Electronic Journal of Differential Equations, Vol. 2015 (2015), No. 303, pp. 1–7.
ISSN: 1072-6691. URL: http://ejde.math.txstate.edu or http://ejde.math.unt.edu
ftp ejde.math.txstate.edu

DIFFERENTIAL OPERATORS OVER PARTICULAR ELLIPTIC CURVES SPACES WITH CRYPTOGRAPHIC APPLICATIONS

OANA ADRIANA ŢICLEANU

Abstract. Finding optimal implementations to solve differential equations in the case of boundary conditions is an open problem. In the particular case of using nonsupersingular elliptic curves there are applications in the asymmetric encryption field. Starting from the general implementations, we constructed solutions for the nonsupersingular elliptic curves case. Our developments are of high interest in the domain of nonlinear cryptography and have a good resistance for differential cryptanalysis.

1. Introduction

The study of elliptical curves has a rich history and proves once again the beauty of pure, theoretical mathematics and the way its applicability emerges in time.

Some properties of systems based on elliptical spaces date from the previous century. Foundations in this sense were dated long before, by the study of diophantine equations (3th century, Hellenic mathematician A. Diophantus). This domain was highlighted with articles of mathematicians Koblitz ([4]) and Miller ([7]) which gave a brand new applicability of those equations in the domain of asymmetric cryptosystems.

2. Elliptic equations analysis

We start by defining a set of elliptic curves given by Weierstrass's equation

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

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

Those curves can be divided in two classes namely: supersingular and nonsupersingular ([1]). Modern applicability of this concepts can be found in [13].

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

$$y^2 = x^3 + ax + b \tag{2.2}$$

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

2010 *Mathematics Subject Classification.* 35H20, 35S15, 12H20, 11G07.
Key words and phrases. Elliptic curves; cryptography; differential equation.

Submitted September 12, 2015. Published December 11, 2015.

(2) A nonsupersingular elliptical curve (nonzero j-invariant) is the solution set of equation

$$y^2 + xy = x^3 + ax^2 + b \tag{2.3}$$

where $a, b \in GF(2^k)$, and the discriminant is $\Delta \neq 0$, together with the point $\mathcal{O}$ at infinite.

The pairs of points which are found on this kind of curves that have a particular set of properties, together with a scalar, are the asymmetric keys used in modern cryptography. Given this fact many mathematicians have studied ways to obtain spaces with properties in this sense [1, 9, 11] and model optimizations, by adding new boundary conditions for nonlinear equations systems ([2]).

Essentially, beyond optimal implementations, algorithmic complexity and computing power, it is a proven fact that the only models which are resistant to cryptographic attacks were those that had a mathematical outfit based on the construction of subspaces with particularities. Those subspaces have a solution set characterized by a diferential equation system which is defined over elliptic curves through the Frobenius isomorphisms [14, 10].

There are existing methods available to compute the involved parameters and isomorphisms that define parts of the models. In the domain described above we studied, build, developed and implemented proprietary solutions for unsolved problems from the field of applied mathematics in cryptography, which rely on nonsupersingular elliptic curves.

3. Nonlinearities on elliptic curves. Study implementation for nonsupersingular case

After classifying the construction methods of the fields over which are defined classical elliptical curves, we will describe optimized personal solutions to compute the parameter p of an elliptical curve (algorithm 1).

Let Γ be a subset of points over an elliptical curve for which the inverse was computed, χ the inverse of a number ϕ, t the differentiation level (which defines 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) $\quad i \leftarrow i + 1$, $\phi \leftarrow \phi + \phi_i$, $\xi \leftarrow \lfloor \frac{b^t}{\phi_i} \rfloor$
(5) while $\phi \geq p$ do $\phi \leftarrow \phi - \lfloor \frac{p}{\chi} \rfloor$

4. Boundary solutions on particular subspaces on nonsupersingular elliptic curves

To have an increased resistance to differential attacks in cryptography it is necessary to perform an optimal number of operations over elliptic curves, which were achieved in the implementation 1.

For the developed models we studied endomorphisms over finite fields and the implications given by the differential equations involved in the nonlinear analysis of the cryptographic system [12].

4.1. **Transformation of nonsupersingular elliptic curve $\mathbb{Z}_q^p$ for invariant j.** From equations described by [6] 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

$$(D\Theta)(x_0, \ldots, x_{n-1}) \pmod p$$

is the matrix's diagonal with nonzero elements. It is obvious that the 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. It will be computed 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 written as:

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

and it can be proven that it is divisible with p^k from $\Phi'_p(x_{i+1}, x_i) \equiv 0 \pmod p$. The transformation of the nonsupersingular elliptic curve is described in algorithm 2.

Algorithm 2 Transformation of nonsupersingular elliptic curve $\mathbb{Z}_q^p$

Input: System $j_i^P \in \mathbb{F}_q^P \backslash \mathbb{F}_{p^2}$ with $\Phi_p(j_i^P, j_{i+1}^P) \equiv 0 \pmod p$ for $0 \le i \le n'$ with precision $[m/n]$.

Output: System $j_i^q \in \mathbb{Z}_q$ with $\Phi_p(J_i^P, J_{i+1}^P) \equiv 0 \pmod{p^m}$ and $J_i^q \equiv j_i \pmod p$ for any $0 \le i < n'$.

(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) $m' \leftarrow \lceil \frac{m}{2} \rceil \cdot \lceil \frac{p}{2} \rceil, M \leftarrow m'$, $M' \leftarrow \frac{P}{q}$.
(6) $(J_0^P, \ldots, J_{n'-1}^P)$ will be determined by the canonical inverse of $((j_0^P, \ldots, j_{n'-1}^P), m')$.
(7) for $i = 0$ to $n' - 2$ do
(8) $t \leftarrow \Phi'_p(J_i^P, J_{i+1}^P)^{-1} \pmod{p^M}$; $D_i \leftarrow t\Phi'_p(J_{i+1}^P, J_i^P) \pmod{p^M}$.
(9) $P_i \leftarrow t((\Phi_p(J_i^P, J_{i+1}^P) \pmod{p^m}))/p^M \cdot \frac{1}{p^{M'}}) \pmod{p^M}$
(10) $R \leftarrow \Phi'_p(J_0^P, J_{n-1}^P) \pmod{p^{M'}}$.
(11) $S \leftarrow (((\Phi_p(J_{n-1}^P, J_0^P) \pmod{p^{M'}})))/p^{M'}) \pmod{p^M}$.
(12) if $S \neq 0$ then
(13) for $i = n' - 2$ to 0 by step -1 do
(14) $\varphi_i \leftarrow \varphi_i - D_i\ P_{i+1}^P \pmod{p^{M'}}$
(15) else
(16) for $i = 0$ to $m' - 1$ do $J_i^P \to J_i^P - p^{M'} P_i^P \pmod{p^{M'}}$
(17) return $(J_0^P, \ldots, J_{n'-1}^P)$.

5. Nonlinear method for computing the number of points with cryptographic proprieties - SatOT

Starting from the proof of Satoh's model, we developed a computing method for elliptic curves subspaces with parameter p and a number of points characterized by $\overline{F_{OT}} : \overline{E}(\overline{\mathbb{F}}_q) \to \overline{E}(\overline{\mathbb{F}}_q) : (x, y) \longmapsto (x_p^q, y_p^q)$. We define cryptographic points of degree 1 as the set of potential keys for ECC systems. The method ensures that a subspace has a lower computational complexity to generate such points, furthermore, it keeps the attack complexity on ECDLP at the same level with the general case (implementation 3).

Algorithm 3 Nonlinear method to compute the 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: Cryptographic points of degree 1 from a nonsupersingular elliptic curve $\overline{E}(\mathbb{F}_{p^n}^q)$.

(1) For each point from $\overline{E}$, compute subset $\overline{E}_p$, as an isomorphism, 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) $m' \leftarrow \lceil \frac{m}{2} \rceil \lceil \frac{p}{2} \rceil$,
$M' \leftarrow (m - m') \pmod q$.
(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) $t \leftarrow \Phi_p'(J_i^q, J_{i+1}^q)^{-1} \pmod{p^{M'}}$.
(10) $D_i \leftarrow t\Phi_p'(J_{i+1}^q, J_i^q) \pmod{p^{M'}}$.
(11) $P_i \leftarrow t((\Phi_p(J_i^q, J_{i+1}^q) \pmod{p^{M'}}) \pmod{p^m})$.
(12) $R \leftarrow \Phi_p'(J_0^q, J_{n-1}^q) \pmod{p^{M'}}$.
(13) $S \leftarrow (((\Phi_p(J_{n-1}^q, J_0^q) \pmod{p^{M'}}))/p^m) \pmod{p^M}$.
(14) If either D_i is determined by a point from outside of the nonsupersingular elliptic curve, that point will be eliminated.
(15) For $i = 0$ to $min(M', n - 2)$ do
(16) $S \leftarrow S - RP_i \pmod{p^{M'}}$
(17) $R \leftarrow -RD_i' \pmod{p^{M'}}$
(18) $R^q \leftarrow R + \Phi_p'(J_{n-1}^q, J_0^q) \pmod{p^{M'}}$.
(19) $P_{n-1}^q \leftarrow SR^{-1} \pmod{p^{M'}}$.
(20) If any P characterizes a point from outside of the nonsupersingular elliptic curve, resumes at step 7.
(21) For $i = n - 2$ to 0 by step -1 do
(22) $P_i \leftarrow P_i - D_i\ P_{i+1}^q \pmod{p^{M'}}$.
(23) For $i = 0$ to $n - 1$ do
(24) $J_i^q \leftarrow J_i^q - p^{M'} \cdot P_i/D_i' \pmod{p^{M'}}$.
(25) Return $(J_0^q, \ldots, J_{n-1}^q)$.

5.1. **Transformation of the first invariant j.** The repeated application of Vercauteren's property can be used on nonsupersingular elliptic curves spaces F_p^q to compute the invariants j^q (implementation 4).

Algorithm 4 Converting the first invariant j

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

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

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

The inverse substitution of Frobenius Σ^{-1} has as solving method:

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

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

Starting from those, Kim et all [3] highlighted the possibility to use some finite fields with a Gaussian Normal Base (GNB) of small type. This base can be converted to $\mathbb{Z}_q$, thus, optimizing the computations on 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 [3].

Proposition 6.1. *Let p be a prime number and (n, t) two positive integers such that $(nt + 1)$ is prime and other than p. Let γ be a primitive root of order $(nt + 1)$ of the unit in an extension of field $\mathbb{Q}_p$. If $gcd(nt/e, n) = 1$, with order e of $(p \bmod (nt + 1))$, then every primitive root of order t of the unit τ in $\mathbb{Z}/(nt + 1)\mathbb{Z}$ can be written as*

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

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

In [3] there are values for $\mathbb{Z}_q$ as being elements from the ring

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

The multiplication of two elements from $\mathbb{Z}_q/(p^m\mathbb{Z}_q)$ will require a number of operations with $O((nmt)^\mu)$ complexity, which according to the proposition 6.1 can be optimized at $t \le 2$.

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

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

It is possible to reduce the complexity of the computation from the Frobenius substitution by using a redundant representation based on an inclusion ($\mathbb{Z}_q$ from $\mathbb{Z}_p[x]/(x^{n+1}-1)$) which concludes in $\alpha=\sum_{\mathrm{i}=0}^{n-1}\alpha_i\beta^i$ and $\alpha(x)=\sum_{\mathrm{i}=0}^{n-1}\alpha_i x^i+0x^n$. Then $\Sigma^k(\beta)=\beta^{p^k}$ leads to

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

The obtained result will lead to $\Sigma^k(\alpha)$ operations by permuting its coefficients $\alpha(x)$. This determines the computation method for Satoh-Skjernaa-Taguchi-systems types over elliptical curves which contain cryptographic points of degree 1.

If we consider $\Gamma(X,\Sigma(X))=0$, and $x\in\mathbb{Z}_q$ a root for $\Gamma(X,Y)\in\mathbb{Z}_q[X,Y]$, we compute an approximation $x_m\equiv x\pmod{p^m}$ and define $\delta_m=(x-x_m)/p^m$. By constructing the Taylor series expansion for x_m, will result:

$$\begin{aligned}0&=\Gamma(x,\Sigma(x))=\Gamma(x_m+p^m\delta_m,\Sigma(x_m+p^m\delta_m))\\&\equiv\Gamma(x_m,\Sigma(x_m))+p^m(\delta_n\Delta_x+\Sigma(\delta_m)\Delta_y)\pmod{p^{2m}},\end{aligned}\tag{6.1}$$

where

$$\Delta_x\equiv\frac{\partial\Gamma}{\partial X}(x_m,\Sigma(x_m))\pmod{p^m},$$

$$\Delta_y\equiv\frac{\partial\Gamma}{\partial Y}(x_m,\Sigma(x_m))\pmod{p^m}\Gamma(x_m,\Sigma(x_m))\equiv 0\pmod{p^m}$$

Simplifying with p^m we obtain the relation

$$\frac{\Gamma(x_m,\Sigma(x_m))}{p^m}+\delta_m\Delta_x+\Sigma(\delta_m)\Delta_y\equiv 0\pmod{p^m}\tag{6.2}$$

for $\delta_m \bmod p^m$.

To obtain first degree points it is sufficient to have $\mathrm{ord}_p(\Delta_y)=0$, which means that Δ_y is a unit in $\mathbb{Z}_q$ and $ord_p(\Delta_x)>0$. Performing the reduction operation modulo p for equation (6.2) we get the next result:

$$\delta_m^p=-\frac{\Gamma(x_m,\Sigma(x_m))}{p^m\Delta_y}\pmod{p}\tag{6.3}$$

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

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

From $\Gamma(\Sigma^{-1}(x_m),x_m)\equiv 0\pmod{p^m}$ it is necessary only to compute the inverse of $(\frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_m),x_m) \bmod p)$. Therefore, it can replace Satoh's classical method [8] for nonsupersingular elliptic curve $\mathbb{F}_p^q$ (our solution can be found in the algorithm 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 $x_0\in\mathbb{Z}_q$ which satisfies $\Gamma(\Sigma^{-1}(x_0),x_0)\equiv 0 \pmod p$ and the precision m.
Output: Item $x_m\in\mathbb{Z}_q$ with $\Gamma(\Sigma^{-1}(x_m),x_m)\equiv 0 \pmod{p^m}$ and $x_m\equiv x_0 \pmod p$.

(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 the nonsupersingular elliptic curve then
(4) $\quad$ resumes on step 1
(5) $d\leftarrow \left(\frac{\partial\Gamma}{\partial Y}(\Sigma^{-1}(x_0),x_0)\right)^{-1} \pmod p$.
(6) $y\leftarrow x_0 \pmod p$.
(7) For i=0 to m do
(8) $\quad x\leftarrow \lfloor\frac{\Sigma^{-1}(y) \pmod{p^i}}{x_m^q(i)}\rfloor$.
(9) $\quad y\leftarrow y-d\Gamma(x,y) \pmod{p^i}$.
(10) Return y.

The complexity of the classic algorithm is given by the recalculation of $\Gamma(x,y)$ after every iteration. Therefore, the values of x and y at step $i+1$ are very close to the values from step i. On the other hand, the result given in algorithm 5 uses an approximation of the two parameters which simplify the computations. After determining $x_W\equiv x \pmod{p^W}$ associated to a point W, we select the elements $s\in\mathbb{N}$, for which

$$\Gamma(\Sigma^{-1}(x_{sW+i}),x_{sW+i})\equiv\Gamma(\Sigma^{-1}(x_{sW}),x_{sW})+\Delta(mod\ p^{(s+1)W}) \tag{6.4}$$

with

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

Finally, to obtain the solution, we compute the partial derivatives

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

in $\pmod{p^W}$ case.

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 (6.4).

6.1. **A variant of SatSk-Taguchi's algorithm for nonsupersingular elliptic curves defined over $\mathbb{F}_q$.** Starting from the parameter description of the nonsupersingular elliptic curves (algorithm 2) and the method to compute the points of degree 1, we determined an implementation to compute the elements x_m. This is implemented for the subspaces of invariants which cannot be deduced directly from cryptographic analysis of the ANG system (illustrated in algorithm 6).

For optimal implementations it is necessary to use only the W points which are multiples of the processor registry size.

7. Implementation

Based on the illustrated algorithms, we can construct the encryption system for the case of nonsupersingular elliptic curves. Starting from the Koblitz's general case

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

Input: Polynomial $\Gamma(X,Y) \in \mathbb{Z}_q$, item $x_0 \in \mathbb{Z}_q$ which satisfy $\Gamma(\Sigma^{-1}(x_0), x_0) \equiv 0 \pmod p$ and precision m. Canonical system $(J_0^q, \dots, J_{n-1}^q)$, obtained using algorithm 2.

Output: Item $x_m^q \in \mathbb{Z}_q$, with $\Gamma(\Sigma^{-1}(x_m^q), x_m^q) \equiv 0 \pmod{p^m}$ and $x_m^q \equiv x_0 \pmod p$.

(1) $y \leftarrow$ ALG 5(x_0, W).
(2) $x \leftarrow \Sigma^{-1} \pmod{p^W}$.
(3) $\Delta_x \leftarrow \frac{\partial \Gamma}{\partial X}(x,y) \pmod{p^W}$.
(4) $\Delta_y \leftarrow \frac{\partial \Gamma}{\partial Y}(x,y) \pmod{p^W}$.
(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) $\quad\quad \delta_y \leftarrow -dp^{-(sW+1)}V \pmod p$.
(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.

solution ([5]), a particular algorithm is developed with respect to Hensel's theorem conditions.

Let be the parameters $(\mathcal{F}, \phi, \alpha_E, \beta_E, \Gamma, \rho, \xi)$, η and $\mu = \mu_1, \dots, \mu_n$ the plain message. For each μ_j, $j = 1, \dots, n$, the necessary steps are:

(1) Let μ_j be an integer which respects the condition: $0 \le \mu_j \le \frac{p}{\eta} - 1$
(2) Let $x_i = \eta\mu_j + i$ where $i = 0, 1, 2 \dots, (\eta - 1)$
(3) Compute $c_i = x_i^3 + \alpha_E x_i + \beta_E$ using recursive operations until $c_i^{\frac{\phi-1}{2}} \equiv 1(mod\ \phi)$
(4) ALG 6(Γ, c_i)
(5) Compute $y_i = \sqrt{c_i}$
(6) $\mathcal{M}(x_i, y_i) = (x_i, y_i^{(\phi+1)/4})$ is the point on the elliptical curve that corresponds to the message μ_j.

Conclusions. In the present paper, starting from the classical algorithms which offer solutions in the general cases, we developed our own solutions for the particular case of boundary conditions which are determined by models based on nonsupersingular elliptic curves.

This model is resistant to differential analysis due to Frobenius' isomorphism that was used to the implementation.

Further research will consist in reducing the computation complexity of partial differential equations which are involved in the algorithms.

Acknowledgments. The author acknowledges the support through Grant of The Executive Council for Funding Higher Education, Research and Innovation, Romania-UEFISCDI, Project Type: Advanced Collaborative Research Projects - PCCA, Number 23/2014.

References

[1] G. B. Agnew, R. C. Mullin, S.A. Vastone; An implementation of elliptic curve cryptosystems over $f_{2^{155}}$, *IEEE Journal on Selected areas in Communications*, **5** no. 11 (1993), 804–813.

[2] R. Alsaedi, N. Constantinescu, V. Radulescu; Nonlinearities in Elliptic Curve Authentication, *Entropy*, **16** no.9 (2014), 5144–5158.

[3] H.Y. Kim, J. Y. Park, J. H. Cheon, J. H. Park, J. H. Kim, S. G. Hahn; Fast elliptic curve point counting using Gaussian Normal Basis, *Algorithmic Number Theory, Lecture Notes in Computer Science, Springer Berlin Heidelberg*, **3076** (2004), 292–307.

[4] N. Koblitz; Elliptic curve cryptosystems, *Mathematics of Computation*, **48** no. 177 (1987), 203–209.

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

[6] J. Lubin, J.-P. Serre, 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*, American Mathematical Society (1964).

[7] V. S. Miller; Use of elliptic curves in cryptography, *Advances in Cryptology CRYPTO 85 Proceedings, Lecture Notes in Computer Science, Springer*, **218** (1986), 417–426.

[8] T. Satoh; On p-adic point counting algorithms for elliptic curves over finite fields, *Algorithmic Number Theory, Lecture Notes in Computer Science Springer*, **2369** (2002), 43–66.

[9] J. P. Serre; *Local Fields*, Springer-Verlag, GTM 67, 1979.

[10] N. P. Smart; Elliptic curves over small fields of odd characteristic, *Journal of Cryptography*, **12** no. 2 (1999), 141–151.

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

[12] O. A. Ţicleanu, N. Constantinescu, D. Ebânca; Intelligent data retrieval with hierarchically structured information, *Intelligent Interactive Multimedia Systems and Services - Proceedings of the 6th International Conference on Intelligent Interactive Multimedia Systems and Services, IIMSS 2013, Sesimbra, Portugal*, doi: 10.3233/978-1-61499-262-2-345 (2013), 345–351.

[13] O. A. Ţicleanu; Mathematical Models in Cryptography, *Journal of Knowledge Communication and Computing Technologies*, **4** (2013), 1–9.

[14] O. A. Ţicleanu; Nonlinear analysis on elliptic curves subspaces with cryptographic applications, *Annals of the University of Craiova, Mathematics and Computer Science Series*, **41** no. 2 (2014), 292–299.

Oana Adriana Ţicleanu

University of Craiova, Street: A.I. Cuza 13, 200585 Craiova, Romania

E-mail address: oana.ticleanu@inf.ucv.ro