Universitatea din Craiova
Facultatea de Ştiinţe
Şcoala Doctorală de Ştiinţe

Teză de Doctorat

Rezumat

Autor:
Alin Ionuț GOLUMBEANU

Coordonator ştiinţific:
Prof. Univ. Dr. Vicenţiu RĂDULESCU

Craiova, 2018

Universitatea din Craiova
Facultatea de Ştiinţe
Şcoala Doctorală de Ştiinţe

Optimizări ale sistemelor diferenţiale de analiză criptografică pentru modele care au la bază curbe eliptice nonsupersingulare

Autor:
Alin Ionuț GOLUMBEANU

Coordonator ştiinţific:
Prof. Univ. Dr. Vicenţiu RĂDULESCU

Craiova, 2018

Rezumat teză

Întreaga cale de construcție a unui sistem criptografic diferențial scoate în evidență frumusețea matematicii pure și ilustrează aplicabilitatea ei cu rezultate reale de îmbunatățire a unor parametrii care au factor covârșitor în versiunea finală a unui sistem de analiză criptografică.

În capitolul 1 se prezintă primul pas în construcția necesară pentru un sistem asimetric neliniar, acesta fiind studiul subspațiilor peste care vor fi definite curbele eliptice nonsupersingulare. În acest sens, se pleacă de la modelele existente și evidențiindu-se limitările, vor fi ilustrate subspații particulare ce urmează a fi folosite în construcțiile din capitolele următoare. Fie a, un număr rațional ce poate fi scris ca $a = q^m \frac{r}{s}$; $r \nmid q^k$, $s \nmid q^k$ și $a \neq 0$. Atribuim $\mathrm{ord}_{q^k}(a) = m$ și obținem următoarea regulă:

$$\mathrm{ord}_{q^k}(a+b) \geq min\{\mathrm{ord}_{q^k}(a), \mathrm{ord}_{q^k}(b)\},$$

ca egalitate, în afară de cazul $\mathrm{ord}_{q^k}(a) = \mathrm{ord}_{q^k}(b)$. În același mod, pentru $a \in \mathbb{F}_{q^k}$, atribuim $\mathrm{ord}_{q^k}(a) = m$ dacă $a \in (q^k)^m \mathbb{Z}_{q^k}$
$(q^k)^{m+1}\mathbb{Z}_{q_k}$. Aceeași regulă se aplică și pentru cele două definiții ale ord_{q^k} susțin $\mathbb{F}_{q^k}$. În ambele cazuri, am atribuit $\mathrm{ord}_{q^k}(0) = \infty$. Reținem faptul că ord_{q^k} este un homeomorfism $\mathbb{F}_{q^k}^{\times} \to \mathbb{Z}$.

$E(\mathbb{F}_{q^k})$ are o topologie compactă și $E^0(\mathbb{F}_{q^k})$ este un subgroup deschis. Din moment ce $E(\mathbb{F}_{q^k})$ este o uniune de subseturi ale lui $E^0(\mathbb{F}_{q^k})$, va rezulta că există doar o mulțime finită care îndeplinește proprietățile cerute.

Fie $\mathbb{F}_{q^k} \times \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}$ produsul topologiei, $F_{q^k}^3 \backslash \{0,0,0\}$ subspațiul topologiei și $\mathbb{P}^2(\mathbb{F}_{q^k})$ coeficientul topologiei din $F_{q^k}^3 \backslash \{0,0,0\} \to \mathbb{P}^2(\mathbb{F}_{q^k})$. Rezultă că $\mathbb{P}(\mathbb{F}_{q^k})$ este o asociere de imagini ale seturilor de forma $\mathbb{Z}_{q^k}^{\times} \times \mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}$, $\mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}^{\times} \times \mathbb{Z}_{q^k}$, $\mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k} \times \mathbb{Z}_{q^k}^{\times}$, fiecare fiind compact și deschis iar $\mathbb{P}^2(\mathbb{F}_{q^k})$ este compact. Subsetul $E(\mathbb{F}_{q^k})$ este închis deoarece este setul nul al unei polinomiale. În raport cu această topologie pe $\mathbb{P}(\mathbb{F}_{q^k})$, două puncte care sunt apropiate vor avea același modul de reducere q^k. Deci $E^0(\mathbb{F}_{q^k})$ este intersecția mulțimii $E(\mathbb{F}_{q^k})$ cu un subset deschis din $\mathbb{P}^2(\mathbb{F}_{q^k})$.

Se poate demonstra ușor că relația de reducere $E^0(\mathbb{F}_{q^k}) \to E(\mathbb{F}_{q^k})$ este surjectivă și este definită pe nucleul $E1(\mathbb{F}_{q^k})$.

Presupunem că $E^n(\mathbb{F}_{q^k})$ este un subgrup din $E(\mathbb{F}_{q^k})$. Dacă $\Omega = (x : y : 1)$ se află în $E^1(\mathbb{F}_{q^k})$, atunci vom avea $y \notin \mathbb{Z}_{q^k}$. Fie $x = q^{-m}x_0$ și $y = (q^k)^{-m'}y_0$ cu x_0 și y_0 din $\mathbb{Z}_{q^k}$.

Atunci

$$(q^k)^{-2m'}y_0^2 = (q^k)^{-3m}x_0^3 + ap^{-m}x_0 + b$$

De aici au fost construite subspații peste care sunt definite curbe eliptice nonsupersingulare, a căror proprietate de bază este că majoritatea punctelor de interes criptografic se demonstrează că sunt regăsite.

În capitolul 2, plecând de la limitările sistemelor existente, pentru cazuri particulare necesare în implementări reale, am studiat posibilitatea extinderii studiilor din articolul [154], pentru cazul a doi utilizatori, am extins studiul, pentru cazul unui grup de utilizatori care folosesc device-uri de mică putere. Însă studiile mele nu au constat în reducerea complexității prin optimizări ale implementării algoritmilor, ci prin elaborarea unui model matematic prin luarea în considerare a partiționării unui spațiu peste care sunt definite un set de curbe eliptice particulare, prin aceasta reducând timpul necesar calculului parametrilor dar păstrând aceeași Complexitate Linear Echivalentă de atac, prin modul de partiționare al spațiului peste care sunt definite curbele eliptice particulare.

Rezultatele obținute au fost publicate în [60], [61], [62], [31].

În acest sens, a fost realizat un model de curbe eliptice folosit în cadrul sistemului particularizat, descris pe larg în teză.

În acest sens, fie E o curbă eliptică definită ca fiind

$$Y_2 + \gamma_1 XY + \gamma_3 Y = X^3 + \gamma_2 X^2 + \gamma_4 X + \gamma_6$$

și $A_1 = (\omega_1, \eta_1)$, $A_2 = (\omega_2, \eta_2)$ două puncte de pe o curbă elipitică definită în modul dat.

În acest mod, putem afirma că:

$$-A_1 = (\gamma_1, -\eta_1 - \gamma_1\omega_1 - \gamma_3)$$

unde γ_6 este definit ca fiind o combinație neliniară obținută din parametrii de start folosiți în criptare. De aici, vom obține:

$$\lambda = \frac{\eta_2 - \eta_1}{\omega_2 - \omega_1}$$

și

$$\gamma = \frac{\eta_1\omega_2 - \eta_2\omega_1}{\omega_2 - \omega_1}$$

unde ω_1 și ω_2 satisfac condiția $\omega_1 \neq \omega_2$, ceea ce ne permite să deducem următorul rezultat:

$$\lambda = \frac{3\omega_1^2 + 2\alpha_2\omega_1 + \alpha_4 - \alpha_1\eta_1}{2\eta_1 + \alpha_1\omega_1 + \alpha_3}$$

și

$$\gamma = \frac{-\omega_1^3 + \alpha_4\omega_1 + 2\alpha_6 - \alpha_3\eta_1}{2\eta_1 + \alpha_1\omega_1 + \alpha_3}$$

A fost definită o curbă eliptică peste o subfracțiune a lui $\mathbb{F}_q$, în modul următor: $E(\mathbb{F}_{q^k})$, unde aceasta, se poate deduce ușor, va conține m^2 puncte de ordin m, iar m va divide $q^k - 1$, deoarece, fiind dată $E(m) \times E(m) \to \gamma_m$, unde γ_m este un grup al rădăcinilor de ordin m al unității, în K, va deduce relația $div(g) = \sum_{D \in E(m)} (B_1' + D) - (D)$ cu $B' \in E(\bar{K})$, care îndeplinește condiția $[m]B' = B$. Dar, conform [11], putem avea e_m ca fiind:

$$e_m = \begin{cases} E(m) \times E(m) \to \gamma_m \\ (B_1, B_2) \to \frac{g(X+B_1)}{g(X)} \end{cases}$$

deci subspațiul determinat de fracțiunea m vor îndeplini proprietatea expusă, conform formulei enunțate și g va satisface $g^2 - [t]g + [q] = [0]$.

Plecând de la definiția modelului de acces ierarhizat la comunicații [29] vom defini o funcție de generare a unui set de chei publice bazate pe informații conjugate unde spațiul peste care este definită curba eliptică $\mathbb{F}_{q^n}$ va avea un factor de multiplicare K, care va satisface ralația $|K| \leq \lfloor q/2 \rfloor$. De aici, corespunzător nivelului inițiatorului procesului de comunicație (fie el A_i), din ierarhia utilizatorului, vom defini o funcție de forma

$$\varphi(level, string) \to public\ Key$$

unde string reprezintă parametrii de inițializare al generatorului, conform celor descrise pe larg în teză, iar level reprezintă nivelul de acces la canalul de comunicație securizat, din care face parte A_i.

În sensul obținerii cheii agrementate de criptare, pentru o pereche de participanți, fie ei (A_i, A_j), vor crea o cheie de sesiune, în cazul în care sunt de pe același nivel de securitate din ierarhie, iar în cazul în care aparțin nivelelor diferite, va fi o comunicație inițiată de aparținătorul unui grad superior de securitate, unde aceste principii sunt descrise pe larg în [154], [69], [71]. Pentru descrierea acestora, vom defini:

- $\Pi_{K_{A_i}}$ - cheia secretă a lui A_i
- $\Pi_{P_{A_i}}$ - cheia publică a lui A_i
- $\eta^d_{A_i}(\Pi_{K_{A_i}}, m)$ - criptarea mesajului m cu cheia secretă a lui A_i
- $\eta^e_{A_i}(\Pi_{P_{A_i}}, m)$ - criptarea mesajului m cu cheia publică a lui A_i
- $\text{enc}(s_K, m)$ - cheia simetrică de criptare a mesajului m împreună cu s_K
- inf_{A_i} - valoare pseudorandom generată de A_i pentru fiecare sesiune
- $E(\mathbb{Z}_p)$ - curba eliptică definită peste câmpul $\mathbb{Z}_p$

- M - spațiul mesajelor
- $hf(\cdot)$ - funcția hash $SHA-1$
- $m_1|m_2$ - concatenarea mesajelor m_1,m_2 când m_1, $m_2 \in M$

Un utilizator al sistemelor, fie el A_i (cu respect pentru condițiile expuse în teză, va avea următorii parametri publici:

$$(\Pi_{P_{A_i}}, E(\mathbb{Z}_p), P, Q, n)$$

unde $P, Q \in E(\mathbb{Z}_p)$ reprezintă două puncte de pe curba eliptică $E(\mathbb{Z}_p)$ iar diviziunea p, conform celor expuse în teză, va fi de forma q^k, cu respectarea condițiilor expuse. De asemenea, vom defini funcțiile

- $\eta^d_{A_i}(\Pi_{K_{A_i}}, m)$ și
- $\eta^e_{A_i}(\Pi_{P_{A_i}}, m)$
- $hf(\cdot)$

ca fiind publice.

Pentru utilizatorul A_i, următorii parametrii sunt secreți:

- $\Pi_{K_{A_i}}$
- $infA_i$

Plecând de la parametri reprezentați, putem expune protocolul de stabilire a cheii de sesiune, între participanții A_i și A_j.

- A_i
  1. Se generează un număr aleator $\inf_{A_i} \in [1, n-1]$
  2. Se calculează $A_i^1 = \inf_{A_i}(P^{-1} + Q) = (x_1^{A_i}, y_1^{A_i})$. Fie $x = x_1^{A_i}\ mod\ n$. Dacă $x = 0$ atunci se execută pasul 1
  3. Se calculează $A_i^2 = hf(P_{A_i}|A_i^1)$
  4. Se calculează $A_i^3 = \eta^d_{A_i}(\pi_{K_{A_i}}, A_i^2)$
  5. Primul poas de comunicație (de la A_i către A_j)
     A_i trimite la A_j $(A_i^1|A_i^2)$
- A_j
  1. Se calculează $A_j^1 = hf(P_{A_i}|A_i^1)$
  2. Se calculează $A_j^2 = \eta^e_{A_i}(\pi_{P_{A_i}}, A_i^2)$. Dacă $A_j^1 \neq A_j^2$ se termină, atunci protocolul se încheie cu eșec.

3. Se generează un număr aleator $\inf_{A_j} \in [1, n-1]$
4. Se calculează $A_j^1 = \inf_B(P^{-1} + Q) = (x_1^{A_j}, y_1^{A_j})$. Dacă $x_1^{A_j} = 0$ se întoarce la pasul 3 din etapele executate de A_j
5. Se calculează $A_j^2 = hf(P_{A_j}|A_j^1)$
6. calculates $A_j^3 = \eta^d_{A_j}(\pi_{K_{A_j}}, A_j^2)$
7. $K_{A_j} = \inf_{A_j} A_i^1 = (x_2^{A_j}, y_2^{A_j})$
8. $x = x_2^{A_j} \bmod n$. Dacă $x = 0$ atunci merge la pasul 3 din etapele executate de A_j
9. Al doilea pas de comunicație (de la A_j la A_i)
   A_j trimite către A_i $(A_j^1|A_j^3)$

- A_i

6 Se calculează
$s_1^{A_i} = hf(P_{A_j}, A_j^1)$
$s_2^{A_i} = \eta^e_{A_j}(\pi_{P_{A_i}}, A_j^3)$

7 Dacă $s_1^{A_i} \neq s_2^{A_i}$ se încheie execuția protocolului cu eșec.

8 $K_{A_i} = \inf_{A_i} A_j^1$

În vederea asigurării dublei autentificări a utilizatorilor implicați în procesul de comunicație securizată, definiți ca fiind A_i și A_j, vom defini al treilea pas al protocolului descris.

Plecând de la pașii descriși la protocolul optimizat, descris în teză, se va efectua un pas suplimentar care va asigura confirmarea agrementării cheii de sesiune de către A_i, prin aceasta asigurându-se dubla autentificare a participanților la canalul confidențial de comunicație.

În acest sens, A_i va calcula

$$hf((inf_{A_i}(P^{-1} + Q))) \mid \text{enc}(K_{A_i}, inf_{A_j}(P^{-1} + Q))$$

și va trimite rezultatul către A_j.

În acest punct, la primirea acestui mesaj, A_j va testa egalitatea:

$$\begin{aligned} &hf((\inf_{A_i}(P^{-1} + Q)) \mid \text{enc}(K_{A_i}, \inf_{A_j}(P^{-1} + Q))) \\ &= hf((\inf_{A_i}(P^{-1} + Q)) \mid \text{enc}(K_{A_j}, \inf_{A_j}(P^{-1} + Q))). \end{aligned}$$

Dacă testul acestei egalități va returna succes, cheia de sesiune este confirmată de participanți. În implementarea acestui sistem, am definit ca fiind pasul de confirmare și în sensul măririi vitezei de lucru, este utilizat în cazul când participanții sunt părți ale nivelelor diferite de securitate, deoarece în

cazul eșecului egalității din cel de-al treilea pas, acest protocol va fi reluat de la început.

Din punct de vedere statistic, timpul necesar execuției acestui pas, deci complexitatea atașată, este de ordinul $\Phi(1/4)$ din necesarul primilor doi pași.

A fost creată o versiune personală și pentru algoritmul extins, bazată pe modelul matematic descris mai sus.

O variantă a protocolului expus, poate fi efectuată prin definirea:

$$h'_{int}(h(k))$$

unde $h'_{int} : M \to N$, h' reprezentând funcția care va genera un parametru $\eta \in \mathbb{N}$, $h'_{int}(h(k)) = \eta$, $\eta \in \mathbb{N}$, iar η va respecta inegalitatea $\eta \leq \sqrt{2} \cdot n$, unde n reprezintă numărul de nivele de securitate. Fie L_t, $0 \leq t \leq m$, nivelurile de securitate. În acest caz, cheia pentru fiecare participant A_j^t va fi creată în doi pași.

Primul pasul de autentificare, al utilizatorilor, care este îndeplinit de prima parte din protocol, și al doileapas, de autentificare a cheii, efectuat de pasul suplimentar (al treilea pas).

Această variantă pleacă de la ideea definirii ca fiind entități diferite, participanți la proces și cheile de sesiune folosite, de aceea va fi folosită o parametrizare a $T.S.$, fie ea definită ca fiind M_t^i, numită "parametrizare master", unde t este nivelul de securitate iar i reprezintă indicele participantului care inițiază procesul de comunicație.

Pentru a scoate în evidență funcționalitatea modelului, este necesar a demonstra unicitatea parametrilor definiți în fracțiunea de grad q^k, peste curba eliptică folosită, adică existența curbei eliptice folosite.

În acest sens vom demonstra următoarea teoremă care descrie parametrizarea folosită.

Teorema 1. Fie Γ o proiecție nonsingulară a unei curbe eliptice peste fracțiunea q^k, de genul 1. În acest caz există o curbă eliptică, fie ea $E(\mathbb{F}_{q^k})$ peste q^k astfel încât Γ este spațiu omogen pentru $E(\mathbb{F}_{q^k})$ și $E(\mathbb{F}_{q^k})$ este unic definită de un izomorfism peste q^k.

În teză este prezentată demonstrația completă a teoremei de mai sus, care ilustrează proprietățile spațiului utilizat.

În capitolul 3, plecând de la ideea sistemelor criptografice folosite în generarea cheilor de sesiune au fost construite modele ierarhizate care tratează diverse cazuri de generatori liniari și neliniari, în funcție de domeniul de uitlizare al acestora. Pentru modelele liniare, studiul aplicabilitații acestora se poate reduce la analiza soluțiilor la probleme matematice clasice, la care Complexitatea Liniar Echivalentă este redusă. Din punct de vedere al rezistenței la atacuri criptografice, ca și model informatic, acestea sunt stabile, însă, dacă

se studiază efortul computațional, cu un model de analiză matematică bazat pe soluții ale compușilor atomici construiți pe biecții ale modelelor de bază, se ajunge la modele fezabile a fi studiate în timp real. În acest sens, am construit modelul necesar pentru a enunța și demonstra conjectura de mai jos, care facilitează ilustrarea modelării unui sistem optim de criptare diferențială optimizată.

Conjectură 1. Berlekamp-Massey pentru cazul dependențelor compuse.

Pentru un sistem de ecuații care descriu comportamentul unui set de regiștrii cu dependențe de deplasare liniar, de lungime λ, care va avea drept ieșire un sistem de secvențe

(1) $\alpha_0, \alpha_1, \ldots, \alpha_{N-1}$, pentru cazul liniar, unde $\alpha_0 \neq 0, N \geq \alpha, \lambda'$-lungimea șirului generat

(2) $\alpha_0, \alpha_1, \ldots, \alpha_{M-1}$, pentru cazul compus, unde $\alpha_0 \neq 0, M > N, \lambda''$-lungimea șirului generat
va satisface relațiile:

(3) $\lambda' \geq N + 1 - \lambda,\ \lambda'' \geq M + 1 - \lambda$

(4) $\lambda'' > \lambda'$

Aceasta se concretizează prin următoarele proprietăți asupra implementărilor acestor parametrizări

- Adăugarea unui parametru nu garantează creșterea dimensiunii șirului de ieșire / perioadei generatorului, astfel spus, tipul de comparare "$\circ$" din Conjectură 1 este dat de tipul / gradul de dependență dintre parametri inițiali și parametrul introdus, fie el notat astfel: $DL(\lambda', \lambda'')$
- Cazul ideal, cel al dependenței $DL = 0$, se transpune în faptul că funcția "$\circ$" din Conjectură va deveni operația de multiplicare.

Plecând de la aceasta, am construit un model propriu de parametrizare și construcție al sistemelor de ecuații care definesc un set de regiștrii de deplsare cu dependențe liniare, numit AGNS, care au un factor de eficiență mai mare decât al modelului original folosit în LFSR. Exprimat funcțional avem:

$$\frac{C.L.E.}{Complex.Imp.}(AGNS) > \frac{C.L.E.}{Complex.Imp.}(LFSR)$$

unde $C.L.E.$ este complexitatea liniar echivalentă iar $Complex.Imp.$ reprezintă Complexitatea de calcul a implementării, pentru un sistem de generare de numere pseudoaleatoare. Rezultatele au fost ilustrate în articolul publicat, [31].

În acest caz vom avea:

$$b_k \leq b_{k+1} \leq a_{k+1} \leq a_k \text{ și}$$
$$0 \leq a_{k+1} - b_{k+1} \leq (a_k - b_k)/2$$

Din cele expuse putem construi o propoziție care ilustrează că o iterație de tipul AGM construiește o secvență de curbe eliptice, bazate pe un izomorfism al curbei eliptice inițiale.

Propoziţia 1. [31] Plecând de la alegerea a doi parametrii a și b, astfel încât $a, b \in 1 + 4\mathbb{Z}_q$ cu proprietatea că $a/b \in 1 + 8\mathbb{Z}_q$ și o curbă eliptică $E_{a,b}$ definită prin ecuația $y^2 = x(x - a^2)(x - b^2)$, fie a' și b', doi parametrii astfel încât: $a' = (a + b)/2$, $b' = \sqrt{ab}$ și o curbă eliptică $E_{a',b'}$, definită de ecuația $y^2 = x(x - a'^2)(x - b'^2)$. În acest caz, curbele eliptice $E_{a,b}$ și $E_{a',b'}$ sunt caracterizate de ecuația:

$$\Phi : E_{a,b} \longrightarrow E_{a',b'} : (x, y) \longmapsto \left(\frac{(x + ab)^2}{4x}, y\frac{(x - ab)(x + ab)}{8x^2} \right)$$

și cea mai mare parte din Φ este $\langle (0, 0) \rangle$. Operația Φ asupra intervalului diferențial $\frac{dx}{y}$ va avea forma

$$\Phi^* \left(\frac{dx}{y} \right) = 2\frac{dx}{y}.$$

În capitolul 4 au fost studiate optimizări ale modelelor matematice folosite în sisteme de semnare în grup, astfel, pornind de la conceptul de semnătură de grup prezentat de către Chaum și van Heijst în anul 1991 ([18, 19, 22]), orice membru al unui grup poate semna un mesaj în numele grupului astfel încât oricine poate verifica validitatea semnăturii dar nimeni să nu poată determina care este membrul grupului care a emis mesajul ([40], [117], [168], [97], [98]).

Din construcțiile care au fost făcute în teză au rezultat algoritmii particularizați expuși mai jos.

Toate modelele matematice studiate în cadrul tezei, precum algoritmii descriși au fost implementate în cadrul a două proiecte de cercetare (UEFISCDI PCE și UEFISCDI PCCA) al căror membru am avut și am onoare să fiu. Aceste rezultate au fost ilustrate prin testarea și folosirea sistemului de Declarație Digitală creat, care este unic în Romania și al doilea sistem implementat oficial la nivelul european.

Algoritm 1 Algoritmul de generare a cheii pentru un sistem derivat din Schnorr

1: se generează numere prime mari p și doua puncte (P,Q) nonsingulare pe o curbă eliptică nonsupersingulară, descrisă în capitolul 1 al tezei
2: g este generatorul grupului
3: se alege cheia privată x
4: $y = g^x \pmod p$
5: $\Phi = (p-1)(q-1)$
6: cheia publică este (p, g, y, P)
7: cheia privată este (p, g, x, Q)

Algoritm 2 Algoritmul de semnare pentru un sistem derivat din Schnorr

1: (p, g, x, P) este cheia privată
2: se alege aleator k astfel încât $0 < k < q$
3: $r = P.x, g^k \pmod p$
4: $e = H(m||r||P.y)$
5: $s = (k - xe) \pmod q$
6: semnătura este (e, s)

Algoritm 3 Algoritmul de verificare a semnăturii pentru un sistem derivat din Schnorr

1: (p, g, y, Q) este cheia publică
2: (e, s) este semnătura
3: $r_v = Q.y, g^s y^e$
4: $e_v = H(m||r_v||Q.y)$
5: if $(e_v = e)$ then
6: $\quad (e, s)$ este validă
7: end if

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 inplementation of ellipic curve cryptosystems over $f_{2^{155}}$. IEEE Journal on Selected areas in Communications, 5(11):804–813, June 1993.

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

[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] J.P. Aumasson, L. Henzen, W. Meier, and M. Naya-Plasencia. Quark: A lightweight hash. Journal of Cryptology, 26(2):313–339, 2013.

[6] 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.

[7] L. Babai. Trading group theory for randomness. ACM Symposium on Theory of Computing, 16:421–429, May 1985.

[8] L. Babai and S. Moran. Arthur - merlin games: A randomized proof system, and a hierarchy of complexity classes. Journal of Computer and System Sciences, 36, 1988.

[9] E.R. Berlekamp. Algebraic coding theory. McGraw-Hill, New York, 1968.

[10] E. Biham. Cryptanalysis of triple modes of operation. Journal of Cryptology, 12(3):161–184, 1999.

[11] I. F. Blake, G. Seroussi, and N. P. Smart. Elliptic Curves in Cryptography. Cambridge University Press, 1999. 4

[12] 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.

[13] J. Camenisch. Effcient and generalized group signatures. In In Advances in Cryptology EUROCRYPT '97, volume 1233 of Lecture Notes in Computer Science, pages 465–479. Springer-Verlag, 1997.

[14] J. Camenisch and M. Stadler. Efficient group signatures schemes for large groups. In Advances in Cryptology-Crypto, volume 1294 of Lecture Notes in Computer Science, pages 410–424. Springer-Verlag, 1997.

[15] J. L. Camenisch. Group Signature Schemes and Payment Systems Based on the Discrete Logarithm Problem. PhD thesis, ETH Zurich, 1998.

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

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

[18] D. Chaum and E. van Heyst. Group signatures. Advances in Cryptology EUROCRYPT '91, 547 of Lecture Notes in Computer Science:257–265, 1995. 9

[19] L. Chen and T. P. Pedersen. New group signature schemes. In Advances in Cryptology - EUROCRYPT '94, volume 950 of Lecture Notes in Computer Science, pages 171–181. Springer-Verlag, 1995. 9

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

[21] 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.

[22] H. Cohen. A course in computational algebraic number theory, volume 138 of Graduate texts in mathematics. Springer, 1993. 9

[23] 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.

[24] H. Cohen and H. W. Lenstra jr. Primality testing and jacobi sums. Mathematics of Computation, 42:297–330, 1984.

[25] 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.

[26] N. Constantinescu. The agreement of the common key. Annals of the University of Craiova - Mathematics and Computer Science Series, 30(2):59–65, 2003.

[27] N. Constantinescu. Authentication ranks with identities based on elliptic curves. Annals of the University of Craiova, Mathematics and Computer Science Series, XXXIV(1):94–99, 2007.

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

[29] N. Constantinescu. Authentication hierarchy based on blind signature. Journal of Knowledge Communication and Computing Technologies, 1(1):77–84, 2010. 4

[30] N. Constantinescu. Security system vulnerabilities. Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science, 13(2):175–179, 2012.

[31] N. Constantinescu, O.A. Ţicleanu, and A. Golumbeanu. Nonlinearities on cryptographic shift registers. Annals of the University of Craiova, Mathematics and Computer Science Series, 43(1):27–32, 2016. 3, 8, 9

[32] N. Constantinescu and G. Stephanides. Secure key-exchange. Recent Advances in Communications and Computer Science, 7:162–166, 2003.

[33] N. Constantinescu and G. Stephanides. Identification of parts in identity-based encryption. Technical report, Wessex Institute of Technology, UK, developed with University of Bergen, Norway, 2004. Research Notes in Data Security.

[34] N. Constantinescu, G. Stephanides, M. Cosulschi, and M. Gabroveanu. Rsa-padding signatures with attack studies. In WEBIST 2006,

Proceedings of the Second International Conference on Web Information Systems and Technologies: Internet Technology / Web Interface and Applications, Setúbal, Portugal, April 11-13, 2006, pages 97–100, 2006.

[35] 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.

[36] J.M. Couveignes. Quelques calculs en théorie des nombres. PhD thesis, Universite de Bordeaux, 1994.

[37] 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.

[38] J. Cowie, B. Dodson, R. M. E.-Huizing, A. K. Lenstra, P. L. Montgomery, and J. Zayer. A world wide number field sieve factoring record: On to 512 bits. In Advances in Cryptology-ASIACRYPT '96, volume 1 of Lecture Notes in Computer Science, pages 382–394. Springer-Verlag, 1996.

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

[40] 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. 9

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

[42] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Transactions on Information Theory, 22:644–654, November 1976.

[43] 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.

[44] 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.

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

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

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

[48] U. Feige, A. Fiat, and A. Shamir. Zero knowledge proofs of identity. Journal of Cryptology, 1:77–94, 1987.

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

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

[51] 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.

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

[53] 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.

[54] S.R. Ghorpade, S. Ul Hasan, and M. Kumari. Primitive polynomials, singer cycles and word-oriented linear feedback shift registers. Designs, Codes and Cryptography, 58(2):123–134, 2011.

[55] O. Goldreich, S. Micali, and Avi Wigderson. Proofs that yield nothing but their validity. Journal of the ACM, 38:690–728, July 1991.

[56] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. Proc. 27th Annual Symposium on Foundations of Computer Science, pages 291–304, 1985.

[57] J.Dj. Golić and R. Menicocci. Edit probability correlation attacks on stop/ go clocked keystream generators. Journal of Cryptology, 16(1):41–68, 2003.

[58] J.Dj. Golic and R. Menicocci. Correlation analysis of the alternating step generator. Designs, Codes and Cryptography, 31(1):51–74, 2004.

[59] J.Dj. Golić, M. Salmasizadeh, and E. Dawson. Fast correlation attacks on the summation generator. Journal of Cryptology, 13(2):245–265, 2000.

[60] A.I. Golumbeanu. Digital declaration implementation study. Journal of Knowledge Communication and Computing Technologies, 3(2):1–11, 2011. 3

[61] A.I. Golumbeanu. Application of differential cryptography to a gn authentication hierarchy scheme. Electronic Journal of Differential Equations,, 2017(20):1–8, 2017. 3

[62] A.I. Golumbeanu and O.A. Țicleanu. Elliptic curves differentiation with application to group signature scheme. Electronic Journal of Differential Equations, 2017(237):1–21, 2017. 3

[63] 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.

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

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

[66] 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.

[67] T. Herlestam. On the complexity of functions of linear shift register sequences. In IEEE ISIT, Les Arcs, France. IEEE, 1982.

[68] I. Iancu, N. Constantinescu, and M. Colhon. Fingerprints identification using a fuzzy logic system. International Journal of Computers, Communications and Control, 5(4):525–531, 2010.

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

[70] O.A. Țicleanu. 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.

[71] O.A. Țicleanu. Differential operators over particular elliptic curves spaces with cryptographic applications. Electronic Journal of Differential Equations, 2015(303):1–9, 2015. 4

[72] O.A. Țicleanu. Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography. Electronic Journal of Differential Equations, 2015(214):1–9, 2015.

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

[74] 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.

[75] T. Johansson. A shift register construction of unconditionally secure authentication codes. Designs, Codes and Cryptography, 4(1):69–81, 1994.

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

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

[78] J. Kilian and E. Petrank. Identity escrow. In Advances in Cryptology - CRYPTO '98, volume 1642 of Lecture Notes in Computer Science, pages 169–185, Berlin, 1998.

[79] 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.

[80] A. Klapper and M. Goresky. Feedback shift registers, 2-adic span, and combiners with memory. J. Cryptology, 10(2):111–147, 1997.

[81] D. E. Knuth. The Art of Computer Programming. ddison-Wesley, 1981.

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

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

[84] 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.

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

[86] 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.

[87] A. G. Konheim. Computer Security and Cryptography. Wiley, 2007.

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

[89] A. K. Lenstra and H. W. Lenstra Jr. The development of the number field sieve. In LNCS, volume 1554 of Lecture Notes in Mathematics. Springer-Verlag, 1993.

[90] 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.

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

[92] 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.

[93] R. Lercier and F. Morain. 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.

[94] 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.

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

[96] J. Lubin, J.P. Serre, 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.

[97] A. Lysyanskaya. Signature Schemes and Applications to Cryptographic Protocol Design. PhD thesis, MIT, 2002. 9

[98] A. Lysyanskaya and Z. Ramzan. Group blind digital signatures: A scalable solution to electronic cash. Proc. of Second International Conference on Financial Cryptography, 1998. 9

[99] Zhen Ma, Wen-Feng Qi, and Tian Tian. On affine sub-families of the NFSR in grain. Des. Codes Cryptography, 75(2):199–212, 2015.

[100] J.L. Massey. Shift-register synthesis and bch decoding. IEEE Trans. Inf. Theory, IT-15(1):122–127, 1969.

[101] 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.

[102] W. Meier and O. Staffelbach. Fast correlation attacks on certain stream ciphers. Journal of Cryptology, 1(3):159–176, 1989.

[103] W. Meier and O. Staffelbach. Correlation properties of combiners with memory in stream ciphers. Journal of Cryptology, 5(1):67–86, 1992.

[104] 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.

[105] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography. CRC Press, 1997.

[106] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. Handbook of Applied Cryptography, 5th Ed. CRC Press, 2001.

[107] 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.

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

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

[110] 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.

[111] A. Miyaji, M. Nakabayashi, and S. Takano. New explicit condition of elliptic curve trace for fr-reduction. IEICE Trans. Fundamentals, E84 A(5), 2001.

[112] 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.

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

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

[115] 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.

[116] 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.

[117] U.S. Dept of Commerce/NIST. Digital signature standard (dss), Jan 2000. 9

[118] R. Oppliger. Contemporary Cryptography. Artech House, 2005.

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

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

[121] 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.

[122] 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.

[123] H. Petersen. How to convert any digital signature scheme into a group signature scheme. Security Protocols Workshop, 1997.

[124] N.R. Pillai and S.S. Bedi. Algebraic attacks on a class of stream ciphers with unknown output function. Designs, Codes and Cryptography, 69(3):317–330, 2013.

[125] 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.

[126] J. M. Pollard. A monte carlo method for factorization. BIT, 1975.

[127] J. M. Pollard. Monte carlo methods for index computation (mod p). Mathematics of Computation, 32:918–924, July 1978.

[128] C. Pomerance. The quadratic sieve factoring algorithm. In Advances in Cryptology, volume 209 of Lecture Notes in Computer Science, pages 169–182. Springer-Verlag, 1985.

[129] M. O. Rabin. Probabilistic algorithm for testing primality. Journal of Number Theory, 12:128–138, 1980.

[130] Certicom Research. Sec 2: Recommended elliptic curve domain parameters, September 2000. Version 1.0.

[131] 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.

[132] S. Ronjom. Improving algebraic attacks on stream ciphers based on linear feedback shift register over $\mathbb{F}_{2^k}$. Designs, Codes and Cryptography, 82(1-2):27–41, 2017.

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

[134] 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.

[135] 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.

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

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

[138] 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.

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

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

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

[142] A. Shamir. Identity-based cryptosystems and signature schemes. In Advances in Cryptology, volume 196 of Lecture Notes in Computer Science, pages 47–53. Springer-Verlag, 1984.

[143] 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.

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

[145] E. Simion and N. Constantinescu. Complexity computations in code cracking problems. In Concurrent Engineering in Electronic Packaging 2001. 24th International Spring Seminar, IEEE Communication, pages 225–232. IEEE, 2001.

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

[147] N. Smart. How secure are elliptic curves over composite extension fields? In EUROCRYPT 2001, volume 2045 of Lecture Notes in Computer Science, pages 30–39. Springer-Verlag, 2001.

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

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

[150] S.C. So, T. Kim, and S. Hong. Accelerating elliptic curve scalar multiplication over gf(2(m)) on graphic hardwares. Journal of parallel and distributed computing, 75:152—167, January 2015.

[151] J.A. Solinas. An improved algorithm for arithmetic on a family of elliptic curves. In Advances in Cryptology - CRYPTO '97, 17th Annual International Cryptology Conference, Santa Barbara, California, USA, August 17-21, 1997, Proceedings, pages 357–371, 1997.

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

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

[154] G. Stephanides and N. Constantinescu. The gn-authenticated key agreement. Applied Mathematics and Computation, 170(1):531–544, 2005. 3, 4

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

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

[157] H. Tanaka. A realization scheme for identity-based cryptosystem. In Advances in Cryptology, volume 293 of Lecture Notes in Computer Science, pages 341–349. Springer-Verlag, 1987.

[158] 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.

[159] T. Tian and Wen-Feng Qi. On the largest affine sub-families of a family of NFSR sequences. Des. Codes Cryptography, 71(1):163–181, 2014.

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

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

[162] 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.

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

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

[165] 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.

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

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

[168] 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. 9

[169] M. Zhang. Maximum correlation analysis of nonlinear combining functions in stream ciphers. Journal of Cryptology, 13(3):301–314, 2000.