In *Direction des Centres d'Expertise et d'Essais*, number 64 in Revue Scientifique et Technique de la Defense, pages 59–66. Délégation générale pour l'armement, June 2004.

Courbes elliptiques et cryptographie

par R. Lercier [1]

Cet article dresse un panorama sur l'utilisation de courbes elliptiques en cryptographie. L'approche suivie est chronologique. On commence par rappeler les articles scientifiques fondateurs. On poursuit par un état de l'art sur les méthodes algorithmiques pour calculer le nombre de points sur courbes elliptiques. On termine par quelques applications.

This paper is an overview on the use of elliptic curves in cryptography. Our approach is chronological. We give at first the foundations of this theory. We continue with a state of the art about the algorithmic methods that were developed to count points on elliptic curves. We terminate with some applications.

De nombreux schémas cryptographiques asymétriques peuvent être mis en œuvre dans un groupe fini G dès lors que le problème du logarithme discret y est considéré comme difficile. Rappelons pour un public non-averti que le problème du logarithme discret consiste, étant donné un élément R du sous-groupe de G engendré par un élément P, à trouver l'entier k tel que $R = kP$. L'ensemble des points $E(\mathbb{F}_q)$ d'une courbe elliptique $E : y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur un corps à $q = p^n$ éléments $\mathbb{F}_q$ forme un groupe fini. La loi de groupe est directement dérivée de constructions à la règle qu'il est facile d'illustrer dans le cas réel (cf. Fig. 1).

Mettre en place une cryptographie reposant sur ces courbes est alléchant. En effet, contrairement aux groupes multiplicatifs de $\mathbb{F}_q$, seuls des algorithmes de complexité asymptotique exponentielle en $\log q$ sont connus pour calculer des logarithmes discrets dans $E(\mathbb{F}_q)$. Le plus gros calcul de ce type est un calcul de logarithme discret pour une courbe définie modulo un nombre premier de 109 bits [36]. À niveau de sécurité égal, il semble donc possible d'utiliser des clefs de chiffrement de taille inférieure (env. 160 bits) à celles qui sont nécessaires pour $\mathbb{F}_q$ (env. 1024 bits).

Ces caractéristiques sont à l'origine d'un engouement récent mais de grande ampleur pour l'utilisation de tels cryptosystèmes en grandeur nature, notamment dans l'élaboration de cartes à puces. Afin de mieux cerner le domaine, nous proposons au lecteur un panorama représentatif que nous avons organisé comme suit : une fois rappelés les premiers articles faisant état de l'utilisation de courbes elliptiques en cryptographie, nous décrivons dans le paragraphe suivant de quelles façons un cryptographe peut construire les courbes dont il a besoin avant de donner ensuite quelques applications.

Les fondations

Il est admis, qu'indépendamment l'un de l'autre, Miller et Koblitz aient introduit la cryptographie fondée sur les courbes algébriques.

En 1985, Miller [33] part du protocole proposé par Diffie et Hellman [11] pour réaliser un échange de clef en utilisant le groupe multiplicatif défini par un nombre premier p. La sécurité du protocole repose en partie sur l'impossibilité (non-prouvée) de calculer des logarithmes discrets. Les algorithmes alors connus pour cela nécessitaient de l'ordre de $\exp(\sqrt{\log p \log\log p})$ opérations [1]. Miller remarque

[1] Laboratoire "Études Cryptographiques", IRIS/CRY, CELAR, Boite Postale 7419, 35174 Bruz Cedex - *Reynald.Lercier@m4x.org*

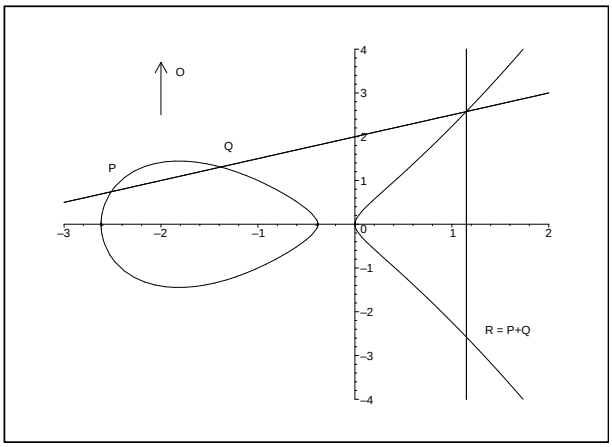

FIG. 1 – Addition de points P et Q sur la courbe elliptique $E/\mathbb{R} : y^2 = x^3 + 3x^2 + x$.

qu'un tel protocole peut se généraliser à d'autres groupes finis, notamment au groupe des points définis par une courbe elliptique.

Koblitz [19], de son côté, propose à la même époque les analogues des cryptosystèmes à clef publique de Massey-Omura et d'El Gamal pour les courbes elliptiques. Pour la mise en place de ces schémas, il est essentiel de pouvoir trouver un sous-groupe cyclique d'une courbe E dont l'ordre est divisible par un grand nombre premier. Il émet des suggestions variées sur le choix de E et du sous-groupe afin d'obtenir des schémas cryptographiques plus sûrs que ceux obtenus à partir de $\mathbb{F}_q^*$.

Quelles courbes ?

Pour pouvoir, comme souligné par Koblitz, s'assurer que les courbes elliptiques que l'on utilise en cryptographie ont un ordre divisible par un grand nombre premier il est indispensable de déterminer leur cardinalité. Dans ce domaine, la recherche scientifique a réalisé depuis 1985 d'énormes progrès, d'abord suite aux nombreuses améliorations d'Atkin, Elkies,... qui ont suivies la publication de l'algorithme de Schoof, et plus récemment suite à des idées dues à Satoh et Mestre.

Courbes obtenues à l'aide du théorème de Weil

Pour une courbe définie sur $\mathbb{F}_q$, il est facile d'obtenir sa cardinalité sur $\mathbb{F}_{q^k}$ (k, un entier positif) à partir de celle sur $\mathbb{F}_q$ avec le théorème de Weil [44].

Théorème 1. *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ de cardinalité $q+1-c$. Alors la cardinalité de $E(\mathbb{F}_{q^k})$ avec k strictement positif est égale à $q^k + 1 - \alpha^k - \beta^k$ où α et β sont les racines complexes du polynôme $X^2 - cX + q$.*

Ainsi, une fois par exemple fixée une courbe E sur $\mathbb{F}_{2^{16}}$ dont il est aisé de déterminer la cardinalité du groupe des points $E(\mathbb{F}_{2^{16}})$ par une recherche exhaustive, il est immédiat de déterminer la cardinalité des groupes $E(\mathbb{F}_{2^{16k}})$.

Courbes supersingulières

L'inconvénient de la construction précédente est que d'une part, elle restreint le cryptographe à un petit nombre de courbes et que d'autre part, elle n'est d'aucun secours pour des corps finis de grande caractéristique. C'est pourquoi, les chercheurs se sont tout d'abord portés vers une autre famille de courbes, les courbes supersingulières. Ces courbes ont pour particularité que leur cardinalité est égale à $p^n + 1 - c$ avec $c \bmod p = 0$.

Ainsi, Bender et Castagnoli [5] proposent en 1989 une sous-famille des courbes supersingulières. Comme le calcul de la cardinalité de ces courbes est immédiat, cela permet de répondre facilement aux contraintes cryptographiques, notamment l'utilisation d'une courbe dont l'ordre est le multiple d'un grand nombre premier. Un autre avantage de ces courbes est une légère simplification des opérations de groupe.

Malheureusement, l'usage en cryptographie de telles courbes s'est avéré problématique suites aux travaux menés en 1993 par Menezes, Okamoto et

Vanstone [29]. Leur résultat principal montre qu'en toute généralité il est possible de ramener via une réduction appelée "accouplement de Weil" le calcul du logarithme discret dans $E(\mathbb{F}_q)$ à celui du calcul d'un logarithme discret dans $\mathbb{F}_{q^k}$ où $k \in \mathbb{N}^*$. Pour le cas des courbes elliptiques supersingulières, k est égal à 1, 2, 3, 4 ou 6 et la réduction se fait donc en temps probabiliste polynomial en $\log q$, ce qui conduit pour ces courbes à un algorithme probabiliste sous-exponentiel de résolution du logarithme discret.

Multiplication complexe

Pour pallier l'attaque MOV [29], on s'est intéressé à un autre type de courbes, les courbes "à multiplication complexe" par un ordre dans un corps quadratique $\mathbb{Q}(\sqrt{-D})$ avec D petit. En fait, pour toute courbe elliptique non-supersingulière $E(\mathbb{F}_q)$ de cardinalité $q+1-c$, il existe un entier D sans facteur carré et deux entiers W et V tels que

$$\begin{cases} 4q &= W^2 + DV^2, \\ c &= \pm W. \end{cases}$$

Une des retombées des travaux d'Atkin-Morain dans le domaine de la primalité [3] est une construction de telles courbes pour de "petits" D fixés par avance.

Koblitz [21] explicita en 1991 la construction des courbes à multiplication complexe en caractéristique deux. Les courbes de Koblitz ont les propriétés suivantes :

- elles sont non-supersingulières (l'attaque MOV [29] est donc caduque) ;
- l'ordre du groupe est le multiple d'un grand facteur premier ;
- le doublement de points peut être effectué plus ou moins aussi efficacement que dans le cas des courbes supersingulières ;
- les courbes sont faciles à trouver.

À la même époque, le cas des corps premiers $\mathbb{F}_p$ fut explicité par Morain [37].

Les publications suivantes cherchent à améliorer la mise en œuvre de ces courbes. Miyaji [34], par exemple, cherche à réduire au maximum la taille des données ainsi que les calculs à réaliser sur des cartes à puces pour mettre en œuvre des schémas de signature ou d'authentification à base de courbes elliptiques. Il propose une famille de courbes à multiplication complexe sur $\mathbb{F}_p$ qui respecte ces contraintes tout en conservant un niveau de sécurité suffisamment élevé. Dans le même ordre d'idée, Miyaji souligne dans [35] que l'attaque MOV se complique pour des courbes dont le nombre de points est divisible par la caractéristique p du corps de définition. En fait, des travaux ultérieurs [8] détermineront explicitement le degré de l'extension auquel conduit l'attaque MOV.

Courbes générales

Si les méthodes précédentes sont efficaces en pratique, il faut tout de même admettre qu'elles restreignent l'ensemble des courbes utilisables. C'est pourquoi les méthodes de calculs *a posteriori* de la cardinalité d'une courbe elliptique fixée *a priori* ont attiré l'attention de la communauté. Cet intérêt était initialement tempéré par la complexité des calculs correspondants mais, après les nombreuses améliorations apportées depuis 15 ans, ces méthodes sont plus que jamais d'actualité.

L'avancée majeure date de 1985. Elle est due à Schoof [41] qui, le premier, exhiba un algorithme dont la complexité est polynomiale en $\log q$ pour calculer la cardinalité de $E(\mathbb{F}_q)$, précisément, $O(\log^{5+\varepsilon} q)$. Koblitz [20] décrit dans le détail pour le cas particulier des corps $\mathbb{F}_{2^n}$ l'algorithme de Schoof pour calculer la cardinalité d'une courbe quelconque. Il estimait alors qu'une implantation capable d'effectuer 66000 multiplications dans $\mathbb{F}_{2^{135}}$ en 1 seconde (sur une puce par exemple) serait en mesure de trouver une courbe elliptique dont l'ordre serait deux fois un nombre premier en environ 5 jours.

Suivent alors des avancées dues à Elkies, Atkin, Couveignes,... qui permettent de faire tomber la complexité à $O(\log^{4+\varepsilon} q)$ [42]. L'algorithme correspondant est appelé l'algorithme SEA. En 1995, on rend compte dans [27] des retombées. Il apparaît notamment que le calcul de la cardinalité d'une courbe définie sur $\mathbb{F}_{2^{155}}$ est réalisable en une dizaine de minutes sur une station de travail classique.

Deux ans plus tard, ce temps tombe à moins d'une minute [25]. De plus, il devient possible d'accélérer la recherche d'une courbe à nombre de points "quasi-premier" en tirant avantage de la structure de l'algorithme de Schoof. Ainsi, on trouve sur $\mathbb{F}_{2^{155}}$ une courbe dont le nombre de points est deux fois un nombre premier en moins d'une heure.

Corps finis de petite caractéristique $\mathbb{F}_{p^n}$

Au contraire des algorithmes précédents que l'on peut voir comme étant de type "ℓ-adique", une autre voie privilégie pour les corps finis de petite ca-

ractéristique des techniques se ramenant à des calculs dans l'ensemble $\mathbb{Z}_p$ des p-adiques. L'idée commune derrière ces algorithmes est de construire un relevé en caractéristique zéro du Frobenius. Le premier algorithme qui fonctionne plus rapidement que l'algorithme SEA est dû à Satoh [39]. L'idée est de calculer un relevé de E tel que son anneau des endomorphismes est identique à celui de E. Un tel relevé s'appelle le relevé canonique de E. À p fixé (qui doit être petit dans la pratique), le temps de calcul de cet algorithme quand n tend vers l'infini est $O(n^3)$ et la consommation mémoire, $O(n^3)$. Peu de temps après, Vercauteren, Preneel, Vandewalle [47] réduisent l'espace nécessaire à $O(n^2)$. Indépendamment, pour la caractéristique deux, un algorithme de même complexité asymptotique a été découvert par Mestre [31]. Il est basé sur la moyenne arithmético-géométrique (AGM). L'algorithme correspondant (que nous donnons ci-dessous) est remarquablement simple.

Algorithme `AGM`
Cardinalité d'une courbe elliptique $E(\mathbb{F}_{2^n}) : y^2 + xy = x^3 + \alpha$.
Entrée : $\alpha \in \mathbb{F}_{2^n}$.
Sortie : L'entier c tel que $2^n + 1 - c$ soit la cardinalité de E.

1. $a := 1 + 8\alpha \in \mathbb{Z}_{2^n}; b := 1 \in \mathbb{Z}_{2^n}$;
2. for $(i := 1; i < n/2 + 5; i := i + 1)$ {
3. $\quad a, b := \frac{a+b}{2}, \sqrt{ab}$;
4. }
5. A := a ; B := b ;
6. for $(i := 1; i < n; i := i + 1)$ {
7. $\quad a, b := \frac{a+b}{2}, \sqrt{ab}$;
8. }
9. return $A/a \bmod 2^n \in [-2\sqrt{2^n}, 2\sqrt{2^n}]$.

En 2001, Satoh, Skjernaa et Taguchi [40] améliorent sensiblement la complexité de l'algorithme de Satoh pour atteindre une complexité en temps de $O(n^{2.5})$ et une complexité en espace de $O(n^2)$ après un précalcul en $O(n^3)$.

Récemment, on a finalement pu montrer que l'on peut réduire la complexité du calcul du nombre de points à $O(n^2)$ [26, 12]. Pour comparer avec les méthodes ℓ-adiques, le temps de calcul de la cardinalité d'une courbe sur $\mathbb{F}_{2^{155}}$ est maintenant inférieur à la seconde. À titre indicatif, on donne des temps de calcul sur station DEC Alpha pour des corps finis de grandes tailles (cf. Tab. 1).

Remarquons cependant que les courbes définies sur $\mathbb{F}_{p^n}$ peuvent être sensibles à l'attaque dite de "descente de Weil" qui permet de ramener le logarithme discret sur courbes elliptiques définies sur une extension $\mathbb{F}_{p^n}$ d'un petit corps fini $\mathbb{F}_{p^m}$ à celui du logarithme discret pour une courbe de plus grand genre, mais définie seulement sur $\mathbb{F}_{p^m}$. Elle fut principalement proposée par Frey en 1998, approfondie par Galbraith et Smart en 1999, puis rendue efficace par Gaudry, Hess et Smart en 2000. Cette dernière est néanmoins inopérante lorsque n est un nombre premier.

Quelle cryptographie ?

Bien sûr, tout système cryptographique reposant sur le problème du logarithme discret s'étend au cas des courbes elliptiques. Nous nous concentrons ici aux résultats spécifiques pour trois types de cryptosystèmes : les générateurs pseudo-aléatoires, les analogues de Diffie-Hellman et les analogues de RSA. Mais plus originalement, la difficulté à inverser des accouplements bilinéaires définis à partir de courbes elliptiques à conduit à de nouvelles applications cryptographiques. Elles font brièvement l'objet d'un dernier paragraphe.

Générateurs pseudo-aléatoires prouvés

Kaliski présente dans [17] un générateur pseudo-aléatoire qui produit des bits qui sont aussi difficiles à deviner que de résoudre le problème de logarithme discret sur une courbe elliptique. Notons que les courbes qu'il préconise sont des courbes supersingulières.

Quelques permutations définies à l'aide de courbes elliptiques sont aussi présentées dans [18]. Kaliski espère que la majeure partie de ces permutations sont des fonctions à sens unique. Les courbes elliptiques $y^2 \equiv x^3 + b \bmod p$, avec $p \equiv 2 \bmod 3$, $y^2 \equiv x^3 + ax \bmod p$, avec $p \equiv 3 \bmod 4$ et $(a/p) = 1$ ou les paires composées d'une courbe elliptique et de sa tordue, $y^2 \equiv x^3 + ax + b \bmod p$, $y^2 \equiv x^3 + au^2x + bu^3 \bmod p$, avec $(u/p) = -1$ sont utilisées dans la construction.

Pour le petit nombre de courbes elliptiques E définies sur $\mathbb{F}_2$, mais regardées comme des courbes définies sur une extension $\mathbb{F}_{2^n}$, Meyer et Staffelbach développent un nouvel algorithme pour calculer des multiples d'un point arbitraire de E [28]. L'algorithme est présenté comme trois fois plus rapide que la méthode binaire usuelle, plus facile à implanter et ne nécessite aucun précalcul ou mémoire additionnelle. Il est utilisé pour calculer des

n	1018	2052	4098	8218	16420	32770	65538	100002
Temps	5 s	20 s	2 mn	10 mn	1 h	6 h	1 j 5 h	3 j 10 h

TAB. 1 – Temps de calcul de la cardinalité de courbes définies sur $\mathbb{F}_{2^n}$ (DEC alpha 613 MHz)

permutations à sens unique efficaces mettant en jeu des paires composées d'une courbe elliptique et sa tordue en généralisant la construction de [18] aux corps de caractéristique deux.

Les analogues de RSA

Le préalable à une cryptographie de type RSA est d'exhiber des fonctions à sens unique à trappe. C'est ce que font en 1991 les auteurs de [23]. En fait, trois nouvelles familles de fonctions, basées sur des courbes elliptiques définies sur $\mathbb{Z}/N\mathbb{Z}$ où N est composé, sont proposées. La première famille est une construction naïve uniquement utilisable dans un schéma de signature. La seconde famille peut se substituer aux fonctions à sens unique de type RSA. La troisième famille a les mêmes caractéristiques que les fonctions à sens unique de Rabin. La sûreté de ces fonctions repose sur la difficulté de factoriser N.

Demytko [10] étend les résultats précédents. Il amoindrit les restrictions relatives aux types de courbes elliptiques et de nombres premiers utilisables. D'autre part, il évite les problèmes liés au plongement de messages dans la courbe en travaillant sur une structure de groupe multiple, ce qui permet des opérations de cryptage et de décryptage uniquement basées sur l'abscisse des points de la courbe.

En 1995, Koyama [22] propose un système cryptographique à clef publique reposant, non pas sur des courbes elliptiques, mais sur les courbes singulières $y^2 + axy = x^3$ définies sur $\mathbb{Z}/N\mathbb{Z}$. Les caractéristiques de ce schéma sont similaires à celles de RSA, excepté, peut-être, une rapidité accrue. Peu après, les auteurs de [32] utilisent les mêmes idées que Williams [48] pour obtenir un système dont il est, cette fois, prouvé que toute attaque est *équivalente* à la factorisation d'entiers.

Une analyse plus fine de ses idées impose néanmoins une certaine prudence. Par exemple, Hastad [14] a montré qu'utiliser de petits exposants e dans RSA n'est pas sûr si un même message est chiffré à destination de multiples destinataires. Cela est vrai même si une estampille datée est utilisée pour chaque receveur. Si par exemple $e = 3$ et le nombre de destinataires est sept, l'attaquant peut retrouver le message en clair à partir des sept chiffrés. De même, les auteurs de [24] montrent que les cryptosystèmes à base de courbes elliptiques précédents ne sont pas sûrs si $e = 5$, si N est supérieur à 2^{1024} et le nombre de destinataires est égal à 428. Dans la version de Demytko, e peut prendre la valeur 2. Dans ce cas, le schéma n'est pas sûr si le nombre de receveurs est 11 pour $N \geq 2^{175}$.

En fait, utiliser un analogue du RSA sur courbes elliptiques plutôt que le RSA lui-même ne semble pas clairement plus avantageux. Nous renvoyons le lecteur aux travaux de Joye [16] pour un panorama complet sur la question.

Les analogues de Diffie-Hellman

La majeure partie de la cryptographie courbes elliptiques d'aujourd'hui repose sur les idées de Diffie-Hellman et utilise le fait que le problème du logarithme discret est réputé difficile sur ces groupes. En retracer l'historique dépasse largement la portée de ce texte. Disons simplement que l'une des avancées majeures de la cryptographie moderne est la recherche de preuves de sécurité pour les protocoles cryptographiques. Une idée récurrente consiste à supposer qu'un attaquant est capable de casser le cryptosystème étudié et d'en déduire un algorithme capable de résoudre le problème mathématique sous-jacent. S'il se trouve par ailleurs que ce problème est réellement difficile, alors on en déduit par la contraposée qu'un tel attaquant ne peut exister. La spécificité liée au fait que l'on utilise dans un protocole une courbe elliptique est généralement gommée en modélisant ce groupe comme un "groupe générique". Nous renvoyons le lecteur intéressé par ces sujets à l'excellente synthèse réalisée dans le cadre du projet européen NESSIE [38].

Signature. L'algorithme de signature électronique le plus connu est l'algorithme ECDSA. Sa sécurité repose sur l'impossibilité de résoudre le logarithme discret dans un sous-groupe d'une courbe elliptique. Il a été proposé en premier par Vanstone en 1992 en réponse à une requête du NIST [46]. C'est un standard ISO depuis 1998, un standard

ANSI depuis 1999 et un standard IEEE et NIST depuis 2000.

Excepté une tentative récente de preuve dans le modèle du groupe générique [7], il n'existe pas de preuve de sécurité pour cet algorithme. Seules des variantes semblent pour le moment en bénéficier.

Chiffrement asymétrique. Une façon usuelle d'utiliser un mécanisme de chiffrement asymétrique est de se servir du mécanisme pour chiffrer uniquement une clef (*i. e.* un message de petite taille) et ensuite se servir de celle-ci pour chiffrer par un algorithme de chiffrement symétrique le message proprement dit.

Une formalisation récente de ces protocoles due à Cramer et Shoup [9] s'appelle le modèle "KEM-DEM" ("Key/Data Encapsulation Mechanism"). Cette formalisation permet plus facilement d'exhiber des preuves de sécurité sur les protocoles.

Les systèmes à clefs publiques arbitraires

Dans une infrastructure asymétrique classique, les clefs publiques sont issues des clefs privées. Il n'existe en fait que depuis peu une solution réellement satisfaisante pour construire des systèmes dans lesquels tout identifiant puisse être la clef publique d'une clef privée calculable *a posteriori*.

Une première tentative reposait sur une variation de l'échange de clef Diffie-Hellman due à Mc Curley. Dans ce protocole, un attaquant doit à la fois casser le problème de Diffie-Hellman tout en factorisant de grands entiers. Il est fait état dans [45] d'une généralisation de ce schéma aux courbes elliptiques.

Très récemment, on a pris conscience que l'accouplement de Weil, initialement utilisé dans l'attaque MOV [29], peut à l'inverse être mis à profit pour la construction. Les fondements de cette nouvelle approche est un article de Joux publié en 2000 [15] où il est expliqué qu'il est possible à trois partenaires de faire un échange Diffie-Hellman en une passe à l'aide de l'accouplement de Weil. Avec cette brique de base, Boneh et Franklin [6] ont proposé un schéma de chiffrement asymétrique pour lequel n'importe quelle chaîne de caractères peut être une clef publique. Le schéma correspondant est prouvé sûr dans le modèle de l'oracle aléatoire et en supposant une variante calculatoire du problème Diffie-Hellman pour courbes elliptiques. Une messagerie construite sur ces idées aurait des propriétés fonctionnelles intéressantes. Les abonnés pourraient en particulier envoyer du courrier à des destinataires qui ne disposent pas encore de clef privée.

Depuis, cette cryptographie a littéralement explosée. La plupart des fonctionnalités habituellement rendues par la cryptographie asymétrique peuvent l'être par des schémas qui reposent sur l'accouplement de Weil ou de Tate. Un panorama de ce domaine en plein mouvement peut par exemple être trouvé à [4].

Les applications

Les premières expérimentations pratiques mettant en œuvre de la cryptographie à base de courbes elliptiques sont des résultats de laboratoire.

Ainsi, en 1989, Mullin et Vanstone [2] présentent pour la première fois une carte électronique implantant des opérations sur des courbes elliptiques [2]. Cette carte était construite autour d'un processeur Motorola M68008. En 1992, la faisabilité de cryptosystèmes construits à base de courbes elliptiques avec des clefs de l'ordre de 100 bits est étudiée dans [13]. Des taux de 2Kbits/s sont atteints sur station de travail. En 1993, Menezes et Vanstone [30] explorent la faisabilité d'implanter en hardware un processeur arithmétique pour effectuer des calculs sur des courbes elliptiques définies sur des corps finis de caractéristique deux. Enfin, en 1995, Schroeppel et al. [43] décrivent une implantation logicielle d'un échange de clef à la Diffie-Hellman à base de courbes elliptiques définies sur $\mathbb{F}_{2^{155}}$ dont les performances sont, à niveau de sécurité équivalent, légèrement meilleures que celles du Diffie-Hellman usuel.

Depuis ces expérimentations, plusieurs normes déjà approuvées ou en cours d'approbation ont vu le jour. Nous rappelons les principales ci-dessous.

ANSI, "American National Standards Institute".

- `ANSI X9.62` : "Elliptic Curve Digital Signature Algorithm " (ECDSA) est un standard de signature électronique.
- `ANSI X9.63` : "Elliptic Curve Key Agreement and Key Management" normalise l'utilisation de courbes elliptiques à des fins de chiffrement.

FIPS, "Federal Information Processing Standard" du NIST (US government's "National Institute of Standards and Technology"). Il s'agit d'une

extension du standard de signature électronique (DSS) pour inclure l'algorithme ECDSA (`ANSI X9.62`).

IEEE. La norme IEEE 1363-2000 couvre la cryptographie asymétrique à base de logarithmes discrets (corps finis ou courbes elliptiques) ainsi que celle à base de RSA. Elle spécifie les mécanismes ECDSA, ECDH et ECMQV.

PKCS, émis par la société RSA inc. Cette norme adresse de nombreux aspects : la génération des clés et des paramètres, la signature électronique, le chiffrement asymétrique, etc.

Conclusion

D'abord l'apanage des mathématiciens avant de devenir un sujet d'étude privilégié pour les cryptographes, les courbes elliptiques commencent à être connues d'un plus large public. Gageons que dans un monde dominé par la cryptographie à clef publique RSA, ces dernières deviennent à terme une alternative crédible.

Remerciements

L'auteur remercie S. Alt et D. Lubicz pour leur lecture attentive de ce texte.

Références

[1] L. Adleman. A subexponential algorithm for the discrete logarithm problem with applications to cryptography. *IEEE*, pages 55–60, 1979. Twentieth annual symposium on foundations of computer science.

[2] G.B. Agnew, R.C. Mullin, and S.A. Vanstone. A fast elliptic curve cryptosystem. In J.-J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89*, pages 706–708, Berlin, 1989. Springer-Verlag. Lecture Notes in Computer Science Volume 434.

[3] A.O.L. Atkin and F. Morain. Elliptic curves and primality proving. *Mathematics of Computations*, 61 :29–68, 1993.

[4] P. Barreto. Weil and Tate pairings. *http ://planeta.terra.com.br/informatica/paulobarreto/pblounge.html*, 2004.

[5] A. Bender and G. Castagnoli. On the implementation of elliptic curve cryptosystems. In G. Brassard, editor, *Advances in Cryptology — CRYPTO '89*, pages 186–193, Berlin, 1989. Springer-Verlag. Lecture Notes in Computer Science Volume 435.

[6] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In *Crypto '2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229, 2001.

[7] D.-R.-L. Brown. Generic groups, collision resistance, and ECDSA. Available at *http ://eprint.iacr.org/2002/026/*, 2002.

[8] J. Chao, K. Tanada, and S. Tsujii. Design of elliptic curves with controllable lower boundary of extension degree for reduction attacks. In Y. Desmedt, editor, *Advances in Cryptology — CRYPTO '94*, pages 50–55, Berlin, 1994. Springer-Verlag. Lecture Notes in Computer Science Volume 839.

[9] R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. Available at *http ://shoup.net/*, 2002.

[10] N. Demytko. A new elliptic curve based analogue of RSA. In T. Helleseth, editor, *Advances in Cryptology — EUROCRYPT '93*, pages 40–49, Berlin, 1993. Springer-Verlag. Lecture Notes in Computer Science Volume 765.

[11] W. Diffie and M.E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, 22(6) :644–654, 1976.

[12] R. Harley. Asymptotically optimal p-adic point-counting. Email sur la mailing liste NMBRTHRY, December 2002.

[13] G. Harper, A. Menezes, and S.A. Vanstone. Public-key cryptosystems with very small key lengths. In R.A. Rueppel, editor, *Advances in Cryptology — EUROCRYPT '92*, pages 163–173, Berlin, 1992. Springer-Verlag. Lecture Notes in Computer Science Volume 658.

[14] J. Hastad. On using RSA with low exponent in a public key network. In H.C. Williams, editor, *Advances in Cryptology — CRYPTO '85*, pages 403–408, Berlin, 1986. Springer-Verlag. Lecture Notes in Computer Science Volume 218.

[15] A. Joux. A one round protocol for tripartite diffie-hellman. In *Fourth Algorithmic Number Theory Symposium*, volume 1838 of *Lec-*

ture Notes in Computer Science, pages 385–394, 2000.

[16] M. Joye. *Security Analysis of RSA-type Cryptosystems*. PhD thesis, Université catholique de Louvain, October 1997.

[17] B.S. Kaliski. A pseudo-random bit generator based on elliptic logarithms. In A.M. Odlyzko, editor, *Advances in Cryptology — CRYPTO '86*, pages 84–103, Berlin, 1986. Springer-Verlag. Lecture Notes in Computer Science Volume 263.

[18] B.S. Kaliski. One-way permutations on elliptic curves. *Journal of Cryptology*, 3 :187–199, 1991.

[19] N. Koblitz. Elliptic curve cryptosystems. *Mathematics of Computation*, 48(177) :203–209, January 1987.

[20] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In A.J. Menezes and S.A. Vanstone, editors, *Advances in Cryptology — CRYPTO '90*, pages 156–168, Berlin, 1990. Springer-Verlag. Lecture Notes in Computer Science Volume 537.

[21] N. Koblitz. CM-curves with good cryptographic properties. In J. Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 279–287, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 576.

[22] K. Koyama. Fast RSA-type schemes based on singular cubic curves $y^2 + axy = x^3$ (mod n). In L.C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology — EUROCRYPT '95*, pages 329–340, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 921.

[23] K. Koyama, U.M. Maurer, T. Okamoto, and S.A. Vanstone. New public-key schemes based on elliptic curves over the ring Z_n. In J. Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 252–266, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 576.

[24] K. Kurosawa, K. Okada, and S. Tsujii. Low exponent attack against elliptic curve RSA. In *Advances in Cryptology — ASIACRYPT '94*, Lecture Notes in Computer Science, pages 376–383, Berlin, 1994. Springer-Verlag.

[25] R. Lercier. Finding good random elliptic curves for cryptosystems defined over F_{2^n}. In W. Fumy, editor, *Advances in Cryptology — EUROCRYPT '97*, pages 379–392, Berlin, 1997. Springer-Verlag. Lecture Notes in Computer Science Volume 1233.

[26] R. Lercier and D. Lubicz. Counting Points on Elliptic Curves over Finite Fields of Small Characteristic in Quasi Quadratic Time. In E. Biham, editor, *Advances in Cryptology — EUROCRYPT 2003*, volume 2656 of *Lecture Notes in Computer Science*, pages 360–373, Berlin, May 2003. Springer.

[27] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields : strategies and performances. In L.C. Guillou and J.-J. Quisquater, editors, *Advances in Cryptology — EUROCRYPT '95*, pages 79–94, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 921.

[28] W. Meier and O. Staffelbach. Efficient multiplication on certain nonsupersingular elliptic curves. In E.F. Brickell, editor, *Advances in Cryptology — CRYPTO '92*, pages 333–344, Berlin, 1992. Springer-Verlag. Lecture Notes in Computer Science Volume 740.

[29] A.J. Menezes, T. Okamoto, and S.A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. *IEEE Transactions on Information Theory*, 39(5) :1639–1646, 1993.

[30] A.J. Menezes and S.A. Vanstone. Elliptic curve cryptosystems and their implementation. *Journal of Cryptology*, 6 :209–224, 1993.

[31] J.-F. Mestre. AGM pour le genre 1 et 2, 2001. Lettre à Gaudry et Harley. Available at *http ://www.math.jussieu.fr/˜mestre*.

[32] B. Meyer and V. Mueller. A public key cryptosystem based on elliptic curves over Z/nZ equivalent to factoring. In U. Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 49–59, Berlin, 1996. Springer-Verlag. Lecture Notes in Computer Science Volume 1070.

[33] V.S. Miller. Use of elliptic curves in cryptography. In H.C. Williams, editor, *Advances in Cryptology — CRYPTO '85*, pages 417–428, Berlin, 1986. Springer-Verlag. Lecture Notes in Computer Science Volume 218.

[34] A. Miyaji. Elliptic curves over $\mathbf{F}_p$ suitable for cryptosystems. In *Advances in Cryptology — AUSCRYPT '92*, Lecture Notes in Computer

Science, pages 479–491, Berlin, 1992. Springer-Verlag.

[35] A. Miyaji. On ordinary elliptic curve cryptosystems. In *Advances in Cryptology — AUSCRYPT '92*, Lecture Notes in Computer Science, pages 460–469, Berlin, 1992. Springer-Verlag.

[36] C. Monico. The ECCp-109 challenge. Available at *http ://www.nd.edu/˜cmonico/eccp109/*.

[37] F. Morain. Building cyclic elliptic curves modulo large primes. In D.W. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, pages 328–336, Berlin, 1991. Springer-Verlag. Lecture Notes in Computer Science Volume 547.

[38] B. Preneel, A. Biryukov, E. Oswald, B. van Rompay, L. Granboulan, E. Dottax, S. Murphy, A. Dent, J. White, M. Dichtl, S. Pyka, Schafheutle, P. Serf, E. Biham, E. Barkan, O. Dunkelman, M. Ciet, F. Sica, L. Knudsen, and H. Raddum. Nessie security report. Technical report, NESSIE, October 2002. NES/DOC/ENS/WP5/D20/1.

[39] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4) :247–270, 2000.

[40] T. Satoh, B. Skjernaa, and Y. Taguchi. Fast computation of canonical lifts of elliptic curves and its application to point counting. *Finite Fields and Their Applications*, 9(1) :89–101, 2003.

[41] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44 :483–494, 1985.

[42] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Theorie des nombres de Bordeaux*, 7 :219–254, 1995. Available at *http ://www.emath.fr/Maths/Jtnb/jtnb1995-1.html*.

[43] R. Schroeppel, H. Orman, S. O'Malley, and O. Spatscheck. Fast key exchange with elliptic curve systems. In D. Coppersmith, editor, *Advances in Cryptology — CRYPTO '95*, pages 43–56, Berlin, 1995. Springer-Verlag. Lecture Notes in Computer Science Volume 963.

[44] J.H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986. Corrected reprint of the 1986 original.

[45] C. Smith, A. et Boyd. An elliptic curve analogue of McCurley's key agreement scheme. In *Cryptography and Coding (Cirencester, 1995)*, pages 150–157, 1995.

[46] S.A. Vanstone. Responses to NIST's proposal. *Communications of the ACM*, 35 :50–52, 1992.

[47] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of Satoh's algorithm. In *Advances in Cryptology — EUROCRYPT 2001 (Innsbruck)*, volume 2045 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2001.

[48] H.C. Williams. A modification of the RSA Public Key cryptosystem. *IEEE Trans. Inform. Theory*, 6 :726–729, 1980.