Universitatea din Craiova
Facultatea de Ştiinţe
Şcoala Doctorală de Ştiinţe

Teză de Doctorat

Rezumat

Autor:
Oana Adriana ŢICLEANU

Coordonator ştiinţific:
Prof. Univ. Dr. Vicenţiu RĂDULESCU

Craiova, 2015

Universitatea din Craiova
Facultatea de Ştiinţe
Şcoala Doctorală de Ştiinţe

Procese neliniare peste curbe eliptice nonsupersingulare cu aplicaţii în criptografie

Autor:
Oana Adriana ŢICLEANU

Coordonator ştiinţific:
Prof. Univ. Dr. Vicenţiu RĂDULESCU

Craiova, 2015

Rezumat teză

Studiul curbelor eliptice are o istorie bogată care demonstrează încă odată frumuseţea matematici pure, teoretice şi modalităţile în care aplicabilitatea ei iese la iveală după definirea unor noi concepte care la început sunt percepute de societatea ştiinţifică precum concepte abstracte dar în momente ulterioare ale istoriei ştiinţei se vede că acel model a fost o premoniţie matematică de formalizare a unui concept din natură.

Astfel, unele propietăţi ale sistemelor bazate pe spaţii eliptice sunt datate din ultimul secol, dar modelari în acest sens sunt datate cu mult înainte, prin studiul ecuaţiilor diofantice (secolul III, matematicianul elen A. Diophantus). Evidenţierea şi recunoaşterea acestui domeniu a venit odată cu articolele matematicienilor N. Koblitz ([46]) şi V. Miller ([61]) care au ilustrat o aplicabilitate a acestora în domeniul criptosistemelor asimetrice.

Se pleacă de la definirea unei curbe eliptice care este dată de ecuaţia lui Weierstrass:

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

unde $a_i \in K$ si K este spaţiul peste care curba E este definită. Aceste curbe pot fi împărţite în două clase şi anume cele care sunt supersingulare şi curbe eliptice non-supersingulare ([2]) cu aplicabilităţi de actualitate ([20]).

1. O curbă supersingulară (zero j-invariant) este setul de soluţii al ecuaţiei:

$$y^2 = x^3 + ax + b \tag{2}$$

   unde $a, b, c \in GF(2^k)$, iar discriminantul este $\Delta = 4a^3 + 27b^2 \neq 0$, împreună cu punctul la infinit $\mathcal{O}$.

2. O curbă eliptică non-supersingulară (nonzero j-invariant) este setul de soluţii al ecuaţiei:

$$y^2 + xy = x^3 + ax^2 + b \tag{3}$$

   unde $a, b, c \in GF(2^k)$, iar discriminantul este $\Delta \neq 0$, împreună cu punctul la infinit $\mathcal{O}$.

Perechi de puncte de pe o astfel de curbă, care au un set de propietăţi particulare, împreună cu un scalar, sunt de fapt cheile asimetrice folosite în criptografia modernă.

De aici, numeroşi matematicieni au studiat modalităţile de obţinere a unor spaţii cu propietăţi în acest sens ([2], [81], [88]) şi optimizări ale modelului prin

adăugarea de condiţii la limita unor sisteme de ecuaţii neliniare care au soluţii la frontieră, acestea fiind de fapt parametrii necesari în condiţii reale din cadrul securizării fluxului informaţional ([3]).

Firul roşu care a parcurs studiile este acela că dincolo de implementări optimale, complexităţi ale algoritmilor folosiţi şi putere de calcul, s-a demonstrat că singurele modele rezistente la atacuri criptografice au fost cele al căror aparat matematic era bazat pe construcţia unor subspaţii cu particularităţi ce le făceau ca mulţimea soluţiilor la frontieră să fie caracterizată de un sistem de ecuaţii diferenţiale care sunt definite peste curbe eliptice, cu definirea izomorfismelor de tip Frobenius ([21], [86]).

Studii precum modalităţi de calcul ale parametrilor implicaţi, izomorfisme care definesc părţile componente ale modelelor implicate şi, mai ales, spaţii particulare peste care sunt definite curbele eliptice, studiul analizei diferenţiale cât şi soluţiile la frontieră pentru ecuaţii diferenţiale peste curbe eliptice, toate acestea au definit cercetările care au urmat şi domeniile în care sunt probleme deschise din punct de vedere al aplicabilităţii. În domeniul spaţiilor particulare peste care sunt definite curbele eliptice şi soluţiile la frontieră pentru sisteme diferenţiale cu aplicabilitate în sisteme neliniare de analiză a rezistenţei la atacuri pentru modelele criptografice, în acest sens am studiat, construit, algoritmizat şi implementat soluţii personale pentru unele probleme deschise în domeniul matematicii aplicate în criptografie.

Plecând de la clasificarea modalităţilor de construcţie a câmpurilor peste care sunt definite curbele eliptice clasice, sunt descrise în capitolul 2 construcţia ecuaţiilor peste curbe eliptice, modalităţile de calcul a parametrilor implicaţi în spaţii finite de tipul $GF(2^k)$, cu aplicabilităţi în domeniul curbelor eliptice nonsupersingulare, rezultate care au fost publicate în articolul ([20]).

În cadrul acestui capitol sunt descrise soluţii personale, optimizate, de calcul diferenţial al parametrului p al unei curbe eliptice precum şi studiile efectuate asupra nivelului de infeasibilitate al modelului matematic studiat, prezentate în algoritmul 1 (rezultate publicate in [19]). Fie Γ submulţimea punctelor de pe o curbă eliptică pentru care s-a calculat inversul, χ inversul unui număr ϕ, t nivelul de diferenţiere (va defini gradul de siguranţă al sistemului generat).

Algoritm 1 Calculul diferenţial al parametrului p al unei curbe eliptice

1. $\phi_0 \leftarrow \lfloor \chi/b^t \rfloor, \phi_0 \leftarrow \phi - \theta_0 b^t,\ \phi \leftarrow \phi_0,\ i \leftarrow 0,\ \xi \leftarrow \phi_0$
2. Atâta timp cât $\xi > 0$ execută
3. $\quad \theta_{i+1} \leftarrow \lfloor \theta_i/\xi^t \rfloor,\ \phi_{i+1} \leftarrow \theta_i a - \theta_{i+1}\frac{b^t}{\xi}$
4. $\quad i \leftarrow i+1,\ \phi \leftarrow \phi + \phi_i,\ \xi \leftarrow \left\lfloor \frac{b^t}{\phi_i} \right\rfloor$
5. Atâta timp cât $\phi \geq p$ execută $\phi \leftarrow \phi - \left\lfloor \frac{p}{\chi} \right\rfloor$

În acest fel, funcţia de reducere va folosi doar operaţii de shift-are în vederea definirii gradului submulţimii punctelor cu propietăţi criptografice.

Calculul clasic al parametrilor aflaţi în sisteme implementate în practică foloseşte RNSA(Residue Number System Arithmetic = Sistemul aritmetic de numere reziduale).

În capitolul 3 a fost studiată modalitatea de determinare a subspaţiilor finite particulare cu propietăţi criptografice avansate, rezultatele fiind publicate în ([21]). Astfel, s-a descris modul în care se fac operaţiile peste curbele eliptice, caracteristicile pe care trebuie să le îndeplinească un spaţiu pentru a fi rezistent la atacuri criptografice şi au fost studiate căile folosite pentru analiza criptografică a unui model matematic al sistemului criptografic de acest tip. Pentru modelele dezvoltate, definite peste subspaţii particulare cu aplicabilitate în domeniul măririi complexităţii de atac, au fost studiate endomorfismele peste câmpurile finite definite în capitolul 2 şi implicaţiile date de ecuaţiile diferenţiale care întervin în analiza neliniară a sistemului criptografic, rezultatele fiind publicate în articolul ([22]). Modelele descrise îşi au originea din studiul problemelor existente în unele sisteme de extragere automată a unor parametrii, studii efectuate şi ale căror rezultate au fost publicate în ([24]). Din rezultatele acestor studii au fost concluzionate modalităţi de optimizare a unor modele de construcţie a algoritmilor implicaţi în calculul parametrilor necesari în determinarea soluţiilor de interes ale ecuaţiilor diferenţiale definite peste curbe eliptice, astfel în cadrul acestui capitol au fost construite variante personale de implementări optime pentru:

Transformarea nonsupersingularei $\mathbb{Z}_q^p$ pentru invariantul j

Din ecuaţiile descrise de către [40] se poate concluziona că matricea Jacobiană este inversabilă peste câmpul $\mathbb{Z}_q$ şi $\delta = ((D\Theta)^{-1}\Theta)(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{Z}_q^n$, deoarece $(D\Theta)(x_0, \ldots, x_{n-1})(modulo\ p)$ este diagonala matricei cu elemente nenule. Se deduce că putem aplica metoda lui Gauss de eliminare, în rezolvarea ecuaţiei

$$(D\Theta)(x_0, \ldots, x_{n-1})\delta = \Theta(x_0, \ldots, x_{n-1})$$

în care propietatea ce permite acest lucru este aceea că elementele diagonalei sunt inversabile. Se va calcula pe fiecare linie, mutându-se elementul din partea stângă-jos, $\Phi'_p(x_0, x_{n-1})$, spre dreapta. După efectuarea a k operaţiuni de acest tip, elementul va putea fi scris:

$$(-1)^k \Phi'_p(x_0, x_{n-1}) \prod_{\mathrm{i}=0}^{k-1} \frac{\Phi'_p(x_{i+1}, x_i)}{\Phi'_p(x_i, x_{i+1})},$$

care se poate demonstra că este divizibil cu p^k de la $\Phi'_p(x_{i+1}, x_i) \equiv 0(modulo\ p)$. Plecând de la procedura standard am construit un model de calcul al invariantului j peste un subspaţiu nonsupersingular al unei curbe eliptice standard, definind astfel o submulţime de puncte standard care pot fi sisteme de soluţii pentru chei criptografice, şi pentru care calculul se va face conform unei proceduri de extragere care va fi definită în cadrul algoritmului pe care l-am creat în acest sens, implementarea 3 (rezultate publicate in [19]). Transformarea nonsupersingularei este descrisă în algoritmul 2.

Metodă neliniară de calcul a numărului de puncte cu propietăţi criptografice - SatOT

Plecând de la modelul demonstraţiilor lui Satoh, am dezvoltat o metodă de calcul a subspaţiilor de puncte peste o curba eliptică ce are caracteristica p şi numărul de puncte caracterizat de $\overline{F_{OT}} : \overline{E}(\overline{\mathbb{F}}_q) \to \overline{E}(\overline{\mathbb{F}}_q) : (x, y) \longmapsto (x_p^q, y_p^q)$, unde vom defini numărul de puncte criptografice de grad 1 ca fiind soluţiile slabe ale punctelor criptografice, puncte care pot fi chei pentru sisteme de tip ECC. Acest sistem de puncte asigură un subspaţiu care are o complexitate de calcul mai mică la generarea punctelor păstrând complexitatea de atac asupra ECDLP la acelaşi nivel, descris în implementarea 3 (rezultate publicate in [19]).

Algoritm 2 Transformarea nonsupersingularei $\mathbb{Z}_q^p$ pentru invariantul j

Intrare: Sistemul $j_i^P \in \mathbb{F}_q^P \backslash \mathbb{F}_{p^2}$ cu $\Phi_p(j_i^P, j_{i+1}^P) \equiv 0(modulo\ p)$ pentru $0 \leq i \leq n'$ şi precizia $m|n$.
Iesire: Sistemul $j_i^q \in \mathbb{Z}_q$ cu $\Phi_p(J_i^P, J_{i+1}^P) \equiv 0(modulo\ p^m)$?i $J_i^q \equiv j_i(modulo\ p)$ pentru orice $0 \leq i < n'$.

1. Pentru $m = 1$ la n' execută
2. Dacă $j_i^m \neq 0$ atunci
3. $J_i \leftarrow j_i^m$
4. altfel
5. $m' \leftarrow \left\lceil \frac{m}{2} \right\rceil \cdot \left\lceil \frac{p}{2} \right\rceil, M \leftarrow m',\ M' \leftarrow \frac{P}{q}$.
6. $(J_0^P, \ldots, J_{n'-1}^P)$ va fi determinat prin inversarea canonică a $((j_0^P, \ldots, j_{n'-1}^P), m')$.
7. Pentru $i = 0$ la $n' - 2$ execută
8. $t \leftarrow \Phi_p'(J_i^P, J_{i+1}^P)^{-1}(mod\ p^M)$.
9. $D_i \leftarrow t\Phi_p'(J_{i+1}^P, J_i^P)(mod\ p^M)$.
10. $P_i \leftarrow t((\Phi_p(J_i^P, J_{i+1}^P)(mod\ p^m))/p^M \cdot \frac{1}{p^{M'}})(mod\ p^M)$
11. $R \leftarrow \Phi_p'(J_0^P, J_{n-1}^P)(mod\ p^{M'})$.
12. $S \leftarrow (((\Phi_p(J_{n-1}^P, J_0^P)(mod\ p^{M'})))/p^{M'})(mod\ p^M)$.
13. Dacă $S \neq 0$ atunci
14. Pentru $i = n' - 2$ la 0 cu pas -1 execută
15. $\varphi_i \leftarrow \varphi_i - D_i\ P_{i+1}^P(mod\ p^{M'})$
16. altfel
17. Pentru $i = 0$ la $m' - 1$ execută
18. $J_i^P \rightarrow J_i^P - p^{M'} P_i^P(mod\ p^{M'})$
19. Returnează $(J_0^P, \ldots, J_{n'-1}^P)$.

Algoritm 3 Metodă neliniară de calcul a numărului de puncte cu propietăţi criptografice - SatOT

Intrare: Nonsupersingulara $\overline{E}_p$, derivată din $\overline{E} : y^2 = x^3 + ax + b$ definită peste subspaţiul $\mathbb{F}_{p^n}^q$, $j(\overline{E}_{OT}) \notin \mathbb{F}_{p^2}$.
Ieşire: Numărul de puncte cu proprietăţi criptografice de grad 1, de pe curba $\overline{E}(\mathbb{F}_{p^n}^q)$.

1. Pentru toate punctele din $\overline{E}$, calculează submulţimea $\overline{E}_p$, ca un izomorfism al canonicului faţă de q, folosind algoritmul 2.
2. Dacă m are valoarea 1 atunci
3. Pentru $i = 0$ la $n - 1$ execută
4. $J_i \leftarrow j_i^q$
5. altfel
6. $m' \leftarrow \lceil \frac{m}{2} \rceil \ \lceil \frac{p}{2} \rceil$, $M' \leftarrow (m - m')(mod\ q)$.
7. $(J_0^q, \ldots, J_{n-1}^q) \xleftarrow{2} ((j_0^q, \ldots, j_{n-1}^q), M')$.
8. Pentru $i = 0$ la $n - 2$ execută
9. $t \leftarrow \Phi'_p(J_i^q, J_{i+1}^q)^{-1}(mod\ p^{M'})$.
10. $D_i \leftarrow t\Phi'_p(J_{i+1}^q, J_i^q)(mod\ p^{M'})$.
11. $P_i \leftarrow t((\Phi_p(J_i^q, J_{i+1}^q)(mod\ p^{M'}))(mod\ p^m))$.
12. $R \leftarrow \Phi'_p(J_0^q, J_{n-1}^q)(mod\ p^{M'})$.
13. $S \leftarrow (((\Phi_p(J_{n-1}^q, J_0^q)(mod\ p^{M'})))/p^m)(mod\ p^M)$.
14. Dacă oricare dintre D_i este determinat de un punct din afara nonsupersingularei, se elimină acel punct.
15. Pentru $i = 0$ la $min(M', n - 2)$ execută
16. $S \leftarrow S - RP_i(mod\ p^{M'})$
17. $R \leftarrow -RD'_i(mod\ p^{M'})$
18. $R^q \leftarrow R + \Phi'_p(J_{n-1}^q, J_0^q)(mod\ p^{M'})$.
19. $P_{n-1}^q \leftarrow SR^{-1}(mod\ p^{M'})$.
20. Dacă oricare P caracterizează un punct din afara nonsupersingularei, se reia de la pasul 6.
21. Pentru $i = n - 2$ la 0 cu pas -1 execută
22. $P_i \leftarrow P_i - D_i\ P_{i+1}^q(mod\ p^{M'})$.
23. Pentru $i = 0$ la $n - 1$ execută
24. $J_i^q \leftarrow J_i^q - p^{M'} \cdot P_i/D'_i(mod\ p^{M'})$.
25. Returnează $(J_0^q, \ldots, J_{n-1}^q)$.

Tranformarea Primului Invariant j

Aplicarea în mod repetat a propietăţii lui Vercauteren se poate efectua şi asupra spaţiului nonsupersingularei F_p^q, în calculul invarantei j^q, rezultând

implementarea din 4 (rezultate publicate in [19]).

Algoritm 4 Tranformarea Primului Invariant j

Intrare: Un j^q invariant $j \in \mathbb{F}_{p^n}^q/\mathbb{F}_{p^2}$ şi precizia m' conform algoritmului 2.
Ieşire: $J^q \in \mathbb{Z}_q$ cu $J^q \equiv j^{p^{m-1}}(modulo\ p)$ si $\Phi_p(J^q, \Sigma(J^q)) \equiv 0(modulo\ p^m)$.

1. $J^q \leftarrow jm'\ (mod\ p)$.
2. Pentru $i = 2$ la m execută
3. $\quad J^q \leftarrow$ Newton_Iteration $(\Phi_p(X, J), J^p J^q\ (mod\ p), i)$.
4. Dacă J^q are caracteristici din afara nonsupersingularei atunci
5. $\quad$ reia de la pasul 1.
6. Returnează J^q.

Varianta simplificată a SST pentru nonsupersingulara $\mathbb{F}_p^q$

Substituţia inversei Frobenius Σ^{-1} are ca modalitate de rezolvare

$$\Sigma^{-1}(\alpha) = \Sigma^{-1}\left(\sum_{\mathrm{i}=0}^{n-1}\alpha_i t^i\right) = \sum_{\mathrm{j}=0}^{p-1}\left(\sum_{0\le \mathrm{pk+j}<\mathrm{n}}\alpha_{pk+j}t^k\right)C_j(t),$$

unde $C_j(t) = \Sigma^{-1}(t^j) \equiv t^{jp^{n-1}}(modulo\ f(t))$. Dacă vom calcula înainte $C_j(t)$ pentru $j = 0, \ldots, p-1$, calculul lui $\Sigma^{-1}(\alpha)$ pentru $\alpha \in \mathbb{Z}_q$ va conţine numai $p-1$ înmulţiri în $\mathbb{Z}_q$.

Plecând de la această cale de rezolvare, H.Y. Kim, J.Y. Park, J. Cheon, J.H. Park, J.H. Kim şi S. Hahn [44] au scos în evidenţă posibilitatea utilizării unor câmpuri finite cu o bază Gaussian normală (GNB) de tip mic. Această bază se poate transfera la $\mathbb{Z}_q$ şi în acest mod se poate optimiza calculul iteraţiilor Frobenius deoarece B din $\mathbb{Q}_q/\mathbb{Q}_p$ este normală dacă $\exists\beta \in \mathbb{Q}_q$ astfel încât $B = \{\Lambda(\beta)|\Lambda \in Gal(\mathbb{Q}_q/\mathbb{Q}_p)\}$. De aici se deduce următoarea propoziţie, cu implicaţii directe în aflarea punctelor de interes criptografic, a cărei demonstraţie poate fi găsită în [44].

Propoziţia 0.1. Fie p un număr prim şi n, t doi întregi pozitivi astfel încât $nt+1$ este un prim diferit de p. Fie γ o rădăcină primitivă de ordinul $nt+1$ a unitaţii într-o extensie a câmpului $\mathbb{Q}_p$. Dacă $gcd(nt/e, n) = 1$, cu e ordinul lui p modulo $nt+1$, atunci pentru orice rădăcină primitivă de ordinul t a unităţii τ in $\mathbb{Z}/(nt+1)\mathbb{Z}$ de forma

$$\beta = \sum_{\mathrm{i}=0}^{t-1}\gamma^{\tau^i}$$

este un element normal şi $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] = n$. O astfel de bază este numită o bază Gaussian normală de tipul t.

În lucrarea [44] sunt prezentate valorile din $\mathbb{Z}_q$ ca fiind elemente ale inelului

$$\mathbb{Z}_p[x]/(x^{nt+1}-1).$$

Produsul a două elemente $\mathbb{Z}_q/(p^m\mathbb{Z}_q)$ va necesita un număr de operaţii de complexitate $O((nmt)^\mu)$, reducându-se conform propoziţiei precedente la $t \leq 2$.

Pentru $t = 1$ avem $\beta = \tau$ şi polinomul minimal al lui β este

$$f(x) = \frac{x^{n+1}-1}{x-1} = x^n + x^{n-1} + \ldots + x + 1.$$

Reducerea complexităţii de calcul din substituţia Frobenius, conform H.Y. Kim, este posibilă prin utilizarea unei reprezentări redundante, prin folosirea unei incluziuni, $\mathbb{Z}_q$ din $\mathbb{Z}_p[x]/(x^{n+1}-1)$, ceea ce se concluzionează în $\alpha = \sum_{\mathrm{i}=0}^{n-1} \alpha_i \beta^i$ în $\alpha(x) = \sum_{\mathrm{i}=0}^{n-1} \alpha_i x^i + 0x^n$. Atunci $\Sigma^k(\beta) = \beta^{p^k}$, ceea ce ne duce la

$$\Sigma^k(\alpha(x)) = \sum_{\mathrm{i}=0}^{n} \alpha_i x^{ip^k} = a_0 + \sum_{\mathrm{j}=1}^{n} \alpha_{j/p^k} (modulo\ (n+1))^{x^j}.$$

Rezultatul obţinut va determina obţinerea $\Sigma^k(\alpha)$ permutând coeficienţii lui $\alpha(x)$, cu o complexitate de calcul de ordinul $O(n)$. Aceasta determină modalitatea de calcul a sistemelor de tipul Satoh-Skjernaa-Taguchi peste curbe eliptice care conţin puncte criptografice de grad 1.

Dacă avem $\Gamma(X, \Sigma(X)) = 0$, şi $x \in \mathbb{Z}_q$ o rădăcină a sa, pentru $\Gamma(X, Y) \in \mathbb{Z}_q[X, Y]$, vom calcula o aproximare $x_m \equiv x(modulo\ p^m)$ şi definim $\delta_m = (x - x_m)/p^m$, în acest mod dezvoltarea în serie Taylor pentru x_m va determina:

$$\begin{aligned} 0 &= \Gamma(x, \Sigma(x)) = \Gamma(x_m + p^m\delta_m, \Sigma(x_m + p^m\delta_m)) \\ &\equiv \Gamma(x_m, \Sigma(x_m)) + p^m(\delta_n\Delta_x + \Sigma(\delta_m)\Delta_y)(modulo\ p^{2m}), \end{aligned} \tag{4}$$

unde $\Delta_x \equiv \frac{\partial\Gamma}{\partial X}(x_m, \Sigma(x_m))(modulo\ p^m)$ si $\Delta_y \equiv \frac{\partial\Gamma}{\partial Y}(x_m, \Sigma(x_m))(modulo\ p^m)$, iar $\Gamma(x_m, \Sigma(x_m)) \equiv 0(modulo\ p^m)$ deci simplificând prin p^m se obţine relaţia

$$\frac{\Gamma(x_m, \Sigma(x_m))}{p^m} + \delta_m\Delta_x + \Sigma(\delta_m)\Delta_y \equiv 0(modulo\ p^m). \tag{5}$$

pentru δ_m modulo p^m.

În vederea obţinerii punctelor de gradul 1 este suficient ca $ord_p(\Delta_y) = 0$, adică Δ_y este o unitate în $\mathbb{Z}_q$ si ca $ord_p(\Delta_x) > 0$. Efectuând operaţia de reducere modulo p pentru ecuaţia (5), va rezulta

$$\delta_m^p = -\frac{\Gamma(x_m, \Sigma(x_m))}{p^m\Delta_y}(modulo\ p) \tag{6}$$

care are o rădăcină de ordinul p (unică), $\delta_m \in \mathbb{F}_q$, se obţine o aproximare a lui x, care este mai eficientă, dată de $x_m + p^m\delta_m \equiv x(modulo\ p^{m+1})$. Rădăcina de ordin p are o complexitate de calcul de ordin mare şi au fost date soluţii de simplificare în acest sens (Satoh, Skjernaa şi Taguchi) prin înlocuirea în ecuaţia $\Gamma(X, \Sigma(X)) = 0$ cu $\Gamma(\Sigma^{-1}(X), X) = 0$. Astfel δ_m va fi definit ca:

$$\delta_m \equiv -\frac{\Gamma(\Sigma^{-1}(x_m), x_m)}{p^m \frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_m), x_m)}(modulo\ p).$$

Din $\Gamma(\Sigma^{-1}(x_m), x_m) \equiv 0(modulo\ p^m)$ este necesară doar aflarea inversei lui $\frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_m), x_m)$ modulo p. Implementând această metodă vom determina Algoritmul 5, ce poate înlocui metoda clasică a lui Satoh [76] pentru nonsupersingulara $\mathbb{F}_p^q$, implementarea fiind în 5 (rezultate publicate in [19]).

Algoritm 5 Varianta simplificată a SST pentru nonsupersingulara $\mathbb{F}_p^q$

Intrare: Polinomul $\Gamma(X, Y) \in \mathbb{Z}_q$, elementul $x_0 \in \mathbb{Z}_q$ satisface $\Gamma(\Sigma^{-1}(x_0), x_0) \equiv 0(modulo\ p)$ şi precizia m.
Ieşire: Elementul $x_m \in \mathbb{Z}_q$ cu $\Gamma(\Sigma^{-1}(x_m), x_m) \equiv 0(modulo\ p^m)$ si $x_m \equiv x_0(modulo\ p)$.

1. Pentru $i = 2$ la m execută
2. $\quad x_m^q(i) \leftarrow$ ALG 4(x_m, m)
3. Dacă $x_m^q(i)$ nu se află pe nonsupersingulară atunci
4. $\quad$ Se reia pasul 1
5. $d \leftarrow \left(\frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_0), x_0)\right)^{-1}\ (mod\ p)$.
6. $y \leftarrow x_0(mod\ p)$.
7. Pentru $i = 0$ la m execută
8. $\quad x \leftarrow \left\lfloor \frac{\Sigma^{-1}(y)(mod\ p^i)}{x_m^q(i)} \right\rfloor$.
9. $\quad y \leftarrow y - d\Gamma(x, y)(mod\ p^i)$.
10. Returnează y.

Complexitatea algoritmului clasic este dată de apelul la fiecare iteraţie în vederea recalculării $\Gamma(x, y)$ deşi valorile lui x şi y la pasul $i + 1$ sunt foarte apropiate de cele de la pasul i, pe când în soluţia dată în 5 se foloseşte aproximare celor doi parametrii şi se consideră numai subspaţiul nonsupersingular. După determinarea $x_W \equiv x(modulo\ p^W)$ asociată unui W se consideră elementele $s \in \mathbb{N}$, pentru care

$$\Gamma(\Sigma^{-1}(x_{sW+i}), x_{sW+i}) \equiv \Gamma(\Sigma^{-1}(x_{sW}), x_{sW}) + \Delta(modulo\ p^{(s+1)W}), \qquad (7)$$

cu

$$\Delta = p^{sW}\left(\frac{\partial\Gamma}{\partial X}(\Sigma^{-1}(x_{sW}), x_{sW})\Sigma^{-1}(\delta) + \frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_{sW}), x_{sW})\delta\right).$$

Necesarul în aflarea soluţiilor se reduce la calculul derivatelor parţiale

$$\frac{\partial \Gamma}{\partial X}(\Sigma^{-1}(x_{sW}), x_{sW}) \quad \text{şi} \quad \frac{\partial \Gamma}{\partial Y}(\Sigma^{-1}(x_{sW}), x_{sW})$$

în cazul modulo p^W.

Pentru $\Gamma(\Sigma^{-1}(x_{sW}), x_{sW})$ şi $i < W$ se poate determina $\Gamma(\Sigma^{-1}(x_{sW+i}), x_{sW+i})$, utilizând ecuaţia (7).

Varianta algoritmului SatSk-Taguchi pentru nonsupersingulara $\mathbb{F}_q$

Plecând de la descrierile parametrilor nonsupersingularelor din algoritmul 2 şi modalitatea de calcul a punctelor de pe nonsupersingulară, luând în calcul ecuaţia (7) pentru a determina fiecare actualizare a $\Gamma(x, y)$, am determinat un model de calcul al elementului x_m, pentru subspaţiul invarianţilor care nu pot fi deduşi direct în analiza criptografică a sistemului ANG, ilustrat în 6.

Algoritm 6 Varianta a algoritmului SatSk-Taguchi pentru nonsupersingulara $\mathbb{F}_q$

Intrare: Polinomul $\Gamma(X, Y) \in \mathbb{Z}_q$, elementul $x_0 \in \mathbb{Z}_q$ satisface $\Gamma(\Sigma^{-1}(x_0), x_0) \equiv 0(modulo\ p)$ şi precizia m. Canonicul sistemului $(J_0^q, \ldots, J_{n-1}^q)$, obţinut conform algoritmului 2.
Ieşire: Elementul $x_m^q \in \mathbb{Z}_q$, cu $\Gamma(\Sigma^{-1}(x_m^q), x_m^q) \equiv 0(modulo\ p^m)$ si $x_m^q \equiv x_0(modulo\ p)$.

1. $y \leftarrow ALG5(x_0, W)$.
2. $x \leftarrow \Sigma^{-1}(mod\ p^W)$.
3. $\Delta_x \leftarrow \frac{\partial \Gamma}{\partial X}(x, y)(mod\ p^W)$.
4. $\Delta_x \leftarrow \frac{\partial \Gamma}{\partial Y}(x, y)(mod\ p^W)$.
5. Pentru $s = 1$ la $\lfloor (m-1)/W \rfloor$ execută
6. $\quad x \leftarrow \Sigma^{-1}(y)(mod\ p^{(s+1)W})$.
7. $\quad V \leftarrow \Gamma(x, y)(mod\ p^{(s+1)W})$.
8. $\quad$ Pentru $i = 0$ la $W - 1$ execută
9. $\quad\quad \delta_y \leftarrow -dp^{-(sW+1)}V(mod\ p)$.
10. $\quad\quad \delta_x \leftarrow \Sigma^{-1}(\delta_y)(mod\ p^{W-i})$.
11. $\quad\quad y \leftarrow y + p^{sW+i}\delta_y(mod\ p^{(s+1)W})$.
12. $\quad\quad V \leftarrow V + p^{(sW+i)}(\Delta_x\delta_x + \Delta_y\delta_y)(mod\ p^{(s+1)W})$.
13. Returnează y.

Satoh, Skjernaa şi Taguchi demostrează că pentru $W \cong n^{\mu/(1+\mu)}$, varianta pentru o curbă eliptică oarecare a algoritmului 6 are o complexitate de calcul de ordinul $O(n^\mu m^{\mu+1/(1+\mu)})$. În implementările eficiente se consideră a se determina numai acei W care sunt multipli ai dimensiunii structurii interne a procesoarelor utilizate.

În capitolul 4 au fost studiate deficienţe matematice în calculul parametrilor peste curbe eliptice, mai exact subspaţiile neconcludente din punct de vedere criptografic, pentru a scoate în evidenţă care sunt acele subspaţii optime în sistemele criptografice, cât şi exemplificări de implementare în practică, rezultate publicate în [23], astfel pentru a obţine informaţii despre punctele de torsiune m trebuie să examinăm funcţiile raţionale g_m şi h_m, care au ca soluţii aceste puncte. Oricum, nu avem informaţii despre zerourile lor şi soluţiile sunt cel puţin duble pentru m prime între ele (cu p). Această secţiune are ca scop clarificarea acestui model prin definirea funcţiilor raţionale cu zerouri simple (exact în punctele de torsiune m) şi soluţiile doar din $\mathcal{O}$. Dacă o astfel de funcţie există, aceasta trebuie să fie un polinom. Prin izomorful lui E cu partea de grad zero a grupului Picard, un astfel de polinom există dacă punctele de torsiune m se adună şi au ca rezultat $\mathcal{O}$. Acesta este într-adevar cazul pentru m şi p prime între ele: pentru orice punct P de torsiune m, inversa lui $\bar{P}$ este un punct de torsiune m. Aşadar, suma tuturor punctelor de torsiune m ce nu sunt de ordinul 2 este $\mathcal{O}$. Dacă $E[m]$ conţine un punct de ordinul 2, atunci m trebuie să fie par, $E[2] \subseteq E[m]$ şi $p \neq 2$. În acest caz sunt trei puncte de ordinul 2, cu suma $\mathcal{O}$, deoarece există o funcţie raţională cu divizorul $\langle E[2] \rangle - 4 \langle \mathcal{O} \rangle$, mai exact dreapta $2Y + a_1X + a_3$.

În capitolul 5 sunt aduse contribuţii în domeniul subspaţiilor particulare definite peste curbe eliptice nonsupersingulare cu aplicaţii în calculul parametrilor folosiţi în criptarea fluxului informaţional, astfel pentru toate criptosistemele bazate pe curbe eliptice, definite de endomorfisme pentru sisteme generale, conform modelelor matematice definite de Menezes, Okamoto şi Vanstone, se pot crea particularizări, cu respectarea teoremei lui Hensel, care să aducă îmbunătăţiri modelării cheilor folosite în sisteme informaţionale înalt securizate. Astfel, mesajul care va fi transmis este transformat în unul sau mai multe puncte (în funcţie de lungimea mesajului) de pe curba eliptică utilizată. În implementările reale am folosit un sistem bazat pe algoritmii 2 şi 3, care necesită în calculul lor algoritmul 4, algoritmi propii, dezvoltaţi prin optimizarea celor descrişi de Satoh, pentru cazul în care setul de curbe eliptice luate în calcul sunt nonsupersingulare, prin aceasta determinând o mai mare complexitate a analizei criptografice asupra ECDLP. Pentru a determina modalitatea de atac asupra sistemului, de analiză criptografică diferenţială, vom defini gradual termenii implicaţi şi soluţia de reducere a problemei la una de complexitate de calcul redusă, prin reducerea modelului matematic la cazuri particulare care trebuiesc calculate. O metodă de calcul care se foloseşte pentru curbe eliptice generale a fost propusă de Koblitz în [48] şi plecând de la această soluţie am dezvoltat o metodă proprie, pentru sisteme nonsupersingulare, care foloseşte implementările dezvoltate în capitolul 3, în vederea obţinerii dezideratului final: mesajul criptat. În acest sens se consideră parametri de domeniu care definesc

curba eliptică $(\mathcal{F}, \phi, \alpha_E, \beta_E, \Gamma, \rho, \xi)$, η un parametru care depinde de sistemul pe care se implementează şi $\mu = \mu_1, ..., \mu_n$, mesajul în clar. Paşi necesari în această construcţie, pentru fiecare $\mu_j,\ j = 1, ..., n$ sunt:

1. Se consideră μ_j un număr întreg cu propietatea că $0 \leq \mu \leq \frac{p}{\eta} - 1$
2. Fie $x_i = \eta\mu_j + i$ unde $i = 0, 1, 2 \ldots, (\eta - 1)$
3. Se obţine $c_i = x_i^3 + \alpha_E x_i + \beta_E$ prin operaţii recursive până când $c_i^{\frac{\phi-1}{2}} \equiv 1(mod\ \phi)$
4. ALG 6(Γ, c_i)
5. Se calculează $y_i = \sqrt{c_i}$
6. $\mathcal{M}(x_i, y_i) = (x_i, y_i^{(\phi+1)/4})$ este punctul de pe curba eliptică care corespunde mesajului μ_j.

Aceasta este metoda de obţinere a unor criptări pentru sisteme criptografice bazate pe parametrii definiţi peste curbe eliptice nonsupersingulare, ea folosind modelele matematice şi implementările dezvoltate pe parcursul tezei.

Întreaga lucrare are un caracter de studiu fundamental şi de evidenţiere a aplicabilităţii cercetării, prin soluţiile algoritmice personale date în cazurile particulare definite peste curbele eliptice nonsupersingulare.

Bibliografie

[1] L.M. Adleman, J. DeMarrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields. In LeonardM. Adleman and Ming-Deh Huang, editors, Algorithmic Number Theory, volume 877 of Lecture Notes in Computer Science, pages 28–40. Springer Berlin Heidelberg, 1994.

[2] G.B. Agnew, R.C. Mullin, and S.A. Vastone. An implementation of elliptic curve cryptosystems over $f_{2^{155}}$. IEEE Journal on Selected areas in Communications, 5(11):804–813, June 1993. 1

[3] R. Alsaedi, N. Constantinescu, and V. Radulescu. Nonlinearities in elliptic curve authentication. Entropy, 16(9):5144—5158, September 2014. 2

[4] A.O.L. Atkin. The number of points on an elliptic curve modulo a prime, 1992. Series of emails to the NMBRTHRY mailing list.

[5] R. Avanzi, W.D. Benits, S.D. Galbraith, and J. Mckee. On the distribution of the coefficients of normal forms for frobenius expansions. Designs codes and cryptography, 61(1):71—89, October 2011.

[6] I.F. Blake, G. Seroussi, and N.P. Smart. Elliptic Curves in Cryptography. Cambridge University Press, 1999.

[7] J. Buchmann and H. Baier. Efficient construction of cryptographically strong elliptic curves. In Bimal Roy and Eiji Okamoto, editors, Progress in Cryptology —INDOCRYPT 2000, volume 1977 of Lecture Notes in Computer Science, pages 191–202. Springer Berlin Heidelberg, 2000.

[8] D.G. Cantor. Computing in the jacobian of an hyperelliptic curve. Math. Comp., 48(177):95–101, 1987.

[9] R. Carls. A generalized arithmetic geometric mean (GAGM) sequence. PhD thesis, Rijksuniversiteit Groningen, 2004.

[10] M. Ciet. Aspects of Fast and Secure Arithmetics for Elliptic Curve Cryptography. PhD thesis, Universite Catholique de Louvain, 2003.

[11] C. Clavier and M. Joye. Universal exponentiation algorithm a first step towards provable spa-resistance. In CetinK. Koc, David Naccache, and Christof Paar, editors, Cryptographic Hardware and Embedded Systems — CHES 2001, volume 2162 of Lecture Notes in Computer Science, pages 300–308. Springer Berlin Heidelberg, 2001.

[12] H. Cohen. A Course in Computational Algebraic Number Theory. Springer-Verlag New York, Inc., 1993.

[13] H. Cohen and G. Frey. Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics And Its Applications Series Editor Kenneth H.Rosen, Chapman & Hall/CRC, 2006.

[14] H. Cohen, A. Miyaji, and T. Ono. Efficient elliptic curve exponentiation using mixed coordinates. In Kazuo Ohta and Dingyi Pei, editors, Advances in Cryptology — ASIACRYPT'98, volume 1514 of Lecture Notes in Computer Science, pages 51–65. Springer Berlin Heidelberg, 1998.

[15] N. Constantinescu. Criptografie. Editura Academiei Române, Bucureşti, 2009.

[16] J.S. Coron, D. Lefranc, and G. Poupard. A new baby-step giant-step algorithm and some applications to cryptanalysis. In JosyulaR. Rao and Berk Sunar, editors, Cryptographic Hardware and Embedded Systems - CHES 2005, volume 3659 of Lecture Notes in Computer Science, pages 47–60. Springer Berlin Heidelberg, 2005.

[17] J.-M Couveignes. Computing l-isogenies with the p-torsion. In ANTS-II: Algorithmic Number Theory, Lecture, volume 1122, pages 59–65. Springer-Verlag, 1996.

[18] R.E. Crandall. Method and apparatus for public key exchange in a cryptographic system, October 1992. US Patent 5,159,632.

[19] O.A. Ţicleanu. Differential operators for boundary solutions on elliptic curves spaces with cryptographic applications. Electronic Journal of Differential Equations, ISI Indexed, IF = 0.524, accepted. 2, 4, 7, 9

[20] O.A. Ţicleanu. Mathematical models in cryptography. Journal of Knowledge Communication and Computing Technologies, 4(1):1–9, 2013. 1, 2

[21] O.A. Ţicleanu. Nonlinear analysis on elliptic curves subspaces with cryptographic applications. Annals of the University of Craiova, Mathematics and Computer Science Series, 41(2):292–299, 2014. 2, 3

[22] O.A. Ţicleanu. Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography. Electronic Journal of Differential Equations, ISI Indexed, IF = 0.524, 2015(214):1–9, 2015. 3

[23] O.A. Ţicleanu and N. Constantinescu. Studying models issues on e-commerce cashing. In International Conference on Applied Mathematics and Computational Methods in Engineering II (AMCME '14), IOS Press - ISI indexed, pages 116–128, 2014. 11

[24] O.A. Ţicleanu, N. Constantinescu, and D. Ebânca. Intelligent data retrieval with hierarchically structured information. In Intelligent Interactive Multimedia Systems and Services - Proceedings of the 6th International Conference on Intelligent Interactive Multimedia Systems and Services, IIMSS 2013, Sesimbra, Portugal, 26-28 June 2013, ISI indexed, pages 345–351, 2013. 3

[25] M. Deuring. Die typen der multiplikatorenringe elliptischer funktionenkorper. Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg, 14(1):197–272, 1941.

[26] I.M. Duursma, P. Gaudry, and F. Morain. Speeding up the discrete log computation on curves with automorphisms. In Kwok-Yan Lam, Eiji Okamoto, and Chaoping Xing, editors, Advances in Cryptology - ASIACRYPT'99, volume 1716 of Lecture Notes in Computer Science, pages 103–121. Springer Berlin Heidelberg, 1999.

[27] N. Elkies. Elliptic and modular curves over finite fields and related computational issues. In Computational Perspectives on Number Theory (Chicago, IL, 1995) AMS/IP Stud. Adv. Math., Amer. Math. Soc., Providence, RI, 7(2):21–76, 1998.

[28] A. Enge. Computing discrete logarithms in high-genus hyperelliptic jacobians in provably subexponential time. Mathematics of Computation, 71(238):729–742, November 2001.

[29] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. Acta Arithmetica, 102:83–103, 2002.

[30] A. Enge and A. Stein. Smooth ideals in hyperelliptic function fields. Mathematics of Computation, 71(239):1219–1230, October 2001.

[31] R. Flassenberg and S. Paulus. Sieving in function fields. Experimental Mathematics, 8(4):339–349, 1999.

[32] M. Fouquet, P. Gaudry, and R. Harley. On satoh's algorithm and its implementation. Journal Ramanujan Mathematical Society, 15(2):281–318, 2000.

[33] S.D. Galbraith, XB. Lin, and M. Scott. Endomorphisms for faster elliptic curve cryptography on a large class of curves. Journal of cryptology, 24(3):446—469, July 2011.

[34] R. Gallant, R. Lambert, and S. Vanstone. Improving the parallelized pollard lambda search on binary anomalous curves. Mathematics of Computation, 69:1699–1705, 1998.

[35] S. Gao, J. von Zur Gathen, D. Panario, and V. Shoup. Algorithms for exponentiation in finite fields. Journal of Symbolic Computation, 29(6):879–889, 2000.

[36] J. Guajardo and C. Paar. Itoh-tsujii inversion in standard basis and its application in cryptography and codes. desing. Codes and Cryptography, 2(25):207–216, February 2002.

[37] R. Harley. Asymptotically optimal p-adic point-counting, December 2002. Email to normal font NMBRTHRY mailing list.

[38] R. Harley. Method for solving frobenius equations for elliptic-curve cryptography, 2004. US Patent App. 10/733,320.

[39] R. Harley and J.F. Mestre. Method for generating secure elliptic curves using an arithmetic-geometric mean iteration, April 2003. US Patent App. 10/172,776.

[40] J.-P. Serre J. Lubin and J. Tate. Elliptic curves and formal groups. Lecture notes prepared in connection with the seminars held at the Summer Institute on Algebraic Geometry, Woods Hole, 1964. American Mathematical Society. 3

[41] M. Jacobson and A. van der Poorten. Computational aspects of nucomp. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 2369 of Lecture Notes in Computer Science, pages 120–133. Springer Berlin Heidelberg, 2002.

[42] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on automata. Soviet Physics Doklady, 7(7):595–596, 1963.

[43] K. S. Kedlaya. Counting points on hyperelliptic curves using monsky-washnitzer cohomology. J. Ramunujan Mathematical Society, pages 323–338, 2001.

[44] H.Y. Kim, J.Y. Park, J.H. Cheon, J.H. Park, J.H. Kim., and S.G. Hahn. Fast elliptic curve point counting using gaussian normal basis. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 3076 of Lecture Notes in Computer Science, pages 292–307. Springer Berlin Heidelberg, 2004. 7, 8

[45] N. Koblitz. p-Adic Numbers, p-Adic Analysis, and Zeta-Functions. Springer-Verlag, GTM 58, 1984.

[46] N. Koblitz. Elliptic curve cryptosystems. Mathematics of Computation, 48(177):203–209, January 1987. 1

[47] N. Koblitz. Constructing elliptic curve cryptosystems in characteristic 2. In AlfredJ. Menezes and ScottA. Vanstone, editors, Advances in Cryptology-CRYPT0' 90, volume 537 of Lecture Notes in Computer Science, pages 156–167. Springer Berlin Heidelberg, 1991.

[48] N. Koblitz. A Course in Number theory and Cryptography. New York. Springer, 1994. 11

[49] D.R. Kohel. The $agm - x_0(n)$ heegner point lifting algorithm and elliptic curve point counting. In Chi-Sung Laih, editor, Advances in Cryptology - ASIACRYPT 2003, volume 2894 of Lecture Notes in Computer Science, pages 124–136. Springer Berlin Heidelberg, 2003.

[50] T. Lange. Formulae for arithmetic on genus 2 hyperelliptic curves. Applicable Algebra in Engineering, Communication and Computing, 15(5):295–328, February 2005.

[51] R. Lercier. Computing isogenies in $\mathbb{F}_{2^n}$. In Henri Cohen, editor, Algorithmic Number Theory, volume 1122 of Lecture Notes in Computer Science, pages 197–212. Springer Berlin Heidelberg, 1996.

[52] R. Lercier. Algorithmique des courbes elliptiques dans les corps finis. PhD thesis, Ecole Polytechnique, 1997.

[53] R. Lercier and D. Lubicz. Counting points on elliptic curves over finite fields of small characteristic in quasi quadratic time. In Advances in Cryptology—EUROCRYPT '2003, Lecture Notes in Computer Science, volume 2656, pages 360–373. Springer-Verlag, 2003.

[54] C. Lim and P. Lee. A key recovery attack on discrete log-based schemes using a prime order subgroup. In Jr. Kaliski, BurtonS., editor, Advances in Cryptology — CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 249–263. Springer Berlin Heidelberg, 1997.

[55] D. Lorenzini. An Invitation to Arithmetic Geometry (Graduate Studies in Mathematics, Vol.9). American Mathematical Society, 1996.

[56] G. McGuire and E.S. Yilmaz. Further results on the number of rational points of hyperelliptic supersingular curves in characteristic 2. Designs codes and cryptography, 77(2-3):653—662, 2015.

[57] A. Menezes, S. Vanstone, and T. Okamoto. Reducing elliptic curve logarithms to logarithms in a finite field. In Proceedings of the Twenty-third Annual ACM Symposium on Theory of Computing, STOC '91, pages 80–89. ACM, 1991.

[58] A.J. Menezes, Y.-H. Wu, and R. Zuccherato. An elementary introduction to hyperelliptic curves. In N.Koblitz, editor, Algebraic Aspects of Cryptography, pages 155–178. Springer-Verlag, 1996.

[59] W. Messing. The crystals associated to Barsotti-Tate groups: with applications to abelian schemes. Springer-Verlag, 1972. Lecture Notes in Mathematics (Book 264).

[60] J.F. Mestre. Lettre adressée á gaudry et harley, December 2000. Available at http://webusers.imj-prg.fr/ jean-francois.mestre/.

[61] V. S. Miller. Use of elliptic curves in cryptography. In HughC. Williams, editor, Advances in Cryptology — CRYPTO '85 Proceedings, volume 218 of Lecture Notes in Computer Science, pages 417–426. Springer Berlin, 1986. 1

[62] R.T. Moenck. Fast computation of gcds. In Proceedings of the Fifth Annual ACM Symposium on Theory of Computing, STOC '73, pages 142–151. ACM, 1973.

[63] P.L. Montgomery. Modular multiplication without trial division. Mathematics of Computation, 170(44):519–521, 1985.

[64] V. Muller. Fast multiplication on elliptic curves over small fields of characteristic two. Journal of Cryptology, 11(4):219–234, 1998.

[65] V. Muller, A. Stein, and C. Thiel. Computing discrete logarithms in real quadratic congruence function fields of large genus. Mathematics of Computation, 68(226):807–822, April 1999.

[66] K. Nagao. Improving group law algorithms for jacobians of hyperelliptic curves. In Wieb Bosma, editor, Algorithmic Number Theory, volume 1838 of Lecture Notes in Computer Science, pages 439–447. Springer Berlin Heidelberg, 2000.

[67] IEEE P1363. Standard specifications for public-key cryptography, September 1998. Draft version 7.

[68] Certicom White Paper. The elliptic curve cryptosystem for smart card, May 1998.

[69] S. Paulus and A. Stein. Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves. In JoeP. Buhler, editor, Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, pages 576–591. Springer Berlin Heidelberg, 1998.

[70] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curve cryptosystems: Closing the performance gap to elliptic curves. In ColinD. Walter, ÇetinK. Koç, and Christof Paar, editors, Cryptographic Hardware and Embedded Systems - CHES 2003, volume 2779 of Lecture Notes in Computer Science, pages 351–365. Springer Berlin Heidelberg, 2003.

[71] S.C. Pohlig and M.E. Hellman. An improved algorithm for computing logarithms over gf(p) and its cryptographic significance. Information Theory, IEEE Transactions on, 24(1):106–110, January 1978.

[72] F. Morain R. Lercier. Counting points in elliptic curves over f_{p^n} using couveignes algorithm. Technical report, Ecole polytechnique - LIX, September 1995. Research Report LIX/RR/95/09.

[73] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM, 21(2):120–126, February 1978.

[74] H.G. Ruck. On the discrete logarithm in the divisor class group of curves. Mathematics of Computation, 68(226):805–806, April 1999.

[75] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. Journal of the Ramanujan Mathematical Society, 15(4):247–270, January 2000.

[76] T. Satoh. On p-adic point counting algorithms for elliptic curves over finite fields. In Claus Fieker and DavidR. Kohel, editors, Algorithmic Number Theory, volume 2369 of Lecture Notes in Computer Science, pages 43–66. Springer Berlin Heidelberg, 2002. 9

[77] C. P. Schnorr. Eficient signature generation by smart cards. Journal of Cryptology, 4(3):161–174, January 1991.

[78] C.P Schnorr. Efficient identification and signatures for smart cards. In Proceedings of the 9th Annual International Cryptology Conference on Advances in Cryptology, CRYPTO '89, pages 239–252. Springer-Verlag, 1990.

[79] A. Schonhage and V. Strassen. Schnelle multiplikation grosser zahlen. Computing (Arch. Elektron. Rechnen), 7(3-4):281–292, 1971.

[80] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp., 44:483–494, 1985.

[81] J.P. Serre. Local Fields. Springer-Verlag, GTM 67, 1979. 1

[82] D. Shanks. On gauss and composition i and ii. In R. Mollin, editor, Number Theory and its Applications, volume 265, pages 163–204. Kluwer Academic Publishers, 1989.

[83] J.H. Silverman. The Arithmetic of Elliptic Curves. Springer-Verlag, GTM 106, 1986.

[84] B. Skjernaa. Satoh's algorithm in characteristic 2. Mathematics of Computation, 72(241):477–487, March 2002.

[85] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. Journal of Cryptology, 12(3):193–196, 1999.

[86] N.P. Smart. Elliptic curves over small fields of odd characteristic. Journal of Cryptography, 12(2):141–151, 1999. 2

[87] J.A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. Springer-Verlag, 1997.

[88] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. Journal of the Ramanujan Mathematical Society, 16(2):1–86, January 2001. 1

[89] G. Stephanides and N. Constantinescu. he gn-authenticated key agreement. Applied mathematics and computation, 170(1):531–544, November 2005.

[90] H. Stichtenoth. Algebraic Function Fields and Codes. Springer-Verlag, 1993.

[91] D.R. Stinson. Cryptography Theory and Practice - Second Edition. CRC Press, 2002.

[92] B. Skjernaa T. Satoh 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.

[93] E. Teske. Speeding up pollard's rho method for computing discrete logarithms. In JoeP. Buhler, editor, Algorithmic Number Theory, volume 1423 of Lecture Notes in Computer Science, pages 541–554. Springer Berlin Heidelberg, 1998.

[94] J.T. van Lint. Introduction to Coding Theory. Springer-Verlag New York, Inc., 1982.

[95] P.C. van Oorschot and M.J.Wiener. Parallel collision search with cryptanalytic applications. Journal of Cryptology, Springer-Verlag, 12(1):1–28, 1999.

[96] S. Vaudenay. The security of dsa and ecdsa - bypassing the standard elliptic curve certification scheme. In Public Key Cryptography'03, pages 309–323. Springer-Verlag, 2003.

[97] J. Velu. Isogenies entre courbes elliptiques. C.R. Acad. Sc. Paris, Seerie A, 273:238–241, 1971.

[98] F. Vercauteren. Computing Zeta Functions of Curves over Finite Fields. PhD thesis, Katholieke Universiteit Leuven, 2003.

[99] F. Vercauteren, B. Preneel, and J. Vandewalle. A memory efficient version of satoh's algorithm. In Birgit Pfitzmann, editor, Advances in Cryptology — EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 1–13. Springer Berlin Heidelberg, 2001.

[100] J. von zur Gathen and J. Gerhard. Modern Computer Algebra. Cambridge University Press, 1999.

[101] A. Weil. Numbers of solutions of equations in finite fields. Bulletin of the American Mathematical Society, 55(5):497–508, 1949.

[102] D. Yong and G. Feng. High speed modular divider based on gcd algorithm over gf(2m). Journal on Communications, 29(10):199–204, October 2008.