

Soutenance de Thèse de Doctorat
Discipline Informatique

CONTRIBUTIONS À LA CRYPTOGRAPHIE POST-QUANTIQUE

Jean-Christophe Deneuville
[<jean-christophe.deneuville@xlim.fr>](mailto:jean-christophe.deneuville@xlim.fr)

1^{er} décembre 2016

Cryptographie

Cryptographie



Contexte :

souhaite envoyer le message



à

Cryptographie



Contexte :

souhaite envoyer le message



à

Objectifs de la crypto : Assurer

- ① Authentification
- ② Confidentialité
- ③ Intégrité
- ④ Non-Répudiation

Cryptographie



Contexte :

souhaite envoyer le message



à

Objectifs de la crypto : Assurer

- ① Authentification
- ② Confidentialité
- ③ Intégrité
- ④ Non-Répudiation



Cryptographie



Contexte :

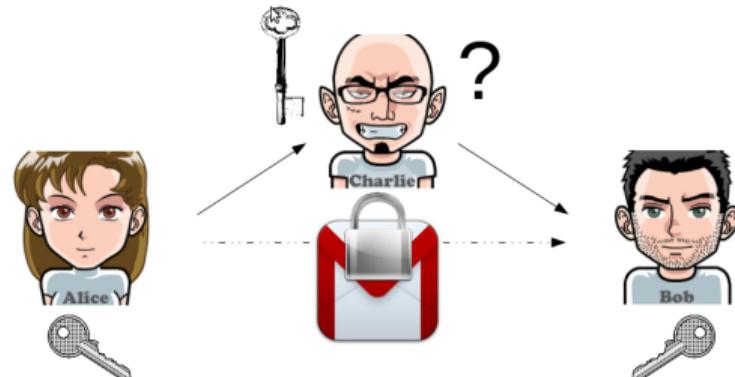
souhaite envoyer le message



à

Objectifs de la crypto : Assurer

- ① Authentification
- ② Confidentialité
- ③ Intégrité
- ④ Non-Répudiation



Cryptographie



Contexte :

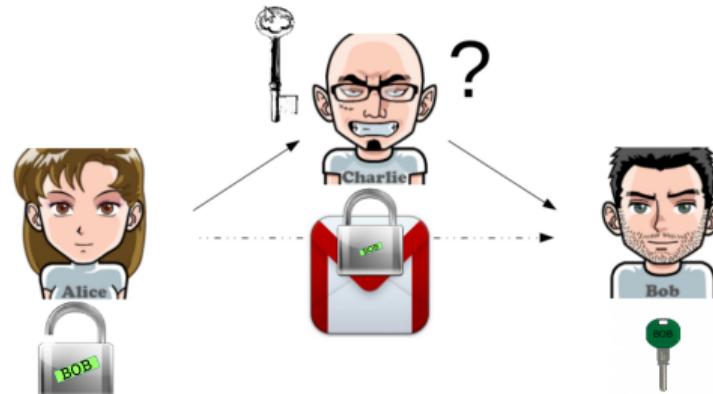
souhaite envoyer le message



à

Objectifs de la crypto : Assurer

- ① Authentification
- ② Confidentialité
- ③ Intégrité
- ④ Non-Répudiation



Cryptographie



Contexte :

souhaite envoyer le message



à

Objectifs de la crypto : Assurer

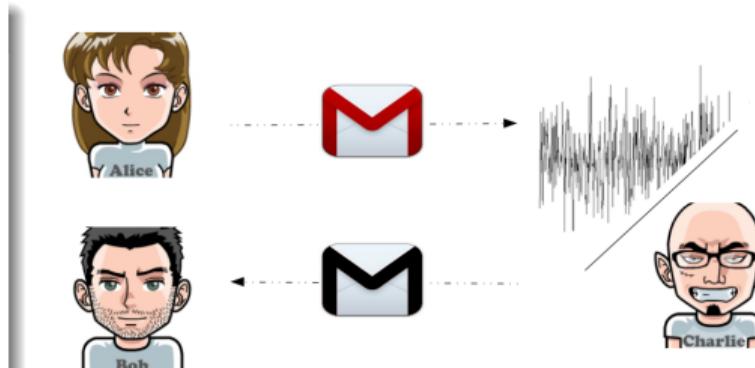
① Authentification



② Confidentialité



③ Intégrité



④ Non-Répudiation

Cryptographie



Contexte :

souhaite envoyer le message



à

Objectifs de la crypto : Assurer

① Authentification



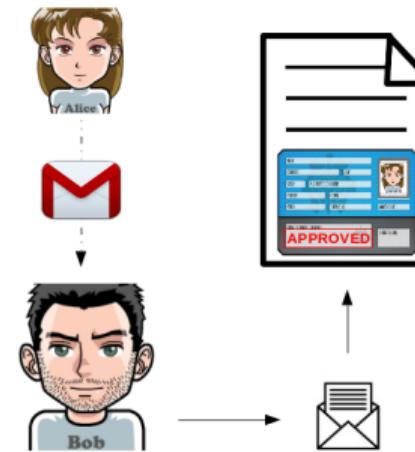
② Confidentialité



③ Intégrité



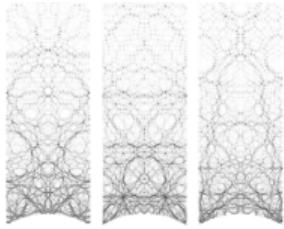
④ Non-Répudiation



Techniques actuelles et limitations

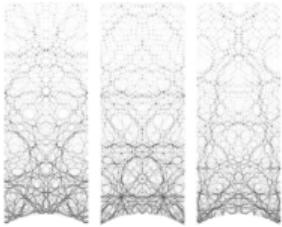
Techniques actuelles et limitations

Factorisation de
grands entiers

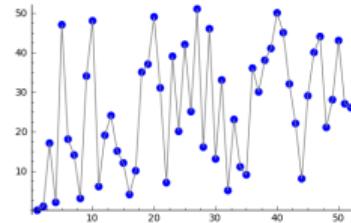


Techniques actuelles et limitations

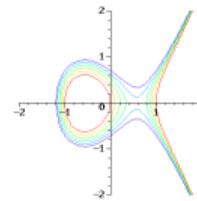
Factorisation de grands entiers



Logarithme Discret sur les Corps Finis

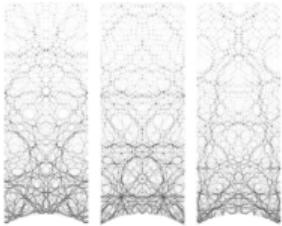


Logarithme Discret sur les Courbes Elliptiques

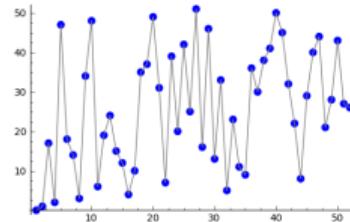


Techniques actuelles et limitations

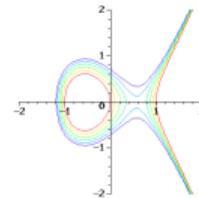
Factorisation de grands entiers



Logarithme Discret sur les Corps Finis



Logarithme Discret sur les Courbes Elliptiques

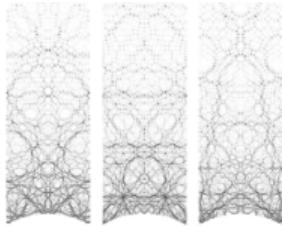


Avantages

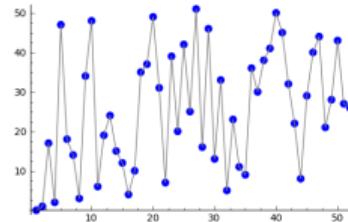
- Bien étudiés \Rightarrow Confiance
- Répandus \Rightarrow Embarqués presque partout

Techniques actuelles et limitations

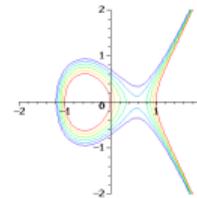
Factorisation de grands entiers



Logarithme Discret sur les Corps Finis



Logarithme Discret sur les Courbes Elliptiques



Avantages

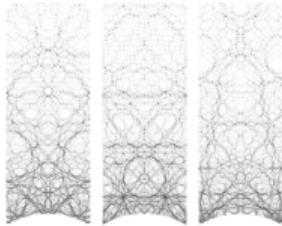
- Bien étudiés \Rightarrow Confiance
- Répandus \Rightarrow Embarqués presque partout

Inconvénients

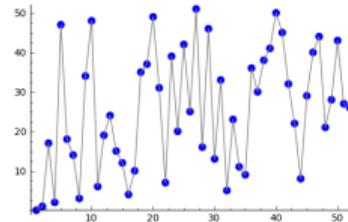
- Gourmands ! Nécessitent des entiers de très grande taille

Techniques actuelles et limitations

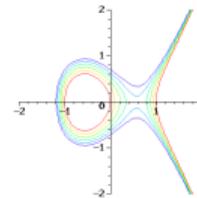
Factorisation de grands entiers



Logarithme Discret sur les Corps Finis



Logarithme Discret sur les Courbes Elliptiques



Avantages

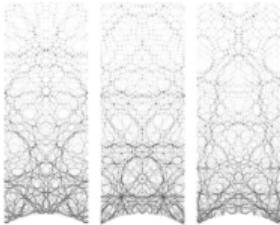
- Bien étudiés \Rightarrow Confiance
- Répandus \Rightarrow Embarqués presque partout

Inconvénients

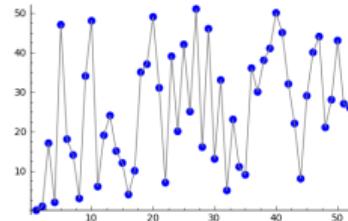
- Gourmands ! Nécessitent des entiers de très grande taille
- Ne pourront pas résister aux futurs ordinateurs quantiques [Sho97]

Techniques actuelles et limitations

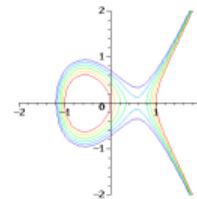
Factorisation de grands entiers



Logarithme Discret sur les Corps Finis



Logarithme Discret sur les Courbes Elliptiques



Avantages

- Bien étudiés \Rightarrow Confiance
- Répandus \Rightarrow Embarqués presque partout

Inconvénients

- Gourmands ! Nécessitent des entiers de très grande taille
- Ne pourront pas résister aux futurs ordinateurs quantiques [Sho97]



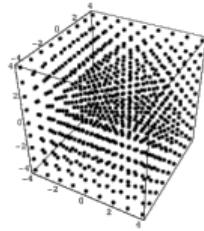
Intérêt de la Crypto Post-Quantique

Intérêt de la Crypto Post-Quantique

Outils mathématiques
a priori résistants
à un ordinateur
quantique

Intérêt de la Crypto Post-Quantique

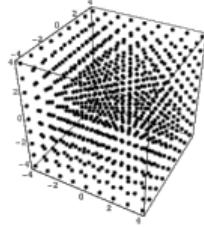
Réseaux Euclidiens



Outils mathématiques
a priori résistants
à un ordinateur
quantique

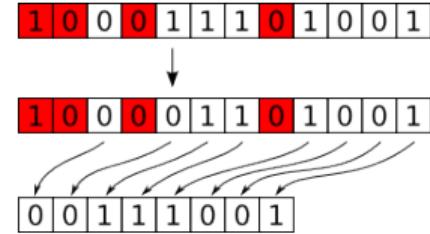
Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



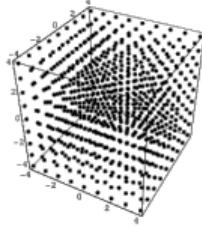
Outils mathématiques
a priori résistants
à un ordinateur
quantique

Codes Correcteurs d'Erreurs



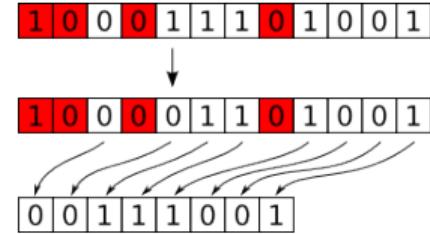
Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



Outils mathématiques
a priori résistants
à un ordinateur
quantique

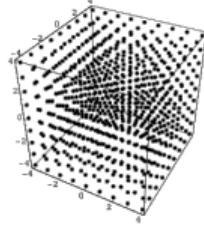
Codes Correcteurs d'Erreurs



Avantages :

Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens

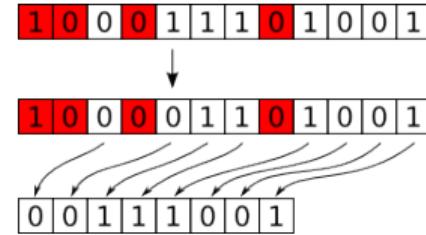


Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers

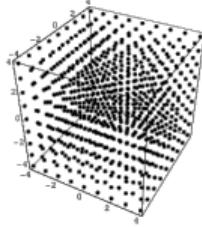
Avantages :

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens

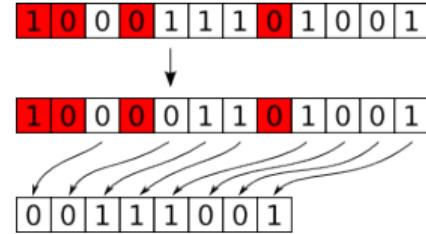


Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers
- opérations simples (algèbre linéaire)

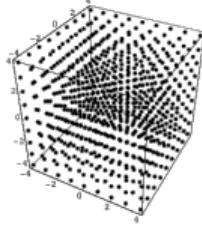
Avantages :

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens

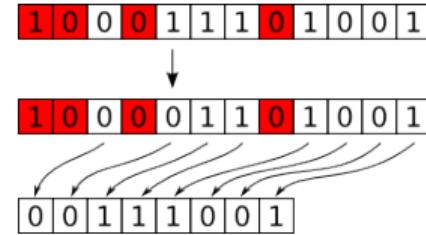


Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers
- opérations simples (algèbre linéaire)
- réductions de sécurité

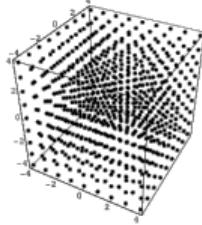
Avantages :

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens

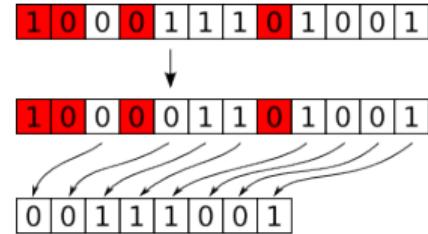


Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers
- opérations simples (algèbre linéaire)
- réductions de sécurité
- Chiffrement complètement homomorphe

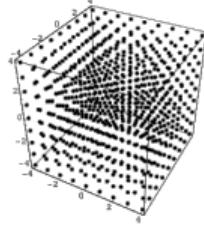
Avantages :

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



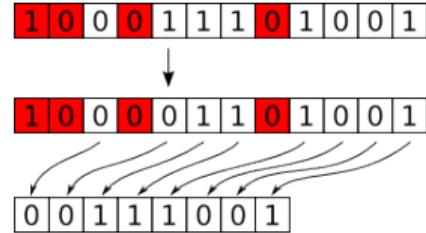
Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers
- opérations simples (algèbre linéaire)
- réductions de sécurité

Avantages :

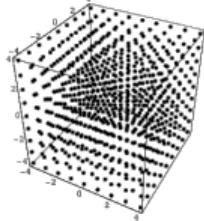
- Chiffrement complètement homomorphe
- Chiffrement basé sur les attributs

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



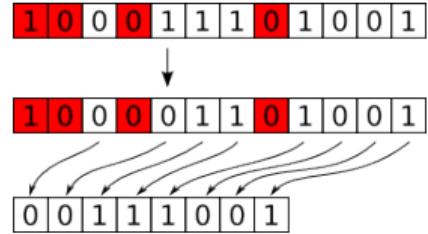
Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers
- opérations simples (algèbre linéaire)
- réductions de sécurité

Avantages :

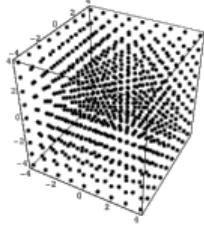
- Chiffrement complètement homomorphe
- Chiffrement basé sur les attributs
- Obfuscation, ...

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



Outils mathématiques
a priori résistants
à un ordinateur
quantique

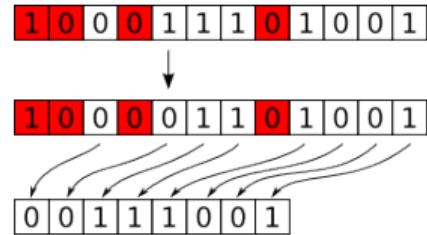
- arithmétique petits entiers
- opérations simples (algèbre linéaire)
- réductions de sécurité

Avantages :

- Chiffrement complètement homomorphe
- Chiffrement basé sur les attributs
- Obfuscation, ...

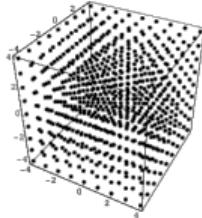
→ **Objectif de la Thèse :**

Codes Correcteurs d'Erreurs



Intérêt de la Crypto Post-Quantique

Réseaux Euclidiens



Outils mathématiques
a priori résistants
à un ordinateur
quantique

- arithmétique petits entiers

Avantages :

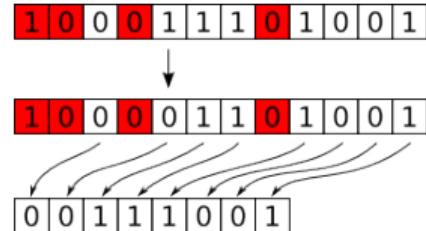
- opérations simples (algèbre linéaire)
- réductions de sécurité

- Chiffrement complètement homomorphe
- Chiffrement basé sur les attributs
- Obfuscation, ...

→ **Objectif de la Thèse :**

Concevoir de nouveaux schémas a priori résistants aux ordinateurs quantiques en utilisant des outils alternatifs. (réseaux euclidiens et codes correcteurs d'erreurs)

Codes Correcteurs d'Erreurs



Plan

- 1 Cryptographie Post-Quantique
- 2 Signature basée sur les Réseaux
- 3 Cryptosystèmes sur les Codes

Plan

1 Cryptographie Post-Quantique

- Problèmes et Métriques
- Outils Mathématiques

2 Signature basée sur les Réseaux

3 Cryptosystèmes sur les Codes

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
- Logarithme Discret } Pré-Quantique
- Vecteur le plus court / proche → réseaux
- Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \xleftarrow{\$} \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$
tel que $\mathbf{Hx} = \mathbf{s}$.

Difficulté du problème :

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$ tel que $\mathbf{Hx} = \mathbf{s}$.

Difficulté du problème : simple (pivot de Gauss)

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$ de poids faible (pour une certaine métrique) tel que $\mathbf{Hx} = \mathbf{s}$.

Difficulté du problème : NP-difficile

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$ de poids faible (pour une certaine métrique) tel que $\mathbf{Hx} = \mathbf{s}$.

- Distance Euclidienne → Cryptographie sur les Réseaux

Difficulté du problème : NP-difficile

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$ de poids faible (pour une certaine métrique) tel que $\mathbf{Hx} = \mathbf{s}$.

Difficulté du problème : NP-difficile

- Distance Euclidienne → Cryptographie sur les Réseaux
 - Distance de Hamming → Cryptographie sur les Codes

La cryptographie repose sur des **problèmes difficiles**

- Factorisation
 - Logarithme Discret } Pré-Quantique
 - Vecteur le plus court / proche → réseaux
 - Décodage de syndrômes → codes correcteurs } Post-Quantique

Sécurité en codes et en réseaux → un problème d'algèbre linéaire

Étant donnés $\mathbf{H} \in \mathbb{F}^{(n-k) \times n}$ et $\mathbf{s} \in \mathbb{F}^{n-k}$, trouver $\mathbf{x} \in \mathbb{F}^n$ de poids faible (pour une certaine métrique) tel que $\mathbf{Hx} = \mathbf{s}$.

Difficulté du problème : NP-difficile

- Distance Euclidienne → Cryptographie sur les Réseaux
 - Distance de Hamming → Cryptographie sur les Codes
 - Distance Rang → Cryptographie sur la Métrique Rang

Plan

1 Cryptographie Post-Quantique

- Problèmes et Métriques
- Outils Mathématiques

2 Signature basée sur les Réseaux

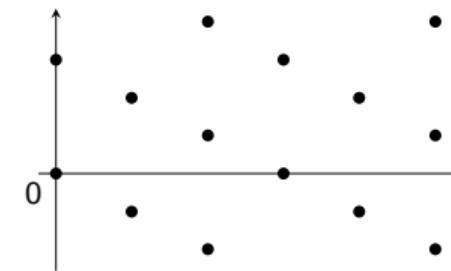
3 Cryptosystèmes sur les Codes

Réseaux Euclidiens

- Ensemble périodique de point

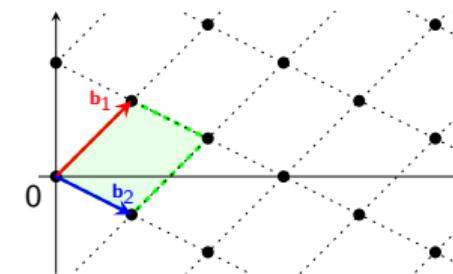
Réseaux Euclidiens

- Ensemble périodique de point



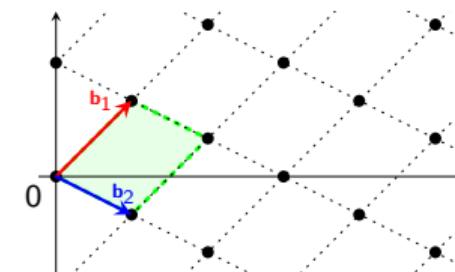
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base



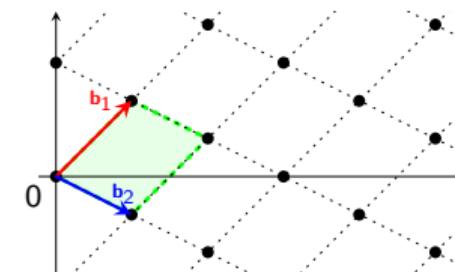
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes **entières** de vecteurs



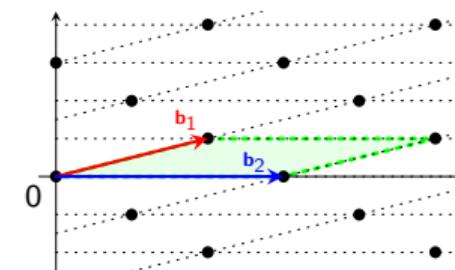
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



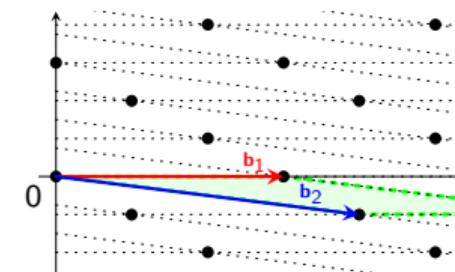
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



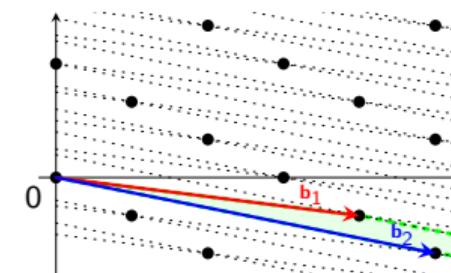
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



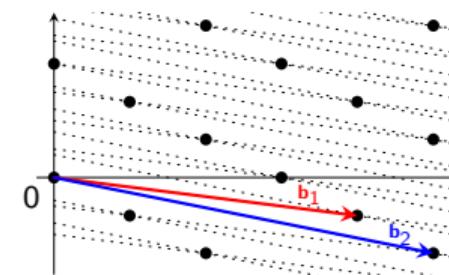
Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles

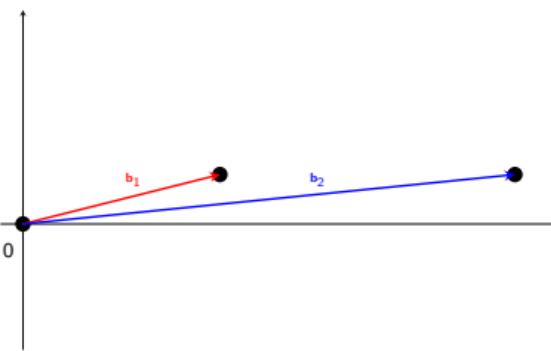


Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles

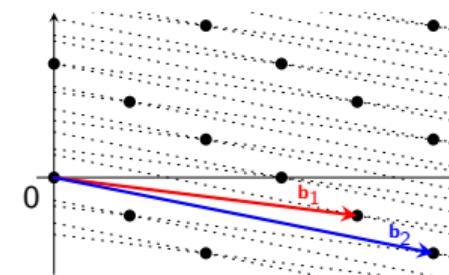


Closest Vector Problem

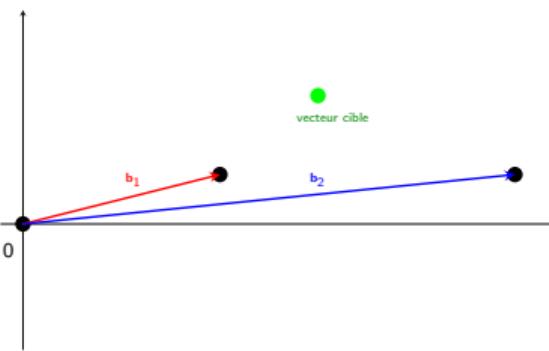


Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles

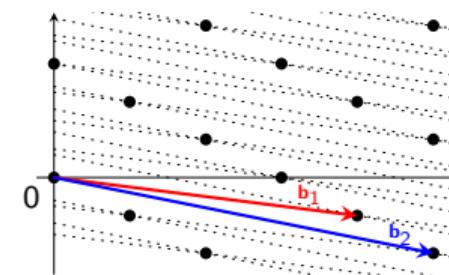


Closest Vector Problem

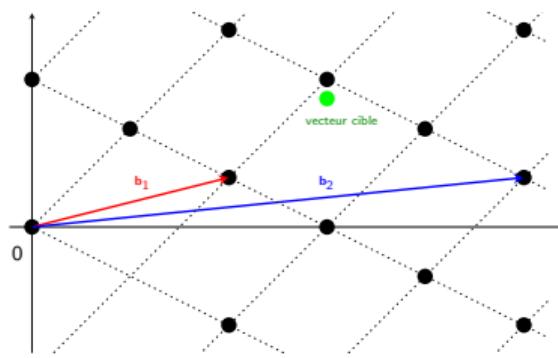


Réseaux Euclidiens

- Ensemble périodique de points
 - Muni d'une base
 - Sommes entières de vecteurs
 - Infinité de bases possibles

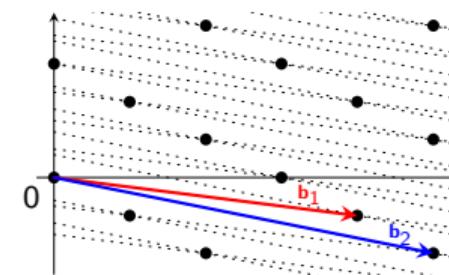


Closest Vector Problem

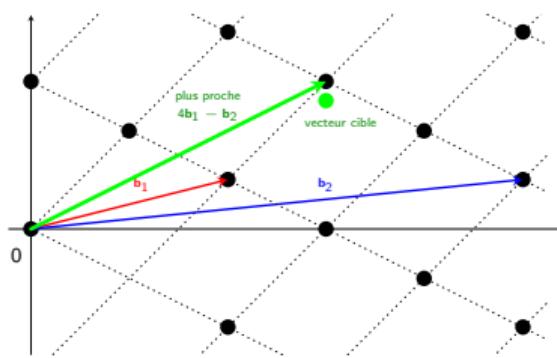


Réseaux Euclidiens

- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles

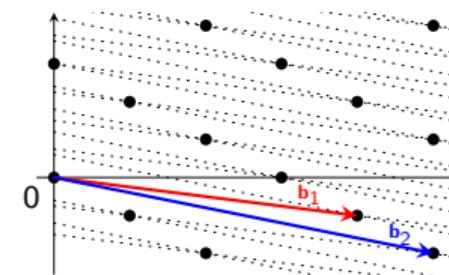


Closest Vector Problem

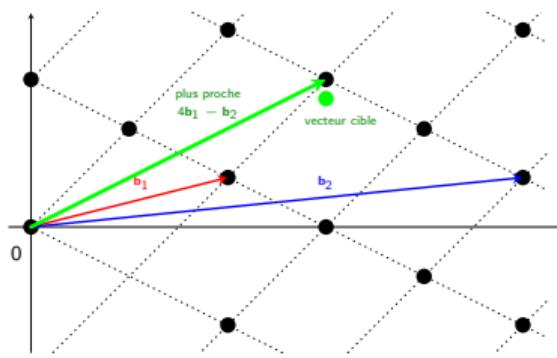


Réseaux Euclidiens

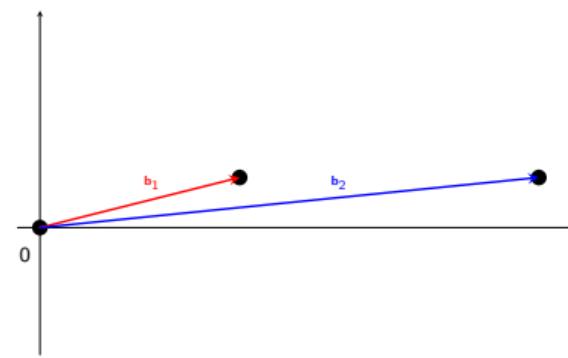
- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



Closest Vector Problem

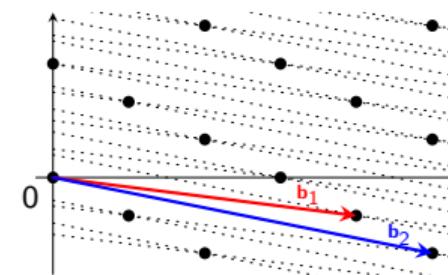


Shortest Vector Problem

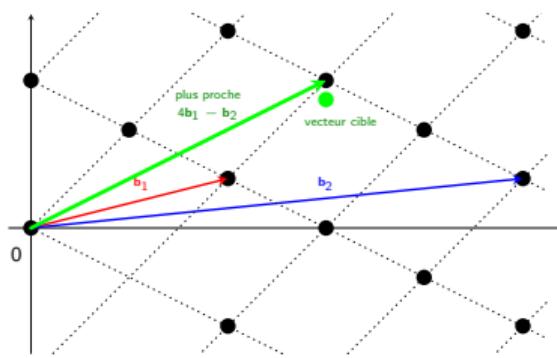


Réseaux Euclidiens

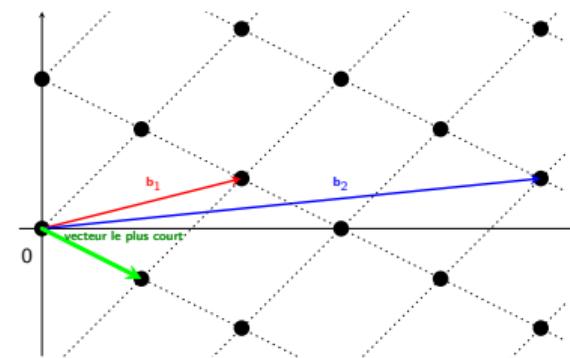
- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



Closest Vector Problem

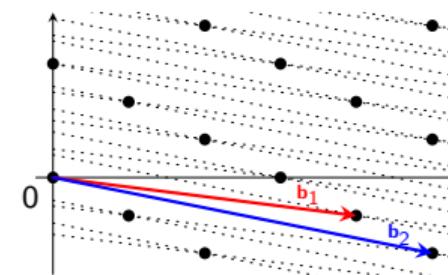


Shortest Vector Problem

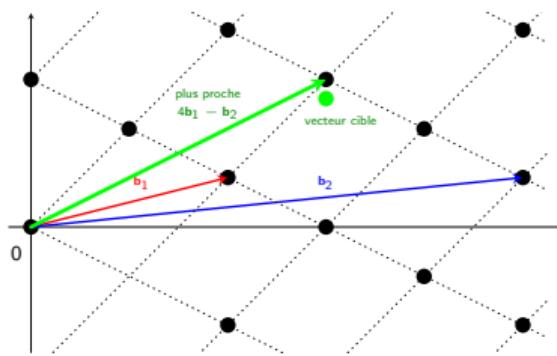


Réseaux Euclidiens

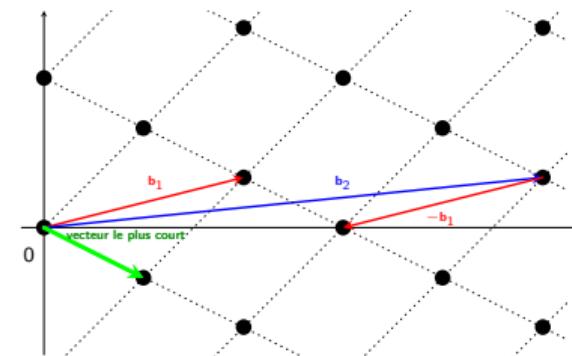
- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



Closest Vector Problem

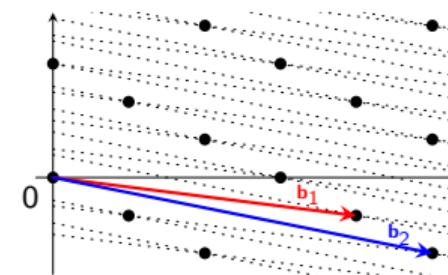


Shortest Vector Problem

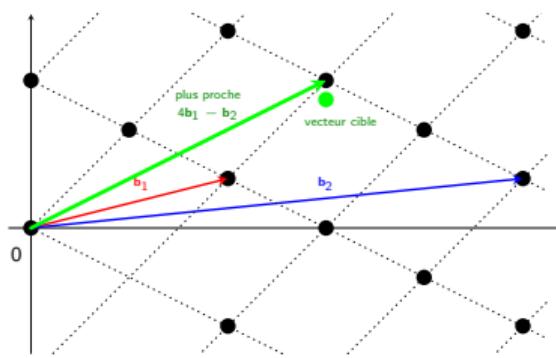


Réseaux Euclidiens

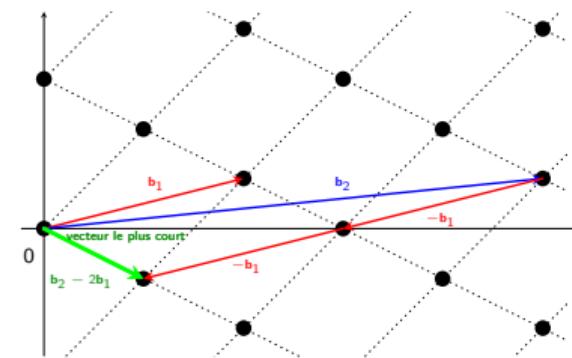
- Ensemble périodique de point
- Muni d'une base
- Sommes entières de vecteurs
- Infinité de bases possibles



Closest Vector Problem



Shortest Vector Problem



Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur ⇒ Renvoi
 - De corriger l'erreur

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons \mathbb{F}_5^7

$$\begin{aligned}\mathbf{u} &= \boxed{3 \quad 3 \quad 2 \quad 4 \quad 4 \quad 5 \quad 2} \\ \mathbf{v} &= \boxed{5 \quad 3 \quad 1 \quad 2 \quad 4 \quad 5 \quad 5}\end{aligned}$$

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons \mathbb{F}_5^7

$$\begin{aligned}\mathbf{u} &= \boxed{\begin{array}{ccccccc} 3 & 3 & 2 & 4 & 4 & 5 & 2 \end{array}} \\ \mathbf{v} &= \boxed{\begin{array}{ccccccc} 5 & 3 & 1 & 2 & 4 & 5 & 5 \end{array}}\end{aligned}$$

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons $\mathbb{F}_5^7 \rightarrow d_H(\mathbf{u}, \mathbf{v}) = 4$

$$\begin{aligned}\mathbf{u} &= \boxed{3 \quad 3 \quad 2 \quad 4 \quad 4 \quad 5 \quad 2} \\ \mathbf{v} &= \boxed{5 \quad 3 \quad 1 \quad 2 \quad 4 \quad 5 \quad 5}\end{aligned}$$

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons $\mathbb{F}_5^7 \rightarrow d_H(\mathbf{u}, \mathbf{v}) = 4$

$$\begin{aligned}\mathbf{u} &= \boxed{3 \quad 3 \quad 2 \quad 4 \quad 4 \quad 5 \quad 2} \\ \mathbf{v} &= \boxed{5 \quad 3 \quad 1 \quad 2 \quad 4 \quad 5 \quad 5}\end{aligned}$$

- Métrique bien étudiée

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons $\mathbb{F}_5^7 \rightarrow d_H(\mathbf{u}, \mathbf{v}) = 4$

$$\begin{aligned}\mathbf{u} &= \boxed{3 \quad 3 \quad 2 \quad 4 \quad 4 \quad 5 \quad 2} \\ \mathbf{v} &= \boxed{5 \quad 3 \quad 1 \quad 2 \quad 4 \quad 5 \quad 5}\end{aligned}$$

- Métrique bien étudiée
- Nombreuses familles avec différentes propriétés

Codes Correcteurs

Théorie des Codes

- Ajout de redondance à l'information
- En cas d'erreur(s), la redondance permet soit :
 - De détecter l'erreur \Rightarrow Renvoi
 - De corriger l'erreur

Exemple basique : code à 3-répétition

- Alice souhaite envoyer $1 \cdot 0 \cdot 1$
- Elle envoie $111 \cdot 000 \cdot 111$ à Bob
- Bob reçoit $101 \cdot 001 \cdot 111$
- Il interprète correctement en $1 \cdot 0 \cdot 1$

Métrique de Hamming

$\mathbf{u}, \mathbf{v} \in \mathbb{F}_q^n$, disons $\mathbb{F}_5^7 \rightarrow d_H(\mathbf{u}, \mathbf{v}) = 4$

$$\begin{array}{c} \mathbf{u} = \boxed{3 \quad 3 \quad 2 \quad 4 \quad 4 \quad 5 \quad 2} \\ \mathbf{v} = \boxed{5 \quad 3 \quad 1 \quad 2 \quad 4 \quad 5 \quad 5} \end{array}$$

- Métrique bien étudiée
- Nombreuses familles avec différentes propriétés
- Attaques plus directes qu'en métrique rang

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
 - Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 2 \\ 2 & 0 & 2 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 3 & 2 \\ 2 & 0 & 2 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

Définitions

Rang d'un vecteur $\mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ rang de la matrice ainsi obtenue

(ne dépend pas de la base choisie)

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

Définitions

Rang d'un vecteur $\mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ rang de la matrice ainsi obtenue

(ne dépend pas de la base choisie)

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

Définitions

Rang d'un vecteur $\mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ rang de la matrice ainsi obtenue

(ne dépend pas de la base choisie)

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$

$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

$$\rightarrow \text{rang}(\mathbf{v}) = 2$$

Définitions

Rang d'un vecteur $\mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ rang de la matrice ainsi obtenue

(ne dépend pas de la base choisie)

Métrique Rang

- Extension de corps fini \mathbb{F}_{q^m} , disons \mathbb{F}_{5^3}
- Base (b_1, \dots, b_m) de \mathbb{F}_{q^m} sur \mathbb{F}_q
- disons $(1, \alpha, \alpha^2)$, α racine de $X^3 + X + 1$,
 $\mathbb{F}_{5^3} \cong \mathbb{F}_5/(X^3 + X + 1)$
- $\mathbf{v} \in \mathbb{F}_{q^m}^n$ s'écrit comme une matrice
 $\mathbf{V} \in \mathbb{F}_q^{m \times n}$ dans cette base

Exemple avec $q = 5$, $m = 3$, et $n = 3$:

$$\mathbf{v} = \begin{pmatrix} 1 + 4\alpha + 2\alpha^2 & 2 + 3\alpha & 3 + 2\alpha + 2\alpha^2 \end{pmatrix}$$
$$\mathbf{V} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{matrix} 1 \\ \alpha \\ \alpha^2 \end{matrix}$$

→ $\text{rang}(\mathbf{v}) = 2$

Définitions

Rang d'un vecteur $\mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ rang de la matrice ainsi obtenue

(ne dépend pas de la base choisie)

Distance rang entre deux vecteurs $\mathbf{u}, \mathbf{v} \in \mathbb{F}_{q^m}^n$:

→ $d_R(\mathbf{u}, \mathbf{v}) = \text{rang}(\mathbf{U} - \mathbf{V})$

(symétrie, séparation, inégalité triangulaire)

Attaques sur ces Métriques

Idée : Compter le nombre de mots possibles de longueur n et de poids t

Attaques sur ces Métriques

Idée : Compter le nombre de mots possibles de longueur n et de poids t

Hamming : nombre d'ensembles à t éléments parmi les ensembles à n éléments : binôme de Newton
 $\binom{n}{t}$ ($\leq 2^n$)

Attaques sur ces Métriques

Idée : Compter le nombre de mots possibles de longueur n et de poids t

Hamming : nombre d'ensembles à t éléments parmi les ensembles à n éléments : binôme de Newton
 $\binom{n}{t}$ ($\leq 2^n$)

Rank : nombre de sous-espaces vectoriels de dimension t sur \mathbb{F}_q dans un espace de dimension n sur \mathbb{F}_{q^m} : binôme de Gauss $\begin{bmatrix} n \\ t \end{bmatrix}_q (\sim q^{t(n-t)})$

Attaques sur ces Métriques

Idée : Compter le nombre de mots possibles de longueur n et de poids t

Hamming : nombre d'ensembles à t éléments parmi les ensembles à n éléments : binôme de Newton
 $\binom{n}{t}$ ($\leq 2^n$)

Rank : nombre de sous-espaces vectoriels de dimension t sur \mathbb{F}_q dans un espace de dimension n sur \mathbb{F}_{q^m} : binôme de Gauss $\begin{bmatrix} n \\ t \end{bmatrix}_q (\sim q^{t(n-t)})$

En résumé : les attaques en **métrique Rang** ont une complexité **quadratiquement** exponentielle $2^{\mathcal{O}(n^2)}$, contre **simplement** exponentielle $2^{\mathcal{O}(n)}$ pour la **métrique de Hamming**

Plan

1 Cryptographie Post-Quantique

2 Signature basée sur les Réseaux

- Réparation de NTRUSign
- Extension en une Signature Traçable

3 Cryptosystèmes sur les Codes

NTRUSign

Historique

- Initialement NSS [HPS01]
- NTRUSign [HHGP⁺03]

NSS: An NTRU Lattice-Based Signature Scheme

Jeffrey Hoffstein, Jill Pipher, and Joseph H. Silverman

NTRU Cryptosystems, Inc., 5 Burlington Woods,
Burlington, MA 01803 USA,
jhoff@ntru.com, jpipher@ntru.com, jhs@ntru.com

Abstract. A new authentication and digital signature scheme called the NTRU Signature Scheme (NSS) is introduced. NSS provides an authentication/signature method complementary to the NTRU public key cryptosystem. The hard lattice problem underlying NSS is similar to the hard problem underlying NTRU, and NSS similarly features high speed, low footprint, and easy key creation.

NTRUSign

Historique

- Initialement NSS [HPS01]
- Rapidement cassé [GS02]
- NTRUSign [HHGP⁺03]

Cryptanalysis of the Revised NTRU Signature Scheme

Craig Gentry¹ and Mike Szydlo²

¹ DoCoMo USA Lab, San Jose, CA, USA,
cgentry@docomolabs-usa.com

² RSA Laboratories, Bedford, MA, USA,
mszydlo@rsa.com

Abstract. In this paper, we describe a three-stage attack against Revised NSS, an NTRU-based signature scheme proposed at the Eurocrypt 2001 conference as an enhancement of the (broken) proceedings version of the scheme. The first stage, which typically uses a transcript of only 4 signatures, effectively cuts the key length in half while completely avoiding the intended hard lattice problem. After an empirically fast second stage, the third stage of the attack combines lattice-based and congruence-based methods in a novel way to recover the private key in polynomial time. This cryptanalysis shows that a passive adversary observing only a few valid signatures can recover the signer's entire private key. We also briefly address the security of NTRUSign, another NTRU-based signature scheme that was recently proposed at the rump session of Asiacrypt 2001. As we explain, some of our attacks on Revised NSS may be extended to NTRUSign, but a much longer transcript is necessary. We also indicate how the security of NTRUSign is based on the hardness of several problems, not solely on the hardness of the usual NTRU lattice problem.

NTRUSign

Historique

- Initialement NSS [HPS01]
Rapidement cassé [GS02]
- NTRUSign [HHGP⁺03]

NTRUSign

Historique

- Initialement NSS [HPS01]
Rapidement cassé [GS02]
- NTRUSign [HHGP⁺03]

$$\mathbf{P} = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{h} \\ \mathbf{0} & \mathbf{q} \end{array} \right) \quad \mathbf{S} = \left(\begin{array}{c|c} \mathbf{f} & \mathbf{F} \\ \mathbf{g} & \mathbf{G} \end{array} \right)$$

NTRUSign

Historique

- Initialement NSS [HPS01]
- Rapidement cassé [GS02]
- NTRUSign [HHGP⁺03]

$$\begin{aligned} \mathbf{f}, \mathbf{g} &= \begin{cases} d \text{ coefficients } + 1 \\ N - d \text{ coefficients } 0 \end{cases} \\ \mathbf{F}, \mathbf{G} &\text{ tels que } \mathbf{f} * \mathbf{G} - \mathbf{F} * \mathbf{g} = q \\ \mathbf{h} &= \mathbf{F} * \mathbf{f}^{-1} \stackrel{\$}{\rightsquigarrow} \mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1 \rangle \end{aligned}$$

$$\mathbf{P} = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{h} \\ \hline \mathbf{0} & \mathbf{q} \end{array} \right) \quad \mathbf{S} = \left(\begin{array}{c|c} \mathbf{f} & \mathbf{F} \\ \hline \mathbf{g} & \mathbf{G} \end{array} \right)$$

NTRUSign

Historique

- Initialement NSS [HPS01]
- Rapidement cassé [GS02]
- NTRUSign [HHGP⁺03]

$$\begin{aligned} \mathbf{f}, \mathbf{g} &= \begin{cases} d \text{ coefficients } + 1 \\ N - d \text{ coefficients } 0 \end{cases} \\ \mathbf{F}, \mathbf{G} &\text{ tels que } \mathbf{f} * \mathbf{G} - \mathbf{F} * \mathbf{g} = q \\ \mathbf{h} &= \mathbf{F} * \mathbf{f}^{-1} \stackrel{\$}{\rightsquigarrow} \mathcal{R}_q = \mathbb{Z}_q[X]/\langle X^N + 1 \rangle \end{aligned}$$

$$\mathbf{P} = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{h} \\ \hline \mathbf{0} & \mathbf{q} \end{array} \right) \quad \mathbf{S} = \left(\begin{array}{c|c} \mathbf{f} & \mathbf{F} \\ \hline \mathbf{g} & \mathbf{G} \end{array} \right)$$

$$\text{Réseau NTRU : } \Lambda_{\mathbf{h}, q} = \{(\mathbf{u}, \mathbf{u} * \mathbf{h} \mod q), \mathbf{u} \in \mathcal{R}_q\}$$

NTRUSign

Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

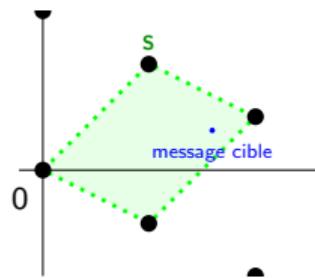
- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}

NTRUSign

Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}

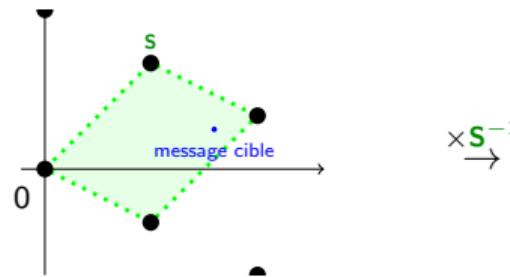


NTRUSign

Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}

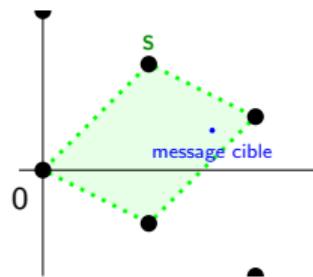


NTRUSign

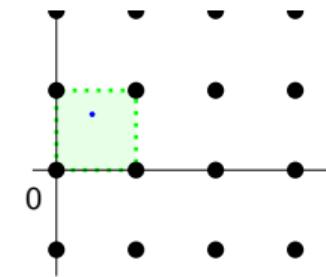
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times \mathbf{S}^{-1}$

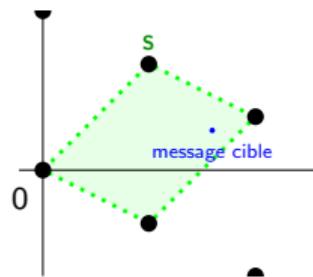


NTRUSign

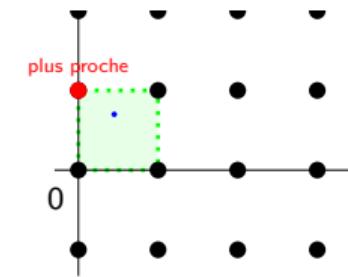
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times S^{-1}$

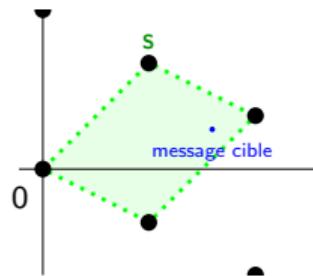


NTRUSign

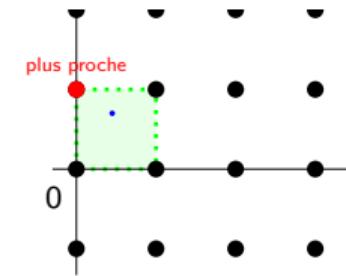
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times \mathbf{S}^{-1}$



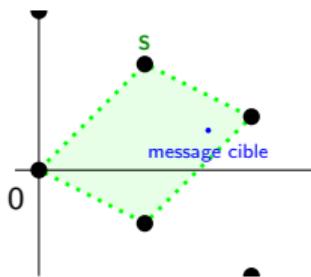
$\times \mathbf{S}$

NTRUSign

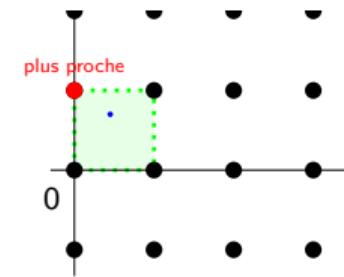
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

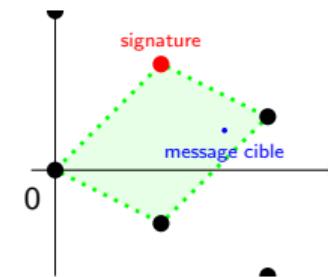
- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times \mathbf{S}^{-1}$



$\times \mathbf{S}$

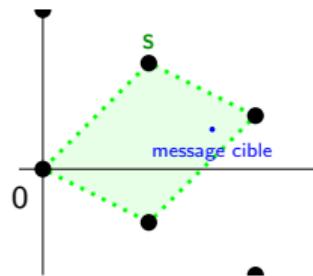


NTRUSign

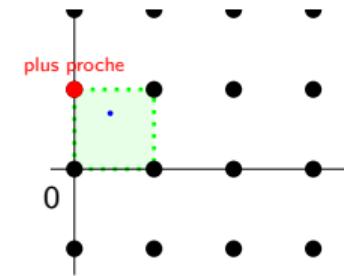
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

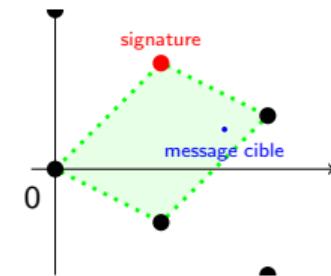
- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times \mathbf{S}^{-1}$



$\times \mathbf{S}$



Verify

Étant donné la signature \mathbf{s} , vérifier que :

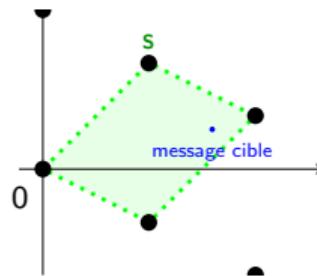
- c'est un point du réseau (en utilisant \mathbf{P})
- il n'est pas trop loin de $(\mathbf{0}, \mathbf{m})$

NTRUSign

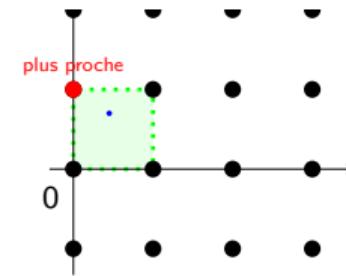
Sign

Pour $\mu \in \{0, 1\}^*$ à signer :

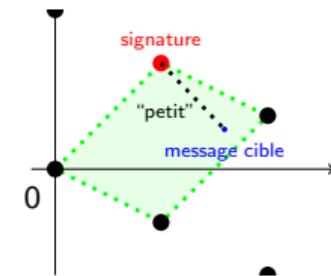
- Soit $\mathbf{m} = \mathcal{H}(\mu)$
- Résoudre CVP sur $(\mathbf{0}, \mathbf{m})$ en utilisant \mathbf{S}



$\times \mathbf{S}^{-1}$



$\times \mathbf{S}$



Verify

Étant donné la signature \mathbf{s} , vérifier que :

- c'est un point du réseau (en utilisant \mathbf{P})
- il n'est pas trop loin de $(\mathbf{0}, \mathbf{m})$

NTRUSign

TAILLE DES SIGNATURES (EN BITS)

sécurité	80	112	128	160
NTRUSign	1256	1576	1784	2367
ECDSA _{sign}	320	448	512	640
RSA	1024	2048	3072	4096

NTRUSign

TAILLE DES SIGNATURES (EN BITS)

sécurité	80	112	128	160
NTRUSign	1256	1576	1784	2367
ECDSA _{sign}	320	448	512	640
RSA	1024	2048	3072	4096

NTRUSign est très rapide !

NTRUSign

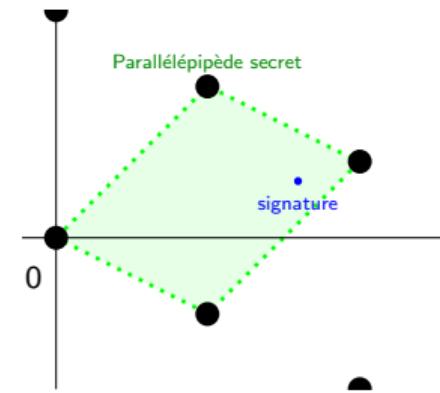
TAILLE DES SIGNATURES (EN BITS)

sécurité	80	112	128	160
NTRUSign	1256	1576	1784	2367
ECDSA _{sign}	320	448	512	640
RSA	1024	2048	3072	4096

NTRUSign est très rapide ! Mais...

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

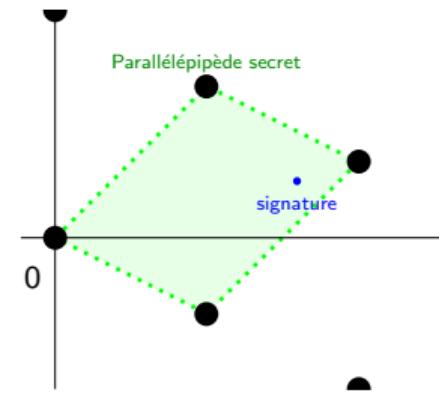


Nombre de signatures publiées : 1

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]

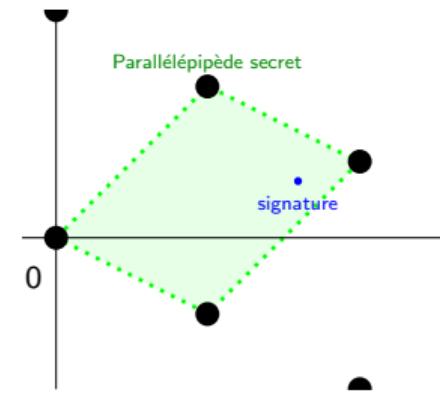


Nombre de signatures publiées : 1

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

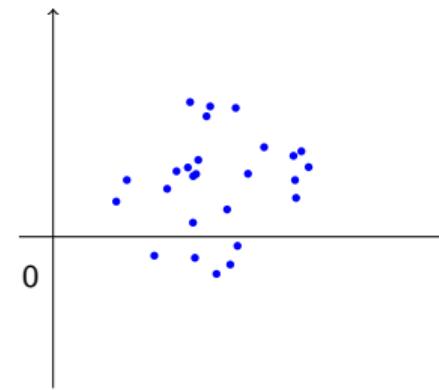


Nombre de signatures publiées : 1

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

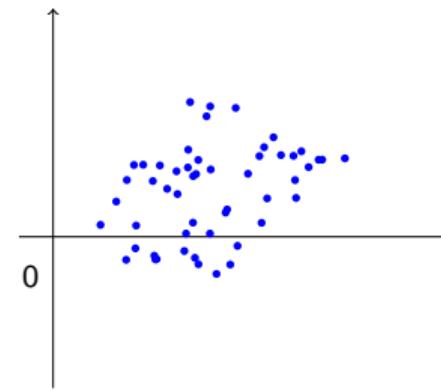


Nombre de signatures publiées : 25

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

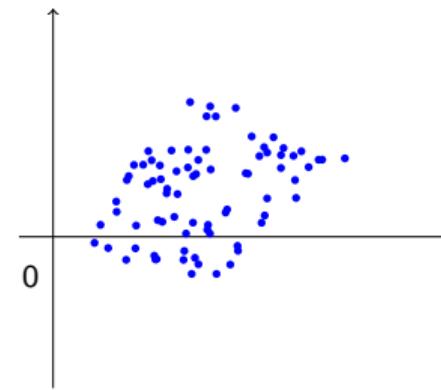


Nombre de signatures publiées : 50

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

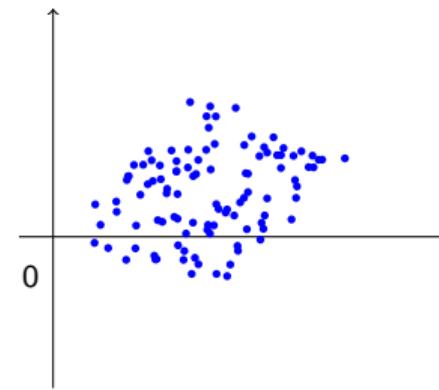


Nombre de signatures publiées : 75

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

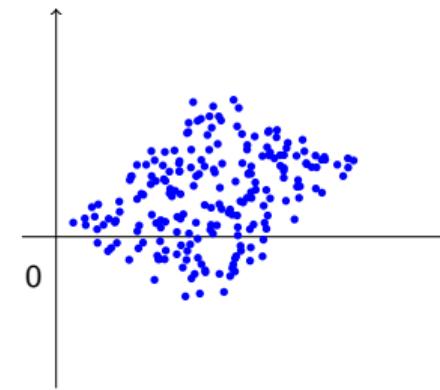


Nombre de signatures publiées : 100

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

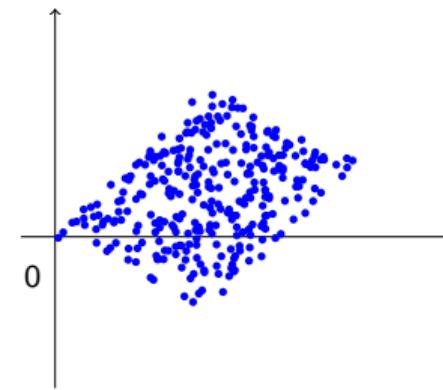


Nombre de signatures publiées : 200

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

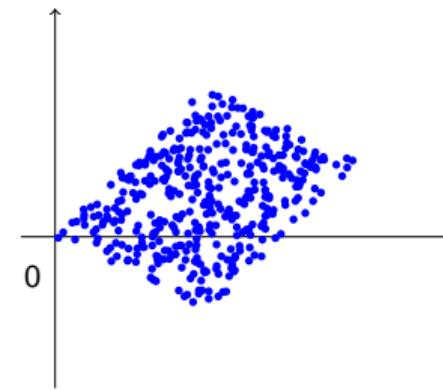


Nombre de signatures publiées : 300

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

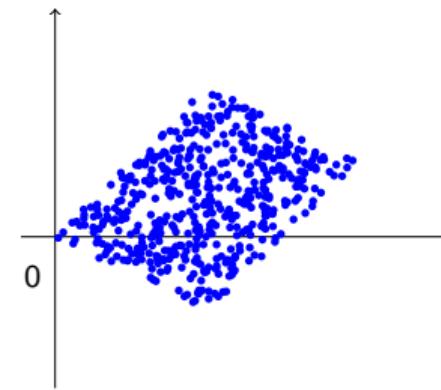


Nombre de signatures publiées : 400

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

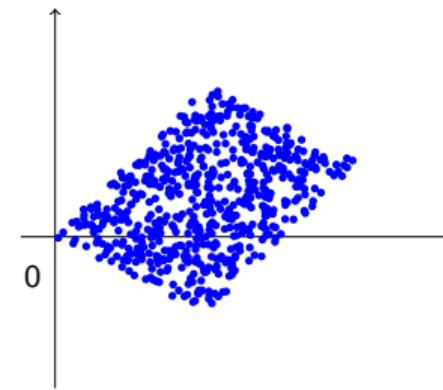


Nombre de signatures publiées : 500

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

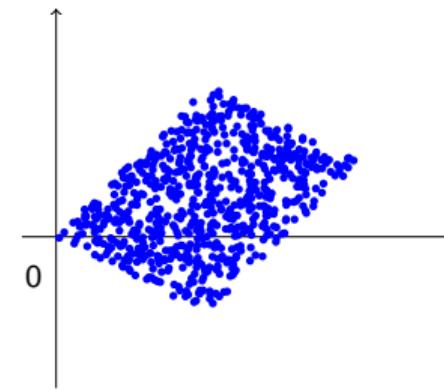


Nombre de signatures publiées : 600

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

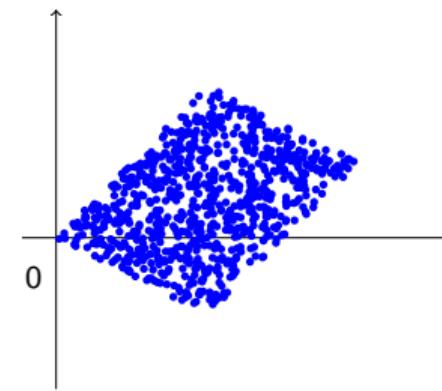


Nombre de signatures publiées : 700

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

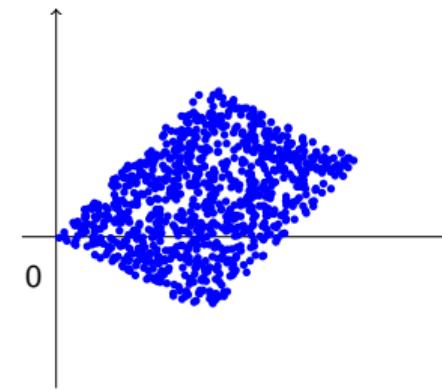


Nombre de signatures publiées : 800

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]

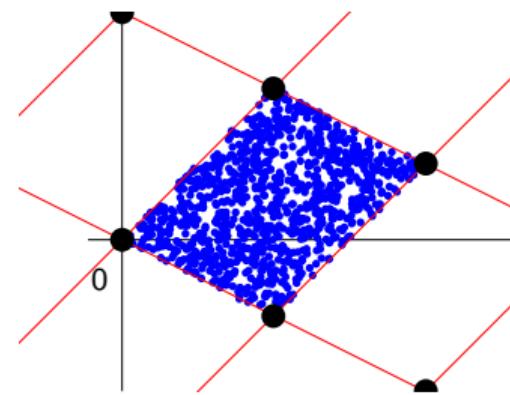


Nombre de signatures publiées : 900

Problème : Fuite d'information

Attaques permettant de retrouver la clé secrète

- Seulement quelques signatures pour le schéma original [NR06]
- Un peu plus pour cryptanalyser les contremesures [DN12]



Nombre de signatures publiées : 1000

Schéma de Lyubashevsky [Lyu12]

KeyGen

- Clé secrète : $\mathbf{S} \xleftarrow{\$} \{-d, \dots, 0, \dots, d\}^{m \times k}$
- Clé Publique : $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ et $\mathbf{T} = \mathbf{A} \cdot \mathbf{S} \in \mathbb{Z}_q^{n \times k}$

Sign

Schéma de Lyubashevsky [Lyu12]

KeyGen

- Clé secrète : $\mathbf{S} \xleftarrow{\$} \{-d, \dots, 0, \dots, d\}^{m \times k}$
- Clé Publique : $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ et $\mathbf{T} = \mathbf{A} \cdot \mathbf{S} \in \mathbb{Z}_q^{n \times k}$

Sign

Première étape [Générer une pré-image]

- transformer μ en un élément de l'espace \mathbf{c} (+ engagement de \mathbf{y})
- \mathbf{Sc} est une pré-image courte de \mathbf{Tc}

Schéma de Lyubashevsky [Lyu12]

KeyGen

- Clé secrète : $\mathbf{S} \xleftarrow{\$} \{-d, \dots, 0, \dots, d\}^{m \times k}$
- Clé Publique : $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}$ et $\mathbf{T} = \mathbf{A} \cdot \mathbf{S} \in \mathbb{Z}_q^{n \times k}$

Sign

Première étape [Générer une pré-image]

- transformer μ en un élément de l'espace \mathbf{c} (+ engagement de \mathbf{y})
- \mathbf{Sc} est une pré-image courte de \mathbf{Tc}

Seconde étape [Masquer la pré-image]

- Ajouter le bruit gaussien \mathbf{y} à \mathbf{Sc}
- Appliquer un algorithme de rejet afin d'éviter toute fuite d'information

Schéma de Lyubashevsky [Lyu12]

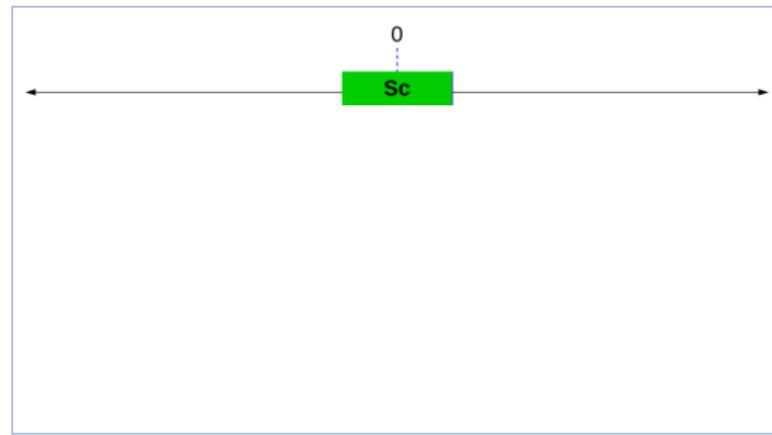


Schéma de Lyubashevsky [Lyu12]

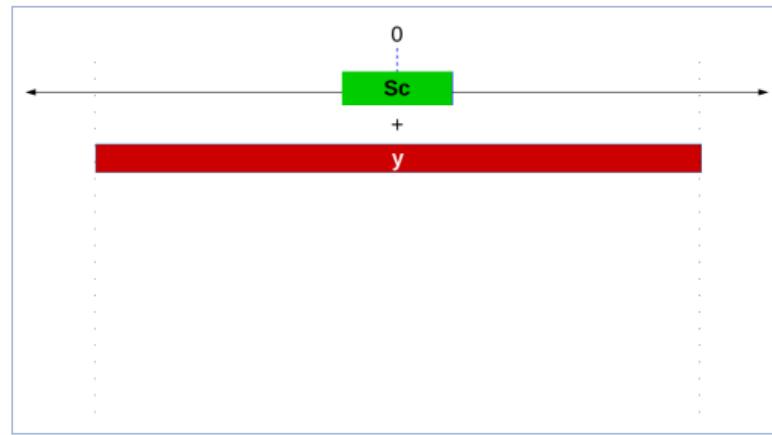


Schéma de Lyubashevsky [Lyu12]



Schéma de Lyubashevsky [Lyu12]

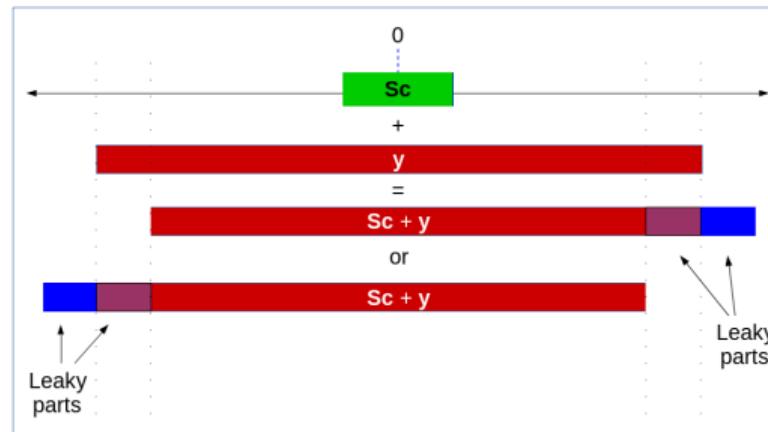


Schéma de Lyubashevsky [Lyu12]

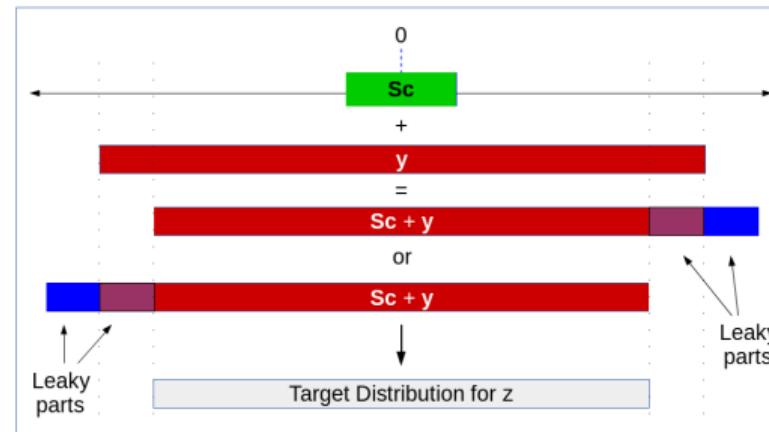


Schéma de Lyubashevsky [Lyu12]



Verify

Étant donnés (\mathbf{z} , \mathbf{c}), vérifier que :

- $H(\underbrace{\mathbf{Az} - \mathbf{Tc}}_{\mathbf{A(Sc+y)} - \mathbf{ASc}}, \mu) = \mathbf{c}$ → c'est un vecteur du réseau
- $\|\mathbf{z}\| \leq \eta\sigma\sqrt{m}$ → il est raisonnablement court

Jeux de paramètres

100 bits de sécurité

n	512	512	512	512	512
m	8,786	8,139	3,253	1,024	1,024
k	80	512	512	512	512
$\log_2(q)$	27	25	33	18	26
d	1	1	31	1	31
M (# essais moy.)	2.72	2.72	2.72	7.4	7.4
~ taille de signature	163,000	142,300	73,000	14,500	19,500
~ taille de sk	2^{20}	$2^{22.5}$	2^{23}	$2^{19.5}$	$2^{21.5}$
~ taille de pk	2^{20}	$2^{22.5}$	2^{23}	$2^{22.1}$	$2^{22.7}$

Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba

Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba



Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba



Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba



Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba



Notre proposition

KeyGen

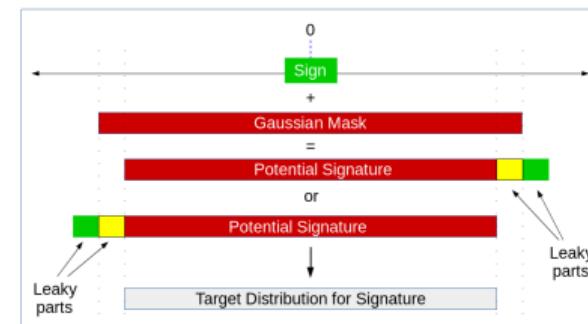
$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba



Notre proposition

KeyGen

$\mathbf{S} = (\mathbf{f}, \mathbf{F}) \in \mathcal{R}_q$ et $\mathbf{P} = (\mathbf{1}, \mathbf{h} = \mathbf{F} * \mathbf{f}^{-1})$ comme pour NTRUSign

Sign

Soit $\mu \in \{0, 1\}^*$ à signer :

- $\mathbf{y} \xleftarrow{\$} D_{\sigma}^{2N}$
- $\mathbf{e} = \mathcal{H}(\mathbf{Py}, \mu)$
- $\mathbf{s} = \text{NTRUSign}_{\mathbf{S}}(\mathbf{e})$

Retourner $\mathbf{x} = \mathbf{e} - \mathbf{s} + \mathbf{y}$ avec une certaine proba

Verify

Étant donné \mathbf{x} , vérifier que :

- $\mathcal{H}(\mathbf{Px} - \mathbf{e}, \mu) = \mathbf{e}$
- $\|\mathbf{x}\| \leq \eta \sigma \sqrt{2N}$

Esquisse de preuve

Retrouver la clé secrète

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Nécessiterait un algorithme de réduction avec un facteur d'Hermite exceptionnellement bas...

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Nécessiterait un algorithme de réduction avec un facteur d'Hermite exceptionnellement bas...

Retrouver la partie laissant fuire de l'information

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Nécessiterait un algorithme de réduction avec un facteur d'Hermite exceptionnellement bas...

Retrouver la partie laissant fuire de l'information

Statistiquement infaisable dû au masquage gaussien et à l'algorithme de rejet

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Nécessiterait un algorithme de réduction avec un facteur d'Hermite exceptionnellement bas...

Retrouver la partie laissant fuire de l'information

Statistiquement infaisable dû au masquage gaussien et à l'algorithme de rejet

Forger une signature

Esquisse de preuve

Retrouver la clé secrète

i.e. retrouver $\mathbf{S} = (\mathbf{f}, \mathbf{F})$ à partir de $\mathbf{P} = (\mathbf{1}, \mathbf{h})$

Nécessiterait un algorithme de réduction avec un facteur d'Hermite exceptionnellement bas...

Retrouver la partie laissant fuire de l'information

Statistiquement infaisable dû au masquage gaussien et à l'algorithme de rejet

Forger une signature

Alors nous pouvons résoudre SIS

Instanciation

sécurité	100-taille	100-vitesse	128-taille	128-vitesse
M (# essais moy.)	7.492	2.728	7.465	2.725
~ taille de la signature	10,700	12,700	14,500	17,100
~ taille de sk	1,400	1,400	1,750	1,750
~ taille de pk	6,900	6900	8,700	8,700

Instanciation

sécurité	100-taille	100-vitesse	128-taille	128-vitesse
M (# essais moy.)	7.492	2.728	7.465	2.725
~ taille de la signature	10,700	12,700	14,500	17,100
~ taille de sk	1,400	1,400	1,750	1,750
~ taille de pk	6,900	6900	8,700	8,700

100 bits de sécurité	[Lyu12]	[ABDG14]
~ taille de la signature	14,500	10,700
~ taille de sk	$2^{19.5}$	6,900
~ taille de pk	$2^{22.1}$	1,400

Instanciation

sécurité	100-taille	100-vitesse	128-taille	128-vitesse
M (# essais moy.)	7.492	2.728	7.465	2.725
~ taille de la signature	10,700	12,700	14,500	17,100
~ taille de sk	1,400	1,400	1,750	1,750
~ taille de pk	6,900	6900	8,700	8,700

100 bits de sécurité	[Ring-Lyu12]	[ABDG14]
~ taille de la signature	14,500	10,700
~ taille de sk	8,800	6,900
~ taille de pk	1,500	1,400

Plan

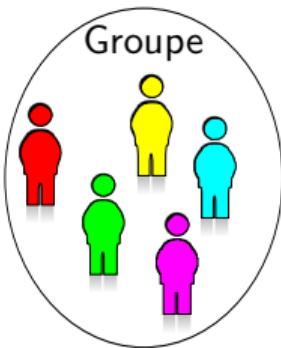
1 Cryptographie Post-Quantique

2 Signature basée sur les Réseaux

- Réparation de NTRUSign
- Extension en une Signature Traçable

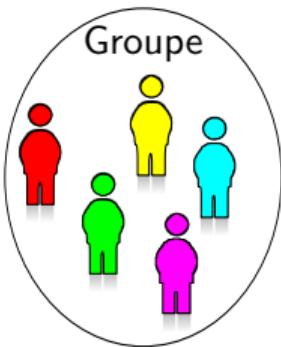
3 Cryptosystèmes sur les Codes

Signature de Groupe / Signature Traçable



- Les membres du groupe peuvent **signer de manière à rester anonyme** au sein de ce groupe

Signature de Groupe / Signature Traçable

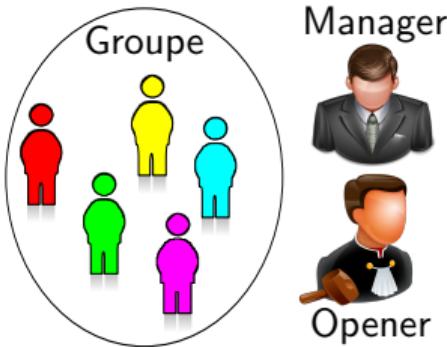


Manager



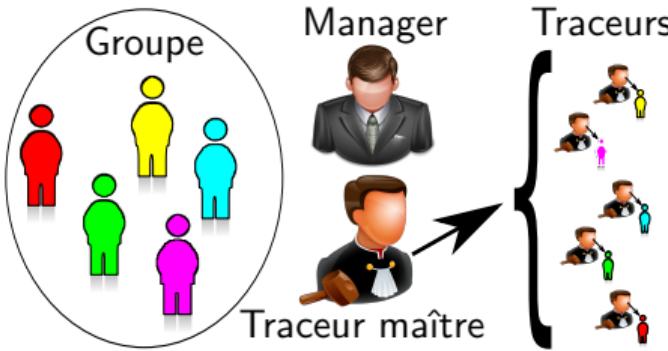
- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe

Signature de Groupe / Signature Traçable



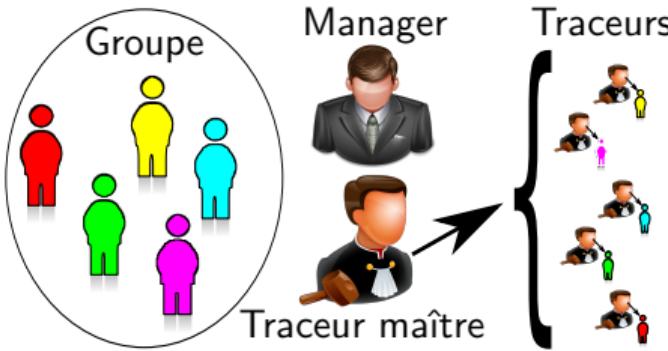
- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat

Signature de Groupe / Signature Traçable



- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Signature de Groupe / Signature Traçable

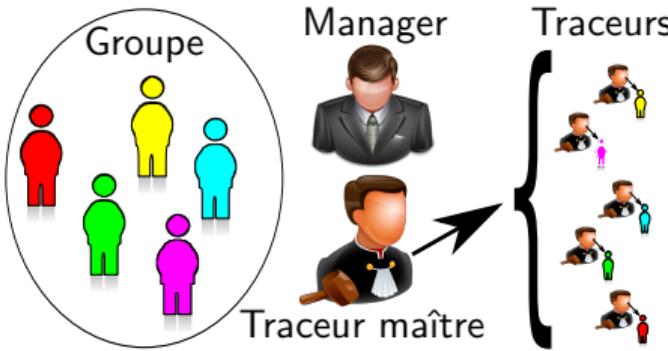


- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable

Signature de Groupe / Signature Traçable

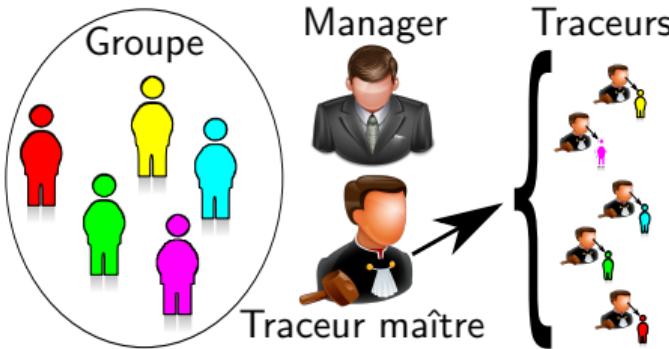


- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable → Meilleur respect de la vie privée + meilleur efficacité (à paramètres égaux)

Signature de Groupe / Signature Traçable

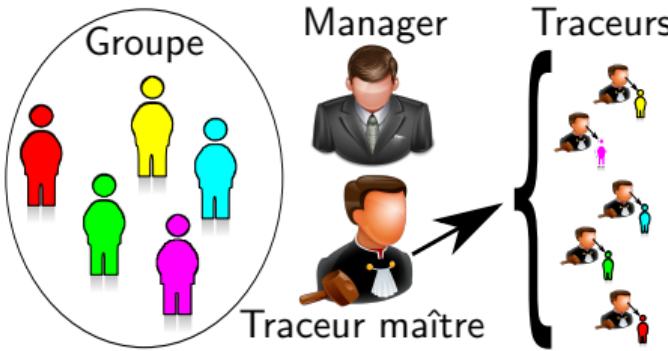


- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable → Meilleur respect de la vie privée + meilleur efficacité (à paramètres égaux)
- Non-framabilité

Signature de Groupe / Signature Traçable

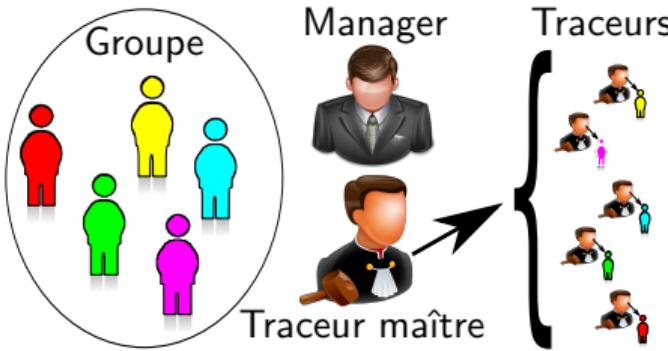


- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable → Meilleur respect de la vie privée + meilleur efficacité (à paramètres égaux)
- Non-framabilité → Le manager ne peut abuser les membres du groupe

Signature de Groupe / Signature Traçable

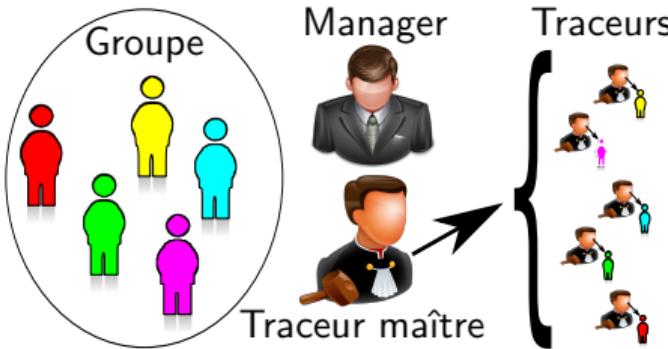


- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable → Meilleur respect de la vie privée + meilleur efficacité (à paramètres égaux)
- Non-framabilité → Le manager ne peut abuser les membres du groupe
- Dynamique

Signature de Groupe / Signature Traçable



- Les membres du groupe peuvent signer de manière à rester anonyme au sein de ce groupe
- Group manager → Gère les clés des membres du groupe
- Opener → Peut lever l'anonymat
- Les traceurs ont la capacité de vérifier si une signature appartient à un utilisateur donné

Notre proposition

- Signature Traçable → Meilleur respect de la vie privée + meilleur efficacité (à paramètres égaux)
- Non-framabilité → Le manager ne peut abuser les membres du groupe
- Dynamique → Le nombre d'utilisateurs peut évoluer

Techniques

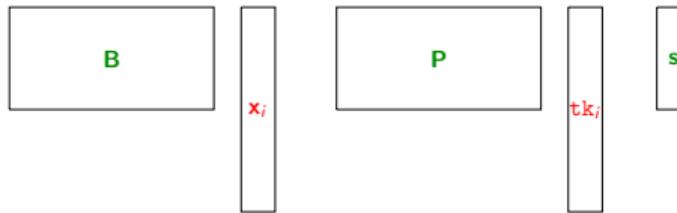
B

P

s

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$

Techniques



- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign

Techniques

$$\begin{matrix} \mathbf{B} \\ \mathbf{x}_i \end{matrix} + \begin{matrix} \mathbf{P} \\ \mathbf{tk}_i \end{matrix} = \begin{matrix} \mathbf{s} \end{matrix}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Techniques

$$\begin{matrix} \mathbf{B} \\ \mathbf{x}_i \end{matrix} + \begin{matrix} \mathbf{P} \\ \mathbf{tk}_i \end{matrix} = \begin{matrix} \mathbf{s} \end{matrix}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

Techniques

$$\begin{matrix} \mathbf{B} \\ \mathbf{x}_i \end{matrix} + \begin{matrix} \mathbf{P} \\ \mathbf{tk}_i \end{matrix} = \begin{matrix} \mathbf{s} \end{matrix}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

- $\mathbf{x}_i \xleftarrow{\$} \mathbb{F}_q^m$ tel que $\|\mathbf{x}_i\| \leq \beta$

Techniques

$$\begin{matrix} \mathbf{B} \\ \mathbf{x}_i \end{matrix} + \begin{matrix} \mathbf{P} \\ \mathbf{tk}_i \end{matrix} = \begin{matrix} \mathbf{s} \end{matrix}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

- $\mathbf{x}_i \xleftarrow{\$} \mathbb{F}_q^m$ tel que $\|\mathbf{x}_i\| \leq \beta$
- $\mathbf{tk}_i \leftarrow \text{mNTRUSign}(\mathbf{s} - \mathbf{B}\mathbf{x}_i)$

Techniques

$$\begin{array}{|c|} \hline \mathbf{B} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \mathbf{x}_i \\ \hline \end{array} + \begin{array}{|c|} \hline \mathbf{P} \\ \hline \end{array} \quad \begin{array}{|c|} \hline \mathbf{tk}_i \\ \hline \end{array} = \begin{array}{|c|} \hline \mathbf{s} \\ \hline \end{array}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

- $\mathbf{x}_i \xleftarrow{\$} \mathbb{F}_q^m$ tel que $\|\mathbf{x}_i\| \leq \beta$
- $\mathbf{tk}_i \leftarrow \text{mNTRUSign}(\mathbf{s} - \mathbf{B}\mathbf{x}_i)$

GroupSign

Preuve testable à divulgation nulle de connaissance :

Techniques

$$\begin{matrix} \mathbf{B} \\ \mathbf{x}_i \end{matrix} + \begin{matrix} \mathbf{P} \\ \mathbf{tk}_i \end{matrix} = \begin{matrix} \mathbf{s} \end{matrix}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

- $\mathbf{x}_i \xleftarrow{\$} \mathbb{F}_q^m$ tel que $\|\mathbf{x}_i\| \leq \beta$
- $\mathbf{tk}_i \leftarrow \text{mNTRUSign}(\mathbf{s} - \mathbf{B}\mathbf{x}_i)$

GroupSign

Preuve testable à divulgation nulle de connaissance :

- Faisant intervenir un haché du message

Techniques

$$\begin{array}{|c|} \hline \mathbf{B} \\ \hline \end{array} + \begin{array}{|c|} \hline \mathbf{P} \\ \hline \end{array} \begin{array}{|c|} \hline \mathbf{x}_i \\ \hline \end{array} = \begin{array}{|c|} \hline \mathbf{s} \\ \hline \end{array}$$

$$\begin{array}{|c|} \hline \mathbf{tk}_i \\ \hline \end{array}$$

- $\mathbf{B} \xleftarrow{\$} \mathbb{F}_q^{n \times m}$ aléatoire, \mathbf{P} matrice mNTRUSign, $\mathbf{s} \in \mathbb{F}_q^n$
- $\mathbf{x}_i \in \mathbb{F}_q^m$ petit, \mathbf{tk}_i signature mNTRUSign
- Équation d'appartenance au groupe → Anonymat

Join

L'utilisateur interagit avec le manager pour obtenir :

- $\mathbf{x}_i \xleftarrow{\$} \mathbb{F}_q^m$ tel que $\|\mathbf{x}_i\| \leq \beta$
- $\mathbf{tk}_i \leftarrow \text{mNTRUSign}(\mathbf{s} - \mathbf{B}\mathbf{x}_i)$

GroupSign

Preuve testable à divulgation nulle de connaissance :

- Faisant intervenir un haché du message
- Connaissance d'un petit $(\mathbf{x}_i, \mathbf{tk}_i)$ vérifiant l'équation de l'anonymat

Techniques

Verify

Techniques

Verify

- Aucun utilisateur révoqué n'a signé

Techniques

Verify

- Aucun utilisateur révoqué n'a signé
- Vérification de la preuve

Techniques

Verify

- Aucun utilisateur révoqué n'a signé
- Vérification de la preuve

Trace

À partir d'une clé de traçage tk^* :

Techniques

Verify

- Aucun utilisateur révoqué n'a signé
- Vérification de la preuve

Trace

À partir d'une clé de traçage tk^* :

- Test si tk^* a été utilisée pour créer la signature

Techniques

Verify

- Aucun utilisateur révoqué n'a signé
- Vérification de la preuve

Trace

À partir d'une clé de traçage tk^* :

- Test si tk^* a été utilisée pour créer la signature

Nombre de membres	4	10	20	50
Taille mpk	900 o	22 ko	429 ko	21 Mo
Taille msk	175 o	3.9 ko	61.9 ko	2.4 Mo
Taille usk	1.3 ko	40.2 ko	800ko	38.5 Mo
Taille signature	156 ko	4.87 Mo	97.6 Mo	4.7 Go

Plan

- 1 Cryptographie Post-Quantique
- 2 Signature basée sur les Réseaux
- 3 Cryptosystèmes sur les Codes
 - Chiffrement sur les Codes
 - Un nouveau paradigme

Intuition

Chiffrement :



Intuition

Chiffrement :

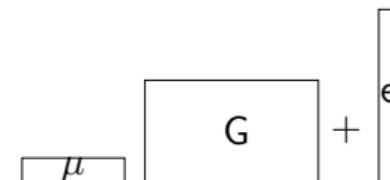
- message encodé



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} + \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} \quad \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

Indistinguabilité de la famille de codes utilisée

Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée



Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} \quad \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

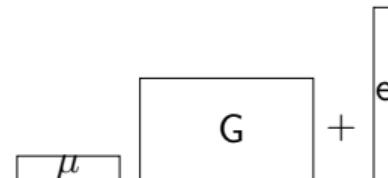
Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée



Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

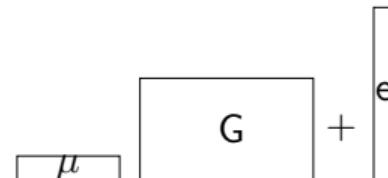
- McEliece [McE78] → code très structuré



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée



Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

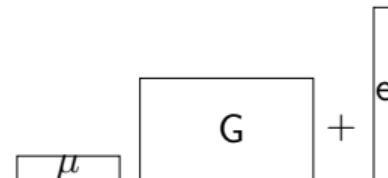
- McEliece [McE78] → code très structuré



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée



Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distinguiseur pour de nombreuses familles de codes

- McEliece [McE78] → code très structuré



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} \quad \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

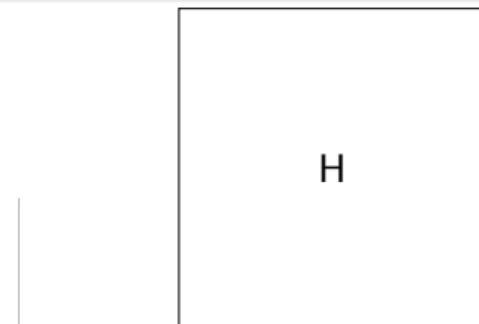
Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

- McEliece [McE78] → code très structuré
- MDPC [MTSB13] → matrice duale creuse



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} \quad \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

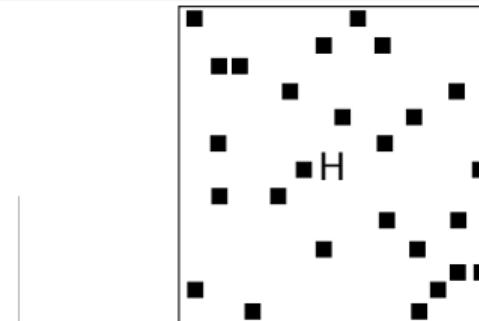
Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

- McEliece [McE78] → code très structuré
- MDPC [MTSB13] → matrice duale creuse



Intuition

Chiffrement :

- message encodé
- petite erreur ajoutée

$$\boxed{\mu} \quad \boxed{G} + \boxed{e}$$

Déchiffrement :

- Décodage du chiffré pour enlever l'erreur

Sécurité

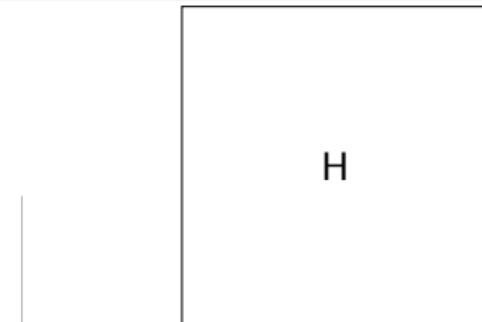
Décodage de Syndromes (SD)

- Prouvé NP-dur en métrique de Hamming
- Réduction à H.-SD en métrique Rang

Indistinguabilité de la famille de codes utilisée

- Hypothèse plus subtile à appuyer
- Distingueur pour de nombreuses familles de codes

- McEliece [McE78] → code très structuré
- MDPC [MTSB13] → matrice duale creuse
- LRPC [GMRZ13] → similaire, en rang



Chiffrement sur les Codes (1/3) : McEliece

Génération des clés :

- $\mathcal{C}[n, k]$ code linéaire, engendré par $\mathbf{G} \in \mathbb{F}_q^{k \times n}$, décodant jusqu'à t erreurs
- $\mathbf{S} \xleftarrow{\$} \mathbb{F}_q^{k \times k}$ inversible, $\mathbf{P} \xleftarrow{\$} \mathbb{F}_2^{n \times n}$ permutation
 $\rightarrow \text{pk} = (\tilde{\mathbf{G}} = \mathbf{SGP}, t), \text{sk} = (\mathbf{S}, \mathbf{G}, \mathbf{P})$

Chiffrement (de $\mu \in \mathbb{F}_q^k$) :

- $\mathbf{e} \xleftarrow{\$} \mathbb{F}_q^n$, avec $\omega(\mathbf{e}) = t$
 $\rightarrow \mathbf{c} = \mu \tilde{\mathbf{G}} + \mathbf{e}$

Déchiffrement :

- $\tilde{\mu} = \mathcal{C}.\text{Decode}(\mathbf{c}\mathbf{P}^{-1})$
 $\rightarrow \tilde{\mu} \mathbf{S}^{-1}$

Chiffrement sur les Codes (2/3) : MDPC

Génération des clés :

- $\mathcal{C}[n, k]$ code MDPC, de matrice de parité $\mathbf{H} \in \mathbb{F}_q^{k \times n}$, décodant jusqu'à t erreurs
- $\mathbf{G} \in \mathbb{F}_q^{(n-k) \times n}$ matrice génératrice sous forme échelonnée
 - $\text{pk} = (\mathbf{G}, t)$, $\text{sk} = \mathbf{H}$

Chiffrement (de $\mu \in \mathbb{F}_2^{n-k}$) :

- $\mathbf{e} \xleftarrow{\$} \mathbb{F}_2^n$, avec $\omega(\mathbf{e}) = t$
 - $\mathbf{c} = \mu\mathbf{G} + \mathbf{e}$

Déchiffrement :

- $\tilde{\mu} = \mu\mathbf{G} \leftarrow \mathcal{C}.\text{Decode}_{\mathbf{H}}(\mu\mathbf{G} + \mathbf{e})$
 - extraire μ des $(n - k)$ premières positions de $\tilde{\mu}$

Chiffrement sur les Codes (3/3) : LRPC

Génération des clés :

- $\mathcal{C}[n, k]$ code LRPC, de support \mathcal{S} de petit rang r
- matrice de parité $\mathbf{H} \in \mathbb{F}_{q^m}^{(n-k) \times n}$, matrice génératrice $\mathbf{G} \in \mathbb{F}_{q^m}^{k \times n}$
 $\rightarrow \text{pk} = (\mathbf{G}, r), \text{sk} = \mathbf{H}$

Chiffrement (de $\mu \in \mathbb{F}_{q^m}^k$) :

- $\mathbf{e} \xleftarrow{\$} \mathbb{F}_{q^m}^n$, avec $\text{rang}(\mathbf{e}) \leq r$
 $\rightarrow \mathbf{c} = \mu \mathbf{G} + \mathbf{e}$

Déchiffrement :

- $\mathbf{e} = \mathcal{C}.\text{Decode}(\mathbf{c}\mathbf{H})$
 $\rightarrow \mu \mathbf{G} = \mathbf{c} - \mathbf{e}$, retourner μ

Comparaisons / Motivations

Taille des clés

Gestion des erreurs

Structure cachée

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece

Gestion des erreurs

Structure cachée

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

Structure cachée

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC

Structure cachée

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC
- Bonne estimation pour LRPC, théorique et peu précise pour MDPC

Structure cachée

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC
- Bonne estimation pour LRPC, théorique et peu précise pour MDPC

Structure cachée

- Forte pour McEliece

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC
- Bonne estimation pour LRPC, théorique et peu précise pour MDPC

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC
- Bonne estimation pour LRPC, théorique et peu précise pour MDPC

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous

Comparaisons / Motivations

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- Aucune erreur pour McEliece, erreurs pour MDPC et LRPC
- Bonne estimation pour LRPC, théorique et peu précise pour MDPC

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- Problème du décodage de syndromes en métrique rang moins étudié qu'en Hamming

Plan

- 1 Cryptographie Post-Quantique
- 2 Signature basée sur les Réseaux
- 3 Cryptosystèmes sur les Codes
 - Chiffrement sur les Codes
 - Un nouveau paradigme

Présentation

Intuition

Chiffrement

- Le message est encodé en utilisant le code public \mathcal{C} (capacité de correction : δ)
- Une erreur est ajoutée à l'aide d'un autre code \mathcal{Q} quasi-cyclique

Déchiffrement

- sk sert à enlever la plupart des erreurs
- Le code \mathcal{C} est utilisé pour corriger le peu qu'il en reste

Présentation

Intuition

Chiffrement

- Le message est encodé en utilisant le code public \mathcal{C} (capacité de correction : δ)
- Une erreur est ajoutée à l'aide d'un autre code \mathcal{Q} quasi-cyclique

Déchiffrement

- sk sert à enlever la plupart des erreurs
- Le code \mathcal{C} est utilisé pour corriger le peu qu'il en reste

Génération des clés

- $sk = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{x}), \omega(\mathbf{y}) = w$
- $pk = (\mathbf{G}, \mathbf{Q}, \mathbf{s} = sk \cdot \mathbf{Q}^\top, w)$

Présentation

Intuition

Chiffrement

- Le message est encodé en utilisant le code public \mathcal{C} (capacité de correction : δ)
- Une erreur est ajoutée à l'aide d'un autre code \mathcal{Q} quasi-cyclique

Déchiffrement

- sk sert à enlever la plupart des erreurs
- Le code \mathcal{C} est utilisé pour corriger le peu qu'il en reste

Génération des clés

- $sk = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{x}), \omega(\mathbf{y}) = w$
- $pk = (\mathbf{G}, \mathbf{Q}, \mathbf{s} = sk \cdot \mathbf{Q}^\top, w)$

$$\mathbf{Q} = \left(\begin{array}{c|c} \mathbf{1} & \mathbf{q}_r \end{array} \right)$$

Présentation

Intuition

Chiffrement

- Le message est encodé en utilisant le code public \mathcal{C} (capacité de correction : δ)
- Une erreur est ajoutée à l'aide d'un autre code \mathcal{Q} quasi-cyclique

Déchiffrement

- sk sert à enlever la plupart des erreurs
- Le code \mathcal{C} est utilisé pour corriger le peu qu'il en reste

Génération des clés

- $sk = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{x}), \omega(\mathbf{y}) = w$
- $pk = (\mathbf{G}, \mathbf{Q}, \mathbf{s} = sk \cdot \mathbf{Q}^\top, w)$

Chiffrement

- Encrypt(pk, μ) : $\epsilon \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{r}_1), \omega(\mathbf{r}_2) = w$, et $\omega(\epsilon) = 3w$
 - $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$
 - $\rho = \mu\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \epsilon$

Présentation

Intuition

Chiffrement

- Le message est encodé en utilisant le code public \mathcal{C} (capacité de correction : δ)
- Une erreur est ajoutée à l'aide d'un autre code \mathcal{Q} quasi-cyclique

Déchiffrement

- sk sert à enlever la plupart des erreurs
- Le code \mathcal{C} est utilisé pour corriger le peu qu'il en reste

Génération des clés

- $sk = (\mathbf{x}, \mathbf{y}) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{x}), \omega(\mathbf{y}) = w$
- $pk = (\mathbf{G}, \mathbf{Q}, \mathbf{s} = sk \cdot \mathbf{Q}^\top, w)$

Déchiffrement

- $\text{Decrypt}(sk, \mathbf{c} = (\mathbf{v}, \rho))$: retourner $\mathcal{C}.\text{Decode}(\rho - \mathbf{v} \cdot \mathbf{y})$.

Chiffrement

- $\text{Encrypt}(pk, \mu) : \epsilon \xleftarrow{\$} \mathcal{V}$, $\mathbf{r} = (\mathbf{r}_1, \mathbf{r}_2) \xleftarrow{\$} \mathcal{V}^2$ tels que $\omega(\mathbf{r}_1), \omega(\mathbf{r}_2) = w$, et $\omega(\epsilon) = 3w$
 - $\mathbf{v}^\top = \mathbf{Q}\mathbf{r}^\top$
 - $\rho = \mu\mathbf{G} + \mathbf{s} \cdot \mathbf{r}_2 + \epsilon$

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

\mathcal{C} .Decode décode correctement $\rho - \mathbf{v} \cdot \mathbf{y}$ tant que

l'erreur ajoutée **n'est pas trop grande**

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

\mathcal{C} .Decode décode correctement $\rho - \mathbf{v} \cdot \mathbf{y}$ tant que

l'erreur ajoutée **n'est pas trop grande**

$$\omega(\mathbf{s} \cdot \mathbf{r}_2 - \mathbf{v} \cdot \mathbf{y} + \epsilon) \leq \delta$$

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

\mathcal{C} .Decode décode correctement $\rho - \mathbf{v} \cdot \mathbf{y}$ tant que

l'erreur ajoutée **n'est pas trop grande**

$$\omega(\textcolor{green}{s} \cdot \textcolor{blue}{r}_2 - \mathbf{v} \cdot \mathbf{y} + \epsilon) \leq \delta$$

$$\omega((\textcolor{red}{x} + \mathbf{q}_r \cdot \mathbf{y}) \cdot \textcolor{blue}{r}_2 - (\mathbf{r}_1 + \mathbf{q}_r \cdot \mathbf{r}_2) \cdot \mathbf{y} + \epsilon) \leq \delta$$

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

\mathcal{C} .Decode décode correctement $\rho - \mathbf{v} \cdot \mathbf{y}$ tant que

l'erreur ajoutée **n'est pas trop grande**

$$\omega(\textcolor{green}{s} \cdot \mathbf{r}_2 - \mathbf{v} \cdot \mathbf{y} + \epsilon) \leq \delta$$

$$\omega((\mathbf{x} + \mathbf{q}_r \cdot \mathbf{y}) \cdot \mathbf{r}_2 - (\mathbf{r}_1 + \mathbf{q}_r \cdot \mathbf{r}_2) \cdot \mathbf{y} + \epsilon) \leq \delta$$

$$\omega(\mathbf{x} \cdot \mathbf{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \epsilon) \leq \delta$$

Consistance

Consistance du schéma

$$\text{Decrypt}(\textcolor{red}{sk}, \text{Encrypt}(\textcolor{green}{pk}, \mu, \theta)) = \mu$$

\mathcal{C} .Decode décode correctement $\rho - \mathbf{v} \cdot \mathbf{y}$ tant que

l'erreur ajoutée **n'est pas trop grande**

$$\omega(\textcolor{green}{s} \cdot \textcolor{blue}{r}_2 - \mathbf{v} \cdot \mathbf{y} + \epsilon) \leq \delta$$

$$\omega((\mathbf{x} + \mathbf{q}_r \cdot \mathbf{y}) \cdot \textcolor{blue}{r}_2 - (\mathbf{r}_1 + \mathbf{q}_r \cdot \mathbf{r}_2) \cdot \mathbf{y} + \epsilon) \leq \delta$$

$$\omega(\textcolor{red}{x} \cdot \textcolor{blue}{r}_2 - \mathbf{r}_1 \cdot \mathbf{y} + \epsilon) \leq \delta$$

Analyse de la distribution de l'erreur → Meilleure compréhension de la probabilité d'échec

Sécurité

Définition (Distribution SD)

$n, k, w \in \mathbb{N}^*$, la Distribution $SD(n, k, w)$ choisit $\mathbf{H} \xleftarrow{\$} \mathbb{F}^{(n-k) \times n}$ et $\mathbf{x} \xleftarrow{\$} \mathbb{F}^n$ tel que $\omega(\mathbf{x}) = w$, et retourne $(\mathbf{H}, \mathbf{H}\mathbf{x}^\top)$.

Définition (Problème Décisionnel s-QCSD)

$n, k, w, s \in \mathbb{N}^*$, \mathbf{H} matrice de parité aléatoire d'un code QC \mathcal{C} et $\mathbf{y} \xleftarrow{\$} \mathbb{F}^n$, le problème Décisionnel $s\text{-DQCSD}(n, k, w)$ demande de décider avec un avantage non-négligeable si $(\mathbf{H}, \mathbf{y}^\top)$ provient de la distribution $s\text{-QCSD}(n, k, w)$ ou uniforme sur $\mathbb{F}^{(n-k) \times n} \times \mathbb{F}^{n-k}$.

Théorème

Notre schéma est IND-CPA sous l'hypothèse que les problèmes 2-DQCSD et 3-DQCSD sont difficiles.

Esquisse de preuve

- Jeu usuel :

 $\text{Exp}_{\mathcal{E}, \mathcal{A}}^{\text{ind}-b}(\lambda)$

1. $\text{param} \leftarrow \text{Setup}(1^\lambda)$
2. $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(\text{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\text{FIND} : \text{pk})$
4. $\mathbf{c}^* \leftarrow \text{Encrypt}(\text{pk}, \mu_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\text{GUESS} : \mathbf{c}^*)$
6. RETURN b'

Esquisse de preuve

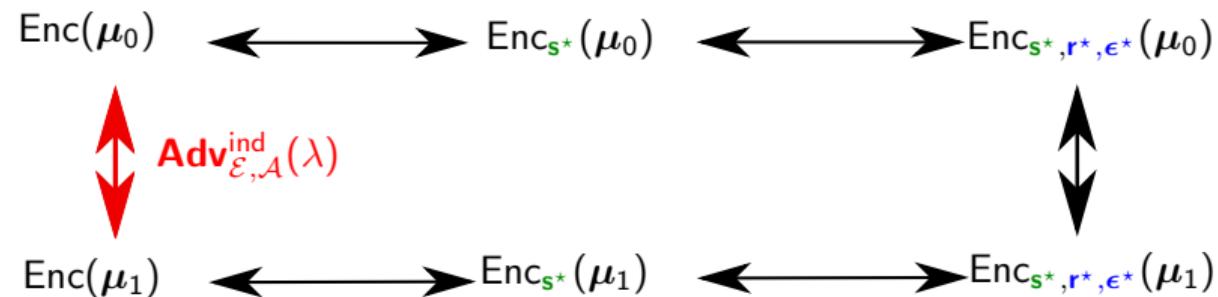
- Jeu usuel :

 $\text{Exp}_{\mathcal{E}, \mathcal{A}}^{\text{ind}-b}(\lambda)$

1. $\text{param} \leftarrow \text{Setup}(1^\lambda)$
2. $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(\text{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\text{FIND} : \text{pk})$
4. $\mathbf{c}^* \leftarrow \text{Encrypt}(\text{pk}, \mu_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\text{GUESS} : \mathbf{c}^*)$
6. RETURN b'

- Alternative : Argument hybride

Construire une suite de jeux 2 à 2 indistinguables de $\text{Enc}(\mu_0)$ à $\text{Enc}(\mu_1)$



Esquisse de preuve

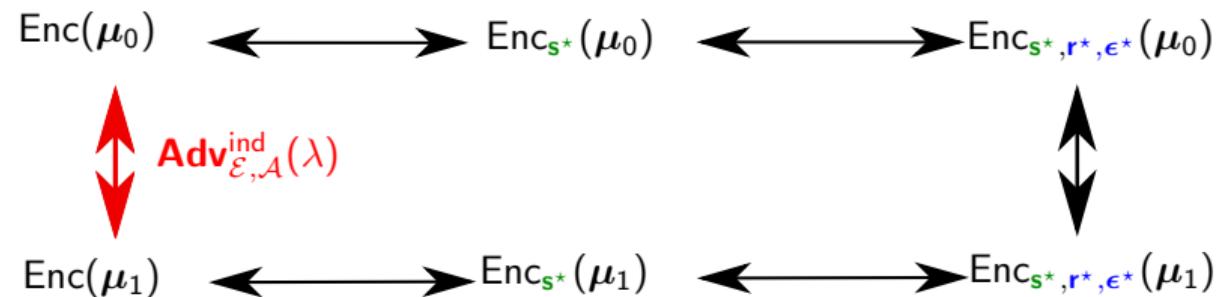
- Jeu usuel :

$\text{Exp}_{\mathcal{E}, \mathcal{A}}^{\text{ind}-b}(\lambda)$

1. $\text{param} \leftarrow \text{Setup}(1^\lambda)$
2. $(\text{pk}, \text{sk}) \leftarrow \text{KeyGen}(\text{param})$
3. $(\mu_0, \mu_1) \leftarrow \mathcal{A}(\text{FIND} : \text{pk})$
4. $\mathbf{c}^* \leftarrow \text{Encrypt}(\text{pk}, \mu_b, \theta)$
5. $b' \leftarrow \mathcal{A}(\text{GUESS} : \mathbf{c}^*)$
6. RETURN b'

- Alternative : Argument hybride

Construire une suite de jeux 2 à 2 indistinguables de $\text{Enc}(\mu_0)$ à $\text{Enc}(\mu_1)$



$$\mathbf{Adv}_{\mathcal{E}, \mathcal{A}}^{\text{ind}}(\lambda) \leq 2 \cdot \left(\mathbf{Adv}^{\text{2-DQCSD}}(\lambda) + \mathbf{Adv}^{\text{3-DQCSD}}(\lambda) \right)$$

Paramètres (1/2)

Instanciation en métrique de Hamming (HQC)

	Instance	Paramètres du Cryptosystème								
		n_1	n_2	$n' \approx n_1 n_2 = n$	k'	δ	w	$\epsilon = 3w$	sécurité	p_{fail}
Classique	Jouet	255	25	6,379	63	30	36	108	64	$< 2^{-64}$
	Faible	255	37	9,437	79	27	45	135	80	$< 2^{-80}$
	Modérée	255	53	13,523	99	23	56	168	100	$< 2^{-100}$
	Forte	511	41	20,959	121	58	72	216	128	$< 2^{-128}$
Quantique	Jouet	255	65	16,603	63	87	72	216	64	$< 2^{-64}$
	Faible	511	47	24,019	76	85	89	267	80	$< 2^{-80}$
	Modérée	255	141	35,963	99	23	112	336	100	$< 2^{-100}$
	Forte	511	109	55,711	121	58	143	429	128	$< 2^{-128}$

Taille de clés : $2n$ ou $n + \lambda$ bits en donnant une graine

Paramètres (2/2)

Instanciation en métrique Rang (RQC)

Paramètres du Cryptosystème										
Instance	n	k'	m	q	w	ϵ	clair	taille clés	sécurité	SQE*
RQC-I	37	13	37	4	3	3	962	2,738	90	45
RQC-II	53	13	53	2	4	4	689	2,809	95	47
RQC-III	61	3	61	2	5	4	183	3,721	140	70
RQC-IV	83	3	83	2	6	4	249	6,889	230	115
RQC-V	61	3	61	4	5	4	366	7,442	264	132

*Sécurité Quantique Équivalente

Comparaison (1/2)

Paramètres asymptotiques pour différents cryptosystèmes sur les codes en fonction

Cryptosystème	Longueur du code	Taille clé publique	Taille du chiffré	Structure masquée	Structure cyclique
Goppa-McEliece [McE78]	$\mathcal{O}(\lambda \log \lambda)$	$\mathcal{O}(\lambda^2 (\log \lambda)^2)$	$\mathcal{O}(\lambda \log \lambda)$	Forte	Non
MDPC [MTSB13]	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	Faible	Oui
LRPC [GMRZ13]	$\mathcal{O}(\lambda^{\frac{2}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	Faible	Oui
HQC	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	$\mathcal{O}(\lambda^2)$	Non	Oui
RQC	$\mathcal{O}(\lambda^{\frac{2}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	$\mathcal{O}(\lambda^{\frac{4}{3}})$	Non	Oui

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- McEliece : aucune erreur
- LRPC : bonne estimation
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC

Gestion des erreurs

- McEliece : aucune erreur
- LRPC : bonne estimation
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- LRPC : bonne estimation
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- Aucune erreur pour RQC
- LRPC : bonne estimation
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- Aucune erreur pour RQC
- LRPC : bonne estimation
- Fine pour HQC
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- Aucune erreur pour RQC
- LRPC : bonne estimation
- Fine pour HQC
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Aucun masquage de la structure du code utilisé !
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- Aucune erreur pour RQC
- LRPC : bonne estimation
- Fine pour HQC
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Aucun masquage de la structure du code utilisé !
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- Bonne pour HQC et RQC
- LRPC → problème moins étudié qu'en Hamming

Comparaison (2/2)

Taille des clés

- Importante pour McEliece
- Bonne pour HQC
- Bonne pour MDPC, très bonne pour LRPC
- Très bonne pour RQC

Gestion des erreurs

- McEliece : aucune erreur
- Aucune erreur pour RQC
- LRPC : bonne estimation
- Fine pour HQC
- MDPC : estimation peu précise

Structure cachée

- Forte pour McEliece
- Aucun masquage de la structure du code utilisé !
- Moindre pour MDPC et LRPC

Sécurité

- Satisfaisante pour tous
- Bonne pour HQC et RQC
- LRPC → problème moins étudié qu'en Hamming
- Même constat cependant pour RQC

Conclusions

- Importance de concevoir de nouveaux schémas face à de futurs ordinateurs quantiques

Conclusions

- Importance de concevoir de nouveaux schémas face à de futurs ordinateurs quantiques
- Nos contributions :

Conclusions

- Importance de concevoir de nouveaux schémas face à de futurs ordinateurs quantiques
- Nos contributions :
 - ① Proposition d'un schéma de signature basé sur les réseaux :
 - Permet de réparer NTRUSign (très efficace) de manière prouvée sûre
 - Tout en restant plus performant que les techniques utilisées dans [Lyu12]
 - Moins performant que [DDLL13]
 - S'étend en une signature traçable avec une propriété de non-framabilité

Conclusions

- Importance de concevoir de nouveaux schémas face à de futurs ordinateurs quantiques
- Nos contributions :
 - ① Proposition d'un schéma de signature basé sur les réseaux :
 - Permet de réparer NTRUSign (très efficace) de manière prouvée sûre
 - Tout en restant plus performant que les techniques utilisées dans [Lyu12]
 - Moins performant que [DDLL13]
 - S'étend en une signature traçable avec une propriété de non-framabilité
 - ② Délégation de signature ECDSA à l'aide de chiffrement complètement homomorphe (non présenté)

Conclusions

- Importance de concevoir de nouveaux schémas face à de futurs ordinateurs quantiques
- Nos contributions :
 - ① Proposition d'un schéma de signature basé sur les réseaux :
 - Permet de réparer NTRUSign (très efficace) de manière prouvée sûre
 - Tout en restant plus performant que les techniques utilisées dans [Lyu12]
 - Moins performant que [DDLL13]
 - S'étend en une signature traçable avec une propriété de non-framabilité
 - ② Délégation de signature ECDSA à l'aide de chiffrement complètement homomorphe (non présenté)
 - ③ Conception d'une nouvelle approche pour construire des cryptosystèmes sur les codes
 - Ne nécessite pas de masquage du code utilisé
 - Approche générique : métrique de Hamming + métrique Rang
 - Analyse fine de la probabilité d'échec pour HQC, pas d'échec pour RQC
 - Cryptosystèmes compétitifs, voir très efficace pour RQC

Perspectives

➊ Réparation de NTRUSign

- Utiliser LWE plutôt que SIS [Lyu12]
- Utiliser une approche de type BLISS [DDLL13]
- Comparer à des approches de type GPV

Perspectives

① Réparation de NTRUSign

- Utiliser LWE plutôt que SIS [Lyu12]
- Utiliser une approche de type BLISS [DDLL13]
- Comparer à des approches de type GPV

② Signature Traçable

- Trouver une réduction / un problème plus adaptée pour diminuer les paramètres
- Peut-on obtenir la “backward-unlinkability” ?
- Sortir du modèle de l'oracle aléatoire...

Perspectives

① Réparation de NTRUSign

- Utiliser LWE plutôt que SIS [Lyu12]
- Utiliser une approche de type BLISS [DDLL13]
- Comparer à des approches de type GPV

② Signature Traçable

- Trouver une réduction / un problème plus adaptée pour diminuer les paramètres
- Peut-on obtenir la “backward-unlinkability” ?
- Sortir du modèle de l'oracle aléatoire...

③ Délégation de signatures ECDSA

- Peut-on obtenir des résultats similaires pour RSA ?

Perspectives

① Réparation de NTRUSign

- Utiliser LWE plutôt que SIS [Lyu12]
- Utiliser une approche de type BLISS [DDLL13]
- Comparer à des approches de type GPV

② Signature Traçable

- Trouver une réduction / un problème plus adaptée pour diminuer les paramètres
- Peut-on obtenir la “backward-unlinkability” ?
- Sortir du modèle de l’oracle aléatoire...

③ Délégation de signatures ECDSA

- Peut-on obtenir des résultats similaires pour RSA ?

④ Cryptosystème sur les Codes

- Algorithme de décodage VS codes utilisés ?
- Implémentation et soumission au NIST

Merci de votre présence et de votre attention.

Questions du jury

Merci de votre présence et de votre attention.



Carlos Aguilar Melchor, Xavier Boyen,
Jean-Christophe Deneuville, and Philippe Gaborit.
Sealing the leak on classical ntru signatures.
In *PQCrypto'14*, pages 1–21, 2014.



Léo Ducas, Alain Durmus, Tancrède Lepoint, and
Vadim Lyubashevsky.
Lattice signatures and bimodal Gaussians.
In Ran Canetti and Juan A. Garay, editors,
CRYPTO 2013, Part I, volume 8042 of *LNCS*, pages
40–56. Springer, Heidelberg, August 2013.



Léo Ducas and Phong Q. Nguyen.
Learning a zonotope and more : Cryptanalysis of
NTRUSign countermeasures.
In Xiaoyun Wang and Kazue Sako, editors,
ASIACRYPT 2012, volume 7658 of *LNCS*, pages
433–450. Springer, Heidelberg, December 2012.



Philippe Gaborit, Gaétan Murat, Olivier Ruatta, and
Gilles Zémor.
Low rank parity check codes and their application to
cryptography.
In *Proceedings of the Workshop on Coding and
Cryptography WCC'2013*, Bergen, Norway, 2013.



Craig Gentry and Michael Szydlo.
Cryptanalysis of the revised NTRU signature scheme.
In Lars R. Knudsen, editor, *EUROCRYPT 2002*,
volume 2332 of *LNCS*, pages 299–320. Springer,
Heidelberg, April / May 2002.



Jeffrey Hoffstein, Nick Howgrave-Graham, Jill Pipher,
Joseph H. Silverman, and William Whyte.
NTRUSIGN : Digital signatures using the NTRU
lattice.
In Marc Joye, editor, *CT-RSA 2003*, volume 2612 of
LNCS, pages 122–140. Springer, Heidelberg, April
2003.



Jeffrey Hoffstein, Jill Pipher, and Joseph H.
Silverman.
NSS : An NTRU lattice-based signature scheme.
In Birgit Pfitzmann, editor, *EUROCRYPT 2001*,
volume 2045 of *LNCS*, pages 211–228. Springer,
Heidelberg, May 2001.



Vadim Lyubashevsky.
Lattice signatures without trapdoors.
In David Pointcheval and Thomas Johansson, editors,
EUROCRYPT 2012, volume 7237 of *LNCS*, pages
738–755. Springer, Heidelberg, April 2012.



Robert J. McEliece.
A public-key cryptosystem based on algebraic coding
theory.
Deep Space Network Progress Report, 44 :114–116,
January 1978.



Rafael Misoczki, Jean-Pierre Tillich, Nicolas Sendrier,
and Paulo SLM Barreto.
Mdpc-mceliece : New mceliece variants from
moderate density parity-check codes.
In *Information Theory Proceedings (ISIT), 2013 IEEE
International Symposium on*, pages 2069–2073. IEEE,
2013.



Phong Q. Nguyen and Oded Regev.
Learning a parallelepiped : Cryptanalysis of GGH and
NTRU signatures.
In Serge Vaudenay, editor, *EUROCRYPT 2006*,
volume 4004 of *LNCS*, pages 271–288. Springer,
Heidelberg, May / June 2006.



Peter W. Shor.
Polynomial-time algorithms for prime factorization
and discrete logarithms on a quantum computer.
SIAM J. Comput., 26(5) :1484–1509, 1997.

Questions du jury