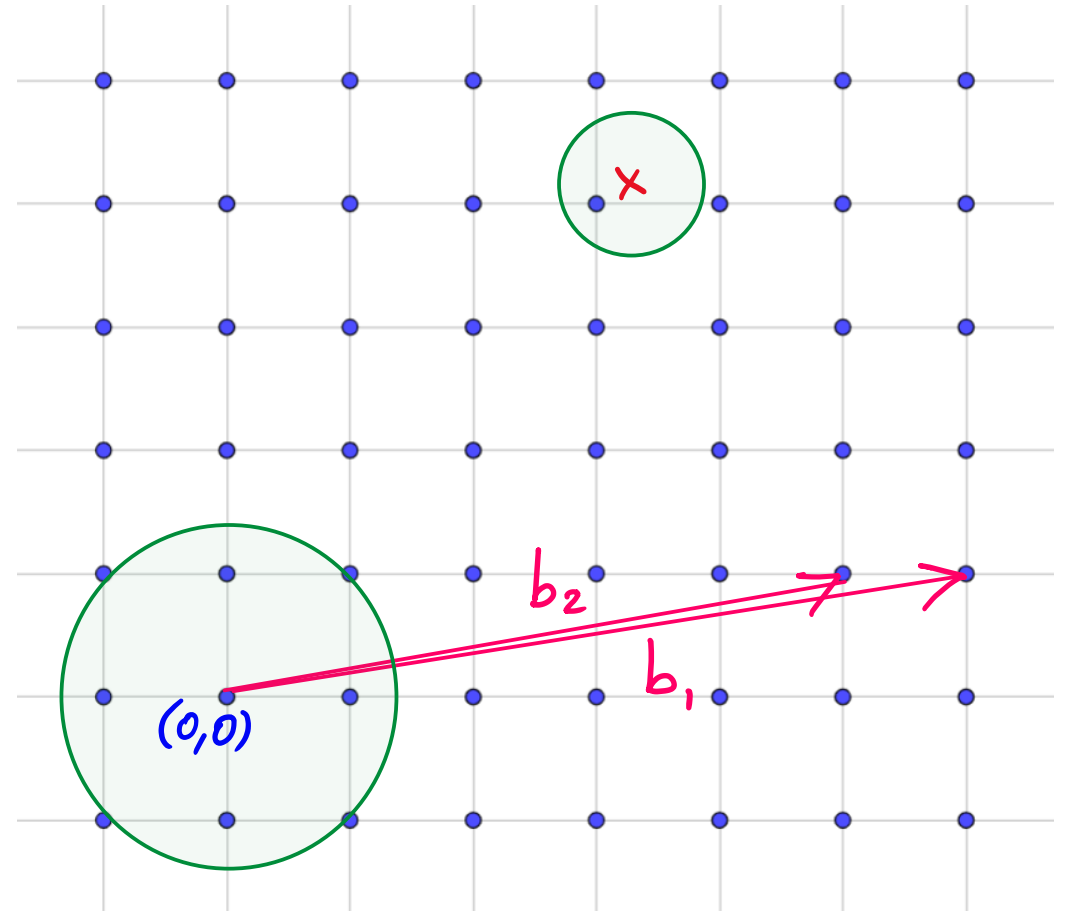


Cryptographie à base de réseaux Euclidiens

$$\mathcal{L} = \left\{ \sum_{i=1}^n a_i b_i \mid (a_1, \dots, a_n) \in \mathbb{Z}^n \right\}$$

Nouveaux problèmes « durs » pour remplacer la factorisation :

- Trouver un vecteur court
- Trouver un point du réseau proche d'un point donné
- Trouver une base de vecteurs courts



Et en pratique ?

Contraintes d'efficacité

$n \approx 1000$ (C'est gros)

Il faut choisir des réseaux spéciaux issus de la théorie algébrique des nombres.

De nouvelles faiblesses à exploiter ?

Choisir les bons paramètres

Protocole crypto

est au moins aussi dur que

Problème mathématique
(plus court vecteur)

affecte les paramètres

Meilleur algorithme
(attaque)

se résout avec

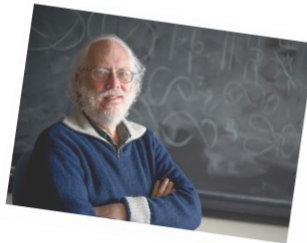
Des questions ?

NEWS | 06 January 2023

Are quantum computers about to break online privacy?

IBM dévoile un processeur quantique record, avec 433 qubits au compteur

8,6 Md\$ dépensés en projets d'informatique quantique en 2022



Peter Shor wins Breakthrough Prize in Fundamental Physics
MIT professor to share \$3 million prize with three others; Daniel Spielman PhD '95 wins Breakthrough Prize in Mathematics.
September 22, 2022

Who's winning the quantum computing race? China and the U.S. are neck and neck