

# 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

- 1 Introduction
- 2 Schéma de signature Wave
- 3 Décodage
- 4 Uniformisation des sorties
- 5 Sécurité EUF-CMA
- 6 Implémentation et résultats
- 7 Références

- arrivée ordinateur quantique  $\rightarrow$  alternative RSA + DH
- code correcteur  $\rightarrow$  quantiquement sûr
- chiffrement ok signature pas ok
- NIST

	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.

Wave solution au problème pour les signatures poids grands

- 1 Introduction
- 2 **Schéma de signature Wave**
- 3 Décodage
- 4 Uniformisation des sorties
- 5 Sécurité EUF-CMA
- 6 Implémentation et résultats
- 7 Références

## Définition

Soient  $n$  un entier pair,  $U$  et  $V$  deux codes définis comme précédemment. Le code  $(U, U + V)$ -généralisé correspond à l'ensemble :

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

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

- fonction syndrome : sens unique
- trappe : structure du code



$\text{Sign}^{sk}(s)$ :

$e \leftarrow \text{InvertAlg}(s, T)$

renvoie  $e$

$\text{Verify}^{pk}(s, e')$ :

Si  $e'H^T = s$  et  $|e'| = \omega$

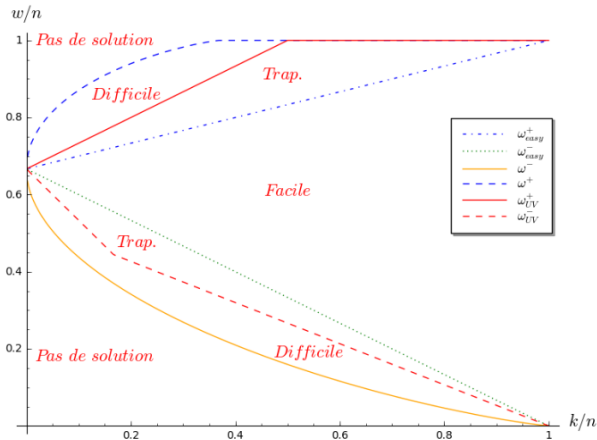
renvoie 1

renvoie 0

décodage classique

décoder  $UV \iff$  décoder  $U$  puis décoder  $V$

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



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

fuite d'info  
m1 donne les info sur la permutation

---

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

---

**Entrées:**  $\varphi, \mathbf{s} \in \mathbb{F}_q^{n-k}$  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:    $\mathbf{e}_U \leftarrow \text{DecodeU}(\varphi, \mathbf{e}_V, \mathbf{s}^U, \mathbf{H}_U)$
  - 4:    $\mathbf{e} \leftarrow \varphi(\mathbf{e}_U, \mathbf{e}_V)$
  - 5: **Tant que**  $\text{rand}([0, 1]) > r(m_1(\mathbf{e}), |\mathbf{e}_V|)$
  - 6: **Retourne**  $\mathbf{e}$
-

preuve générique rejet

application à nous



---

**Algorithme 4**  $\text{Init}(\lambda)$ 

---

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

---

**Algorithme 5**  $\text{Sign}(s)$ 

---

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

---

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

---

- 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.

**Le problème DOOM.** Soient des paramètres  $(n, q, k, \omega, N)$ , où  $N$  est un entier.

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

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

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

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	~5%
400	5	17	~4%

**Ratio moyen de l'article : ~10%**

- [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.