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

Mardi 25 Février 2020

Plan

Introduction

université de BORDEAUX

- Éventualité de l'arrivée de l'ordinateur quantique:
  - → On cherche des alternatives à RSA et DH
  - → Appel du NIST
- Utilisation des codes correcteurs
  - → Sont quantiquement sûrs
  - → Déjà des systèmes de chiffrement les utilisant
  - → Peu (pas) utilisés 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 inutilisable dans la pratique

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

Plan

Codes $(U, U+V)$-généralisés

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

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

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

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

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

Décodage

Soit

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

et soient $\mathbf{e}_U$ et $\mathbf{e}_V$ de $\mathbb{F}_q^{n/2}$ tels que

$$(\mathbf{e}_U,\mathbf{e}_V) = \varphi_{a,b,c,d}^{-1}(\mathbf{e}).$$

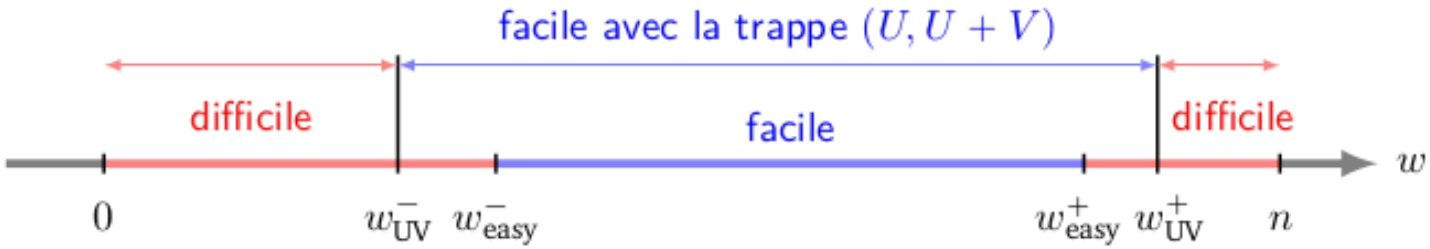
Proposition

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 $\mathbf{s}^U \in \mathbb{F}_q^{n/2-k_U}$ et $\mathbf{s}^V \in \mathbb{F}_q^{n/2-k_V}$.

Décodage



- poids haut -> conditions sur les coordonnées de e_U avant le décodage
- alors e aura un grand poids

Décodage

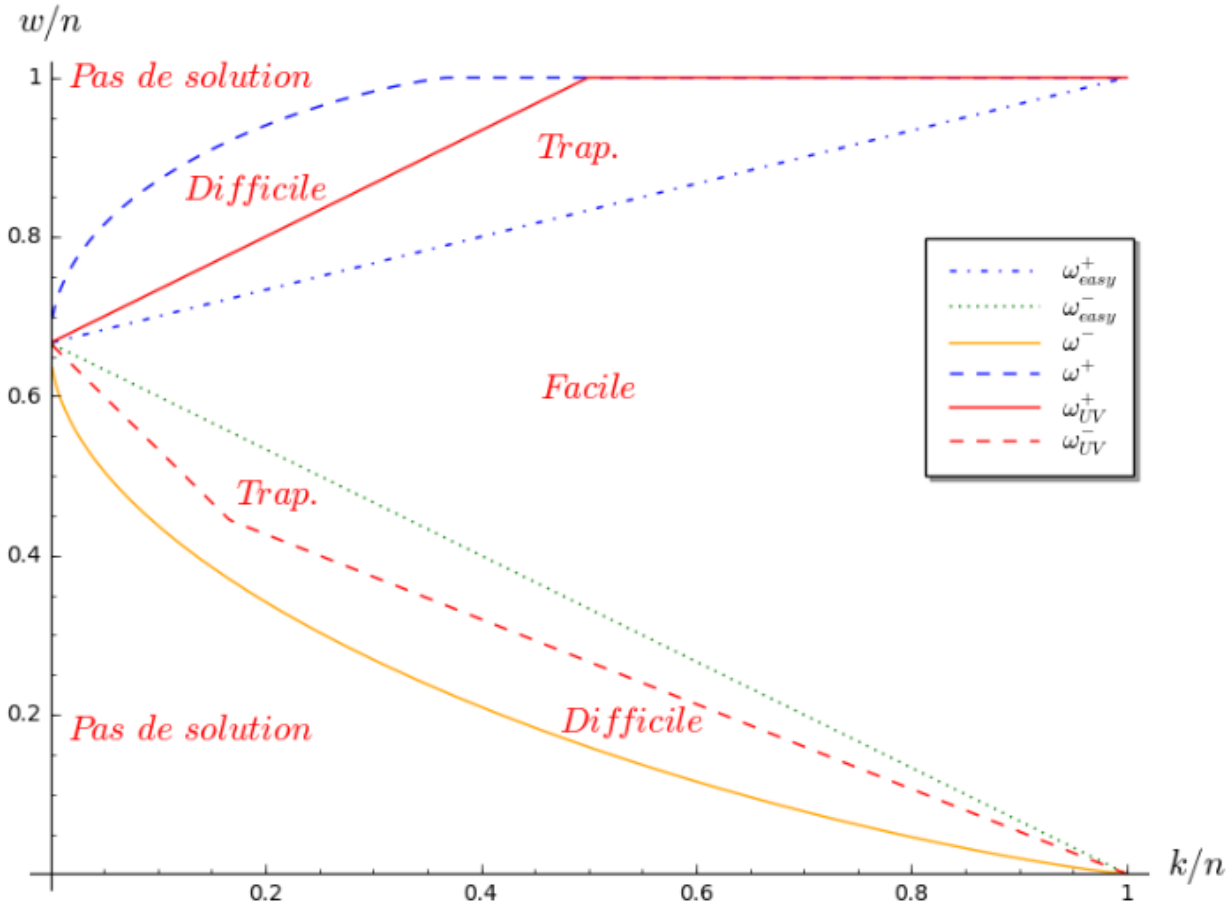


Figure: Comparaison des distances w/n avec et sans trappe en fonction du rendement.

Uniformisation des sorties

fuite d'info
m1 donne les info sur la permutation

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** $\mathbf{e}$

La méthode du rejet

preuve générique rejet

La méthode du rejet

application à nous

Sécurité EUF-CMA

université de BORDEAUX

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** $\mathbf{H}_{pk}$

Algorithme 5 Sign(s)

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

Algorithme 6 Fin((s, e))

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

Le jeu EUF-CMA se déroule comme suit. $\mathcal{A}$ fait appel à `Init`. Il peut ensuite faire N_{sign} requêtes à `sign`. Le jeu est dit réussi si $\mathcal{A}$ est capable de donner (s, e) accepté par `Fin` et tel que s n'est jamais été demandé à `Sign`.
On définit alors le succès EUF-CMA comme :

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

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

Sécurité EUF-CMA

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 $w := \lfloor \omega n \rfloor$.

On définit alors le succès de DOOM comme :

$$Succ^{DOOM(n,q,k,N)}(t) := \max_{\mathcal{A};|A|\leq t} (\mathbb{P}(\mathcal{A}(\mathbf{H}, \mathbf{s}_1, ..., \mathbf{s}_n) = \mathbf{e} \text{ tel que}$$

$$\mathbf{e}\mathbf{H}^T = \mathbf{s}_j \text{ pour un certain } j \in \{1, ..., N\})).$$

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.