MajecSTIC 2009
Avignon, France, du 16 au 18 novembre 2009

Nouveaux résultats en cryptographie basée sur les codes correcteurs d'erreurs

Pierre-Louis CAYREL

Université Paris VIII
Département de Mathématiques
2, rue de la Liberté
93526 - SAINT-DENIS cedex 02, France

Contact : cayrelpierrelouis@gmail.com

Résumé
Dans cet article, on s'intéresse à l'étude de systèmes de chiffrement ainsi que de schémas de signature dont la sécurité repose sur des problèmes difficiles de théorie des codes correcteurs d'erreurs. Ces activités de recherche ont été motivées, d'une part d'un point de vue théorique par la création de nouveaux schémas de signature avec des propriétés spéciales ainsi que d'une manière de réduire la taille de clés du schéma de McEliece, et d'autre part, d'un point de vue pratique visant à utiliser des propriétés structurelles afin d'obtenir des implémentations effectives d'un schéma de signature fondé sur les codes correcteurs d'erreurs. Comme l'indique son titre, cet article traite de la construction de cryptosystèmes basés sur des codes correcteurs d'erreurs et plus particulièrement de cinq nouveaux protocoles. On présente ici une version sécurisée du schéma de Stern dans un environnement à faibles ressources, une nouvelle construction du schéma de Kabatianski, Krouk et Smeets, un schéma de signature basé sur l'identité prouvé sûr dans le modèle de l'oracle aléatoire, un schéma de signature de cercle à seuil et enfin une réduction de la taille de clés du schéma de McEliece à l'aide de codes alternants quasi-cycliques.

Abstract
In this article, we are interested in the study of encryption systems as well as signature schemes whose security relies on difficult problems of error-correcting codes. These research activities have been motivated, a part of a theoretical point of view by creating : new signature schemes with special properties and a way of reducing the size of the key of the McEliece scheme, and on the other hand, a practical point of view to use structural properties to obtain effective implementations of a signature scheme which is based on error-correcting codes. As its title indicates, this article deals with the construction and optimization of cryptosystems based on error-correcting codes and more particularly five new protocols. It presents a secure version of the Stern scheme in a low-resources environment, a new construction of the Kabatianski, Krouk and Smeets scheme, a signature scheme based on the identity proved secure in the random oracle model, a threshold ring signature scheme and a reduction of the size of the key of the McEliece scheme using quasi-cyclic alternant codes.

Mots-clés : Cryptologie, codes correcteurs d'erreurs, authentification, signature, sécurité.

Keywords: Cryptology, error correcting codes, authentication, signature, security proof.

Dans cet article nous allons parler de cryptographie. Mais attention pas de cryptographie 'traditionnelle' basée sur des problèmes de théorie des nombres comme la factorisation [1] ou le logarithme discret [2] mais sur des problèmes différents, basés sur les codes correcteurs d'erreurs et qui ont le bon goût d'être NP-complet et de résister à l'ordinateur quantique.
Le premier, McEliece eut l'idée, en 1978, d'utiliser la théorie des codes correcteurs d'erreurs à des fins cryptographiques, et plus précisément pour un algorithme de chiffrement asymétrique. Le principe du protocole qu'il décrivit consiste à faire envoyer par Alice un message contenant un grand nombre d'erreurs, erreurs que seul Bob sait détecter et corriger.

1. Chiffrer avec des codes

1.1. Le cryptosystème de McEliece

La sécurité du système repose donc sur deux problèmes distincts :
– l'indistingabilité entre un code structuré et un code aléatoire ;
– le problème du décodage d'un code aléatoire.

1.1.1. Le cryptosystème de base

Soit $n = 2^m$, x le message, G la matrice génératrice sous forme systématique d'un code, $x' = xG$ est de la forme $(x|y)$ où y est $(n-k)$-bits. Ce sont ces $n-k$ bits (*redondance*) qui permettent de corriger des erreurs. Il faut m bits pour corriger une erreur, soit, pour corriger t erreurs, mt bits au plus (généralement moins car les erreurs sont interchangeables). Comme on a $2^m - k$ redondances, on peut corriger t_0 erreurs, avec $t_0 \geq (2^m - k)/m$. Par exemple, avec $m = 10$ (donc $n = 1024$) et $k = 512$, on peut corriger 52 erreurs au moins. Un tel code est généré par un polynôme de degré t de $\mathbb{F}_{2^m}$.
Dans le cryptosystème de McEliece, la matrice génératrice G est la clé secrète de Bob. Pour fabriquer une clé publique, on multiplie G à gauche par une matrice binaire non singulière (i.e. inversible) S de dimension (k, k). Cette nouvelle matrice $G'' = SG$ sera donc toujours une matrice génératrice d'un code : le produit de S par G revient, en effet, à prendre une combinaison linéaire des lignes de G.
Cependant, il est facile de retrouver G à partir de G''. Il suffit de faire une élimination gaussienne pour obtenir la matrice identité en première partie de G. Pour parer cette attaque, on multiplie à droite G par une matrice de permutation P de dimension (n, n). La clé publique de Bob sera alors :

$$G' = SGP.$$

Le principal avantage de cette méthode est sa facilité d'implémentation : les seules opérations sont des opérations bit à bit. Par contre, l'implémentation nécessite beaucoup de place mémoire.
Ce cryptosystème, reposant sur un problème difficile de la théorie des codes, n'a pas rencontré de véritable soutien dans la communauté cryptographique. L'une des principales raisons de cet état de fait est la taille de la clé. Pourtant, le cryptosystème de McEliece possède des propriétés intéressantes, citons notamment
– la sécurité croît beaucoup plus avec la taille des clés que pour le système RSA ;
– la rapidité du chiffrement.
Un autre avantage est de reposer sur un problème très différent des algorithmes asymétriques usuels. En conséquence de quoi une percée théorique dans le domaine de la factorisation, qui ruinerait RSA, n'affecterait en rien ce cryptosystème.
Le cryptosystème de McEliece résiste à ce jour à toute tentative de cryptanalyse, mais est rarement utilisé en pratique du fait de la grande taille des clés. On peut cependant noter qu'il a été utilisé pour le chiffrement dans Entropy, une alternative à Freenet.

1.2. La variante de Niederreiter

En 1986, Harald Niederreiter a proposé un autre cryptosystème fondé sur la théorie des codes. Le cryptosystème de Niederreiter a été prouvé équivalent à celui de McEliece en 1994 par Y.X. Li, R.H. Deng et X.M. Wang [10].

1. Soit $n = pq$ avec p et q premiers, retrouvez p connaissant n
2. Soit $q = g^e$ dans un groupe qui convient, trouvé e connaissant q

1. [Génération de clés] Soit G la matrice génératrice sous forme systématique d'un code, on choisit aléatoirement S une matrice binaire inversible de dimension (k, k) et une matrice de permutation P de dimension (n, n). On calcule la clé ublique :
$$G' = SGP.$$
2. [Chiffrement] Bob publie $G' = SGP$. Si Alice veut envoyer le message x (constitué de k bits) à Bob. Alice génère un mot de n bits aléatoires e de poids t, elle calcule et envoie à Bob
$$y = xG' + e.$$
3. [Déchiffrement] Pour $y = xG' + e$, la connaissance des secrets permet :
   (a) de calculer $u = yP^{-1}$, u est alors un mot du code de Goppa de matrice génératrice SG contenant t erreurs ;
   (b) de déterminer u' en corrigeant les erreurs de u ;
   (c) calculer $x = u'S^{-1}$.

FIGURE 1 – Le protocole de McEliece

1. [Génération de clés] Soit $\mathcal{C}$ un code linéaire q-aire t-correcteur de longueur n et de dimension k. Soit H une matrice de parité de $\mathcal{C}$. On choisit aléatoirement S inversible et P une matrice de permutation. On calcule H' telle que :
$$H' = SHP$$
où H' sera publique, et sa décomposition constituera le secret, avec la connaissance d'un algorithme de décodage par syndromes efficace dans $\mathcal{C}$.
2. [Chiffrement] Pour un texte clair x choisi dans l'espace $E_{q,n,t}$ des mots de $\mathbb{F}_q^n$ de poids de Hamming t (l'espace des erreurs) : y est le cryptogramme correspondant à x ssi :
$$y = H'x^T.$$
3. [Déchiffrement] Pour $y = H'x^T$, la connaissance des secrets permet :
   (a) de calculer $S^{-1}y (= HPx^T)$;
   (b) de trouver Px^T à partir de $S^{-1}y$ grâce à l'algorithme de décodage par syndromes de $\mathcal{C}$;
   (c) de trouver x en appliquant P^{-1} à Px^T.

FIGURE 2 – Le protocole de Niederreiter

2. Signer avec des codes

2.1. Le schéma de signature de Courtois, Finiasz et Sendrier

La construction d'un schéma de signature pour les codes correcteurs n'est pas aussi naturelle que pour RSA. En effet, l'opération de décodage n'est pas inversible, c'est-à-dire qu'il n'est possible de décoder un élément aléatoire dans l'espace entier que si cet élément est à une distance suffisamment petite du code. En général, la proportion de tels éléments est très faible. Le schéma que Courtois, Finiasz et Sendrier proposent [7], utilise des codes de Goppa avec une faible capacité de correction t, dans ce cas, la proportion de mots décodables est $\frac{1}{t!}$. Le schéma de signature consiste alors en la concaténation d'un haché du message $h(M)$, une suite d'éléments croissants 0,1,2,... et qui calcule la valeur du haché jusqu'à ce que la valeur du haché $h(M|i_0)$ corresponde à un mot décodable. La signature est alors le mot décodé associé à la valeur du haché $h(M|i_0))$. Les paramètres proposés par les auteurs sont $n = 2^{16} - 1$ et $t = 9$.
Soit M un message à signer. Soit h une fonction de hachage à valeurs dans $\{0,1\}^{n-k}$. On cherche un moyen de trouver un $s \in E_{q,n,t}$ tel que $h(M) = H's^T$. Il s'agit donc de déchiffrer $h(M)$. Le principal problème est que $h(M)$ n'est pas *a priori* dans l'espace d'arrivée de $x \rightarrow H'x^T$. C'est à dire que $h(M)$ n'est pas *a priori* dans l'espace des chiffrés par le système de Niederreiter. Pour contourner cette difficulté on utilise le protocole proposé par Courtois, Finiasz et Sendrier dans [7].
Soit $D()$ un algorithme de décodage par syndrome :

1. $i \leftarrow 0$
2. tant que $h(M|i)$ n'est pas un syndrome décodable faire $i \leftarrow i + 1$
3. calculer $s = D(h(M|i))$

FIGURE 3 – Protocole de Courtois-Finiasz-Sendrier

On obtient en sortie un couple $\{s, j\}$ tel que $h(M|j) = H's^T$. On peut remarquer qu'on a nécessairement s de poids t.
Dans [8], une preuve de sécurité est donnée dans le modèle de l'oracle aléatoire.

2.2. Le schéma d'identification de Stern

2.2.1. Le schéma de base

Le schéma de Stern est un schéma interactif à divulgation nulle de connaissance qui a pour protagonistes un *prouveur* noté P et un *vérifieur* noté V. Le prouveur cherchera à s'identifier auprès du vérifieur.
Soient n et k deux entiers tels que $n \geq k$. Le schéma de Stern nécessite une $(n-k) \times n$ matrice publique H' définie sur $\mathbb{F}_2$.
Soit $t \leq n$ un entier. Pour des raisons de sécurité (discutées dans [12]) il est recommandé que t soit choisi juste au dessus de la borne de Gilbert-Varshamov (voir [11]). La matrice H' et le poids t sont des paramètres du protocole et seront utilisés par plusieurs prouveurs différents.
Chaque prouveur P reçoit une clé secrète de n-bits s_P (aussi notée s s'il n'y a pas d'ambiguité sur le prouveur) de poids de Hamming t et calcule un *identifiant public* i_P tel que $i_P = H's_P^T$. Cet identifiant est calculé une fois pour toute pour H' donnée et peut alors être utilisé pour de nombreuses authentifications. Quand un utilisateur P a besoin de prouver à V qu'il est la personne associée à son identifiant public i_P, alors les deux protagonistes suivent le protocole suivant où h est une fonction de hachage standard :

Remarque 1 *Lorsque* b *vaut* 1, *durant la quatrième étape du schéma de Stern, on peut noter que* $H'y^T$ *vient directement de la relation* $H'(y \oplus s)^T$ *car nous avons :*

$$H'y^T = H'(y \oplus s)^T \oplus i_P = H'(y \oplus s)^T \oplus H's^T \ .$$

1. [Commitment Step] P choisit aléatoirement $y \in \mathbb{F}^n$ et une permutation σ définie sur $\mathbb{F}_2^n$. Alors P envoie à V les engagements c_1, c_2 et c_3 tels que :
$$c_1 = h(\sigma | H' y^T);\ c_2 = h(\sigma(y));\ c_3 = h(\sigma(y \oplus s)).$$
2. [Challenge Step] V envoie $b \in \{0, 1, 2\}$ à P.
3. [Answer Step] Trois possibilités :
   - si $b = 0$: P révèle y et σ.
   - si $b = 1$: P révèle $(y \oplus s)$ et σ.
   - si $b = 2$: P révèle $\sigma(y)$ et $\sigma(s)$.
4. [Verification Step] Trois possibilités :
   - si $b = 0$: V vérifie que c_1, c_2 sont corrects.
   - si $b = 1$: V vérifie quec_1, c_3 sont corrects.
   - si $b = 2$: V vérifie que c_2, c_3 sont corrects, et que le poids de $\sigma(s)$ est bien t.
5. Itère les étapes 1,*2*,*3*,*4* jusqu'à ce que le niveau de sécurité recherché soit atteint.

FIGURE 4 – Le protocole de Stern

Comme prouvé dans [12], le protocole est à divulgation nulle de connaissance. Pour un tour d'exécution, la probabilité qu'une personne malhonnête réussisse à tricher est de $2/3$. Afin d'obtenir un degré de sécurité β, le protocole doit être exécuté un nombre de fois k tel que l'on ait la relation $(2/3)^k \leq \beta$. Quand le nombre d'itérations vérifie la dernière condition, alors la sécurité du problème repose sur le problème NP-complet de décodage par syndrome (SD).

Remarque 2 *En utilisant l'heuristique de Fiat-Shamir, il est possible théoriquement de convertir le protocole d'identification de Stern en un protocole de signature, mais la signature obtenue est très longue (quelque* 150*-kbit pour une sécurité de* 2^{80} *opérations binaires).*

Le schéma de Stern possède de nombreux avantages. Le premier de tous, sa sécurité repose sur un problème qui n'est pas un des deux problèmes utilisés traditionnellement en cryptographie, à savoir la factorisation et le problème du logarithme discret. Ceci donne une bonne alternative aux nombreux cryptosystèmes dont la sécurité repose sur les deux problèmes précédents, spécialement dans l'éventualité ou un ordinateur quantique puisse exister. Le second avantage du schéma de Stern est qu'il ne nécessite que des opérations très simples (tel que : x-or ou décalage binaire) et ne nécessite aucun crypto-processeur contrairement au cas d'une identification basée sur des problèmes d'arithmétique.
En dépit de ces avantages, le schéma de Stern n'a que rarement été utilisé depuis sa publication en 1993. En effet, le schéma présente les deux inconvénients suivants, qui à eux deux rendent le schéma impraticable dans de nombreuses applications :

1. de nombreux tours sont nécessaires (typiquement 28 si nous voulons que le tricheur ait une probabilité de succès inférieur à 2^{-16}),
2. la clé publique H' est très grande (typiquement 150-kbit).

Le premier point est inhérent au protocole interactif et ne constitue pas un réel inconvénient. Par exemple, si le prouveur et le vérifieur peuvent être connectés ensemble pendant une longue période, alors l'identification peut être effectuée graduellement. Dans ce cas, le processus d'identification complet est réalisé en exécutant, de temps en temps durant une période prescrite (*i.e.* une heure), une itération de l'algorithme jusqu'à ce que le niveau de sécurité espéré soit atteint. De tels schémas d'authentification *graduels* peuvent être de grand intérêt dans la télévision à péage ou dans les systèmes où une machine (*i.t.* une photocopieuse ou une machine à café) veut identifier un matériel physique (*i.t.* une cartouche d'encre ou de café).
Le deuxième inconvénient a été récemment traité par Gaborit et Girault dans [9]. Dans leur article, les auteurs proposent d'utiliser des *matrices doublement circulantes* pour décroître la taille de la clé

publique sans apparemment dégrader le niveau de sécurité du protocole. Nous décrivons cette idée dans la section suivante :

2.2.2. Construction quasi-cyclique

L'idée de [9] est de remplacer la matrice aléatoire H' par la matrice de parité d'un type particulier de codes aléatoires : les *codes doublement circulants*.

Cette idée vient du fait que dans le cryptosystème NTRU [3] la clé publique consiste en le quotient $\frac{f}{g}$ où f et g sont des polynômes tronqués de l'anneau quotient $R = \mathbb{Z}_q[x]/(x^n - 1)$ pour n et q des paramètres du système (typiquement 251 et 128). Pour chiffrer, nous devons multiplier ces deux polynômes dans l'anneau R. Ce produit peut être vu comme la multiplication de deux matrices circulantes.

Soit ℓ un entier. Une matrice aléatoire doublement circulante $\ell \times 2\ell$ H est une matrice de la forme :

$$H = (I|A) \ ,$$

où A est une *matrice circulante*, qui est de la forme suivante :

$$A = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_\ell \\ a_l & a_1 & a_2 & \cdots & a_{\ell-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_2 & a_3 & a_4 & \cdots & a_1 \end{pmatrix} \ ,$$

où $(a_1, a_2, a_3, \cdots, a_\ell)$ est un vecteur de $\mathbb{F}_2^\ell$.

Comme nous pouvons facilement le vérifier, représenter H ne nécessite pas de stocker tous les coefficients de la matrice (comme c'est le cas dans le schéma de Stern originel) mais nécessite seulement le vecteur de ℓ-bits $(a_1, a_2, a_3, \cdots, a_\ell)$ (qui constitue la première ligne de A). Soit n égal à 2ℓ, les paramètres du nouveau schéma ont les tailles suivantes :

- **Données privées :** le secret s de n-bits.
- **Données publiques :** le syndrome public i_P de taille $\frac{n}{2}$ et la première ligne de A de taille $\frac{n}{2}$, soit n bits.

Comme expliqué dans [9] le comportement de ces matrices en terme de distance minimale est le même que celui des matrices aléatoires. De même, il semble que le problème du décodage par syndrome reste difficile dans le cas particulier des codes doublement circulants (voir [9] pour plus de détails).

Comme la nouvelle version du schéma de Stern nécessite des paramètres de plus petite taille et n'utilise toujours que des opérations élémentaires. Cette version devient très attractive pour des implémentations. Ceci est spécialement vrai dans des environnements à mémoire (RAM,PROM,etc.) limitée.

Dans le but de résister aux attaques par décodage, les auteurs de [9] préconisent des paramètres d'au moins $\ell = 347$ et $t = 74$. Ces choix mènent en effet à un niveau de sécurité d'au moins 2^{85} opérations binaires avec une clé (publique et secrète) de 694 bits.

3. Mes travaux

Durant ma thèse, j'ai réalisé 5 travaux distincts je donne ici les principales idées et renvoie le lecteur vers les références pour plus de précisions. Tous ces travaux tournent autour de l'application des codes en cryptographie et reposent essentiellement sur les protocoles présentés dans la section précédente.

L'implémentation sûre du schéma de Stern

Dans [5],nous décrivons la première implémentation du protocole de Stern sur carte à puce (en fait, cela constitue aussi, plus généralement, le premier cryptosystème basé sur des codes correcteurs d'erreurs implémenté sur carte à puce avec peu de ressources). Ce protocole est une nouvelle

3. NTRU= Number Theorists aRe Us ou encore N-th degree TRUncated polynomial ring. Le schéma de chiffrement a été proposé en 1996, le schéma de signature en 2002 mais partiellement cassé par Nguyen et Regev en 2006 (voir `www.ntru.com`)

option pour réaliser une identification forte et rapide sur carte à puce. De plus, l'utilisation d'un co-processeur d'algèbre linéaire dédié devrait améliorer sensiblement les performances de notre implémentation. De même qu'une version hardware de SHA-256 au lieu d'une implémentation software améliorerait sérieusement les performances (en temps) de notre protocole. Des travaux futurs envisagent des attaques d'injection de fautes et la mise en oeuvre d'autres variantes du protocole de Stern qui peuvent avoir d'autres avantages pour des variations du protocole.

Le schéma de signature de Kabatianskii Krouk et Smeets
Je pense que notre étude ([6]) montre les limites de ce schéma de signature. L'utilisation de matrices quasi-circulantes permet de réduire la taille des clés publiques tandis qu'un choix judicieux des paramètres permet d'augmenter le nombre de signatures nécessaires à la découverte de la clé secrète.

Le schéma de signature basé sur l'identité prouvé sûr
C'est certainement la partie de ma thèse qui est la plus aboutie, du point de vue de la sécurité théorique. Le schéma que l'on présente dans [4] combine deux schémas bien connus et hérite malheureusement des mauvaises propriétés de ces deux systèmes, à savoir une grande taille des données publiques et un coût de communication, pour le schéma d'authentification, élevé ainsi qu'une taille de signature également très grande. Mais malgré ces faiblesses, ce système présente la première alternative à la théorie des nombres pour la cryptographie basée sur l'identité et permet d'ouvrir de nouveaux domaines de recherche. De plus, la preuve de sécurité en fait le premier schéma d'authentification et de signature basée sur l'identité n'utilisant pas de problèmes de théorie des nombres prouvé sûr. Ce chapitre montre l'étendue des possibilités des codes correcteurs en cryptographie à clé publique.
La question de l'existence d'un schéma de chiffrement basé sur l'identité utilisant un problème de théorie des codes correcteurs d'erreurs reste ouverte.

Le schéma de signature de cercle à seuil
Dans [1], nous avons présenté un nouveau schéma de signature de cercle à seuil complètement anonyme basé sur la théorie des codes correcteurs d'erreurs. Notre protocole est une généralisation naturelle du schéma d'authentification de Stern et notre preuve est basée sur la preuve originelle de Stern. Nous avons montré que le choix du poids d'un vecteur particulier rend applicable ce schéma dans le cas des signatures de cercle et que la notion de groupe ad hoc correspond bien à la notion de somme directe de matrices génératrices.
Nous obtenons un protocole complètement anonyme basé sur une preuve de connaissance. Alors que les schémas pré-existants ne pouvaient traiter que des cas où $t \approx \mathcal{O}(\log(N))$, notre schéma permet de traiter n'importe quel t et en particulier $t \approx N/2$.
Le fait que notre construction ne soit pas basée sur des problèmes de théorie des nombres mais sur des problèmes de codes représente, une fois encore, une alternative intéressante.

McEliece avec des codes alternants quasi-cycliques
La sécurité du schéma de McEliece que nous proposons repose directement sur les mêmes problèmes que dans le système de McEliece originel. Or, ce système ayant été étudié en détails depuis près de 30 ans, peut être considéré comme suffisamment robuste. Il suffit donc de vérifier que les quelques modifications que nous avons apportées dans [2], dues au fait qu'on utilise des codes alternants quasi-cycliques, soient des sous-codes sur un sous-corps de code de Reed-Solomon Généralisé, n'affaiblissent pas le système originel. L'utilisation de codes quasi-cycliques permet d'obtenir une clé publique de 6 000 bits. Les premiers comparatifs de vitesse que nous avons fait montrent que le système possède une vitesse similaire au système NTRU. De tels paramètres et une telle rapidité ouvrent les portes de nouvelles applications pour la cryptographie basée sur les codes correcteurs d'erreurs, sur carte à puce par exemple, où un tel algorithme peut être utilisé pour l'échange de clés ou l'authentification.
Nous avons construit, à l'aide de magma, les codes alternants quasi-cycliques, il reste à implémenter leur algorithme de décodage ainsi que le protocole en lui même.

4. Conclusion

Si vous deviez choisir un type de cryptographie à conseiller aux générations futures entre la cryptographie classique, basée sur les problèmes de factorisation ou de logarithme discret, et la cryptographie basée sur les codes correcteurs d'erreurs, quel serait votre choix ?
La réponse à cette question n'est pas triviale. La cryptographie classique, dirons nous, possède de nombreux avantages : rapide, énormément étudiée, très variée (multitudes de protocoles différents bien que basés sur les mêmes problématiques), munie de preuve de sécurité. Mais aussi des inconvénients : des calculs lourds (exponentiation modulaire, calcul sur des courbes elliptiques, ...), fragile face à l'ordinateur quantique (algorithme de Shor), des paramètres difficilement modifiables ...
La cryptographie basée sur les codes correcteurs quant à elle ne souffre pas des mêmes faiblesses : opérations très rapides car basées sur de l'algèbre linéaire, ne nécessitent pas de crypto-processeur (intéressant dans des milieux à très faible ressource), des paramètres très facilement modifiables, une résistance face à l'ordinateur quantique. Mais elle souffre d'autres faiblesses : très grande taille de clés publiques, peu d'études (par rapport à la cryptographie classique), pas beaucoup de propriétés particulières (signature de groupe, à propriétés spéciales).
Dans ma thèse, j'ai montré que l'on pouvait combler certaines de ces faiblesses en proposant des schémas avec des propriétés particulières, des tailles de clés publiques raisonnables, ainsi que des implémentations effectives.
En conclusion, je me refuse à trancher et je dirai simplement que la cryptographie basée sur les codes correcteurs d'erreurs constitue une alternative aux systèmes de chiffrement à clé publique *classiques* à ne pas négliger.

La cryptographie basée sur les codes correcteurs d'erreurs a encore de beaux jours devant elle !

Bibliographie

1. C. Aguilar Melchor, P.-L. Cayrel and P. Gaborit : A new efficient threshold ring signature scheme based on coding theory. PQ CRYPTO 2008, *Lecture Notes in Computer Science*.
2. T. Berger, P.-L. Cayrel, P. Gaborit and A. Otmani : Reducing Key Lengths with Quasi-cyclic Alternant Codes for Code-Based Cryptography AFRICACRYPT 2009, *Lecture Notes in Computer Science*.
3. P.-L. Cayrel and L. Dallot : Schémas de signature prouvés sûrs fondés sur la théorie des codes correcteurs d'erreurs. *MAJECSTIC 2008.*
4. P.-L. Cayrel, P. Gaborit and M. Girault : Identity-based identification and signature schemes using correcting codes. In D. Augot, N. Sendrier and J.-P. Tillich, editors, *WCC 2007*. INRIA, 2007.
5. P.-L. Cayrel, P. Gaborit and E. Prouff : Secure Implementation of the Stern Authentication and Signature Schemes for Low-Resource Devices Eighth Smart Card Research and Advanced Application Conference *CARDIS 2008* In G. Grimaud and F.-X. Standaert, editors, Lecture Notes in Computer Science, Vol. 5189, pages 191-205, 2008.
6. P.-L. Cayrel, A. Otmani and D. Vergnaud : On Kabatianskii-Krouk-Smeets signatures. *WAIFI 2007*, Springer Carlet C. and Sunar B. Lecture Notes in Computer Science :237–251, 2007.
7. N. T. Courtois, M. Finiasz and N. Sendrier : How to achieve a McEliece-based digital signature scheme. *Lecture Notes in Computer Science*, 2248 :157–174, 2001.
8. L. Dallot : Towards a concrete security proof of Courtois Finiasz and Sendrier signature scheme. *Weworc 2007*.
9. P. Gaborit and M. Girault : Lightweight code-based identification and signature. In *Proceeedings of ISIT'07*, 2007.
10. Y. Li, R. Deng and X. Wang : On the equivalence of McEliece's and Niederreiter's cryptosystems. *IEEE Trans. on Information Theory IT-40*, 40 no. 1 :271–273, 1994.
11. F. J. McWilliams and N. J. A. Sloane : The Theory of Error-Correcting Codes. *North–Holland, Amsterdam, fifth edition*, 1986.
12. J. Stern : A new identification scheme based on syndrome decoding. In D. Stinson, editor. *Advances in Cryptology – CRYPTO '93*, volume 773,pages 13–21, 1993.