Cryptanalyse algébrique des systèmes basés sur les codes

Soutenance de stage

Stage encadré par Jean-Charles Faugère, Ludovic Perret (LIP6),
Jean-Pierre Tillich et Ayoub Otmani (INRIA)

Mohamed Amine Najahi

Université Pierre et Marie Curie

Mardi, 6 septembre 2011

Sommaire

Sommaire

Enjeux de la cryptographie à clef publique

Constats

1. Les cryptosystèmes à clef publique reposent sur un problème difficile avec trappe.
2. La majorité des problèmes exploités aujourd'hui sont issus de la thèorie des nombres (factorisation, logarithme discret, courbes elliptiques ...).
3. En 1994, Shor a publié un algorithme quantique de factorisation et de résolution de logarithme discret en temps polynômial.

$\rightsquigarrow$ une grande partie des cryptosystèmes à clef publique en usage aujourd'hui sera obsolète si l'on construisait un ordinateur quantique.

Solutions : Cryptosystèmes post-quantiques

Des alternatives sont fournies par :

- Les codes correcteurs d'erreurs.
- Les réseaux euclidiens.
- Les systèmes polynômiaux.
- ...

Enjeux de la cryptographie à clef publique

Constats

1. Les cryptosystèmes à clef publique reposent sur un problème difficile avec trappe.
2. La majorité des problèmes exploités aujourd'hui sont issus de la thèorie des nombres (factorisation, logarithme discret, courbes elliptiques ...).
3. En 1994, Shor a publié un algorithme quantique de factorisation et de résolution de logarithme discret en temps polynômial.

$\rightsquigarrow$ une grande partie des cryptosystèmes à clef publique en usage aujourd'hui sera obsolète si l'on construisait un ordinateur quantique.

Solutions : Cryptosystèmes post-quantiques

Des alternatives sont fournies par :

- Les codes correcteurs d'erreurs.
- Les réseaux euclidiens.
- Les systèmes polynômiaux.
- ...

Sommaire

Théorie des codes correcteurs

Principe

- Codage : Ajouter de la redondance à un message avant de le transmettre sur un canal bruité.
- Décodage : Retrouver le message initial à partir du message (probablement erroné) reçu.

34 *The Mathematical Theory of Communication*

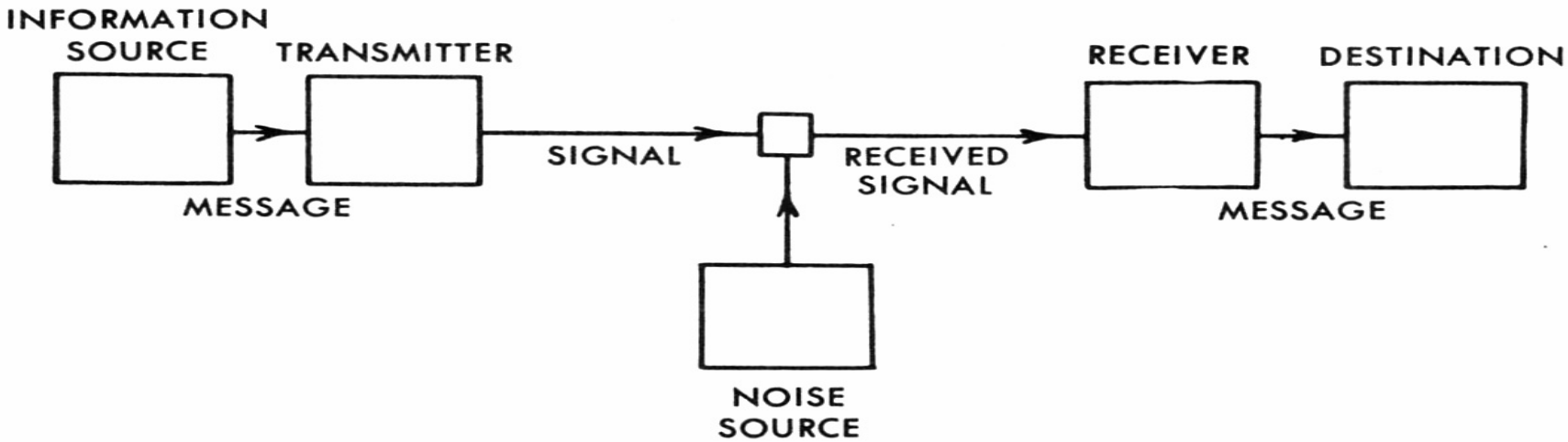


Fig. 1. — Schematic diagram of a general communication system.

Théorie des codes correcteurs d'erreurs

Codes linéaires

Un code linéaire $\mathcal{C}$ est un sous-espace vectoriel de dimension k de $\mathbb{F}_q^n$.

- n la longueur du code
- k la dimension du code
- $\mathbb{F}_q$ l'alphabet du code
- d la distance minimale du code (métrique de Hamming)

On le note $\mathcal{C} = [n, k, d]_q$

Propriétés

- détecte $d - 1$ erreurs.
- corrige de manière unique jusqu'à $\lfloor \frac{d-1}{2} \rfloor$ erreurs.
- admet une base de k vecteurs de longueur $n \Longrightarrow$ Matrice génératrice G.
  - Les mots du codes sont tous les vecteurs xG où $x \in \mathbb{F}_q^{1\times k}$.
- est le noyau d'une matrice de rang $n - k \Longrightarrow$ Matrice de parité.
  - m est un mot du code $\Leftrightarrow mH^T = 0$. En particulier $G \cdot H^T = (0)^{k,n-k}$.

Quelques problèmes difficiles issus de la théorie des codes

Problème du décodage

Berlekamp, McEliece, Van Tilborg '78 : Étant donné la matrice génératrice G d'un code linéaire aléatoire de longueur n et un message m de même longueur.

▷ Le problème du décodage (*i.e.* déterminer le mot du code le plus proche de m) est NP-Complet.

Problème de la distance minimale

Vardy '97 : Étant donné la matrice génératrice G d'un code linéaire aléatoire.

▷ Le problème de déterminer sa distance minimale est NP-Complet.

Rappel sur les codes de Goppa classique

C'est une sous-famille des codes alternants $\Rightarrow$ admet un algorithme de décodage efficace jusqu'à la distance minimale construite.

Définition des codes de Goppa

On se donne une séquence $X = (x_0, \cdots, x_{n-1}) \in \mathbb{F}_{p^m}$ et un polynôme $g(x) \in \mathbb{F}_{p^m}[x]$ de degré t tel que $g(x_i) \neq 0 \, \forall i$.Le code de Goppa $\Gamma(X, g)$ est le code de matrice de parité :

$$H = \begin{pmatrix} g(x_0)^{-1} & \cdots & g(x_{n-1})^{-1} \\ g(x_0)^{-1} x_0 & \cdots & g(x_{n-1})^{-1} x_{n-1} \\ \vdots & \ddots & \vdots \\ g(x_0)^{-1} x_0^{t-1} & \cdots & g(x_{n-1})^{-1} x_{n-1}^{t-1} \end{pmatrix} \in \mathbb{F}_{p^m}^{t*n}$$

Distance minimale des codes de Goppa

- Sur un corps de caratéristique impaire :
  - Un code de Goppa a une distance minimale construite égale à $t + 1$.
- Sur un corps binaire :
  - Un code de Goppa a une distance minimale construite égale à $2t + 1$, si g n'a pas de racines multiples.

McEliece et Niederreiter

On se donne un code $\mathcal{C} = [n, k, d = 2t + 1]$ décodable efficacement et on note :
$G \in \mathbb{F}_q^{k \times n}$ sa matrice génératrice.
$H \in \mathbb{F}_q^{n-k \times n}$ sa matrice de parité.
S une matrice inversible et P une matrice de permutation.

	McEliece '78	*Niederreiter '86*
Public key	$(\tilde{G} = SGP, t)$	$(\tilde{H} = SHP, t)$
Private key	$S \in GL_k(\mathbb{F}_q), G, P \in \mathbb{F}_q^{n \times n}$	$S \in GL_{n-k}(\mathbb{F}_q), H, P \in \mathbb{F}_q^{n \times n}$
Chiffrement	$c = m\tilde{G} + e,\ m \in \mathbb{F}_q^k,\ w(e) = t$	$c = \tilde{H}m^T,\ m \in \mathbb{F}_q^n,\ w(m) = t$
Déchiffement	$m = Dec(cP^{-1})S^{-1}$	$m = P^{-1}DecSyn(S^{-1}c)$

La signature CFS(Courtois, Finiasz, Sendrier)

C'est un schéma de signature basé sur le cryptosystème de Niederreiter et une fonction de hachage $\mathcal{H} : \{0,1\}^* \times \mathbb{N} \to \mathbb{F}_q^k$

CFS

On peut la voir comme 3 algorithmes distincts :

- Keygen : Produit le couple $(H, \mathcal{T})$: H la matrice de parité d'un code $\mathcal{C} = [n, k, 2t+1]_q$, et $\mathcal{T}$ une trappe qui permet de le décoder.
- Sign : Soit m le message à signer.
  - Trouve $c \in \mathbb{N}$ t.q. $syn = \mathcal{H}(m, c)$ est un syndrome décodable.
  - Utilise $\mathcal{T}$ pour obtenir e t.q. $w(e) \leq t$ et $He^T = syn^T$.
  - La signature est (e, c).
- Verify : Accepte la signature si et seulement si $w(e) \leq t$ et $He^T = \mathcal{H}(m, c)^T$

Quels paramètres pour CFS

Dans le cas Goppa binaire :

La densité des syndromes décodables est $d = \frac{1}{2^{mt}} \sum_{w=1}^{t} \binom{n}{w} \approx \frac{n^t}{2^{mt} t!} \approx \frac{1}{t!}$

$\rightsquigarrow$ $t!$ est le nombre moyen d'essais avant d'obtenir la signature.

Avantages et inconvénients des primitives basées sur les codes

Constats

Principal avantage : Rapidité dans le chiffrement (produit matrice vecteur).
Principal inconvénient : La taille des clefs publiques.

Solutions proposées par de récents travaux

- Ajouter de la structure sur la matrice publique pour réduire sa taille.
  - Quasi-cyclicité (Berger *et al.*, AFRICACRYPT 2009)
  - Quasi-dyadicité (Barreto *et al.*, SAC 2009)
- Utiliser des codes de Goppa non-binaires.
  - Wild McEliece (Bernstein *et al.*, SAC 2010)
- ...

Faugère, Perret, Otmani et Tillich

- La plupart des paramètres quasi-cycliques et quasi-dyadiques destinés au chiffrement ont été cassés. (Eurocrypt 2010)
  - Les paramètres quasi-dyadiques binaires résistent encore.
- Un distingueur pour certains codes de Goppa a aussi été proposé. (YACC 2010)

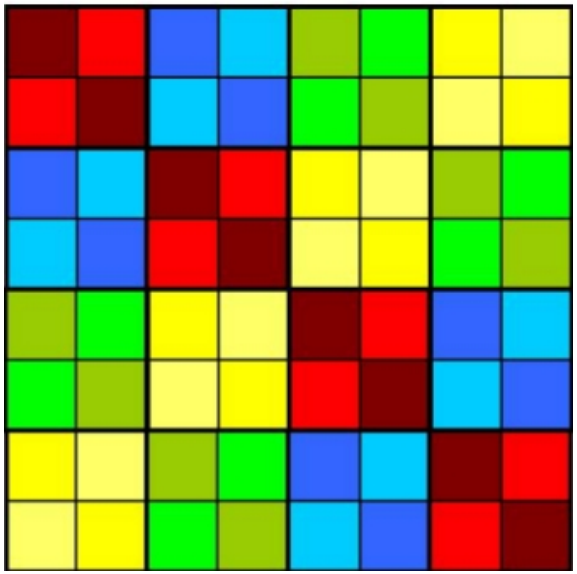
Sommaire

Matrice de Cauchy et codes de Goppa

Définition

Soit $m \in \mathbb{F}_q^n$ un vecteur. On dit que la matrice carré M est dyadique si $M = (m_{i,j}) = (m_{i \oplus j})$.

Une matrice dyadique est totalement déterminée par sa première ligne, on appelle celle-ci la signature.



Condition pour que la matrice de McEliece soit dyadique (Barreto *et al.*, SAC 2009)

$$\frac{1}{m_{i \oplus j}} = \frac{1}{m_i} + \frac{1}{m_j} + \frac{1}{m_0}$$

Sommaire

Les attaques sur les primitives basées sur les codes

Attaques par décodage

1. Information Set Decoding (Stern, Canteaut, ...)
2. Generalized Birthday Attacks (Wagner, ...)
3. ...

Attaques structurelles

Essayer de recouvrer la clef secrète en exploitant la structure de la clef publique.

- Support splitting algorithm (Sendrier)

Principe de l'attaque algébrique

Modélisation du cryptosystème par un système d'équations algébriques tel que :
Résoudre ce système $\Longrightarrow$ Recouvrer une information secrète.

2 étapes

- Modélisation :
  - Tout cryptosystème peut être modélisé par un système d'équations polynômiales.
- Résolution :
  - Les bases de Gröbner (Algorithme de Buchberger et plus récemment F4 et F5 de Faugère).
    - Les SAT solvers dans le cas booléen.
    - La linéarisation.

Les attaques sur les primitives basées sur les codes

Attaques par décodage

1. Information Set Decoding (Stern, Canteaut, ...)
2. Generalized Birthday Attacks (Wagner, ...)
3. ...

Attaques structurelles

Essayer de recouvrer la clef secrète en exploitant la structure de la clef publique.

- Support splitting algorithm (Sendrier)

Principe de l'attaque algébrique

Modélisation du cryptosystème par un système d'équations algébriques tel que :
Résoudre ce système $\Longrightarrow$ Recouvrer une information secrète.

2 étapes

- Modélisation :
  - Tout cryptosystème peut être modélisé par un système d'équations polynômiales.
- Résolution :
  - Les bases de Gröbner (Algorithme de Buchberger et plus récemment F4 et F5 de Faugère).
    - Les SAT solvers dans le cas booléen.
    - La linéarisation.

Objectif

L'objectif de l'attaque est de recouvrer le vecteur $\tilde{h}$ qui a servi à la construction de la matrice publique.

- Trouver la meilleure modélisation.
- Utiliser le meilleur outils pour la résolution.

Comment

La première étape, toujours possible est d'utiliser la relation fondamentale suivante

$$G \cdot H^T = (0)^{k,n-k}$$

H est dyadique, on s'intéressera à sa première ligne
$X := (x_0, \cdots, x_{n-1}) \in \mathbb{F}_{q^m}[x_1, \cdots, x_{n-1}]$.

On dispose de la matrice génératrice G sous la forme systématique suivante :

$$G = \left(\begin{array}{c|cccc} & 1 & 0 & \cdots & 0 \\ & 0 & 1 & \cdots & 0 \\ P \in \mathbb{F}_2^{k\times k} & \vdots & \vdots & \ddots & 0 \\ & 0 & 0 & \cdots & 1 \end{array} \right) \in \mathbb{F}_2^{k\times n} \quad \sum_{j=0}^{n-k-1} p_{i,j}x_j + x_{n-k+i} = 0 \, \forall \, 0 \leq i \leq k-1$$

On a exprimé linéairement k variables inconnues en fonction de $n-k = mt$ variables.

Deux types d'équations sont dérivés de la structure dyadique de la matrice.

Équations inter-blocs

$$\frac{1}{h_{bt+i\oplus j}} = \frac{1}{h_{bt\oplus i}} + \frac{1}{h_{bt\oplus j}} + \frac{1}{h_{bt}}$$

Équations intra-blocs

$$\frac{1}{h_{bt+i}} + \frac{1}{h_{bt}} = \frac{1}{h_i} + \frac{1}{h_0}$$

Scénario de l'attaque (premier bloc connu)

On suppose que l'on connaît $h_0, \cdots, h_{t-1}$ $\rightsquigarrow$ coût en $2^{m(log(t)-1)}$

Des équations quadratiques avec comme paramètres :

Nombre de variables $\Rightarrow \quad n-k-t = (m-1)t$

Nombre d'équations $\Rightarrow \left(\frac{n}{t} - 1\right) \times (t-1)$

Résolution du système

Résolution par linéarisation tableau

C'est une méthode de résolution des systèmes sur-déterminés.

applicable si $\rightsquigarrow$ $\left(\frac{2^m - t}{t} - 1\right) \times (t-1) \geq \binom{(m-1)t+2}{2}$

	m
$t = 4$	≥ 10
$t = 8$	≥ 13
$t = 16$	≥ 15

Valeurs de m et t pour lesquelles l'inégalité est vérifiée.

Impact sur la sécurité

m	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
$t = 4$	$2^{20.8}$	$2^{22.2}$	$2^{23.6}$	$2^{24.9}$	$2^{26.2}$	$2^{27.5}$	$2^{28.7}$	2^{30}	$2^{31.2}$	$2^{32.4}$	$2^{33.6}$	$2^{34.8}$	2^{36}	$2^{37.1}$	$2^{38.3}$	$2^{39.4}$	$2^{40.6}$
$t = 8$				$2^{39.3}$	$2^{41.6}$	$2^{43.9}$	$2^{46.1}$	$2^{48.4}$	$2^{50.6}$	$2^{52.8}$	2^{55}	$2^{57.2}$	$2^{59.3}$	$2^{61.5}$	$2^{63.7}$	$2^{65.8}$	2^{68}
$t = 16$							$2^{63.5}$	$2^{66.7}$	2^{70}	$2^{73.2}$	$2^{76.4}$	$2^{79.5}$	$2^{82.7}$	$2^{85.9}$	2^{89}	$2^{92.2}$	$2^{95.3}$

Complexité de résolution par linéarisation ($\omega = 2,376$).

On a aussi réussi à ramener le cas $t = 12$ au cas $t = 4$

Sommaire

Conclusion

- Nous avons implémenté la variante dyadique de CFS en magma.
- Nous avons proposé quelques améliorations à l'algorithme de génération des clefs.
- Nous avons proposé une attaque structurelle sur la variante dyadique de McEliece destinée à la signature.
- Nous avons implémenté l'attaque et l'avons testé sur plusieurs valeurs.
- Les expériences corroborent l'analyse théorique. La linéarisation a été efficace pour la résolution de la plupart des paramètres.
- Faugère *et al.* ont réussi à casser la plupart des paramètres dyadiques destinés au chiffrement. Nous avons montré la vulnérabilité des paramètres destinés à CFS.

Conclusion

- Nous avons implémenté la variante dyadique de CFS en magma.
- Nous avons proposé quelques améliorations à l'algorithme de génération des clefs.
- Nous avons proposé une attaque structurelle sur la variante dyadique de McEliece destinée à la signature.
- Nous avons implémenté l'attaque et l'avons testé sur plusieurs valeurs.
- Les expériences corroborent l'analyse théorique. La linéarisation a été efficace pour la résolution de la plupart des paramètres.
- Faugère *et al.* ont réussi à casser la plupart des paramètres dyadiques destinés au chiffrement. Nous avons montré la vulnérabilité des paramètres destinés à CFS.

Conclusion

- Nous avons implémenté la variante dyadique de CFS en magma.
- Nous avons proposé quelques améliorations à l'algorithme de génération des clefs.
- Nous avons proposé une attaque structurelle sur la variante dyadique de McEliece destinée à la signature.
- Nous avons implémenté l'attaque et l'avons testé sur plusieurs valeurs.
- Les expériences corroborent l'analyse théorique. La linéarisation a été efficace pour la résolution de la plupart des paramètres.
- Faugère *et al.* ont réussi à casser la plupart des paramètres dyadiques destinés au chiffrement. Nous avons montré la vulnérabilité des paramètres destinés à CFS.