université de BORDEAUX

Projet - Wave

Un procédé de signature à base de codes correcteurs

Suzanne LANSADE, Eva PALANDJIAN

Encadrant : Gilles ZEMOR

Master CSI, Université de Bordeaux, France

25 Février 2020

Plan

Introduction

université de BORDEAUX

- Éventualité de l'arrivée de l'ordinateur quantique:
  - → On cherche des alternatives à RSA et DH
  - → Le NIST lance en 2017 un appel pour la standardisation des systèmes à clef publique

- Les codes correcteurs
  - → Peuvent être quantiquement sûrs
  - → Peuvent déjà être utilisés dans des systèmes de chiffrement
  - → Sont difficilement utilisables pour les signatures

Introduction

	Proportion	Échange de clefs	Signature
Réseaux	46%	9	3
Codes	28%	7	0
Fonctions de hachage	4%	0	1
Multi-varié	15%	0	4
Isogénies	4%	1	0
Preuves ZK	4%	0	1

Figure: Comparaison des soumissions au NIST du second tour.

Introduction

université de BORDEAUX

- Difficile de faire un système de signature à base de codes
  - → Difficile de se placer dans l'ensemble des syndromes facilement et uniquement décodables
  - → Tous les systèmes existant sont cassés ou inutilisables dans la pratique

- Le système Wave
  - → Enlève la restriction au mot le plus proche
  - → Décode en grande distance

Plan

Codes $(U, U+V)$-généralisés

Le système de signature Wave utilise une famille de codes correcteurs appelés codes $(U, U+V)$-généralisés.

Soient n un entier pair, U et V deux codes aléatoires de dimension respectives k_U et k_V et de longueur $n/2$. Le *code* $(U, U+V)$*-généralisé* correspond à l'ensemble des mots :

$$\{(a.u+b.v, c.u+d.v) \text{ tel que } u \in U \text{ et } v \in V\}$$

où $x.y$ est le produit coordonnée par coordonnée des x_i et y_i et a,b,c,d sont quatre vecteurs de $\mathbb{F}_q^{n/2}$.

Signature

- Le système Wave utilise la fonction qui a un vecteur $\mathbf{e}$ de poids ω associe son syndrome par $\mathbf{H}$:

$$f_{\omega,\mathbf{H}} : \mathbf{e} \longrightarrow \mathbf{e}H^T = s$$

  comme fonction à sens unique

- Il utilise un algorithme `InvertAlg` permettant d'inverser la fonction syndrome à l'aide de la trappe T

- La trappe T correspond à la structure du code $(U, U+V)$-généralisé

Signature

Le schéma de signature Wave est donc composé de deux algorithmes :

$\texttt{Sign}^{sk}(s)$:
$\mathbf{e} \leftarrow \texttt{InvertAlg}(s, T)$
renvoie $\mathbf{e}$

$\texttt{Verify}^{pk}(s, e')$:
Si $\mathbf{e}' H^T = s$ et $|\mathbf{e}'| = \omega$
renvoie 1
renvoie 0

- L'algorithme de signature utilise la trappe et un algorithme de décodage pour renvoyer une erreur de poids ω
- L'algorithme de vérification accepte la signature si le syndrome et le poids sont corrects

Décodage

Soit

$$\begin{array}{rccc} \varphi_{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}} & : & \mathbb{F}_q^{n/2} \times \mathbb{F}_q^{n/2} & \to & \mathbb{F}_q^{n/2} \times \mathbb{F}_q^{n/2} \\ & & (\mathbf{x},\mathbf{y}) & \mapsto & (a.\mathbf{x}+b.\mathbf{y}, c.\mathbf{x}+d.\mathbf{y}) \end{array}$$

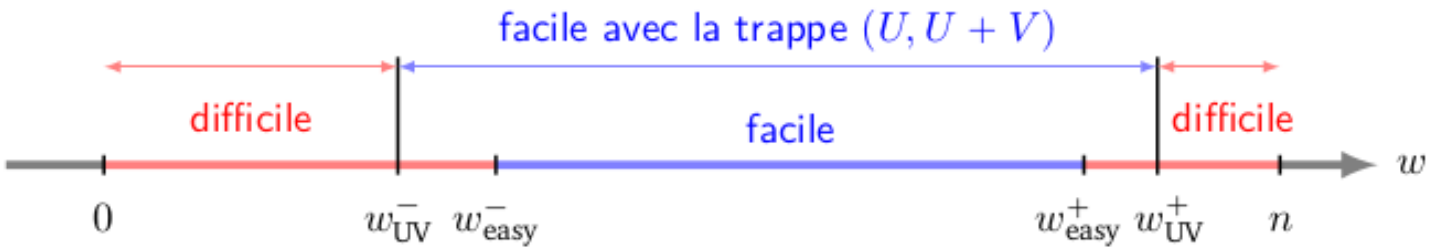
Proposition

Inverser $f_{\omega,\mathbf{H}}$ pour un certain $\mathbf{s} \in F_q^{n-k}$ est équivalent à trouver $\mathbf{e} \in \mathbb{F}_q^n$ tel que:

$$\mathbf{e}_U \mathbf{H}_U^T = \mathbf{s}^U \qquad et \qquad \mathbf{e}_V \mathbf{H}_V^T = \mathbf{s}^V$$

où $\mathbf{s} = (\mathbf{s}^U, \mathbf{s}^V)$ avec $\mathbf{s}^U \in \mathbb{F}_q^{n/2-k_U}$, $\mathbf{s}^V \in \mathbb{F}_q^{n/2-k_V}$ et où $\mathbf{e}_U$ et $\mathbf{e}_V$ de $\mathbb{F}_q^{n/2}$ sont tels que $(\mathbf{e}_U, \mathbf{e}_V) = \varphi_{a,b,c,d}^{-1}(\mathbf{e})$.

Décodage



- On veut se placer dans un intervalle qui permet de décoder, mais uniquement en connaissant la trappe
- On prend $\omega \in [\![\omega_{easy}^+, \omega_{UV}^+]\!]$
- Afin d'obtenir une erreur de poids ω on pose des contraintes sur le vecteur $\mathbf{e}_U$

Décodage

Pour tout $\mathbf{e} = \varphi_{\mathbf{a},\mathbf{b},\mathbf{c},\mathbf{d}}(\mathbf{e_U}, \mathbf{e_V})$, on a pour tout $i \in [\![1, n/2]\!]$:

$$\begin{cases} a_i \mathbf{e}_U(i) + b_i \mathbf{e}_V(i) &= \mathbf{e}(i) \\ c_i \mathbf{e}_U(i) + d_i \mathbf{e}_V(i) &= \mathbf{e}(i + n/2) \end{cases}$$

- On décode $\mathbf{e}_U$ avec une variante du décodage par ensemble d'informations
- On choisi k_U coordonnées de $\mathbf{e}_U$ telles que les lignes du système soient non nulles à ces positions
- Ainsi on aura
  - $\rightarrow$ $2k_U$ coordonnées de $\mathbf{e}$ non nulles
  - $\rightarrow$ Les $n - 2k_U$ autres seront uniformément distribuées dans leur ensemble

Décodage

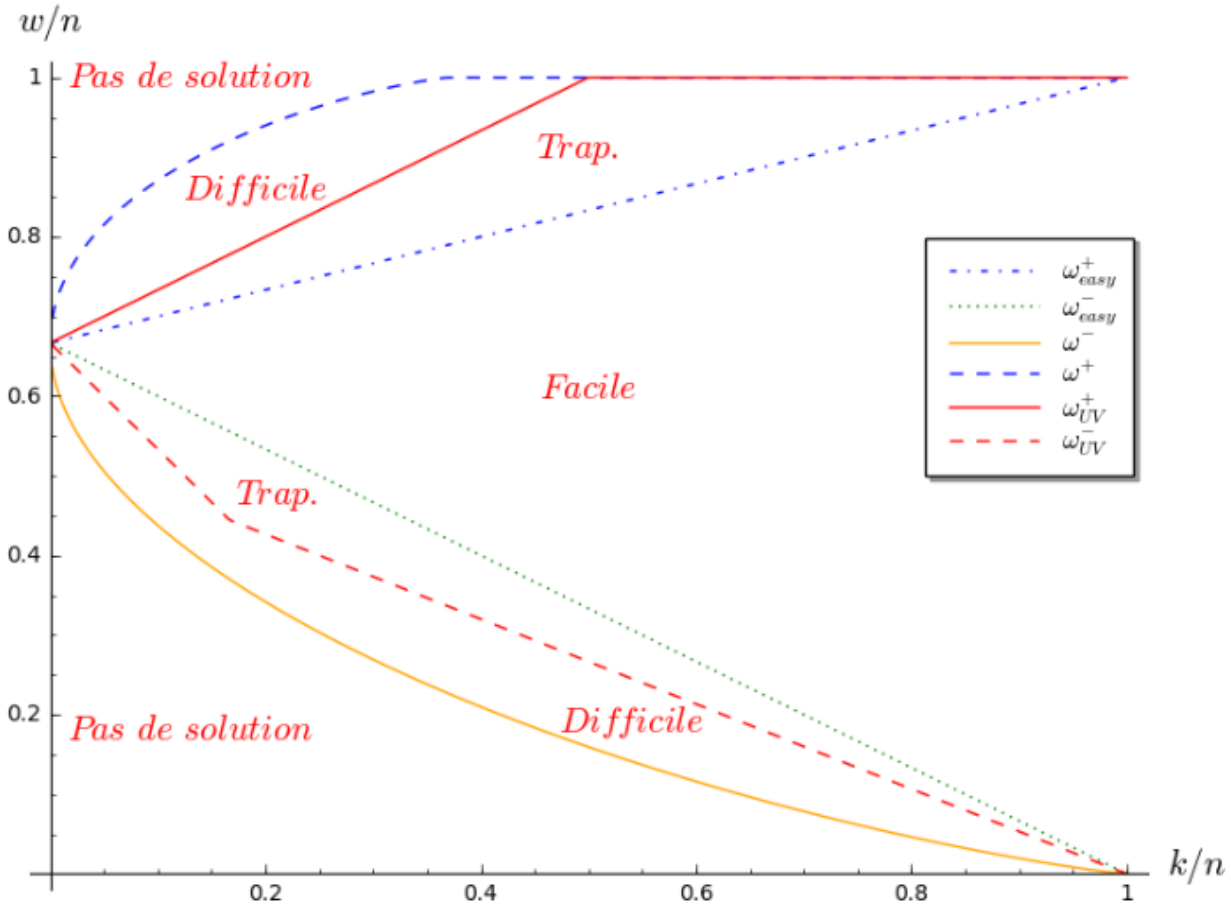


Figure: Comparaison des distances w/n avec et sans trappe en fonction du rendement.

Plan

Uniformisation des sorties

université de BORDEAUX

- Des corrélations vont apparaître entre les coordonnées $\mathbf{e}_i$ et $\mathbf{e}_{i+n/2}$

  $\rightarrow$ Si un attaquant $\mathcal{A}$ récupère suffisamment de signatures, il pourra calculer :

  $$\mathbb{P}(\mathbf{e}_i \neq \mathbf{e}_{i+n/2}) \quad \text{et} \quad \mathbb{P}(\mathbf{e}_i \neq \mathbf{e}_j)$$

- Normalement les coordonnées de $\mathbf{e}$ sont permutées pour cacher la structure du code

  $\rightarrow$ $\mathcal{A}$ peut donc retrouver la permutation

La méthode du rejet

Algorithme 1 DecodeUV$(\varphi, \mathbf{s}, \mathbf{H}_V, \mathbf{H}_U)$

Entrées: φ, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ un syndrome, $\mathbf{H}_V \in \mathbb{F}_q^{(\frac{n}{2}-k_V)\times\frac{n}{2}}$, $\mathbf{H}_U \in \mathbb{F}_q^{(\frac{n}{2}-k_U)\times\frac{n}{2}}$
Sortie: $\mathbf{e} = \varphi(e_U, e_V)$ avec $\mathbf{e}_U\mathbf{H}_U^T = \mathbf{s}^U$ et $\mathbf{e}_V\mathbf{H}_V^T = \mathbf{s}^V$

1: $\mathbf{e}_V \leftarrow \text{DecodeV}(\mathbf{s}^V, \mathbf{H}_V)$
2: **Faire**
3: $\quad \mathbf{e}_U \leftarrow \text{DecodeU}(\varphi, \mathbf{e}_V, \mathbf{s}^U, \mathbf{H}_U)$
4: $\quad \mathbf{e} \leftarrow \varphi(\mathbf{e}_U, \mathbf{e}_V)$
5: **Tant que** $\text{rand}([0,1]) > r(m_1(\mathbf{e}), |\mathbf{e}_V|)$
6: **Retourne** $\mathbf{e}$

Où $m_1(x) := \#\{1 \leq i \leq n/2\ ;\ |(x_i, x_{i+n/2})| = 1\}$

La méthode du rejet

université de BORDEAUX

Algorithme 2 DecodeV($\mathbf{s}^V$)

1: c mot aléatoire du code V
2: $\mathbf{s} \leftarrow$ le syndrome $\mathbf{s}^V$ paddé avec des zéros
3: $\mathbf{e}_V \leftarrow \mathbf{s} + c$
4: **Retourne** $\mathbf{e}_V$

Algorithme 3 DecodeU($\varphi, \mathbf{e}_V, \mathbf{s}^U, \mathbf{H}_U$)

1: $t \leftarrow |\mathbf{e}_V|$
2: $k_0 \hookleftarrow \mathcal{D}_U^t$
3: **Faire**
4: $\quad \mathcal{I} \leftarrow$ ensemble d'information de $\langle \mathbf{H}_U \rangle^\perp$
5: $\quad \mathcal{J} \subset \mathcal{I}$ de taille $k - d$ tel que $|\mathbf{e}_V|_{\mathcal{J}} = k_0$
6: $\quad x_U \hookleftarrow \{x \in \mathbb{F}_3^{n/2} | \forall j \in \mathcal{J}, x_j \notin \{-\frac{b_i}{a_i}\mathbf{e}_{V_i}, -\frac{d_i}{c_i}\mathbf{e}_{V_i}\}\}$
7: $\quad \mathbf{e}_U \leftarrow$ PRANGE $(\mathbf{H}_U, \mathbf{s}^U, \mathcal{I}, x_U)$
8: **Tant que** $|\varphi(\mathbf{e}_U, \mathbf{e}_V)| \neq \omega$
9: **Retourne** $\mathbf{e}_U$

La méthode du rejet

Soient X et X^{unif} deux variables aléatoires à valeur dans un même ensemble $\mathcal{X}$
Pour tout $x \in \mathcal{X}$ on pose :

$$r(x) := \left(\inf_{y \in \mathcal{X}} \frac{\mathbb{P}(X = y)}{\mathbb{P}(X^{unif} = y)} \right) \frac{\mathbb{P}(X^{unif} = x)}{\mathbb{P}(X = x)}$$

Soit la variable aléatoire Y définie telle que:

1. On tire $x \in \mathcal{X}$ selon la distribution X
2. On tire θ uniformément dans l'intervalle $[\![0, 1]\!]$
3. Si $\theta \leq r(x)$, alors Y prend la valeur x
4. Sinon, on recommence

Alors Y suit une loi uniforme.

La méthode du rejet

université de BORDEAUX

Algorithme 1 DecodeUV$(\varphi, \mathbf{s}, \mathbf{H}_V, \mathbf{H}_U)$

Entrées: φ, $\mathbf{s} \in \mathbb{F}_q^{n-k}$ un syndrome, $\mathbf{H}_V \in \mathbb{F}_q^{(\frac{n}{2}-k_V)\times\frac{n}{2}}$, $\mathbf{H}_U \in \mathbb{F}_q^{(\frac{n}{2}-k_U)\times\frac{n}{2}}$
Sortie: $\mathbf{e} = \varphi(e_U, e_V)$ avec $\mathbf{e}_U\mathbf{H}_U^T = \mathbf{s}^U$ et $\mathbf{e}_V\mathbf{H}_V^T = \mathbf{s}^V$

1: $\mathbf{e}_V \leftarrow \text{DecodeV}(\mathbf{s}^V, \mathbf{H}_V)$
2: **Faire**
3: $\quad \mathbf{e}_U \leftarrow \text{DecodeU}(\varphi, \mathbf{e}_V, \mathbf{s}^U, \mathbf{H}_U)$
4: $\quad \mathbf{e} \leftarrow \varphi(\mathbf{e}_U, \mathbf{e}_V)$
5: **Tant que** $\text{rand}([0,1]) > r(m_1(\mathbf{e}), |\mathbf{e}_V|)$
6: **Retourne** $\mathbf{e}$

Où $m_1(x) := \#\{1 \leq i \leq n/2\ ;\ |(x_i, x_{i+n/2})| = 1\}$

Plan

Jeu EUF-CMA

Algorithme 4 Init(λ)

1: $(pk, sk) \leftarrow \mathrm{Gen}(1^\lambda)$
2: $\mathbf{H}_{pk} \leftarrow pk$
3: $(\varphi, \mathbf{H}_U, \mathbf{H}_V) \leftarrow sk$
4: **Retourne** $\mathbf{H}_{pk}$

L'attaquant $\mathcal{A}$ appelle la fonction `init` et récupère la matrice de parité du code $(U, U+V)$-généralisé $\mathbf{H}_{pk}$.

Jeu EUF-CMA

Algorithme 5 Sign(s)

1: $\mathbf{e} \leftarrow \mathcal{D}_{\varphi,\mathbf{H}_U,\mathbf{H}_V}(\mathbf{s})$
2: **Retourne** $\mathbf{e}$

- L'attaquant $\mathcal{A}$ peut faire N_{sign} appels à la fonction `sign` et récupérer N_{sign} couples $(s, \mathbf{e})$
- Il doit alors renvoyer un nouveau couple $(s, \mathbf{e})$ où s n'a jamais été demandé à la fonction `sign`

Jeu EUF-CMA

Algorithme 6 $\mathrm{Fin}((s, e))$

1: **Retourne** $(\mathbf{e}\mathbf{H}_{pk}^{T} = s) \wedge (|\mathbf{e}| = \omega)$

- La fonction `Fin` vérifie la validité de la signature
- L'attaquant $\mathcal{A}$ a réussi le jeu EUF-CMA si la fonction `Fin` renvoie 1

Sécurité EUF-CMA

université de BORDEAUX

On définit alors le succès EUF-CMA comme :

$$Succ_{Wave}^{EUF-CMA}(N_{sign}) := \max_{\mathcal{A}}(\mathbb{P}(\mathcal{A} \text{ réussit le jeu EUF-CMA de Wave})).$$

Le protocole est alors sûr au sens EUF-CMA si ce succès est négligeable.

Pour montrer que le schéma Wave est sûr au sens EUF-CMA, nous pouvons le réduire au problème DOOM.

Réduction au problème DOOM

Le problème DOOM. Soient des paramètres (n, q, k, ω, N), où N est un entier.

I : $\mathbf{H}$ une matrice uniforme de $\mathbb{F}_q^{(n-k)\times n}$ et $(\mathbf{s}_1, ..., \mathbf{s}_N)$ une liste de N syndromes.

Q : Décoder l'un des syndromes à la distance ω.

$$Succ^{DOOM} := \max_{\mathcal{A}} \left[\mathbb{P}\left(\mathcal{A}(\mathbf{H}, \mathbf{s}_1, ..., \mathbf{s}_n) = \mathbf{e} \;\middle|\; \exists j \in \{1, ..., N\} \text{ tq } \mathbf{e}\mathbf{H}^T = \mathbf{s}_j \right) \right].$$

Plan

Résultats de notre implémentation

université de BORDEAUX

nombre d'itérations	d	nombre de rejets	ratio
100	0	6	6%
100	1	3	3%
100	2	6	6%
100	3	3	3%
100	4	6	6%
100	5	4	4%

nombre d'itérations	d	nombres de rejets	ratio
400	3	19	$\sim$5%
400	5	17	$\sim$4%

Ratio moyen de l'article : $\sim$10%

Références

[1] Thomas Debris-Alazard. *Cryptographie fondée sur les codes : nouvelles approches pour constructions et preuves ; contribution en cryptanalyse*. 2019.

[2] Jean-Pierre Tillich, Thomas Debris-Alazard, Nicolas Sendrier. *Wave : A new family of trapdoor one-way preimage sampleable functions based on codes*. 2018.