University of Craiova
Faculty of Sciences
Doctoral School of Sciences

PhD Thessis

Summary

Author:
Oana Adriana ŢICLEANU

Scientific Coordinator:
Prof. Univ. PhD. Vicenţiu RĂDULESCU

Craiova, 2015

University of Craiova
Faculty of Sciences
Doctoral School of Sciences

Nonlinear processes over nonsupersingular elliptic curves with cryptographic applications

Author:
Oana Adriana ŢICLEANU

Scientific Coordinator:
Prof. Univ. PhD. Vicenţiu RĂDULESCU

Craiova, 2015

Summary

The study of elliptical curves has a rich history and proves once again the beauty of pure, theoretical mathematics and the way it's applicability emerges after defining new concepts which in first place are charged as abstract by the scientific society, but in the end it is certain that the model was a math premonition of nature's concepts.

Thus, some properties of systems based on elliptical spaces date from the last century, but formings in this sense were dated long before, by study of diophantine equations (3th century, greek mathematician A. Diophantus). This domain was highlighted with articles of mathematicians N. Koblitz ([46]) and V. Miller ([61]) which gave a brand new applicability of those equations in domain of asymmetric cryptosystem.

It goes from definition of elliptic curve given by Weierstrass's equation:

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

where $a_i \in K$ and K is the space where curve E is defined.

Those curves can be divided in two classes namely those who are supersingular and nonsupersingular curves ([2]) with modern applicability ([20]).

1. A supersingular curve (zero j-invariant) is set of solution for equation:

$$y^2 = x^3 + ax + b \tag{1.2}$$

   where $a, b, c \in GF(2^k)$, discriminant is $\Delta = 4a^3 + 27b^2 \neq 0$, with the point at infinity $\mathcal{O}$.

2. An nonsupersingular elliptical curve (nonzero j-invariant) is the set solutions of the equation

$$y^2 + xy = x^3 + ax^2 + b \tag{1.3}$$

   where $a, b, c \in GF(2^k)$, discriminant is $\Delta \neq 0$, with the point to infinit $\mathcal{O}$.

Asymmetric keys used in modern cryptography are pairs of points which contain a particular set of properties with a scalar.

Hence, many mathematicians have studied ways to obtain spaces with properties in this sense ([2], [81], [88]) and optimizations of the model by adding new boundary conditions for nonlinear equations systems which have boundary

solutions, those being actually required parameters in real conditions of securing the informational flow ([3]).

Essentially, beyond optimal implementations, complexity of algorithms used and computing power, it is proven fact that the only models resistant to cryptographic attacks were those that had an mathematical outfit based on construction of subspaces with particularities that the boundary solution set to be characterized by a system of differential equations which are defined over elliptic curves, defining the necessary type of Frobenius isomorphisms ([21], [86]).

Studies such as methods for calculating of parameters involved, isomorphisms which define parts of the model involved and, especially, some particular spaces in which are defined elliptical curves, differential analysis study and also boundary solutions for differential equations over elliptic curves, all of these defined the researche that followed and areas that have open issues in terms of applicability. In the domain of particular spaces that define elliptical curves and border solutions for differential systems with applications in nonlinear systems of analysis of resistance to attacks for cryptographic models, in this regard, I studied, build the algorithms and implemented proprietary solutions for unsolved problems in applied mathematics for cryptography.

Starting from the classification in terms of structure fields over which are defined classical elliptical curves, in second chapter are described field structures over elliptical curves, methods of calculating the parameters involved in finite spaces of type $GF(2^k)$, applicable in nonsupersingular elliptic curves, results which were published in article ([20]).

In this chapter are described optimized personal solutions of differential calculation of parameter p of an elliptical curve and studies performed on infeasibility level of the studied mathematical model, presented in algorithm 1 (the results where published in [19]). Let Γ subset of points on an elliptical curve for which the inverse was calculated, χ inverse of a number ϕ, t differentiation level (will define the safety degree of the generated system).

Algorithm 1 Differential calculation of the parameter p of an elliptic curve

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. while $\xi > 0$ do
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. while $\phi \geq p$ do $\phi \leftarrow \phi - \left\lfloor \frac{p}{\chi} \right\rfloor$

In this way, the reduction function will use only shifting operations in order

to define the degree of subset of points with cryptographic properties.

The classical calculation of parameters used in implemented system uses RNSA (Residue Number System Arithmetic).

In the third chapter was studied the method to determine the particular finite subspaces with advanced cryptography properties, results being published in ([21]). Thus, it was described how operations over elliptic curves are made, features that must be met by a space in order to be resistant to cryptographic attacks and there were studied ways used for cryptographyc analysis of a mathematical model for a cryptographic system of that kind. For developed models, defined over particular subspaces with applicability to increase the complexity of attack, were studied endomorphisms over finite fields defined in second chapter, and implications of differential equations involved in nonlinear analysis of cryptographic system, results being published in article ([22]). Defined models have there origin given by results of studying existing problems in some extraction systems of necessary parameters, those studies effectuated had result published in ([24]). From those results were concluded methods of optimizations for designing models of algorithms involved in calculation of necessary parameters in order to determinate solutions of interest for differential equations defined over elliptical curves, thus, in this chapter were designed personal variants of optimal implementations for:

Transformation of nonsupersingular elliptic curve $\mathbb{Z}_q^p$ for invariant j

From equations described by [40] can be concluded that Jacobian matrix is invertible over field $\mathbb{Z}_q$ and $\delta = ((D\Theta)^{-1}\Theta)(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{Z}_q^n$, because $(D\Theta)(x_0, \ldots, x_{n-1})(mod\ p)$ is matrix's diagonal with void elements. It is deductible that Gauss method can be applied, in order to solve the equation

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

because diagonal elements are reversible. Will be calculate on each line, by moving the low-left item, $\Phi'_p(x_0, x_{n-1})$, to right. After performing k operations of this kind, the item can be write as:

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

it can be proven that is divisible with p^k from $\Phi'_p(x_{i+1}, x_i) \equiv 0(mod\ p)$. Starting from standard procedure I designed a model to calculate the invariant j over a nonsupersingular subspace of an standard elliptic curve, thus defining a standard subset of points which can be system solutions for cryptographic keys, for which calculation will be according to an extraction procedure which will be

defined in the algorithm developed by myself for this purpose, implementation 3 (the results where published in [19]). Nonsupersingular elliptic curve transform is described in algorithm 2.

Algorithm 2 Transform of nonsupersingular elliptic curve $\mathbb{Z}_q^p$ for invariant j

Input: System $j_i^P \in \mathbb{F}_q^P \backslash \mathbb{F}_{p^2}$ with $\Phi_p(j_i^P, j_{i+1}^P) \equiv 0(mod\ p)$ for $0 \leq i \leq n'$ with precision $m|n$.
Output: System $j_i^q \in \mathbb{Z}_q$ with $\Phi_p(J_i^P, J_{i+1}^P) \equiv 0(mod\ p^m)$ and $J_i^q \equiv j_i(mod\ p)$ for any $0 \leq i < n'$.

1. for $m = 1$ to n' do
2. if $j_i^m \neq 0$ then
3. $J_i \leftarrow j_i^m$
4. else
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. $(J_0^P, \ldots, J_{n'-1}^P)$ will be determined by canonical reverse a $((j_0^P, \ldots, j_{n'-1}^P), m')$.
7. for $i = 0$ to $n' - 2$ do
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. if $S \neq 0$ then
14. for $i = n' - 2$ to 0 by step -1 do
15. $\varphi_i \leftarrow \varphi_i - D_i\ P_{i+1}^P(mod\ p^{M'})$
16. else
17. for $i = 0$ to $m' - 1$ do
18. $J_i^P \rightarrow J_i^P - p^{M'} P_i^P(mod\ p^{M'})$
19. return $(J_0^P, \ldots, J_{n'-1}^P)$.

Nonlinear method of calculation the number of points with cryptographic proprieties - SatOT

Starting from the model's demonstration of Satoh, I developed a calculation method for subspaces over an elliptic curve which has as feature p and number of points characterized of $\overline{F_{OT}} : \overline{E}(\overline{\mathbb{F}}_q) \rightarrow \overline{E}(\overline{\mathbb{F}}_q) : (x, y) \longmapsto (x_p^q, y_p^q)$, where we define the number of grade 1 cryptographic points as being weak solutions of cryptographic points, points that can be keys for ECC systems. This points system ensures a subspace which has a lower computational complexity to generate points keeping attack complexity on ECDLP at the same level described in implementation 3 (the results where published in [19]).

Transformation of the first invariant j

Repeatedly application of Vercauteren's property can be carried out on nonsupersingular's elliptic curve space F_p^q, in invariant's calculation j^q, resulting in the implementation from 4 (the results where published in [19]).

Simplified version if SST for nonsupersingular elliptic curve $\mathbb{F}_p^q$

Inverse substitution of Frobenius Σ^{-1} have as method of solving

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

where $C_j(t) = \Sigma^{-1}(t^j) \equiv t^{jp^{n-1}}(mod\ f(t))$. If we compute before $C_j(t)$ for $j = 0, \ldots, p-1$, compute of $\Sigma^{-1}(\alpha)$ for $\alpha \in \mathbb{Z}_q$ will contain only $p-1$ multiplications in $\mathbb{Z}_q$.

Starting from this way of solving, H.Y. Kim, J.Y. Park, J. Cheon, J.H. Park, J.H. Kim and S. Hahn [44] highlighted the possibility of using some finite fields with a Gaussian normal base (GNB) of small type. This base can convert to $\mathbb{Z}_q$ and in this way computation can optimize calculations of Frobenius iterations because B from $\mathbb{Q}_q/\mathbb{Q}_p$ is normal if $\exists\beta \in \mathbb{Q}_q$ such that $B = \{\Lambda(\beta)|\Lambda \in Gal(\mathbb{Q}_q/\mathbb{Q}_p)\}$. From here can be deduced the next sentence, with direct implications finding points of cryptographic interest, whose demonstration can be found in [44].

Algorithm 3 Nonlinear method for calculating number of points with cryptographic properties - SatOT

Input: Nonsupersingular elliptic curve $\overline{E}_p$, derived from $\overline{E} : y^2 = x^3 + ax + b$ defined over subspace $\mathbb{F}_{p^n}^q,\ j(\overline{E}_{OT}) \notin \mathbb{F}_{p^2}$.

Output: Number of points with grade 1 cryptographic properties on curve $\overline{E}(\mathbb{F}_{p^n}^q)$.

1. For each point from $\overline{E}$, compute subset $\overline{E}_p$, as an isomorphism of canonical towards q, using algorithm 2.
2. if m has value 1 then
3. For $i = 0$ to $n - 1$ do
4. $J_i \leftarrow j_i^q$
5. else
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. For $i = 0$ to $n - 2$ do
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. If either D_i is determined by a point from outside of nonsupersingular elliptic curve, that point will be eliminated.
15. For $i = 0$ to $min(M', n - 2)$ do
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. If any P characterizes a point from outside of nonsupersingular elliptic curve, resumes at step 6.
21. For $i = n - 2$ to 0 by step -1 do
22. $P_i \leftarrow P_i - D_i\ P_{i+1}^q(mod\ p^{M'})$.
23. For $i = 0$ to $n - 1$ do
24. $J_i^q \leftarrow J_i^q - p^{M'} \cdot P_i/D'_i(mod\ p^{M'})$.
25. Return $(J_0^q, \ldots, J_{n-1}^q)$.

Algorithm 4 Converting the first invariant j

Input: A j^q, invariant $j \in \mathbb{F}_{p^n}^q/\mathbb{F}_{p^2}$ and precision m' according to algorithm 2.
Output: $J^q \in \mathbb{Z}_q$ with $J^q \equiv j^{p^{m-1}}(mod\ p)$ and $\Phi_p(J^q, \Sigma(J^q)) \equiv 0(mod\ p^m)$.

1. $J^q \leftarrow jm'\ (mod\ p)$.
2. For $i = 2$ to m do
3. $\quad J^q \leftarrow$ Newton_Iteration $(\Phi_p(X, J), J^p J^q\ (mod\ p), i)$.
4. If J^q haave characteristics from outside of nonsupersingular elliptic curve then
5. $\quad$ Resume from step 1.
6. Return J^q.

Proposition 1.1. Let p a prime number and n, t two positive integers such that $nt+1$ is prime and different p. Let γ a primitive root of order $nt+1$ an unit as an extension of the field $\mathbb{Q}_p$. If $gcd(nt/e, n) = 1$, with e order of p mod $nt+1$, then for every primitive root of order t of unit τ in $\mathbb{Z}/(nt+1)\mathbb{Z}$ wrote as

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

is an normal element and $[\mathbb{Q}_p(\beta) : \mathbb{Q}_p] = n$. Such base is called a Gaussian normal base of type t.

In work [44] are presented values from $\mathbb{Z}_q$ as being elements from the following ring:

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

multiplication of two elements $\mathbb{Z}_q/(p^m\mathbb{Z}_q)$ will require a number of operations with $O((nmt)^\mu)$ complexity, reducing according the previous sentence at $t \leq 2$.

For $t = 1$ we have $\beta = \tau$ and minimal polynomial of β is

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

Reduction of complexity of computation from Frobenius substitution, according to H.Y. Kim, is possible by using of redundant representation, by using an inclusion, $\mathbb{Z}_q$ from $\mathbb{Z}_p[x]/(x^{n+1} - 1)$, what concludes in $\alpha = \sum_{i=0}^{n-1} \alpha_i \beta^i$ in $\alpha(x) = \sum_{i=0}^{n-1} \alpha_i x^i + 0x^n$. Then $\Sigma^k(\beta) = \beta^{p^k}$, which leads to

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

The result will lead to $\Sigma^k(\alpha)$ by permuting it's coefficients $\alpha(x)$, with an compute complexity of order $O(n)$. This determinates how Satoh-Skjernaa-Taguchi computer systems computes over elliptical curves which contains cryptographic points of grade 1.

If we consider $\Gamma(X, \Sigma(X)) = 0$, and $x \in \mathbb{Z}_q$ a root of it, for $\Gamma(X, Y) \in \mathbb{Z}_q[X, Y]$, we compute an approximation $x_m \equiv x(mod\ p^m)$ and define $\delta_m = (x - x_m)/p^m$, in this way Taylor's series developed for x_m will determine:

$$\begin{aligned} 0 &= \Gamma(x, \Sigma(x)) = \Gamma(x_m + p^m\delta_m, \Sigma(x_m + p^m\delta_m)) \\ &\equiv \Gamma(x_m, \Sigma(x_m)) + p^m(\delta_n\Delta_x + \Sigma(\delta_m)\Delta_y)(mod\ p^{2m}), \end{aligned} \tag{1.4}$$

where $\Delta_x \equiv \frac{\partial\Gamma}{\partial X}(x_m, \Sigma(x_m))(mod\ p^m)$ and $\Delta_y \equiv \frac{\partial\Gamma}{\partial Y}(x_m, \Sigma(x_m))(mod\ p^m)$, and $\Gamma(x_m, \Sigma(x_m)) \equiv 0(mod\ p^m)$ so reducing by p^m we get relation

$$\frac{\Gamma(x_m, \Sigma(x_m))}{p^m} + \delta_m\Delta_x + \Sigma(\delta_m)\Delta_y \equiv 0(mod\ p^m). \tag{1.5}$$

for δ_m mod p^m.

In order to obtain points of first grade it is sufficient for $ord_p(\Delta_y) = 0$, which means that Δ_y is a unit in $\mathbb{Z}_q$ and that $ord_p(\Delta_x) > 0$. Performing modulo operation p for equation (1.5) will result:

$$\delta_m^p = -\frac{\Gamma(x_m, \Sigma(x_m))}{p^m\Delta_y}(mod\ p) \tag{1.6}$$

which have a root of p order (unique), $\delta_m \in \mathbb{F}_q$, will obtain an approximation of x, which is more efficient, given by $x_m + p^m\delta_m \equiv x(mod\ p^{m+1})$. Root of order p have an compute complexity with a grater order, by soluions from Satoh, Skjernaa and Taguchi: replacing in equation $\Gamma(X, \Sigma(X)) = 0$ with $\Gamma(\Sigma^{-1}(X), X) = 0$. Thus, δ_m will be defined as:

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

From $\Gamma(\Sigma^{-1}(x_m), x_m) \equiv 0(mod\ p^m)$ it only requires finding the inverse of $\frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_m), x_m)$ mod p. Implementing this method we determine algorithm 5 (the results where published in [19]), than can replace Satoh's classical method [76] for nonsupersingular elliptic curve $\mathbb{F}_p^q$, it's implementation being in 5.

Algorithm 5 SST's simplified version for nonsupersingular elliptic curve $\mathbb{F}_p^q$

Input: Polynomial $\Gamma(X,Y) \in \mathbb{Z}_q$, item $x_0 \in \mathbb{Z}_q$ satisfy $\Gamma(\Sigma^{-1}(x_0), x_0) \equiv 0(mod\ p)$ and precission m.
Output: Item $x_m \in \mathbb{Z}_q$ with $\Gamma(\Sigma^{-1}(x_m), x_m) \equiv 0(mod\ p^m)$ and $x_m \equiv x_0(mod\ p)$.

1. For i=2 to m do
2. $\quad x_m^q(i) \leftarrow$ ALG 4(x_m, m)
3. If $x_m^q(i)$ is not included in nonsupersingular elliptic curve then
4. $\quad$ resumes on step 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. For i=0 to m do
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. Return y.

The complexity of classic algorithm is given by the call, after every iteration, in order to recalculate $\Gamma(x,y)$, although values of x and y at step $i+1$ are very close to values from i step, while result given in 5 uses an approximation of the two parameters and it is took in consideration only nonsupersingular space. After determining $x_W \equiv x(mod\ p^W)$ associated with W are considered elements $s \in \mathbb{N}$, for which

$$\Gamma(\Sigma^{-1}(x_{sW+i}), x_{sW+i}) \equiv \Gamma(\Sigma^{-1}(x_{sW}), x_{sW}) + \Delta(mod\ p^{(s+1)W}), \tag{1.7}$$

with

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

All it remains to find out the solution is to calculate partial derivates

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

for modulus p^W.

For $\Gamma(\Sigma^{-1}(x_{sW}), x_{sW})$ and $i < W$ can be determined $\Gamma(\Sigma^{-1}(x_{sW+i}), x_{sW+i})$, by using equation (1.7).

Variation of SatSk-Taguchi's algorithm for nonsupersingular elliptic curve $\mathbb{F}_q$

Starting from parameters's descriptions of nonsupersingular elliptic curve from algorithm 2 and the method of points calculation on nonsupersingular

elliptic curve, considering equation (1.7) to cause each update of $\Gamma(x, y)$, I determined a computing model of x_m element, for subspace of invariants which can't not be deduced directly from cryptographic analysis of ANG's system, illustrated in 6.

Algorithm 6 Variant of SatSk-Taguchi's algorithm for nonsupersingular elliptic curve $\mathbb{F}_q$

Input: Polynomial $\Gamma(X, Y) \in \mathbb{Z}_q$, item $x_0 \in \mathbb{Z}_q$ satisfy $\Gamma(\Sigma^{-1}(x_0), x_0) \equiv 0(mod\ p)$ and precision m. Canonical system $(J_0^q, \ldots, J_{n-1}^q)$, obtained based on algorithm 2.
Output: Item $x_m^q \in \mathbb{Z}_q$, with $\Gamma(\Sigma^{-1}(x_m^q), x_m^q) \equiv 0(mod\ p^m)$ and $x_m^q \equiv x_0(mod\ p)$.

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. For $s = 1$ to $\lfloor (m-1)/W \rfloor$ do
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. $\quad$ For $i = 0$ to $W - 1$ do
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. Return y.

Satoh, Skjernaa si Taguchi proves that for $W \cong n^{\mu/(1+\mu)}$, variation for some elliptic curve of algorithm 6 have a compute complexity of order $O(n^\mu m^{\mu+1/(1+\mu)})$. In effective implementations is deemed to determine only those W which are multiples of structure's intern dimensions of utilised processors.

In fourth chapter were studied mathematical deficiencies in computing parameters over elliptic curves, more specific, subspaces inconclusive in terms of cryptography, for highlighting those ideal subspaces in cryptographic system, and examples of practical implementations, results being published in [23], thus, in order to get pieces of information about torsion points m we have to look at rational functions g_m and h_m, which has as solutions those specific points. Still, we don't have information about their roots and we end with at least two results for m co-primes (with p). This section is intended to clarify this model by defining rational functions with simple roots (exactly in torsion points m) and solutions only from $\mathcal{O}$. If such function exist, this needs to be polynomial.

By E's isomorphism with zero-degree of Picard's subgroup, such polynomial exists if torsion points m can be gathered and their result is $\mathcal{O}$. Indeed, this is the case for which m and p are co-prime: for any torsion point P (m which are not of order 2 are called $\mathcal{O}$). If $E[m]$ has a point of order 2, then m must be prime, $E[2] \subseteq E[m]$ and $p \neq 2$. In this case, there are three points of order of 2, with sum $\mathcal{O}$, because there exists a rational function with divisor $\langle E[2] \rangle - 4 \langle \mathcal{O} \rangle$, more specific right $2Y + a_1X + a_3$.

In fifth chapter are made contributions in domain of particular subspaces defined over nonsupersingular elliptic curves with applications in parameters computing, used for information flow encryption, thus for all cryptosystem based on elliptical curves, defined the endomorphisms for general systems, according to mathematical models defined by Menezes, Okamoto and Vanstone can be customized but only if Hensel's theorem is assumed, to obtain improvements to keys used in high secured systems. Thus, transmitted message will be converted in one or more points (it depends on the length of the message) on used elliptical curve. In real implementations I used a system based on algorithms 2 and 3, that requires in the computations algorithm 4, proprietary algorithms developed through optimizing Satoh's algorithms, in case of set of elliptical curves took in considerations are nonsupersingular, thereby leading to a more complex cryptographic analysis about ECDLP. In order to determine how to attack the system by cryptographic differential analysis, we will be gradually define the terms involved and the solution for reducing the problem to one that has a lower computational complexity, by reducing the mathematical model used on particular cases. A calculation method used for generated elliptical curves it was proposed by Koblitz in [48] and starting with this solution I have developed my very own method for nonsupersingular systems, which uses implementations designed in third chapter, to get the last desideratum: an encrypted message. In that direction are considered parameters which defines the elliptic curve. $(\mathcal{F}, \phi, \alpha_E, \beta_E, \Gamma, \rho, \xi)$, η is a parameter which depend of implemented system and $\mu = \mu_1, ..., \mu_n$, unencrypted message. Necessary steps in this patters, for every μ_j, $j = 1, ..., n$ there are:

1. It is considered μ_j an integer with property $0 \leq \mu \leq \frac{p}{\eta} - 1$
2. Let $x_i = \eta\mu_j + i$ where $i = 0, 1, 2 \ldots, (\eta - 1)$
3. It's obtained $c_i = x_i^3 + \alpha_E x_i + \beta_E$ by recursive operations $c_i^{\frac{\phi-1}{2}} \equiv 1 (mod\ \phi)$
4. ALG 6(Γ, c_i)
5. Is calculated $y_i = \sqrt{c_i}$
6. $\mathcal{M}(x_i, y_i) = (x_i, y_i^{(\phi+1)/4})$ is point on the elliptical curve that corresponds with message μ_j.

This is the method used to obtain an encryption for cryptographic systems based on parameters defined over nonsupersingular elliptical curves, by using mathematical models and implementations developed along the thesis.

The whole works has theoretical constructions and points it's applicability by pointing out the solutions and by offering a practical way to obtain a nonsupersingular elliptic curves implementation of an encryption system, by personal algorithmic solutions given for particular cases which have better resistance to differential cryptographic analysis.

Bibliography

[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. 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, 5, 8

[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. E. 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. 10

[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. 5, 7

[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. 8

[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.