

CESAM : Les Courbes Elliptiques  
pour la Sécurité des Appareils Mobiles

LIENS-ENS TANC-INRIA

ACI Sécurité 2003

Rapport Final

Octobre 2006



# Résumé

Les appareils et supports mobiles ont des capacités réduites, et pourtant, les opérations qu'ils effectuent ou les données qu'ils transportent sont souvent très sensibles. On pense bien sûr aux multiples cartes à puce qui gèrent nos transactions financières, ou stockent des données médicales, identifient et protègent nos communications téléphoniques, les assistants personnels numériques (ou PDA) et clés USB, mais on parle aussi de plus en plus de *sensor networks*, où des capteurs transmettent des données diverses à un serveur. La sécurité est rarement l'objectif premier de ces appareils, mais elle est cependant cruciale. Malheureusement, avec la technologie répandue actuellement, une bonne sécurité est coûteuse en ressources (stockage, calculs, alimentation, etc.). En effet, les principaux systèmes cryptographiques existants reposent sur RSA, ou tout du moins le calcul sur de très grands nombres. La cryptographie sur les courbes elliptiques a été vue comme une solution à ces problèmes de ressources, mais leur mise en œuvre pratique semble poser problème. Nous proposons donc de combiner les compétences d'une équipe spécialisée en protocoles cryptographiques et une autre spécialisée en la cryptographie avec les courbes elliptiques pour faire avancer une "cryptographie efficace" sur courbes elliptiques. Les courbes elliptiques nous permettent d'ailleurs d'espérer une "efficacité" à facettes multiples : temps de calcul, temps de communication et/ou stockage (en raison de données à transmettre et/ou stocker de petite taille), tout cela conduisant à une consommation d'énergie minimale.

<http://www.di.ens.fr/users/pointche/Projets/CESAM/>

## Table des matières

<b>1</b>	<b>Préliminaires</b>	<b>1</b>
1.1	Participants . . . . .	1
1.2	Rappel des objectifs fixés . . . . .	2
1.2.1	La cryptographie pour les environnements contraints . . . . .	2
1.2.2	Les courbes elliptiques . . . . .	2
<b>2</b>	<b>Résultats</b>	<b>5</b>
2.1	Échange de clés avec authentification à base de mots de passe . . . . .	6
2.1.1	Cas à deux participants . . . . .	6
2.1.2	Proposition de normes . . . . .	7
2.1.3	Serveur d'authentification . . . . .	7
2.2	Échange de clés – Authentification asymétrique . . . . .	9
2.2.1	Étude des normes . . . . .	9
2.2.2	Échange de clés entre appareils de faible puissance . . . . .	9
2.3	Extraction d'entropie . . . . .	10
2.4	Génération de courbes . . . . .	12
2.4.1	Étude du logarithme discret . . . . .	12
2.4.2	Fabrication de courbes sûres . . . . .	12
2.5	Couplages . . . . .	14
2.5.1	Chiffrement basé sur l'identité . . . . .	14
2.5.2	Diffusion chiffrée, et traçage de pirates . . . . .	14
2.5.3	Signatures de groupe . . . . .	14



# Chapitre 1

## Préliminaires

### 1.1 Participants

Ce projet était coordonné par David Pointcheval (CR1 – CNRS – LIENS), et a été effectué par les deux équipes

- Équipe Cryptographie – LIENS – Laboratoire d’informatique de l’École normale supérieure
  - Michel Abdalla, CR1 - CNRS – LIENS  
(post-doctorant d’août 2003 à septembre 2005)
  - Dario Catalano, CR2 - CNRS – LIENS
  - Pierre-Alain Fouque, MdC – ENS – LIENS
  - Sébastien Kunz-Jacques, thésard – LIENS  
(en thèse depuis octobre 2003, Ingénieur Corps Télécom – DCSSI)
  - Duong Hieu Phan, thésard – LIENS  
(en thèse depuis octobre 2002, soutenue en septembre 2005 – allocation de recherche du MENRT)
- Cryptologie – Projet TANC – Théorie algorithmique des nombres pour la cryptologie, INRIA Futurs
  - Régis Dupont, thésard – LIX  
(en thèse depuis septembre 2003, financement INRIA)
  - Andreas Enge, CR2 – INRIA
  - Pierrick Gaudry, CR2 – CNRS – LIX
  - Nicolas Gürel, ATER Marne-la-Vallée – LIX
  - Thomas Houtmann, thésard – LIX  
(en thèse depuis octobre 2004, financement DGA)

en collaboration avec Olivier Chevassut, du département des systèmes distribués, au Lawrence Berkeley National Laboratory (Département d’Énergie de Berkeley, aux États-Unis).

## 1.2 Rappel des objectifs fixés

Notre sujet concernait la cryptographie pour les environnements contraints, avec comme support l'utilisation des courbes elliptiques. Cependant, ces courbes elliptiques peuvent être soit utilisées comme un groupe classique (avec des objets de petite taille, qui ainsi apportent une efficacité supplémentaire) ou comme un groupe spécifique avec une structure particulière qui peut être exploitée par les protocoles cryptographiques.

La cryptographie pour les environnements contraints peut donc être étudiée dans deux directions indépendantes : proposer des protocoles cryptographiques adaptés aux environnements contraints (avec ou sans courbe elliptique), puis voir les apports spécifiques des courbes elliptiques à la cryptographie.

### 1.2.1 La cryptographie pour les environnements contraints

Deux thématiques ont été privilégiées : la cryptographie basée sur l'identité et la cryptographie à base de mots de passe. La première ayant connu un nouvel essor très récemment, à cause de nouvelles propriétés de certaines courbes elliptiques, mais certains protocoles peuvent s'en passer.

#### La cryptographie basée sur l'identité

La cryptographie à clé publique traditionnelle nécessite la mise en place d'une infrastructure (PKI) pour garantir l'authenticité des clés publiques. Déjà dans les systèmes qui abondent de ressources, la mise en œuvre d'une infrastructure de certification de clés est assez lourde. Dans les environnements à fortes contraintes auxquels nous nous intéressons, elle peut s'avérer impossible à mettre en place. Les cryptosystèmes fondés sur l'identité, dans lesquels le lien entre les identités des interlocuteurs et leurs clés publiques est immédiat, se révèlent donc d'un intérêt particulier dans les appareils à faibles ressources.

#### La cryptographie à base de mots de passe

La mise en accord de clé avec authentification mutuelle (*authenticated key exchange*) est certainement la primitive la plus importante. Dans bien des cas, au final, cette authentification des correspondants repose sur le fait que les interlocuteurs partagent un secret de petite taille (quelques dizaines de bits – mot de passe [IEEE]). Ce cas de figure semble le plus adapté aux environnements à fortes contraintes (notamment pour le *e-commerce* et le *m-commerce*), et cependant, il n'est pas encore très développé.

### 1.2.2 Les courbes elliptiques

#### Le logarithme discret elliptique

Les courbes elliptiques sont des courbes très particulières au sens où les points de la courbe forment un groupe : il est possible de définir une loi d'addition qui à deux points de la courbe associe leur somme. Lorsque l'on choisit comme corps de base un corps fini, le groupe obtenu est un groupe fini, et l'on peut envisager de l'utiliser en cryptographie. Cette possibilité a été proposée il y a près de vingt ans [M-86, K-87], et malgré les tentatives de bon nombre de chercheurs renommés, aucun algorithme n'a été trouvé qui résolve

efficacement le problème du logarithme discret elliptique, si ce n'est dans des cas bien particuliers faciles à détecter. Grâce à la difficulté de ce problème, les courbes elliptiques offrent la possibilité de concevoir des cryptosystèmes asymétriques d'une compacité et d'une efficacité inégalées. Pour donner une idée, utiliser un groupe elliptique de taille environ  $2^{160}$  confère une sécurité équivalente à celle dans un groupe classique de taille  $2^{1024}$ . Cela signifie que les calculs à faire lors des opérations cryptographiques se font sur des entiers bien plus petits, et que les tailles des paramètres cryptographiques (clés, signatures, etc.) sont réduites d'autant.

## **Protocoles elliptiques existants : analyse des normes**

Les organismes de normalisation s'intéressent aux schémas cryptographiques sur les courbes elliptiques [Ca-00, Cb-00]. Pour garantir la sécurité, une preuve de sécurité est désormais nécessaire [P-02]. Cependant, si certains schémas admettent une preuve lorsqu'ils sont décrits génériquement (groupe cyclique, point sur la courbe, etc.), il n'en est pas toujours de même en fonction du codage et de la courbe utilisés. Des exemples récents ont montré des différences entre les résultats prouvés dans un cadre général et la sécurité effective du schéma concret [SPMS-02, S-01]. Néanmoins, l'efficacité de ces schémas semble satisfaisante.

## **Optimisations des protocoles**

Un de nos objectifs majeurs est l'exploitation des spécificités des courbes elliptiques pour améliorer considérablement certains protocoles cryptographiques. Notamment, dans un groupe classique, le nombre de bits pour représenter un élément est bien plus grand que ce que l'on peut espérer pour une sécurité donnée (en raison notamment des algorithmes sous-exponentiels). Afin (entre autre) d'éviter de gaspiller la bande passante, on utilise une fonction de hachage afin de concentrer l'entropie dans moins de bits. Dans le cas des courbes elliptiques, la représentation des éléments est particulièrement compacte, voire quasi-optimale puisqu'un élément d'une courbe avec  $2^{160}$  points peut être représenté avec 161 bits (contre plus de 1000 bits lors de l'utilisation de corps finis). Nous espérons donc pouvoir éviter certaines fonctions de hachage dans les protocoles, sans compromettre la preuve de sécurité, ni sacrifier la bande passante. En pratique, cela peut entraîner un gain en terme de temps de calcul, et du point de vue théorique cela permettrait peut-être de se passer de la désormais classique hypothèse de l'oracle aléatoire [BR-94], ou du moins d'en dépendre un peu moins.

## **Génération de paramètres**

En plus de l'adaptation des protocoles, une difficulté lors de l'utilisation de courbes elliptiques à la place des groupes multiplicatifs des corps finis est qu'il faut trouver des courbes dont le cardinal est premier afin de ne pas compromettre la sécurité. Deux approches sont connues : soit l'on fabrique simultanément la courbe et son nombre de points en utilisant la théorie de la multiplication complexe, soit l'on prend des courbes au hasard dont on calcule le nombre de points jusqu'à en trouver une qui convient.

Par ailleurs de nouveaux besoins sont apparus avec les nouveaux protocoles. Les premiers cryptosystèmes se fondant sur l'identité utilisaient des courbes elliptiques supersingulières, dans lesquelles les couplages sous-jacents sont effectivement calculables. En revanche, ces courbes possèdent des structures algébriques très particulières, qui font

douter de leur sécurité. Des courbes aux paramètres raisonnablement élevés sont de plus obtenues seulement en caractéristique 3, qui se prête très peu à des implantations efficaces.

## Bibliographie

- [BR-94] M. Bellare and P. Rogaway. Optimal Asymmetric Encryption – How to Encrypt with RSA. In *Eurocrypt '94*, LNCS 950, pages 92–111. Springer-Verlag, Berlin, 1995.
- [Ca-00] Certicom Corp. SEC 1: Elliptic curve cryptography. Technical report, Standards for Efficient Cryptography Group, September 2000. Available at [http://www.secg.org/collateral/sec1\\_final.pdf](http://www.secg.org/collateral/sec1_final.pdf).
- [Cb-00] Certicom Corp. SEC 2: Recommended elliptic curve domain parameters. Technical report, Standards for Efficient Cryptography Group, September 2000. Available at [http://www.secg.org/collateral/sec2\\_final.pdf](http://www.secg.org/collateral/sec2_final.pdf).
- [IEEE] IEEE Standard 1363.2 Study Group. Password-Based Public-Key Cryptography. Available from <http://grouper.ieee.org/groups/1363/passwdPK>.
- [K-87] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.
- [MV-93] A. J. Menezes and S. A. Vanstone. Elliptic Curve Cryptosystems and their Implementation. *Journal of Cryptology*, 6:209–224, 1993.
- [M-86] V. Miller. Use of elliptic curves in cryptography. In H. Williams, editor, *Advances in Cryptology — CRYPTO '85*, LNCS 218, pages 417–426, Berlin, 1986. Springer-Verlag.
- [P-02] D. Pointcheval. *Le chiffrement asymétrique et la sécurité prouvée*. PhD thesis, université de Paris VII, mai 2002. Thèse d'habilitation.
- [S-01] V. Shoup. A Proposal for an ISO Standard for Public-Key Encryption, Décembre 2001. ISO/IEC JTC 1/SC27.
- [SPMS-02] J. Stern, D. Pointcheval, J. Malone-Lee, and N. Smart. Flaws in Applying Proof Methodologies to Signature Schemes. In *Crypto '02*, LNCS 2442, pages 93–110. Springer-Verlag, Berlin, 2002.

# Chapitre 2

## Résultats

Comme espéré, plusieurs directions ont finalement été très fructueuses. Notamment, la collaboration de nos deux équipes a permis de concrétiser l'intuition évoquée dans le projet initial quant à l'utilisation de la spécificité des courbes elliptiques dans certains protocoles cryptographiques : pour résoudre le problème de l'extraction d'entropie, pour améliorer l'efficacité de la diffusion de contenus chiffrés avec traçage de pirates, et plus récemment pour les signatures de groupe. Nous avons également de nombreux résultats au sujet de la cryptographie à base de mots de passe. Au sujet de la génération de courbes elliptiques, de nouvelles classes de courbes sont à proscrire en raison de leur faiblesse.

Enfin, nous nous sommes intéressés aux normes, avec notamment MQV, le principal protocole de mise en accord de clé sur courbes elliptiques de la norme SEC, puis nous participons à l'introduction de mise en accord de clé à base de mots de passe dans OpenSSL, avec la rédaction d'une RFC.

Comme vont l'illustrer les références bibliographiques de chacune des sections suivantes, tous les travaux menés dans le cadre de cette ACI ont conduit à plus de **20 articles** publiés ou acceptés pour publications au cours de ces 3 années.

## 2.1 Échange de clés avec authentification à base de mots de passe

### 2.1.1 Cas à deux participants

Le principal protocole à base de mots de passe est EKE (pour *Encrypted Key Exchange*) qui est un simple Diffie-Hellman dont les messages sont chiffrés à l'aide du mot de passe : Alice envoie le chiffrement de  $g^x$ , tandis que Bob envoie le chiffrement de  $g^y$ , et la clé de session est dérivée de  $g^{xy}$ . Ce chiffrement avec le mot de passe garantit l'authentification des participants. En effet, intuitivement, seul un message correctement chiffré (avec le bon mot de passe) sera reconstitué par l'interlocuteur qui connaît ce même mot de passe. Dans le cas contraire, ce dernier obtient un message aléatoire, qui conduit donc à une clé aléatoire.

Cependant, si le chiffrement n'est pas bien effectué, ce protocole est faible face à une attaque par dictionnaire : si on chiffre la chaîne de bits  $X$  qui code  $g^x$  avec un schéma de chiffrement classique, lorsque l'attaquant intercepte le chiffré  $X'$ , il lui suffit de tenter le déchiffrement avec tous les mots de passe possibles, très peu conduiront à un élément  $g^x$  (d'ordre  $q$  dans  $\mathbb{Z}_p^*$ , avec  $p$  sur 1024 bits et  $q$  sur 160 bits). Avec probabilité écrasante, un seul mot de passe conviendra : le protocole est cassé.

Il faut donc utiliser un chiffrement dont l'ensemble des messages clairs est le groupe  $G$  engendré par  $g$ . C'est le résultat que nous avons prouvé formellement dans [BCP03]. Cependant, ce résultat nécessite un modèle fort, dit du "chiffrement idéal". Non seulement nous avons besoin d'un chiffrement sur  $G$ , mais pour chaque clé de chiffrement, nous faisons l'hypothèse que la fonction de chiffrement est une permutation parfaitement aléatoire sur  $G$  (puis toutes les permutations sont indépendantes les unes des autres).

Une proposition de chiffrement, supposée conduire à un schéma sûr, et qui est de plus très efficace, est  $E_{pw}(m) = m \times H(pw)$  où la fonction  $H$  retourne des éléments aléatoires dans  $G$ . Cependant, même si cette construction était conjecturée sûre, la sécurité effective était un problème ouvert. Nous l'avons formellement confirmée dans [BCP04]. Nous avons récemment étendu cette preuve à un modèle plus fort : la "forward-secrecy" [ACP05]. Si le mot de passe est corrompu, les clés échangées par le passé restent confidentielles.

Dans les deux articles ci-dessus [BCP03, BCP04], nous avons même montré qu'il était suffisant de chiffrer l'un des deux messages uniquement (et non les deux), à condition d'apporter ultérieurement la confirmation que les participants connaissaient bien la clé finale : être en mesure de calculer la clé prouve aussi bien la capacité à chiffrer qu'à déchiffrer avec le mot de passe.

La technique utilisée dans le dernier article a l'avantage d'être générique, et ne nécessite pas l'utilisation du problème Diffie-Hellman. Le calcul d'exponentielles est tout de même coûteux en pratique, même sur courbes elliptiques. Nous l'avons donc généralisée [CPP04, CPP06], et une application au problème de la résiduosit  quadratique est sans aucun doute le protocole de mise en accord de clé à base de mots de passe le plus efficace : un des participants n'a que quelques carrés modulaires à effectuer.

De plus, nous avons constaté que la technique de chiffrement  $E_{pw}(m) = m \times H(pw)$  pouvait encore être améliorée, en se passant de l'oracle aléatoire :  $E_{pw}(m) = m \times U^{pw}$ , où  $U$  est un élément du groupe dont le logarithme discret est inconnu [AP05b].

## 2.1.2 Proposition de normes

Ces travaux nous ont conduit à étudier l'intégration d'une suite de mise en accord de clé avec authentification à base de mot de passe dans OpenSSL [ABC+06, ABC+06b]. Notre principale motivation était de pouvoir s'affranchir des brevets existants, afin de permettre une telle intégration dans un logiciel libre. Une RFC est en cours de rédaction.

## 2.1.3 Serveur d'authentification

Nous avons également considéré le cas où les interlocuteurs ne partagent pas de mot de passe, mais ont chacun un mot de passe commun avec un serveur d'authentification. Dans un tel scénario, de nouvelles attaques sont à considérer : le serveur ne doit servir qu'à garantir l'authentification, mais ne doit pas ensuite pouvoir prendre connaissance des communications échangées entre les participants ; Bob devient un attaquant privilégié pour apprendre le mot de passe qu'Alice possède en commun avec le serveur. Nous avons tout d'abord précisé le modèle de sécurité, avec un exemple de protocole admettant une preuve formelle [AFP05]. Puis nous avons présenté un schéma très efficace, sous de nouvelles hypothèses calculatoires (variantes du Diffie-Hellman) [AP05a].

## Bibliographie

- [ABC+06] M. Abdalla, E. Bresson, O. Chevassut, B. Moeller, and D. Pointcheval. Provably Secure Password-Based Authentication in TLS. In *1st ACM AsiaCCS*, pages 35–45. ACM Press, 2006.
- [ABC+06b] M. Abdalla, E. Bresson, O. Chevassut, B. Moeller, and D. Pointcheval. Strong Password-Based Authentication in TLS using the Three-Party Group Diffie-Hellman Protocol. *International Journal of Security and Networks*, 2006. À paraître.
- [ACP05] M. Abdalla, O. Chevassut, and D. Pointcheval. One-time Verifier-based Encrypted Key Exchange. In *PKC '05*, LNCS 3386, pages 47–64. Springer-Verlag, Berlin, 2005.
- [AFP05] M. Abdalla, P. A. Fouque, and D. Pointcheval. Password-Based Authenticated Key Exchange In The Three-Party Setting. In *PKC '05*, LNCS 3386, pages 65–84. Springer-Verlag, Berlin, 2005.
- [AP05a] M. Abdalla and D. Pointcheval. Interactive Diffie-Hellman Assumptions With Applications To Password-Based Cryptography. In *FC '05*, LNCS 3570, pages 341–356. Springer-Verlag, Berlin, 2005.
- [AP05b] M. Abdalla and D. Pointcheval. Simple Password-Based Encrypted Key Exchange Protocols. In *CT-RSA '05*, LNCS 3376, pages 191–208. Springer-Verlag, Berlin, 2005.
- [BCP03] E. Bresson, O. Chevassut, and D. Pointcheval. Security Proofs for an Efficient Password-Based Key Exchange. In *10th ACM CCS*, pages 241–250. ACM Press, 2003.
- [BCP04] E. Bresson, O. Chevassut, and D. Pointcheval. New Security Results on Encrypted Key Exchange. In *PKC '04*, LNCS 2947, pages 145–158. Springer-Verlag, Berlin, 2004.

- [CPP04] D. Catalano, D. Pointcheval, and T. Pornin. IPAKE: Isomorphisms for Password-based Authenticated Key Exchange. In *Crypto '04*, LNCS 3152, pages 477–493. Springer-Verlag, Berlin, 2004.
- [CPP06] D. Catalano, D. Pointcheval, and T. Pornin. Trapdoor-Hard-to-Invert Isomorphism and their Application to Password-based Authentication. *Journal of Cryptology*, 2006. À paraître.

## 2.2 Échange de clés – Authentification asymétrique

### 2.2.1 Étude des normes

Nous avons étudié certaines normes utilisant les courbes elliptiques, et notamment les protocoles de mise en accord de clé, tels que ECMQV et MTI/A0, MTI/C0. Aucune preuve de sécurité n’existait. Nous avons déterminé les hypothèses algorithmiques raisonnables [KJP06b], puis nous avons également défini un modèle de sécurité plus fort, qui peut être satisfait par des variantes de ECMQV [KJP06a].

### 2.2.2 Échange de clés entre appareils de faible puissance

Le problème de la mise en accord de clé peut être remplacé par une distribution de clé, ceci diminue considérablement le coût de calcul du côté des clients, tandis que tous les calculs sont reportés sur le serveur. Nous avons donc proposé un schéma de distribution de clé au sein d’un groupe, où seul le serveur a de nombreux calculs à effectuer, mais les clients n’ont presque rien à calculer [BCEP03, BCEP04].

## Bibliographie

- [BCEP03] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval. Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices. In *5th IFIP-TC6 International Conference on Mobile and Wireless Communications Networks*, pages 59–62. World Scientific Publishing, 2003.
- [BCEP04] E. Bresson, O. Chevassut, A. Essiari, and D. Pointcheval. Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices. *Journal of Computer Communications*, 27(17):1730–1737. Elsevier Science, 2004. Special Issue on Security and Performance in Wireless and Mobile Networks.
- [KJP06a] S. Kunz-Jacques and D. Pointcheval. A New Key Exchange Protocol based on MQV Assuming Public Computations. In *SCN ’06*, LNCS 4116, pages 186–200. Springer-Verlag, Berlin, 2006.
- [KJP06b] S. Kunz-Jacques and D. Pointcheval. About the security of MTI/C0 and MQV. In *SCN ’06*, LNCS 4116, pages 156–172. Springer-Verlag, Berlin, 2006.

## 2.3 Extraction d'entropie

Tout en restant dans la mise en accord de clé, nous sommes parvenus à exploiter la spécificité des courbes elliptiques pour améliorer des protocoles. En effet, la plupart des protocoles de mise en accord de clés aboutissent sur un élément commun  $g^{xy}$ , qui est donc indistinguable d'un élément aléatoire  $g^z$  dans le groupe (sous l'hypothèse du Diffie-Hellman décisionnel). Or, par la suite, ce secret commun sera utilisé comme clé de chiffrement symétrique : une chaîne de bits parfaitement aléatoire est nécessaire. Cependant, la chaîne de bits qui représente  $g^z$  est loin d'être aléatoire : dans le cas d'un sous-groupe de  $\mathbb{Z}_p^*$ , avec  $p$  sur 1024 bits, d'ordre  $q$  sur 160 bits, c'est indéniable (ce cas a été étudié dans [FPSZ06], tout en fournissant néanmoins une analyse positive de TLS) ; dans le cas d'une courbe elliptique sur  $\mathbb{Z}_p^*$ , avec  $p$  sur 160 bits, d'ordre  $q$  sur 160 bits, environ une chaîne sur deux apparaît, et il est facile de savoir lesquelles. Ainsi, sans outils supplémentaires (tel que le "left-over hash lemma", mais qui nécessite des aléas certifiés) il n'est pas possible d'extraire, d'un élément aléatoire dans le groupe  $G$ , une chaîne de bits uniformément distribuée (ou proche de la distribution uniforme). En pratique, la seule méthode est alors d'utiliser le modèle de l'oracle aléatoire.

Dans IKE (Internet Key Exchange), normalisé par l'IETF, une famille de fonctions pseudo-aléatoires est utilisée pour faire office d'extracteur d'entropie, ce qui n'est pas correct en général [CFGP05]. Nous avons mis en évidence un certain nombre de problèmes théoriques à ce sujet dans IKE. Puis nous avons proposé une solution originale : un extracteur déterministe (TAU) qui utilise une spécificité des courbes elliptiques, et notamment le twist quadratique [CFGP06]. La génération des courbes spécifiques pour cet usage a également été étudiée.

Une autre piste pour l'extraction d'entropie a été explorée. Si on considère une courbe elliptique définie sur une extension de degré 2 d'un corps premier, alors des bornes adéquates peuvent être prouvées. Le résultat est le suivant [G05] : à partir des coordonnées d'un point qui contient  $2 \log p$  bits d'entropie cachés au sein de  $2 \log p + 1$  bits, on peut extraire  $\log p$  bits. Ainsi, si l'on a besoin d'une clef de 80 bits, en travaillant avec une courbe d'ordre premier définie sur  $GF(p^2)$  avec  $p$  un premier proche de  $2^{80}$ , on a la sécurité souhaitée. La preuve de ce résultat utilise une analyse de la géométrie des courbes qui sont incluses dans la restriction de Weil de la courbe elliptique de départ. Une fois la géométrie maîtrisée, les bornes de Weil permettent de conclure.

## Bibliographie

- [CFGP05] O. Chevassut, P-A. Fouque, P. Gaudry, and D. Pointcheval. Key Derivation and Randomness Extraction. Cryptology ePrint Archive, mars 2005. Archive 2005/061, disponible sur [eprint.iacr.org/](http://eprint.iacr.org/).
- [CFGP06] O. Chevassut, P. A. Fouque, P. Gaudry, and D. Pointcheval. The Twist-Augmented Technique for Key Exchange. In *PKC '06*, LNCS 3958, pages 410–426. Springer-Verlag, Berlin, 2006.
- [FPSZ06] P. A. Fouque, D. Pointcheval, J. Stern, and S. Zimmer. Hardness of Distinguishing the MSB or LSB of Secret Keys in Diffie-Hellman Schemes. In *ICALP '06*, LNCS 4052, pages 240–251. Springer-Verlag, Berlin, 2006.

- [G05] N. Gürel. Extracting bits from coordinates of a point of an elliptic curve. Cryptology ePrint Archive, septembre 2005. Archive 2005/324, disponible sur [eprint.iacr.org/](http://eprint.iacr.org/).

## 2.4 Génération de courbes

Notre travail sur la génération de courbes se divise en deux branches. D’une part, étudier la sécurité de courbes non encore standardisées mais qui présenteraient des avantages pour une utilisation en environnement contraint, et d’autre part améliorer les algorithmes pour fabriquer des courbes vérifiant les critères déduits de cette étude.

### 2.4.1 Étude du logarithme discret

Pour une utilisation des courbes elliptiques en environnement contraint, il est extrêmement tentant de choisir un corps de base “intermédiaire”, c’est-à-dire une extension de degré moyen d’un corps premier lui-même de taille moyenne, adaptée à l’architecture visée. Fabriquer de bonnes courbes pour ces corps est un problème peu étudié, car les paramètres se situent à la limite de validité de divers algorithmes. Avant de s’y atteler, il est prudent d’étudier la sécurité. En effet, une attaque par descente de Weil peut s’appliquer à certaines de ces situations, affaiblissant alors le cryptosystème. Dans le preprint [G04], nous avons modifié l’attaque par descente de Weil, de manière à la rendre applicable à toutes les courbes elliptiques définies sur un corps de la forme  $GF(p^n)$  avec  $n$  petit et  $n \geq 3$ . Ainsi, pour  $n = 3$ , on obtient un algorithme de complexité  $O(p^{1.42})$ , alors que la meilleure attaque connue auparavant (attaque générique) donnait  $O(p^{1.5})$ . Pour  $n = 4$ , la complexité est de  $O(p^{1.55})$  au lieu de  $O(p^2)$  auparavant. Pour  $n \geq 5$ , on obtient aussi des améliorations de complexité, mais la constante impliquée est telle que le résultat n’a pas d’implication pratique pour le moment.

Par ailleurs, les courbes hyperelliptiques fournissent des alternatives crédibles qui auraient elles-aussi des avantages pour une implantation à bas-coût, car le corps fini sur lequel on travaille est alors plus petit. Il est connu que lorsque le genre d’une courbe hyperelliptique devient grand, le logarithme discret devient attaquable par un algorithme meilleur que la méthode Rho. En étudiant les meilleures attaques connues, nous les avons améliorées de manière à réduire encore la complexité d’un calcul de log discret [GTT+06]. Cette attaque est particulièrement adaptée au cas des courbes de genre 3 et 4, ce qui rend leur utilisation déconseillée. Les courbes de genre 2 restent complètement immunisées contre ces attaques.

Dans un travail plus prospectif [EG06], nous avons trouvé une famille de courbes de genre grand pour lesquelles le problème du log discret peut être résolu en temps sous-exponentiel  $L(1/3)$ , alors que les meilleures attaques connues pour les courbes générales sont en temps  $L(1/2)$ .

### 2.4.2 Fabrication de courbes sûres

Nous avons travaillé sur l’algorithme SEA de comptage de points qui est la seule méthode permettant de traiter des courbes aléatoires lorsque la caractéristique du corps de base est grande. Nous avons apporté des améliorations algorithmiques à une des phases de l’algorithme appelée “calcul de valeur propre” [GM06] ainsi qu’au calcul des polynômes modulaires [E06a]. Ces améliorations nous ont permis d’atteindre de nouveaux records [EGM06] pour le comptage de points elliptiques.

Parallèlement au comptage de points, la méthode de la multiplication complexe présente d’autres caractéristiques. Les courbes engendrées sont particulières, mais la méthode permet de forcer certaines propriétés de la courbe. C’est par exemple une méthode utilisée

pour fabriquer des courbes non supersingulières ayant des couplages calculables. Nous avons amélioré la méthode de la multiplication complexe dans le cas elliptique [E06b], ainsi que pour les courbes de genre 2 [GHK+06]. Dans les deux cas, nous avons pu obtenir des exemples de taille bien plus grande que précédemment.

## Bibliographie

- [E06a] A. Enge. Computing modular polynomials in quasi-linear time. Preprint 2006. Available at <http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/modcomp.pdf>.
- [E06b] A. Enge. The complexity of class polynomial computation via floating point approximations. Preprint 2006. Available at <http://www.lix.polytechnique.fr/Labo/Andreas.Enge/vorabdrucke/class.pdf>.
- [EG06] A. Enge and P. Gaudry. An  $L(1/3 + \varepsilon)$  algorithm for the discrete logarithm problem in low degree curves. Preprint 2006. Available at <http://www.loria.fr/~gaudry/publis/113-draft.pdf>.
- [EGM06] A. Enge, P. Gaudry and F. Morain. Record for the SEA algorithm (2100 decimal digits). Announce available at <http://www.lix.polytechnique.fr/~morain/SEA/d2100x.annonce>.
- [G04] P. Gaudry. Index calculus for abelian varieties and the elliptic curve discrete logarithm problem. Cryptology ePrint Archive, mars 2004. Archive 2004/073, disponible sur [eprint.iacr.org/](http://eprint.iacr.org/).
- [GHK+06] P. Gaudry, T. Houtmann, D. Kohel, C. Ritzenthaler and A. Weng. The 2-adic CM method for genus 2 curves with application to cryptography. To appear in Asiacrypt 2006.
- [GM06] P. Gaudry and F. Morain. Fast algorithms for computing the eigenvalue in the Schoof-Elkies-Atkin algorithm. In *Proceedings of ISSAC '06*, pages 109-115, ACM, 2006.
- [GTT+06] P. Gaudry, E. Thomé, N. Thériault and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. To appear in *Math. Comp.*

## 2.5 Couplages

Une propriété importante de certaines courbes elliptiques est l'existence d'une forme bilinéaire (ou couplage) qui a été très utilisée ces dernières années, notamment pour la cryptographie basée sur l'identité. Nous avons exploité cette propriété dans plusieurs directions.

### 2.5.1 Chiffrement basé sur l'identité

Nous avons donc étudié la cryptographie basée sur l'identité, en généralisant la propriété de chiffrement basé sur l'identité. Dans un chiffrement basé sur l'identité classique, l'émetteur chiffre un message à destination d'une identité précise. Dans [ACD+06], on émet un chiffré pour des destinataires dont les identités appartiennent à un ensemble défini par des "wild card".

### 2.5.2 Diffusion chiffrée, et traçage de pirates

La diffusion chiffrée permet à un émetteur de transmettre un contenu numérique de façon à ce que seuls les abonnés puissent déchiffrer l'information. Une solution simple mais insuffisante consiste à fournir la clé (unique) de déchiffrement à tout abonné. Cependant, un traître pourrait donner/vendre cette clé pour produire des décodeurs pirates. Ce traître ne pourra pas être repéré, puisque tout le monde a la même clé. Une solution naturelle serait alors de transmettre l'information chiffrée pour chaque abonné, chacun possédant une clé distincte. Mais ceci induit une communication linéaire en le nombre d'abonnés. Une solution intermédiaire est possible, mais elle ne peut pas exclure, de façon inconditionnelle, la production de décodeurs pirates à partir de la coalition d'un certain nombre d'individus, et donc la combinaison de plusieurs secrets.

Des solutions permettent de garantir, de façon calculatoire, l'impossibilité d'une telle coalition, sous peine de détection d'au moins un des traîtres, à condition que cette coalition ne soit pas trop nombreuse. Cependant, la taille du chiffré reste importante. Dans [CPP05], nous avons exploité les courbes elliptiques et les couplages pour réduire cette taille. Nous avons du même coup introduit une nouvelle fonctionnalité : la traçabilité publique. En effet, malgré la possibilité de retrouver le traître à partir d'un décodeur pirate, cette étape est coûteuse, et nécessitait jusqu'à présent des informations secrètes (permettant de produire des décodeurs pirates anonymes). Nous avons rendu publique la phase la plus coûteuse, permettant ainsi de la distribuer.

### 2.5.3 Signatures de groupe

Les signatures de groupe permettent à un membre d'un groupe de signer au nom du groupe, et de façon anonyme vis-à-vis du destinataire. Ainsi ce dernier n'a aucune idée de la personne qui a signé, mais a la garantie qu'elle fait partie du groupe. Cependant, il est souhaitable qu'en cas d'abus, une autorité ait le pouvoir de lever cet anonymat. Enfin, le groupe doit pouvoir évoluer, pour ajouter ou révoquer des membres. Dans [DP06], nous utilisons les propriétés de couplage sur certaines courbes afin de proposer les signatures de groupe les plus courtes connues à ce jour.

## Bibliographie

- [ACD+06] M. Abdalla, D. Catalano, A. Dent, J. Malone-Lee, G. Neven, and N. Smart. Identity-Based Encryption Gone Wild. In *ICALP '06*, LNCS 4052, pages 300–311. Springer-Verlag, Berlin, 2006.
- [CPP05] H. Chabanne, D. H. Phan, and D. Pointcheval. Public Traceability in Traitor Tracing Schemes. In *Advances in Cryptology – Proceedings of EUROCRYPT '05*, LNCS 3494, pages 542–558. Springer-Verlag, Berlin, 2005.
- [DP06] C. Delerablée and D. Pointcheval. Dynamic Fully Anonymous Short Group Signatures. In *VietCrypt '06*, LNCS. Springer-Verlag, Berlin, 2006. À paraître.