Sécurité des sous-groupes en Cryptographie basée sur les couplages

Mahamadou Abdou TOURE[1], Karim SAMAKE[2], Emmanuel FOUOTSA[3] et Sinaly TRAORE[2]*
[1]Centre de Recherche et de Formation pour l'Industrie Textile (MALI)
[2]Faculté des Sciences et Techniques (FST) de l'Université de Sciences, des Techniques et des Technologies de Bamako (USTTB) (MALI)
[3]UNIVERSITY OF BAMENDA (CAMEROUN)
[*]mahamadou.abdou.toure@gmail.com

Abstract: La cryptographie basée sur les couplages (en anglais Pairing Based Cryptography, PBC) dépend de l'existence de groupes où le problème DDH est facile à résoudre (c'est-à-dire connaissant P, [a]P, [b]P, [c]P, déterminer si c = ab) mais le problème CDH (Connaissant P, [a]P, [b]P, calculer [ab]P) est difficile. C'est le cas des groupes des Courbes Elliptiques (en anglais Elliptic Curves, EC) dont leur degré de plongement est assez grand pour maintenir un bon niveau de sécurité mais assez petit pour les opérations arithmétiques soient possibles. Cependant les degrés de plongement de la plus part des EC sont énormes, et les plus convenables connus ont des degrés k≤6. Barreto, Lynn et Scott (BLS) ont examiné des critères pour des courbes avec k plus grand qui généralise le travail préalable de Miyaji et al. basé sur les propriétés des polynômes cyclotomiques et proposent des représentations efficaces pour les structures algébriques soulignées.

D'autre part, les couplages sont des applications implémentées en utilisant des courbes elliptiques bien adaptées (couplées). Ils ont permis la construction de protocoles originaux et la simplification de protocoles cryptographiquement existants. Etant de même ordre, les deux groupes de départ de la fonction de couplage sont des groupes de points de courbes elliptiques, tandis que le groupe d'arrivé se trouve dans un groupe multiplicatif d'un grand corps fini. Pour atteindre un niveau de sécurité moyen, au moins deux des trois groupes du couplage doivent être nécessairement des sous-groupes propres groupes d'ordres composés de grand facteurs premiers pour résister aux attaques de petits sous-groupes.

Pour minimiser les chances de telles attaques, des études ont été menées avec certaines courbes existantes [2] dans la littérature et dans les librairies sur les couplages disponibles à l'endroit du public. Dans cet article, nous avons repris l'article de BLS [1] qui permet de construire des courbes elliptiques à partir des degrés de plongement en puissance de 3 ou divisibles par 6 en apportant des éclaircissement au niveau de certains formules de bases, en modifiant le cas de puissance de 3 et en ajoutant le cas général divisible par 3. Cette théorie a été appliquée au niveau de la sécurité des sous-groupes en cryptographie basée sur les couplages.

Mots Clés : Couplage, cryptographie, courbe elliptique, small-subgroup attacks, polynômes cyclotomiques.

1. INTRODUCTION

Un sous-groupe G d'une courbe elliptique (EC) $E(\mathbb{F}_q)$ admet k comme degré de plongement ou multiplicateur de sécurité si l'ordre du sous-groupe r divise $q^k - 1$ mais ne divise pas $q^i - 1 \quad \forall i \in \{1;2;\cdots k-1\}$.

En Cryptographie basée sur les couplages (PBC), un problème ouvert est de construire des courbes contenant un sous-groupe avec un degré de plongement k qui est en même temps assez grand pour prévenir l'attaque Frey-Rück, mais assez petit pour calculer le couplage de Tate efficacement ce qui veut dire que l'arithmétique dans $\mathbb{F}_{q^k}$ est faisable. Les seules courbes Elliptiques (EC) connues qui admettent des sous-groupes avec des degrés k raisonnables étaient les courbes supersingulières, particulièrement sur $\mathbb{F}_{3^m}$ où k = *6*. De telles courbes sont construites sur des corps de petites caractéristiques, rendant vulnérables face aux algorithmes du logarithme discret. Miyaji, Nakabayashi et Takano ont montré, en utilisant certaines propriétés d'un polynôme cyclotomique d'ordre k, comment construire des courbes non supersingulières sur d'ordre $\mathbb{F}_{q^k}$ premier avec k = *3, 4, 6* en utilisant la méthode de la multiplication complexe (CM) aussi longue que certaines conditions, que Barreto, Lynn et Scott appellent le critère de MNT dans [1] en fonction de la taille du corps q, la trace de Frobenius t et l'ordre de la courbe n. BLS ont investi des généralités du critère de MNT dans [1] pour des courbes avec de degré de plongement général k, et présenté la construction actuelle de telles courbes. Dans [2], Barreto et al. ont proposé des nouveaux exemples de courbes elliptiques adaptées qui visent à fournir une résistance plus forte contre les attaques de petits sous-groupes (Small-Subgroup Attacks) [3]. Une attaque de petit sous-groupe peut être montée sur un schéma cryptographique basé sur le logarithme discret qui utilise un groupe d'ordre premier qui est

contenu dans un plus grand groupe d'ordre divisible par des petits facteurs premiers. Un attaquant pourrait obtenir facilement de l'information au sur une clé privée en forçant un participant du protocole à réaliser une exponentiation d'un élément d'un groupe d'ordre non premier avec un exposant secret. Cela est possible si la mise en œuvre du protocole ne vérifie pas si l'élément du groupe utilisé appartient bien au bon sous-groupe et donc a bien un grand ordre premier. Sinon, la clé privée de l'utilisateur pourrait être complètement identifiée bien que le problème du logarithme discret (DLP) dans le grand sous-groupe d'ordre premier est calculatoirement infaisable. Ils ont commencé par illustrer la possibilité de telles attaques dans le contexte de (basé sur les couplages) des schémas de la signature numérique, beaucoup d'entre eux sont basés sur le schéma de la signature courte célèbre de Boneh, Lynn et Shacham (BLS) [4]. Barreto et al. ont travaillé sur la famille de courbes Barreto-Naehrig (BN) pour k = 12, la famille Barreto Lynn Scott (BLS) pour k = 12 et 24 et celles de Kachisa–Schaefer–Scott (KSS) pour k = 18.

Dans cet article nous allons apporter des éclaircissements et des corrections dans [1] et proposons des travaux pour des degrés de plongement impairs sur des nouvelles courbes elliptiques en s'appuyant sur les nouvelles méthodes proposées dans la suite :

2. Généralité sur la sécurité en PBC.

2.1. Signatures BLS

Supposons l'existence d'un morphisme efficace, symétrique et bilinéaire $e:\mathbb{G}\times\mathbb{G}\longrightarrow\mathbb{G}_T$ où $\mathbb{G}$ et $\mathbb{G}_T$ sont des groupes cryptographiques d'ordre premier très grand *n*. Soient *P* un générateur public de $\mathbb{G}$ et $\mathcal{H}:\{0;1\}^*\longrightarrow\mathbb{G}$ une fonction de hachage convenablement définie. Boneh, Lynn et Shachan ont proposé un schéma de signature simple [4] qui fonctionne comme suit. Pour signer un message $M\in\{0;1\}^*$ avec sa clé privée $a\in\mathbb{Z}_n$, Alice calcule $Q=\mathcal{H}(M)\in\mathbb{G}$ et envoie la signature $\sigma=[a]Q$ à Bob. Pour vérifier cette signature, Bob calcule également $Q=\mathcal{H}(M)$ et utilise alors la clé publique d'Alice [a]P et s'assure que

$$e([a]P,Q)=e(P,[a]Q)=e(P,\sigma) \qquad (1)$$

2.2. Paramètres forcés du système

Il existe des modèles variés de menaces dans lesquels on pouvait souhaiter réfléchir sur les implications possibles des attaques de petits sous-groupes. Parmi eux se trouve le cas où on suppose qu'il est possible pour un attaquant de falsifier complétement les paramètres publics utilisés dans le système de signature comme la "Digital Signature Standard" (la signature digitale standard) introduit par Vandenay dans [5]. Pour la signature BLS, un attaquant pourrait forcer les paramètres du système à utiliser un point de départ *P* d'ordre non premier. Ainsi, au moins de (par le biais de) l'attaque des petits sous-groupes, Alice révèle des informations sur sa clé privée *a* à l'attaquant par une simple publication de sa clé publique *[a]P*.

Dans un autre cas de manipulation de paramètres publics, on pouvait supposer que la fonction de hachage $\mathcal{H}$ conduit dans un groupe d'ordre composé à la place d'un sous-groupe d'ordre premier. Donc le hachage du message pourrait être un élément du groupe d'ordre composé et la signature BLS pourrait fuiter des informations sur la clé privée d'Alice. Ainsi une fausse fonction de hachage pouvait actuellement être le résultat d'un bogue d'implémentation, par exemple l'omission de l'exponentiation du cofacteur à déplacer les éléments du groupe dans le bon sous-groupe.

2.3. Paramètres valides du système

Même si les paramètres du système sont valides, il y'a des scénarios dans lesquels les attaques de petits sous-groupes pouvaient conduire à une brèche de sécurité. Ainsi, nous supposons que, puisque *P* est un paramètre public fixe (en général dans $\mathbb{G}$) et Alice hache les éléments dans $\mathbb{G}$ soi-même, la clé publique d'Alice et sa signature sont sûres de se trouver dans $\mathbb{G}$ et sont donc protégées par la difficulté de résoudre le problème du logarithme discret dans $\mathbb{G}$. Il n'y a donc pas de menace pour la clé privée d'Alice dans le cas de la signature BLS mais ce n'est pas nécessairement le cas dans le contexte des (signatures aveugles) comme ci-dessous.

2.4. Signatures à l'aveugle

De façon générale, les signatures à l'aveugle laissent Alice signé un message qui est créé par une troisième partie, Carole. Les scénarios typiques exigent que Carole et Alice interagissent avec une autre personne de telle manière que Carole n'obtient aucune information sur la clé privée de signature d'Alice et vice versa. Afin de signer "aveuglement" son message *M*, Carole calcule $Q=\mathcal{H}(M)$ et envoie à Alice le message aveuglé $Q_1=Q+[r]P$ où $r\in\mathbb{Z}_n$ (choisi au hasard par Carole). Alice utilise sa clé privée $a\in\mathbb{Z}_n$ et retourne la valeur signée $[a]Q_1$ à Carole, qui à son tour utilise *r* défini précédemment et la clé publique d'Alice *[a]P* pour calculer $\sigma=[a]Q_1-[r][a]P=[a]Q$. Elle envoie alors cette valeur σ à Bob qui peut s'assurer que c'est une signature BLS valide avec la clé d'Alice.

Contrairement aux signatures BLS originales où Alice hachait le message dans $\mathbb{G}$ soi-même avant de le signer, dans le schéma au-dessus Alice signe le point que Carole lui envoie. Si par malice, Carole envoie à Alice un point qui appartient à un groupe dans lequel le DLP est facile et si cela est indétectable par Alice alors Carole peut restaurer la clé privée d'Alice.

Bien sûr dans une bonne configuration de la version du protocole ci-dessus, Alice vérifie que le point reçu est dans le bon groupe avant d'utiliser sa clé privée pour la signature. Cependant, pour les instanciations des couplages bilinéaires qui sont favoris en pratique, cette validation exige une multiplication par un scalaire complète de courbe elliptique. De plus, les auteurs des protocoles basés sur les couplages supposent souvent que certains éléments de groupe appartiennent aux groupes qu'ils ont imaginés. Si ces descriptions étaient translatées dans le monde réel des implémentations inchangées alors des telles instanciations pourraient être sensibles aux attaques des petits sous-groupes.

2.5. Couplages asymétriques

Les articles originaux qui ont donné naissance à la PBC [6, 7, 8] supposaient l'existence d'une application bilinéaire de la forme $e:\mathbb{G}\times\mathbb{G}\longrightarrow\mathbb{G}_T$. De tels couplages symétriques existent seulement sur les courbes supersingulières qui mettent une dure restriction sur l'efficacité implicite (sous-jacente) et la sécurité du protocole. Il n'a pas fallu du temps jusqu'à ce que les instanciations pratiques des couplages asymétriques de la forme $e:\mathbb{G}_1\times\mathbb{G}_2\longrightarrow\mathbb{G}_T$ (avec $\mathbb{G}_1\neq\mathbb{G}_2$) ont été découverte [9, 10] et ont été démontrés plus efficaces que leurs homologues symétriques, spécialement à une sécurité de haut niveau. Toutes les bibliothèques modernes de couplage sont construites sur des courbes elliptiques ordinaires dans la configuration asymétrique.

En suivant la version asymétrique des signatures BLS [11, 12], dans le schéma de simple « blind signature » de Boldreva, la clé publique d'Alice pourrait être *($[a]P_1$,$[a]P_2$)* pour un générateur $(P_1,P_2) \in \mathbb{G}_1\times\mathbb{G}_2$ donné. Si $\mathcal{H}:\{0,1\}^*\longrightarrow\mathbb{G}_1$ alors Carole peut aveugler le message $Q=\mathcal{H}(M)$ en envoyant $Q_1=Q+[r]P_1$ à Alice. Après réception d'Alice $[a]Q_1$, Carole enlève le facteur d'aveuglement comme avant en prenant $[a]Q_1 - [r][a]P_1=[a]Q = \sigma$ et envoie le résultat à Bob. Bob utilise alors la clé publique d'Alice pour vérifier que $e([a]Q,P_2)=e(Q,[a]P_2)$. Ici ça ne coûtera pas à Alice une multiplication par un scalaire pour confirmer si Q_1 est en fait dans $\mathbb{G}_1$ et Carole pourrait utiliser des attaques de petits sous-groupes pour obtenir la clé privée avec laquelle Alice a signé.

En tous cas les attaques de sous-groupes sont intrinsèques aux «signatures à l'aveugle» où les signatures sont effectuées aveuglement sur des points envoyés par des tierces parties.

2.6. Sécurité du sous-groupe

Une courbe adaptée est dit « sous groupement sûr » si les cofacteurs de tous les groupes de couplage, dès qu'ils ont la même taille comme l'ordre de groupe premier *n* ou plus grand, contiennent seulement des facteurs premiers plus grands que *n*. C'est un scénario réaliste car pour des niveaux de sécurité modernes de ciblage de courbe, au moins 2 des groupes de couplage ont des cofacteurs très grands. Nous relaxons légèrement la condition pour permettre des petits cofacteurs inévitables qui sont imposés par les paramétrisations polynomiales dans les constructions populaires des courbes adaptées. Cela signifie que cette propriété distingue ces courbes dans la famille donnée qui fournissent plus de résistance contre des attaques de petits sous-groupes.

3. GENERALISER LE CRITERE DE MNT.

Toute Courbe Elliptique *E* sur $\mathbb{F}_q$ d'ordre *n* vérifie la condition de borne de Hasse qui dit que la trace *t* de l'endomorphisme de Frobenius sur *E*, lié à *q* et *n* par l'équation $n = q + 1 - t$ est restreint à $|t| \leq 2\sqrt{q}$.

En donnant le degré de plongement *k*, le but de BLS est de trouver un nombre premier *q*, un entier *t* tels que $|t| \leq 2\sqrt{q}$, un grand premier *r* qui satisfait $r/q^k - 1$ mais ne divise pas $q^i - 1\ \forall i \in [\![1; k-1]\!]$ et une courbe elliptique $E(\mathbb{F}_q)$ de trace de Frobenius *t* et d'ordre $n = q+1-t$ satisfaisant r/n c'est-à-dire $n = hr$ pour un h quelconque.

Commençons par noter $q = t - 1 + hr \Rightarrow q^u - 1 \equiv (t-1)^u - 1 (mod\ r)\ \forall u > 0$.

Donc tout r convenable doit satisfaire satisfait $r/(t-1)^k - 1$ mais ne divise pas $(t-1)^i - 1\ \forall i \in [\![1; k-1]\!]$.

Soit ϕ_m le me polynôme cyclotomique. Il est connu que $x^u - 1 = \prod_{d/u} \varphi_d\ \forall u > 0$ Ce qui entraine ce lemme.

Lemme 1 : Tout r convenable satisfait $r/\varphi_k(t-1)^k$ mais ne divise pas $\varphi_i(t-1)^i - 1\ \forall i \in [\![1; k-1]\!]$.

Preuve : Il est nécessaire que r ne divise pas $\varphi_i(t-1)\ \forall i \in [\![1; k-1]\!]$ sinon $r/(t-1)^i - 1\ \forall i \in [\![1, k-1]\!]$. Comme *r* est premier, $r/(t-1)^k - 1 \Rightarrow r/\varphi_d(t-1)$ pour un *d* divisant *k* et la seule possibilité restante est $d = k$. Donc nécessairement $r/\varphi_d(t-1)$.

La stratégie de base de MNT est de choisir une trace *t* de taille convenable, trouver un nombre premier *r* sous la condition du lemme ci-dessus, calculer à partir de *t* et *r* un nombre premier de la forme $q = hr + t - 1$ pour un petit cofacteur *h* et finalement utiliser la méthode CM pour construire la courbe désirée.

3.1. Contrainte de paramètres

BLS ont donnée des contraintes explicites sur la forme de *t* et *q* pour tout *h* et *k* généralisant l'approche originale de Miyaji et al.

Soient *l* un entier avec $|l|>1$, *r* un facteur premier de $\phi_k(l)$ et *d* un entier satisfaisant $1 \leq d \leq deg\ \phi_k/2$. Posons $n = hr$ pour un *h* quelconque, $q = n +$

l^d et $t = l^d + 1$. D'après le lemme 1, r vérifie $r/l^{dk} - 1$ et $\forall\ 0 < i < k$, r ne divise pas $l^{di} - 1$. La restriction $d \leq deg\ \phi_k/2$ est imposée pour assurer la condition de borne de Hasse.

Théorème 1 : Le choix des paramètres proposés ci-dessus donne des courbes contenant un sous-groupe d'ordre r de degré de plongement au plus k.

Preuve : D'après la condition $q = hr + l^d$, on a $q^k - 1 \equiv l^{dk} - 1\ (mod\ r)$. Puisque $\phi_k(l)/l^{dk}-1$ [15, th 2.45(i)], la restriction $r/\phi_k(l) \Rightarrow r/l^{dk}-1$, c'est-à-dire $l^{dk}-1 \equiv 0[r]$. Donc $q^k-1 \equiv 0[r]$, c'est-à-dire $r/\ q^k-1$.

Une observation importante est qu'il faut toujours vérifier que r ne divise pas $q^i - 1$ pour tout $0<i<k$, même pour un tel cas spécial $r = \phi_k(l)$. puisque $l^i - 1 = \prod_{u/i} \varphi_u(l)$, il est évident que $\phi_k(l)$ ne divise pas $l^i - 1$, et donc évidemment r ne divise pas $l^i - 1$. Cependant, ce raisonnement est faux ; la relation $\phi_k(l)/l^i-1$ tient seulement pour les polynômes mêmes, pas nécessairement pour une valeur spécifique l. En opposition au travail original de Miyayaji et al., les critères ci-dessus ne sont pas exhaustifs et il n'est pas difficile de trouver d'autres conditions donnant parfaitement des paramètres valides. Pour exemple, une généralisation évidente est $q = n + \phi_k(l)g(l) + l^d$ pour tout polynôme g(l). ceci n'aide pas beaucoup en général car $\phi_k(l)g(l)$ rend la trace t trop grand pour pouvoir satisfaire la borne de Hasse, excepté quand le terme l^d annule le terme du plus haut degré dans $\phi_k(l)g(l)$ et les termes restant convenable de faible degré (par exemple pour k = 9, en prenant un g approprié, on peut obtenir $q=n-l^3-1$). Egalement si d est pair, k est pair et k/2 est impair, il peut être vérifié que poser $t = -l^d + 1$ et $q = hr - l^d$ est également possible, c'est $r/q^k - 1$ (la restriction à un k pair tel que k/2 est impair assure que $q^{k/2} - 1 \equiv s - (l^{dk} + 1)$ n'est pas $\equiv 0 (mod\ r)$. Parfois, des solutions fortuites à peine ressemblant (mais relatées) au critère MNT peuvent être trouvées pour des choix particuliers de k. cependant, pour simplicité, BLS se sont focalisés sur les paramètres considérés dans le théorème 1 ; étendre la discussion à d'autres paramètres ne devraient pas être difficiles, et seraient durement nécessaires en pratique.

4. RESOUDRE L'EQUATION CM.

La stratégie de construire des courbes donnant les critères ci-dessus semble claire :

- Choisir l et h ;
- Trouver un premier q et une trace correspondante selon les relations proposées ;
- Résoudre pour le discriminant de CM D (et pour V) l'équation de CM $DV^2=4q-t^2$ ou de façon équivalente $DV^2=4n-(t-2)^2$;
- Et utiliser la méthode CM pour calculer les coefficients de l'équation de la courbe.

Puisque n = hr et $r/\phi_k(l)$, on peut écrire $n = m\phi_k(l)$ pour m donnée. Ainsi les équations CM pour les critères de paramètre donnés dans la section 2.1 ont la forme

$$DV^2 = 4m\phi_k(l) - (ld - 1)^2 \qquad (2)$$

Malheureusement, cette approche n'est pas pratique, parce qu'en général D est trop grand (comparable à q), et cryptographiquement des paramètres significatifs auraient $q \approx 2^{160}$ au moins. Par exemple, la courbe E : $y^2 = x^3 - 3x + 183738738969463$ sur $\mathbb{F}_{449018176625659}$ a 4r points où r = 112254544155601. Le sous-groupe d'ordre r a k = 12 comme degré de plongement. Cette courbe satisfait m = 4, $r = \phi_k(l)$, $t = l + 1$ et $q = 4\phi_k(l) + l$ pour $l = 3255$.

L'équation CM est $DV^2 = 4q - t^2$ où D = 13188099 et V = 11670 et le nombre de classe est 2940.

Miyaji et al. résolvent ce problème pour k = 3, 4, 6 en remarquant que l'équation CM conduit, dans ce cas, à une équation diophantienne quadratique réductible à une équation de Pell dont sa solution est bien connue [16]. Le cas d'un k arbitraire est plus dur, puisqu'aucune méthode générale n'est connue pour résoudre une équation diophantienne de degré $deg(\phi k) \geq 4$.

Cependant, Tzanakis [17] décrit comment résoudre des équations diophantiennes elliptiques quartiques de la forme

$$V^2 = al^4 + bl^3 + cl^2 + dl + e^2 \quad \text{où } a > 0$$

Pour k = 5, 8, 10, 12, le degré de ϕ_k est 4, donc cette équation 1 a la forme $DV^2 = al^4 + bl^3 + cl^2 + dl + f$. Si une solution de cette équation en entier court est connu (comme peut être souvent trouvée par une recherche exhaustive), cette équation se réduit à la forme de Tzanakis en multipliant les deux cotés par D et en appliquant une transformation linéaire en estimant la solution connue, ainsi le terme indépendant de l'équation transformée est un carré parfait.

Malheureusement encore, cette approche est prouvée sans succès en pratique. En utilisant l'implémentation Magma de la méthode de Tzanakis, BLS n'ont pas pu trouver des exemples de courbes cryptographiquement significatifs pour k = 5, 8, 10, 12, de tels seuls cas étaient ceux où D est trop grand pour des méthodes CM traditionnelles.

BLS n'avaient pas essayé des variantes de la méthode CM plus récentes comme celles de [18], donc il y'a espoir que des solutions de l'équation 1 avec D grand soient actuellement possible en pratique. Mais même si cette approche directe reste inaccessible, il y'a des chemins de succès à générer de corps convenables et des paramètres de courbes comme montré par la suite.

4.1. Un cas particulier

Soit p un nombre premier (à ne pas confondre avec la taille du corps fini q). BLS ont décrit dans

[1] comment trouver des solutions algébriques de l'équation 2 pour des cas spéciaux de D = 3, d = 1 et $k = 3^i 2^j p^s$, pour certains exposants *i, j, s* et *p>3*. En principe, cette méthode évite le ratio m/r à avoir arbitrairement petit pour des *k* large si *s* = 0.

Les polynômes cyclotomiques sont connus pour satisfaire les propriétés suivantes : si v est un premier divisant u alors $\phi_{uv}(x) = \phi_u(x^v)/\phi_u(x)$. D'autre part, si v ne divise pas u alors $\phi_{uv}(x) = \phi_u(x^v)$.

En utilisant ces propriétés, il est facile de montrer par induction que

$\forall i > 0,\ \varphi_{3^i}(l) = l^{2 3^{i-1}} + l^{3^{i-1}} + 1$ et $\varphi_{2^i 3}(l) = l^{2^i} - l^{2^{i-1}} + 1$

En limitant *l* de sorte que *l≡1[3]*, BLS ont trouvé $4\varphi_{3^i}(l) - 1 = 3\left[\left(2l^{3^{i-1}} + 1\right)/3\right]^2$ et $4\varphi_{2^i 3}(l) - 3 = \left(2l^{2^{i-1}} - 1\right)^2$. Or en développant les deux membres de la première relation, on trouve $4\varphi_{3^i}(l) - 1 = 4l^{2 3^{i-1}} + 4l^{3^{i-1}} + 3$ *et* $3\left[\left(2l^{3^{i-1}} + 1\right)/3\right]^2 = \frac{4}{3}l^{2 3^{i-1}} + \frac{4}{3}l^{3^{i-1}} + \frac{1}{3}$. On constate que les deux expressions sont différentes. La solution que nous avons obtenue est $4\varphi_{3^i}(l) - 3 = \left(2l^{3^{i-1}} + 1\right)^2$.

Dans le premier cas, BLS ont multiplié les deux côtés par $(l-1)^2 \Rightarrow 4(l-1)^2\varphi_{3^i}(l) - (l-1)^2 = 3\left[(l-1)\left(2l^{3^{i-1}} + 1\right)/3\right]^2$ avec notre solution, multiplions les deux côtés par $(l-1)^2/3$. *On a :* $\frac{4}{3}(l-1)^2\varphi_{3^i}(l) - (l-1)^2 = 3\left[(l-1)\left(2l^{3^{i-1}} + 1\right)/3\right]^2$ ce qui donne la solution

$$k = 3^i,\quad r = \varphi_{3^i}(l);\quad t = l+1;$$

$$m = (l-1)^2/3;\quad V = (l-1)\left(2l^{3^i-1} + 1\right)/3$$

Dans le deuxième cas, multiplions les deux côtés par $(l-1)^2/3$. On a :

$$\frac{4}{3}(l-1)^2\varphi_{2^i 3}(l) - (l-1)^2 = 3\left[(l-1)\left(2l^{2^{i-1}} - 1\right)/3\right]^2$$

Ce qui donne la solution :

$$k = 2^i \times 3,\quad r = \varphi_{2^i 3}(l);\quad t = l+1;$$

$$m = (l-1)^2/3;\quad V = (l-1)\left(2l^{3^{i-1}} - 1\right)/3.$$

Dans les deux cas nous supposons que $q = mr + l$ est premier.

Pareillement, on peut montrer par induction que, pour tout premier p>3 et ∀ i, j>0

$$\varphi_{3^i p^j}(l) = \left[\left(2l^{3^{i-1}p^j} + 1\right)^2 + 3\right] / \left[\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right]$$

Multiplions les deux côtés par $12z^2\left[\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right]$ pour tout z, ce qui donne

$4 \times 3z^2\left[\left(2l^{3^{i-1}p^{j-1}} + 1\right)^2 + 3\right]\varphi_{3^i p^j}(l) - (6z)^2 = 3\left[2z\left(2l^{3^{i-1}p^j} + 1\right)\right]^2$.

En choisissant r d'être un grand facteur de $\varphi_{3^i p^j}(l)$, cela donne la solution

$$k = 3^i \times p^j,\quad l = 6z+1$$

$$n = 3z^2\left[\left(2l^{3^{i-1}\,p^{j-1}}\right)\right]\varphi_{3^i\,p^j}(l);\quad V = z\left(2l^{3^{i-1}\,p^{j-1}} - 1\right)$$

Il est également possible de montrer que :

$$\varphi_{3^i 2^j p^s}(l) = \left[\left(2l^{3^{i-1}2^{j-1}p^s} - 1\right)^2 + 3\right] / \left[\left(2l^{3^{i-1}2^{j-1}p^{s-1}} - 1\right)^2 + 3\right]$$

Donc $4 \times 3z^2\left[\left(2l^{3^{i-1}2^{j-1}p^{s-1}} - 1\right)^2 + 3\right]\varphi_{3^i p^j}(l) - (6z)^2 = 3\left[2z\left(2l^{3^{i-1}2^{j-1}p^s} - 1\right)\right]^2$.

qui donne la solution

$$k = 3^i \times 2^j p^s,\quad l = 6z+1\quad m = 3z^2\left[\left(2l^{3^{i-1}2^{j-1}p^{s-1}}\right)\right];$$

$$r = \varphi_k(l);\quad V = 2z\left(2l^{3^{i-1}2^{j-1}p^s} - 1\right)$$

Posons $k = 5^i p^j$ avec p>5. En utilisant les propriétés sur les polynômes cyclotomiques, on obtient : $\forall i > 0,\ \varphi_{5^i}(l) = l^{2 3^{i-1}} + l^{3^{i-1}} + 1$

Dans tous les cas, il est nécessaire de s'assurer que $q = m\phi_k(l) + l$ est premier. Cette solution produit seulement des solutions pour *D = 3*, qui pouvait potentiellement avoir un niveau de sécurité faible, bien qu'aucune vulnérabilité spécifique basée sur la petite valeur *D* n'est connue en ce moment. La méthode suivante décrite par BLS est convenable pour beaucoup de *D*.

4.2. Une méthode générale

La forme générale du critère que BLS avait considérée est $n=m\phi_k(l)$, $t=l^d+1$, $q=n+t-1=m\phi_k(l)+l^d$ où $1 \le d \le (\deg\phi_k)/2$. Généralement, on veut que m soit petit et $\phi_k(l)$ contienne un grand facteur premier r (le meilleur, c'est $\phi_k(l)$ soit premier). Cependant, trouver des solutions sous ces conditions est très difficile pour tout k tel que $\deg \phi_k > 2$. Donc BLS ont relaxé les restrictions sur m en permettant à m d'être comparable à r. Ce qui entraine qu'obtenir des paramètres convenables devient assez facile.

Considérons l'équation CM $DV^2 = 4m\phi_k(l) - (l^d - 1)^2$. On suppose que D et l sont tous 2 choisis et t ne divise pas D, on souhaite trouver une solution m (et V) à cette équation. Pour des raisons de commodité, soient $A = 4\phi_k(l)$ et $B = (l^d - 1)^2$, l'équation devient $DV^2 = mA - B$.

Initialement, trouver le plus petit $m_0 \ge 0$ tel que $D/Am_0 - B$, c'est $Am_0 - B = z_0 D$. Si A est

inversible modulo D, alors m0 = B/A(mod D) et z_0 = (Am_0 – B)/D.

Si A n'est pas inversible modulo D mais B est un multiple de D alors $m_0 = 0$ et z_0 = –B /D. Sinon, il n'existe pas de solution pour ce choix de l et D. Ainsi nous sommes rassuré que m_0 n'est jamais plus grand que D.

$$m_i = m_0 + iD; \quad z_i = z_0 + iA$$

En remplaçant celles-ci dans l'équation CM on obtient $Dz_i = Am_i - \mathcal{B}$. Ce qui signifie que cette équation concerne z_i qui est un carré parfait. Donc résoudre $V^2 = z_0 + iA$ pour *V* et *i*, récupérer la plus petite solution *i* telle que $q = m_i\phi_k(l)+l^d$ est premier. Cela exige que z_0 soit un résidu quadratique (*mod A*). si toutes les solutions i_α peuvent être écrites sous la forme $i_\alpha = i_0 + \alpha A$, où $i_0 = (V_0^2 - z_0)/A$ et $V_0 = \sqrt{z_0}(mod\ A)$. Une stratégie nette pour obtenir un ratio serré entre *log q* et *log r* est de restreindre la recherche à i_0 seul et faire varier seulement *l*.
Des expériences effectuées par BLS et reprises par nous ont montré qu'en pratique, *m* tend vers *r*. Néanmoins, de telles solutions sont parfaitement convenable pour la plus part des PBC, la seule exception étant le schéma de signature courte de [4].

5. ISSUES D'IMPLEMENTATION

Puisque des courbes avec de degré de plongement de taille moyenne peuvent être effectivement construites comme décrit au-dessus, la question naturelle à poser est comment implémenter efficacement l'arithmétique soulignée et particulièrement le couplage de Tate.

BLS ont restreint la discussion au *k* pair. Soit $even(\mathbb{F}_{q^k})$ le sous ensemble de $\mathbb{F}_{q^k}$ constitué de polynôme qui ne contiennent que de monômes de degré pair, c'est-à-dire

$$pair(\mathbb{F}_{q^k}) = even(\mathbb{F}_{q^k})$$
$$= \left\{u \in \mathbb{F}_{q^k} : u(x) = a_{k-2}x^{k-2} + a_{k-4}x^{k-4} + \cdots + a_2x^2 + a_0\right\}$$

De façon analogue

$$impair(\mathbb{F}_{q^k}) = odd(\mathbb{F}_{q^k})$$
$$= \left\{u \in \mathbb{F}_{q^k} : u(x) = a_{k-1}x^{k-1} + a_{k-3}x^{k-3} + \cdots + a_1x\right\}$$

BLS ont proposé représenter $\mathbb{F}_{q^k}$ comme $\mathbb{F}_p[x]/R_k(x)$ avec un polynôme de réduction de forme $R_k(x) = x^k + x^2 + \omega$ pour $\omega \in \mathbb{F}_p$. Ce choix est motivé par l'analyse suivante.

Lemme 2 : Si $R(x) = x^k + x^2 + \omega$ est irréductible sur $\mathbb{F}_q$ alors $r(x) = x^{\frac{k}{2}} + x + \omega$ est irréductible sur $\mathbb{F}_q$.

Preuve : Par contradiction, si $r(x) = f(x)g(x)$ pour $f,g \in \mathbb{F}_q[x]$ alors $R(x) = r(x^2) = f(x^2)g(x^2)$ ce qui contredit l'hypothèse que *R(x)* est irréductible.

Ceci établit que l'application $\psi : \mathbb{F}_q[x]/r(x) \to \mathbb{F}_q[x]/R(x)$, $\psi(f) = F$ tel que $F(x) = f(x^2)$ entraine un isomorphisme entre $\mathbb{F}_{q^{k2}}$ et $even(\mathbb{F}_{q^k})$

Notons que ce lemme resterait valable si *R* contenait plus de monômes de degré pair, mais un trinôme est plus convenable qu'un binôme irréductible $R(x) = x^k + \omega$ existe dans ce cas un choix pair serait mieux.

Lemme 3 : *Soit* $Q = (u,v) \in E(\mathbb{F}_{q^k})$ *où* $E : v^2 = f(u), u \in even(\mathbb{F}_{q^k})$ *et f(u) est un non résidu quadratique. Alors* $v \in odd(\mathbb{F}_{q^k})$.

Preuve : Noter que $f(u) \in even(\mathbb{F}_{q^k})$. Soit $v(x) = \alpha(x) + x\beta(x)$, où $\alpha, \beta \in even(\mathbb{F}_{q^k})$. Alors $v^2(x) = \alpha^2(x) + x^2\beta^2(x) + 2x\alpha(x)\beta(x) \in even(\mathbb{F}_{q^k})$, de sorte que soit $\alpha = 0$ et $\beta = 0$. Mais $\beta = 0$ signifierait que $f(u) = \alpha^2$ est un résidu quadratique, ce qui contredit l'hypothèse. Donc, $\alpha = 0$, c'est-à-dire $v \in odd(\mathbb{F}_{q^k})$.

On peut énoncer le théorème principal.

Théorème 2 : *Soit* $Q = (u,v) \in E(\mathbb{F}_{q^k})$ *où* $E : v^2 = f(u), u \in even(\mathbb{F}_{q^k})$ *et f(u) est un non résidu quadratique. Si* $S = (s,t) \in < Q >$, *alors* $s \in even(\mathbb{F}_{q^k})et\ t \in odd(\mathbb{F}_{q^k})$.

Preuve : C'est une conséquence des règles de l'addition elliptique [19, algo. 2.3]. Il est direct mais fastidieux de montrer que la formule d'addition de points et la formule de doublement satisfont le théorème. Ainsi, nous devons seulement poser *S = mQ* et procéder par induction sur *m*.

Ce chemin, des points de la courbe $Q = (u,v) \in E(\mathbb{F}_{q^k})$ où $f(u) \in even(\mathbb{F}_{q^k})$ est un non résidu quadratique, ne sont pas convenables pour le calcul du couplage de Tate $e(P,Q), \forall P \in E/\mathbb{F}_p$ (car de toute évidence *Q* est linéairement indépendant de *P*) ; ils ont également la bonne propriété que la technique d'élimination du dénominateur [20, section 5.1] est applicable, ainsi presque doubler la performance de l'algorithme de Miller.

6. COURBES BIEN ADAPTEES SOUS GROUPEMENT SURES

Dans cette section, nous rappelons les attaques des sous-groupes et définissons la notion de la sécurité des sous-groupes, une propriété qui est

simple à réaliser en pratique et qui fortifie la résistance des courbes adaptées contre les attaques de sous-groupes.

6.1. Attaques des petits sous-groupes

Les attaques des petits sous-groupes contre les schémas cryptographiques basés sur le DLP étaient introduites par Lim et Lee [3]. Ce qui suit une brève description de l'idée basique dans une configuration générale de groupe.

Supposons que $\mathbb{G}$ soit un groupe additif d'ordre n premier, qui est contenu dans un groupe abélien $\mathcal{G}$ fini plus grand et soit h l'indice de $\mathbb{G}$ dans $\mathcal{G}$, $|\mathcal{G}|=hn$. Supposons que le DLP est difficile dans n'importe quel sous-groupe de $\mathcal{G}$ d'ordre premier assez grand. En particulier, supposons n est assez grand tel que le DLP est infaisable dans $\mathbb{G}$. Si l'indice h a un facteur premier petit r alors il existe un élément de groupe P d'ordre un multiple de r et si r est assez petit, le DLP dans $\langle P\rangle$ peut être facilement résolu modulo r. Si un attaquant arrive à forcer un participant à utiliser P pour une exponentiation de groupe concernant un exposant secret à la place de l'utilisation d'un bon élément de $\mathbb{G}$, en résolvant le DLP dans $\langle P\rangle$ fourni d'information partielle sur l'exposant secret. Si h a plusieurs petits facteurs premiers, l'attaque Pohlig-Hellman [13] peut permettre de recouvrir l'exposant secret en entier.

De telles attaques de sous-groupe peuvent être évitées par le test d'appartenance. Un autre moyen de contrecarrer ces attaques est une exponentiation de cofacteur ou une multiplication de cofacteur (qui est une solution. Si tout élément P reçu est multiplié par l'indice h, qui également signifie que le protocole a besoin d'être ajusté pour travailler avec le point $[h]P$ à la place de P, alors des points d'ordre petit sont mis à $\mathcal{O}$ et n'importe quel point est nettoyé par cette exponentiation.

6.2. Sécurité des sous-groupes

Si $h>1$ et il ne contient aucun facteur premier plus petit que n alors $\mathbb{G}$ est l'un des sous-groupes de $\mathcal{G}$ avec la plus faible sécurité de DLP. En d'autres termes, pour tout $P\in\mathcal{G}$ choisi aléatoirement, le DLP dans $\langle P\rangle$ est garanti d'être au moins aussi difficile que le DLP dans $\mathbb{G}$ puisque même si $|\langle P\rangle|=|\mathcal{G}|$, la réduction Pohlig-Hellman exige la solution à un DLP dans un sous-groupe d'ordre premier au moins n. Dépendant de la conception du protocole, il pouvait être possible d'omettre le test d'appartenance et la multiplication du cofacteur si les paramètres sont choisis tels que h n'ait pas de facteurs premiers plus petit que n.

On pouvait considérer l'omission du test comme si un élément appartient au groupe $\mathbb{G}$ si c'est une opération coûteuse. Par exemple, si le test d'appartenance à $\mathbb{G}$ exige relativement une exponentiation de groupe chère et celui de $\mathcal{G}$ est relativement économique, on peut remplacer le contrôle coûteux par le plus économique étant donné que l'indice h n'a pas de petits facteurs. Quand le groupe $\mathcal{G}$ est le groupe des points rationnels dans $\mathbb{F}_q$ sur une courbe elliptique E et $\mathbb{G}$ est un sous-groupe d'ordre premier alors le test d'appartenance à $\mathcal{G}$ d'un point P est relativement économique parce qu'il exige seulement de contrôler la validité de l'équation de la courbe, tandis que le test d'appartenance d'un point P additionnement à $\mathbb{G}$ exige soit une multiplication scalaire $[n]P$ pour contrôler si P a le bon ordre soit une multiplication par le cofacteur $[h]P$ pour forcer le point à voir le bon ordre. Si le cofacteur est petit, le dernier coût est bas mais pour des grands cofacteurs, il pouvait être plus efficace de ralentir en réalisant n'importe quelles exponentiations quand on travaille avec les paramètres convenables.

Une tentative de définir la notion de sécurité de sous-groupes pourrait être de demander que l'indice h (si $h\neq 1$) contienne des facteurs premiers de taille supérieure ou égale à n, dans quel cas, à la fois les exponentiations sont très coûteux. Cependant dans le cas des Cryptographies basées sur les courbes elliptiques (ECC), ainsi une définition n'a pas de sens, puisque les courbes sont choisies telles que le cofacteur est égal à 1 ou une très petite puissance de 2 (comme 4 ou 8) dépendant du modèle de courbe qui est sélectionné pour des raisons d'efficacité et de sécurité. Alors qu'il y'a des bonnes raisons d'exiger le cofacteur $h=1$, il exclurait non nécessairement des modèles de courbes qui permettent des gains de performance en ayant un petit cofacteur. Donc en demandant seulement des grands facteurs premiers dans h seulement a un sens si le groupe a fondamentalement des larges et incontournables cofacteurs par construction. C'est le cas pour quelques groupes qui donnent des courbes adaptées.

Pour les trois (sous) groupes de couplage $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_T$ définis précédemment, il y'a des choix très naturels de 3 groupes associés $\mathcal{G}_1$, $\mathcal{G}_2$ et $\mathcal{G}_T$ pour lesquels le test d'appartenance est facile. Notamment, nous les définissons comme suit:

$$\mathbb{G}_1\subseteq\mathcal{G}_1=E(\mathbb{F}_p)\quad \mathbb{G}_2\subseteq\mathcal{G}_2=E(F_{p^{(k/d)}})$$

$$G_T \subseteq \mathcal{G}_T = G_{\phi_k(p)}$$

où $G_{\phi_k(p)}$ est le sous-groupe cyclotomique d'ordre $\Phi_k(p)$ dans $F^*_{p^k}$.

Scott choisit également $\mathcal{G}_T$ de cette manière quand des courbes $\mathbb{G}$_T-fort est proposé [14]. Notons que le test d'appartenance dans $\mathcal{G}_1$ ou $\mathcal{G}_2$ simplement ramène à contrôler l'équation de la courbe pour $E(\mathbb{F}_p)$ ou $E'(F_{p^{(k/d)}})$, respectivement, et ce test si un élément est dans $\mathcal{G}_T$ peut également être donné presque sans coût en utilisant le Frobenius" [14, §8.3].

Puisque $|\mathbb{G}_1|=|\mathbb{G}_2|=|\mathbb{G}_T|=n$, les indices h_1, h_2, $h_T \in \mathbb{Z}$ sont ainsi définis:

$$h_1 = \frac{|\mathcal{G}_1|}{n}; \quad h_2 = \frac{|\mathcal{G}_2|}{n}; \quad h_T = \frac{|\mathcal{G}_T|}{n}$$

Les tailles de ces cofacteurs sont déterminées par les propriétés des courbes adaptées. Pour toutes courbes dans cet article, à la fois $\mathbb{G}_2$ et $\mathbb{G}_T$ sont des groupes d'ordre n dans des très grands groupes $\mathcal{G}_2$ et $\mathcal{G}_T$ et les cofacteurs h_2 et h_T sont au moins de taille similaire à n. Le groupe $\mathcal{G}_1$ est typiquement pas aussi grand et vient boucler au cas du groupe utilisé dans l'ECC simple. Donc le cofacteur h_1 est plus petit que n et dans presque tous les cas plus grand que 1.

La prochaine tentative à une définition de sécurité de sous-groupes pourrait demander que pour n'importe quel des trois groupes du couplage pour lesquels le cofacteur est de taille similaire à n ou plus grand, il ne doit pas avoir de facteurs premiers significativement plus petit que n. C'est une définition plus utile puisqu'elle se focalise sur le cas dans lequel des cofacteurs grand existent. Cependant, plus de courbes adaptées ont des instances de familles paramétrisées et leurs paramètres sont dérivés comme l'évaluation des polynômes rationnels en un entier. Et pour certaines familles ces polynômes peuvent également produire nécessairement des petits facteurs dans des indices.

La définition suivant de sécurité de sous-groupes explique ce fait en capturant pour une famille de polynôme donnée de courbes adaptées le meilleur qui peut être réalisé sans cette famille. Nous employons le fait que, pour les familles paramétrisées de l'intérêt dans ce travail, les trois cofacteurs au-dessus sont également paramétrisés comme $h_1(u)$, $h_2(u)$, $h_T(u) \in \mathbb{Q}[u]$.

Définition 1. (sécurité des sous-groupes)

Soient $p(u)$, $t(u)$, $n(u) \in \mathbb{Q}[u]$ paramétrisés une famille de courbes elliptiques adaptées ordinaires et pour tout $u_0 \in \mathbb{Z}$ particulier tel que $p=p(u_0)$ et $n=n(u_0)$ soient premiers, soit E la courbe elliptique adaptée résultante sur $\mathbb{F}_q$ d'ordre divisible par n. Nous disons que E est sous-groupement sûre si tous les cofacteurs $\mathbb{Q}[u]$-irréductible de $h_1(u)$, $h_2(u)$ et $h_T(u)$ qui peuvent représenter des nombres premiers et qui ont des degrés au moins que celui de $n(u)$ et ne contiennent pas de facteurs plus petits que $n(u_0) \in \mathbb{Z}$ quand elles sont évaluées à $u=u_0$.

Il doit être indiqué immédiatement que le libellé de "plus petit que" dans la définition 1 peut être relaxé dans les cas où la différence est relativement étroite. Mettre simplement Définition 1 vise à interdire l'existence de sous-groupe nécessaire de taille plus petite que n dans les grands groupes pour lesquels la validation est facile. Nous notons que pour une simplicité, Définition 1 dit que la sécurité de sous-groupe est dépendante de la courbe adaptée E. Cependant, en donnant que la propriété est dépendante des 3 groupes $\mathbb{G}_1$, $\mathbb{G}_2$ et $\mathbb{G}_T$, il serait plus précise de dire que la propriété est basée sur le "couplage" qui est déterminé par E et n.

7. CONCLUSION

Nous avons montré comme résoudre efficacement le problème de construction des courbes elliptiques à partir de degré de plongement, et avons suggéré de chemins pour implémenter efficacement les courbes qui y proviennent de rendre effectif les courbes résultantes efficacement afin que les cryptosystèmes basés sur les couplages soit pratiques. De plus nous avons défini les mesures prises pour contourner les attaques de petits sous-groupes.

8. REMERCIEMENTS

Nous remercions tous les collègues du Centre de Recherche et de Formation pour l'Industrie Textile pour leurs critiques instructifs et objectifs. Nos remerciements vont également à l'encontre de mes encadrants de la Faculté des Sciences et Techniques de l'USTTB à savoir Pr Karim SAMAKE et Dr Sinaly TRAORE.

REFERENCES

[1] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Constructing elliptic curves with prescribed embedding degrees. In Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano, editors, SCN, volume 2576 of Lecture Notes in Computer Science, pages 257{267. Springer, 2002.

[2] Paulo S. L. M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, and Gustavo Zanon. Subgroup security in pairing-based cryptography 2015

[3] Chae Hoon Lim and Pil Joong Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Burton S. Kaliski Jr., editor, CRYPTO, volume 1294 of Lecture Notes in Computer Science, pages 249-263. Springer, 1997.

[4] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the Weil pairing. In Advances in Cryptology - Asiacrypt 2001, volume 2248 of Lecture Notes in Computer Science, pages 514-532. Springer, 2002.

[5] Serge Vaudenay. Hidden collisions on DSS. In Neal Koblitz, editor, Advances in Cryptology - CRYPTO 96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22,

1996, Proceedings, volume 1109 of Lecture Notes in Computer Science, pages 83-88. Springer, 1996.

[6] Ryuichi Sakai, Kiyoshi Ohgishi, and Masao Kasahara. Cryptosystems based on pairing. In The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, pages 135-148, 2000.

[7] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Kilian [38], pages 213-229.

[8] Antoine Joux. A one round protocol for tripartite Diffie-Hellman. J. Cryptology, 17(4):263-276, 2004.

[9] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate pairing. In Claus Fieker and David R. Kohel, editors, Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings, volume 2369 of Lecture Notes in Computer Science, pages 324-337. Springer, 2002.

[10] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. Efficient implementation of pairing-based cryptosystems. J. Cryptology, 17(4):321-334, 2004.

[11] Alfred Menezes. Asymmetric pairings. Talk at ECC2009. Slides at http://math.ucalgary.ca/ecc/files/ecc/u5/Menezes_ECC2009.pdf.

[12] Sanjit Chatterjee, Darrel Hankerson, Edward Knapp, and Alfred Menezes. Comparing two pairing-based aggregate signature schemes. Des. Codes Cryptography, 55(2-3):141-167, 2010.

[13] Stephen C. Pohlig and Martin E. Hellman. An improved algorithm for computing logarithms over GF(p) and its cryptographic signi¸cance. Information Theory, IEEE Transactions on, 24(1):106-110, 1978.

[14] Michael Scott. Unbalancing pairing-based key exchange protocols. Cryptology ePrint Archive, Report 2013/688, 2013. http://eprint.iacr.org/2013/688.

[15] R. Lidl and H. Niederreiter, "Introduction to finite fields and their applications, "Cambridge University Press, 1986.

[16] N. P. Smart, "The Algorithmic Resolution of Diophantine Equations," London Mathematical Society Student Text 41, Cambridge University Press, 1998.

[17] N. Tzanakis, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations," Acta Arithmetica 75 (1996), pp. 165–190.

[18] A. Agashe, K. Lauter, and R. Venkatesan, "Constructing elliptic curves with a known number of points over a prime field," High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series, Vol. 42, 2002, pp. 1–17.

[19] J. H. Silverman, "Elliptic curve discrete logarithms and the index calculus," Workshop on Elliptic Curve Cryptography (ECC'98), September 14–16, 1998.

[20] P. S. L. M. Barreto, H. Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," Advances in Cryptology – Crypto'2002, Lecture Notes in Computer Science 2442, pp. 354–368, Springer-Verlag, 2002.