DOI: 10.2478/auom-2020-0033
An. Şt. Univ. Ovidius Constanţa
sciendo
Vol. 28(3),2020, 39–49

Nonlinearities on particular elliptic curves subspaces and applications

Ramzi Alsaedi, Abdelwahab Dhifli and Abdeljabbar Ghanmi

Abstract

Researching on mathematical models for cryptography means to, primary, define the optimal spaces and rules for which we can archive the maximum time to find the involved parameters of the keys and, in the same time, to optimise the time for key generation.

In the present work, we treat a particular case of some subspaces from elliptic curves which respect the announced principles.

1 Domain Description

1.1 The Space Study

All researchers are involved, for Public Key Cryptography (PKC), in parameters pair generations ([4, 5, 6, 7]), with respect for

a. complexity cracking period - that means the necessary time to discover the $\{\chi_1, \chi_2\}$ pair values which have the properties to be part of the necessary computations for PKC, that involved the space of solutions, more exactly, the all pair which respect a certain properties set, from s defined space of values, as described in [8, 12, 13, 14].

b. a defined subspaces of the values which are in an area Θ, which is a part of a domain values for PKC, based on results from [17, 20].

Key Words: cryptography, elliptic curves.
2010 Mathematics Subject Classification: Primary 14G50, 94A60; Secondary 11G05, 11G07.
Received: 07.01.2020
Accepted: 17.02.2020

Discussing the point b. is about how to define a domain values, based on a defined equations, and for this domain to define rules that obtain a subdomain that maximise the numbers of pairs that respect certain properties that make than suitable to be named PKC, but this subdomain to respect the next two properties: first is to be of a small dimension, compared with others, second, is to have enough values that are suitable candidates for PKC applications we will focus our research on point b., which is about to define a mathematical model that fulfils the requests.

2 Shao Basic Scheme and Solution to Extended Applicability

Basically, there are two parts, composed by signers and receivers of involved requests of a blid signature from the signer, and the signer issues the blind signatures to the requesters. The general scheme can be described in four phases: (1) the initialisation phase, (2) the requesting phase, (3) the signing phase, and (4) the extraction phase.

First Phase
Signer will compose a computed value $n = pq$, where p, q are defined as two large primes, and $p \equiv q \equiv 3(\bmod 4)$. Let H be a one-way hash function. The signer keeps p and q secret, and publishes n and H.

Second Phase
Message signature is defined as m, where the requester will compute randomly two integers u and b, which respect the rule

$$\alpha = b^2 H(m)(u^2 + 1) \bmod n. \tag{1}$$

The result will be α, and has to be delivered to the signer.

Third Phase
By receiving α, the signer will compute an integer x. Signer knows the values p, q of n, and

$\alpha(x^2+1) \bmod n$ is a QR in $\mathbb{Z}_n^*$, and, in this point, the signer can compute t from

$$t^{-2} = \alpha(x^2 + 1) \bmod n. \tag{2}$$

At this instance, the signer will have the values (t, x) and send it to the requester.

Fourth Phase Having (t, x), the requester will do

$$c = (ux - 1)(x + u)^{-1} \bmod n, \tag{3}$$

and

$$s = bt(x + u) \bmod n. \tag{4}$$

Values (c, s) represents a fingerprint of m. It's validity, for values (c, s), in relation with m, will be represented by the

$$H(m)s^2(c^2 + 1) = 1 \bmod p. \tag{5}$$

The equation will be verified as long as the pair (c, s) will have the computed values for the message m. From these, the next equation represents the condition to have a validation

$$t^2\alpha(x^2 + 1) = t2t - 2 = 1 \bmod n. \tag{6}$$

which will be decomposed in
$H(m)s^2(c^2 + 1)$
$= (\frac{\alpha}{b^2(u^2+1)})(bt(x + u))^2((\frac{ux-1}{x+u})^2 + 1)$
$= (\alpha b^2(u^2 + 1))(bt)^2((ux - 1)2 + (x + u)2)$
$= (\alpha b^2(u^2 + 1))(bt)^2(x^2 + 1)(u^2 + 1)$
$= t^2\alpha(x^2 + 1) = 1(\bmod n)$.

3 Scheme Limitation

In certain cases of nonlinear analysis of the basic scheme, there are a possibility to reveal the involved parameters, which represents the seeds of the keys.

1. Considering RI_i as $i$ss requesters identity. The associated values are $S = \{(RI_i, \alpha_i, t_i, x_i) \mid i = 1, 2, \ldots, z\}$ for z for message m. Signer's values are $(H(m), c, s)$

2. Starting from these, the other part will have to allocate the other values

$$cs = (ux - 1)bt \bmod n. \tag{7}$$

The value t for values S represents basic parameters and are computed by the next equations

$$cst^{-1} = (ux - 1)bt \bmod n, \tag{8}$$

$$(cst^{-1})^2 = (ux-1)^2b^2 = (u^2x^2-2ux+1)b^2 = u^2b^2x^2+b^2-2uxb^2(modn). \tag{9}$$

3. Components of the values sets are

$$\alpha = b^2 H(m)(u^2 + 1) \bmod n,$$

and the other part will generate

$$\alpha H^{-1}(m) = b^2(u^2 + 1) = b^2u^2 + b2(\ \mathrm{mod} n). \tag{10}$$

4. Signer phase are described as

$$(cst^{-1})^2 = u^2b^2 + b^2 - 2ub^2 \bmod n. \tag{11}$$

which can be derived in the next values

$$(cst^{-1})^2 = \alpha H^{-1}(m) - 2ub^2 \bmod n.$$

Consequently,

$$2ub^2 = \alpha H^{-1}(m) - (cst^{-1})^2 \bmod n.$$

which will become

$$ub^2 = 2 - 1(\alpha H - 1(m) - (cst^{-1})^2) \bmod n. \tag{12}$$

5. From these equations, as long as

$$s = tb + tub \bmod n$$

the result become

$$sb = tb^2 + tub^2 \bmod n. \tag{13}$$

2-1(H-1(m)-(cst-1)2) will be the computed value for tub from these equations will be rewrite as

$$sb = tb^2 + t(2^{-1}(\alpha H^{-1}(m) - (cst^{-1})^2)) \bmod n. \tag{14}$$

But

$$tb^2 - sb = -t(2^{-1}(\alpha H^{-1}(m)) - (cst^{-1})^2) \bmod n,$$

can be rewrite as

$$b^2 - st^{-1}b = -(2^{-1}(\alpha H^{-1}(m)) - (cst^{-1})^2) \bmod n.$$

The second participant will have the representation

$$b(b - st^{-1}) = (cst^{-1})^2 - 2^{-1}\alpha H^{-1}(m) \bmod n. \tag{15}$$

which can be computed with parameters from equation 13 without initial conditions, which is a vulnerability of basic scheme. From these, we initiated a study to solve the issues for strong models necessity.

4 Nonlinearities on particular subspaces

Starting from what we expose in the previous section, it is necessary to develop particular mathematical models to have robust implementation. Let be considered as space generations, a class of functions which has as origin an elliptic curves case of space:

A finite field $\mathbb{F}_p$ which has partitions

$$(\mathbb{F}_p) = \{\{0_0, \ldots, (p-1)_0\}^0, \{0_1, \ldots, (p-1)_1\}^1, \ldots, \{o_q, \ldots, (p-1)_q\}^q\}$$

Each partitions represents a subspace that generations values on different curve from a spectre of elliptic curves.

For these, we will define an addition operation as :

- let $a, b \in \mathbb{F}_p$, then $a + b = t,\ t \in \mathbb{F}_p$, where $t \in [0, p-1]$ will be the remainder when the integer $a + b$ is derived by p.

  Analogues, for $a, b \in (\mathbb{F}_p)_q$, then $a + b = t,\ t \in \{(\mathbb{F}_p)_q / \ \exists\ (a_f, b_f)$ which are remainders of divisions form $p\}$.

The second operation is multiplication, that really goes to:

- For two values $(a_1, a_2) \in \mathbb{F}_p$ will be defined the multiplication as $a_1 \cdot a_2 = m$, with m from the same space of $\mathbb{F}_p$, that really goes to $m \in [0, p-1]$ is equal with remainder in the case of a_1, s_2 is divided by p. The operation is a case of computation of modulo the space partition p. In the case of spaces, will be a computation based on a partition q.

With all of these established, for the domain space (unlike in [21], it is a subspace), we will describe an elliptic curve family as:

Let p be a prime value, with two points α_1 and α_2 from $\mathbb{F}_p$, which fulfil $4(\alpha_1)^3 + 27(\alpha_2)^2 \not\equiv 0$.

An elliptic curve $E(\mathbb{F}_p)$ over $\mathbb{F}_p$ will be defined by points $P = (x, y)$, where $x, y \in \mathbb{F}_p$ by the equations

$$y^2 \equiv x^3 + \alpha_1 x + \alpha_2 \pmod p$$

together with a special point O, called the point at infinity. From these, we will have the equation $y^2 \equiv x^3 + \alpha_1 x + \alpha_2 \pmod{p}$ as the equation which will define $E(\mathbb{F}_p)$.

Analogues, will be defined the subspaces $E((\mathbb{F}_p)_q)$ which represents the fractions of the initial space. The study will use a nonlinearities model definitions, to be used like frontier values that are interesting, from PKC point of view.

5 Nonlinearities on Boundary Solutions

As we stated before, to achieve the request is about to define the particular subspace that has (χ_1, χ_2) values pairs with cryptographic properties.

Let be two values χ_1 and χ_2 that denote a solution for boundary cases, in a subspace q from $(\mathbb{F}_p)_q$, χ_0 a frontier value, then

$$\lim_{\chi_1 \to \chi_0} d(\chi_1)^{\alpha} u(\chi_1) = \left(\frac{(\alpha(\alpha+1))^{q-1}}{(\beta(\beta+1))^q} \right)^{\frac{1}{(p-1)(q-1)-q\Theta}}$$

where Θ is the partition rank.

It will become

$$\lim_{\chi_1 \to \chi_0} d(\chi_1)^{\alpha\Theta} u(\chi_1) = \left(\frac{\alpha(\alpha+1)^{q-1} \cdot \Theta}{(\beta(\beta+1))^q} \right)^{\frac{1}{(p-1)(q-1)-q\Theta}}$$

for the first state of the boundary solution

$$\lim_{\chi_1 \to \chi_0} d(\chi_1)^{\beta\Theta} v(\chi_1) = \left(\frac{\beta(\beta+1)^{q-1}}{(\alpha(\alpha+1))^q} \right)^{\frac{1}{(p-1)(q-1)-q\Theta}}$$

From these, we will have

$$\lim_{\chi_1 \to \chi_0} d(\chi_1)^{\alpha+1} \nabla u(\chi_1) v(\chi_0) = \alpha \left(\frac{(\alpha(\alpha+1))^{\Theta-1}}{(\beta(\beta+1))^q} \right)^{\frac{1}{(p-1)(q-1)-q\Theta}}$$

and, analogues:

$$\lim_{\chi_1 \to \chi_0} d(\chi_1)^{\beta+1} \nabla v(\chi_1) v(\chi_0) = \beta \left(\frac{(\beta(\beta+1))^{p-1}}{(\alpha(\alpha+1))^q} \right)^{\frac{1}{(p-1)(q-1)-q\Theta}}$$

For a particular particles Θ, we will have to determine solutions u, v radial and positive, which fulfill the requirement $\Delta u = \alpha^2(q) u_p$ and $\Delta v = \beta^2(q) v_p$ which are near enough by a ball Γ of radius R, such as $\partial\Gamma$ respect:

$$\int_0^R (R-q) \, |\alpha(q) - \beta(q)| \, dq < f$$

where f represents a maximum expected number of pairs (χ_1, χ_2) with cryptographic properties.

By computations, it can be determined that in the case of above defined parameters, the (χ_1, χ_2) pair will have the next fixed where these are inducted

$$\begin{cases} \sum\limits_{i,j=1}^{P} \alpha_i(\xi) \frac{\partial^2 \bar{u}}{\partial \xi_i \partial \xi_j} + \sum\limits_{i=1}^{P} \beta_i(\xi) \frac{\partial \bar{u}}{\partial \xi_i} \cdot \Theta^q \\ \sum\limits_{i,j=1}^{P} \alpha_i(\xi) \frac{\partial^2_{\bar{v}}}{\partial \xi_i \cdot \partial \xi_j} + \sum\limits_{i=1}^{P} \beta_i(\xi) \frac{\partial \bar{v}}{\partial \xi_i} \cdot \Theta^{-q} \end{cases}$$

In the case of multiple solution which satisfies the conditions, in the present, it is computed the subspaces with maximum number of (χ_1, χ_2) pairs.

For the exposed model, these subspaces it is determined by the simple computation of $d(\chi_i)$, in the case of $\chi_i \in (\mathbb{F}_p)_q$, by choosing the frontier value χ_0, for each subspace defined by partition q. It will be denoted by $d(\chi)$ and $u(\chi)$ values

$$\lim_{\chi \to \chi_0} d(\chi)^{\alpha} \cdot u(\chi) = \left(\frac{(\alpha(\alpha+1)^{p-1} \cdot \Theta}{\beta(\beta+1)^q} \right)^{\frac{1}{(p-1)(q-1)-\Theta}}$$

$$\lim_{\chi \to \chi_0} d(\chi)^{\beta} v(\chi) = \left(\frac{(\beta(\beta+1))^{p-1} \cdot \Theta^2}{(\alpha(\alpha+1))^q} \right)^{\frac{1}{(p-1)(q-1)-\Theta^2}}$$

which will determine, in the nonlinear case

$$\begin{cases} \Delta u = u^p \cdot v^q \cdot d(\chi)^{\alpha} \\ \Delta v = u^q \cdot v^p \cdot d(\chi)^{\beta} \end{cases}$$

It bring as the subspace which will have the necessary number of pairs (χ_1, χ_2) with candidates parts of subspace that are part of, to be PKC pairs.

This kind of subspaces are defined by a bilinear function like:

$$F(\chi_1, \chi_2) = \frac{u(\alpha)}{(\alpha - \beta)(\chi_1 - \chi_2)}(x - y)(x_0 - y_0)$$

where points $(\alpha, \beta), (x, y), (x_0, y_0)$ represents a general frontier point, a solution point and a point from ball Γ, near to frontier solutions and $\frac{\partial F}{\partial x} = \chi_1 \cdot y + \chi_0$ and $\frac{\partial F}{\partial y} = \chi_1 x + \chi_0$.

6 The Implementation Study

In the case of nonlinear subspace, determined by the parameter Γ, we will have the adapted case used on [11], that is constructed similarly, for the (χ_1, χ_2)

Algorithm 1 Pair Determined Protocol

1: p and q are defined
2: r is the ball radius
3: the χ_1 parameter is determined by Se co-prime to p such that $1 \leq Se \leq \chi_1 - 1$
4: the prover computes $v = r\chi_1^2 \bmod p$ which is first parameter
5: the prover chooses r_0 such that $1 \leq r \leq n - 1$
6: the prover computes $x = r^2 \bmod n$ and sends it to the verifier
7: the verifier chooses a bit $e \in \{0, 1\}$ and sends it to the prover
8: **if** $e = 0$ **then**
9: the prover computes $y = r\chi_1$
10: **else**
11: the prover computes $y = r\chi_2 \bmod n$
12: **end if**
13: the prover sends y to the verifier
14: the verifier rejects if $y = 0$ or $y^2 \neq \chi_1 * \chi_2^e \pmod n$

values. It will construct the frontier solutions as follow:

These implementation was used on case determinations for medical application, in [15, 18], that was implemented in a particular subspaces (that was based on the [1, 2, 3, 9]) defined as in [23]. The security level of the solution was based with respect for the [22, 19, 16].

7 Conclusions

Starting from the frontier solutions on nonlinear cases that determines partitions on elliptic curves subspaces, where determined particular boundary solutions pairs which are of cryptographically interests, particularly on PKC. These kind of subspaces are determined by parameters which are classified in two categories, as solutions of nonlinear equations and in the neighbourhood of these solutions, which is the defined ball Γ. These results where used on some practical applications ([10]), where are necessary to determines the behaviour of key pairs, in the case of generations on a single nonsupersingular curve. As future study we intend to determine the optimal radius of the Γ in the cases of a nonsupersingular elliptic curves class that have the definition based on boundary solutions determines by a single curve, which was determined on this study.

Acknowledgments:
This work was funded by the University of Jeddah, Saudi Arabia, under grant No. UJ-02-008-ICGR. The authers, therefore, acknowledge with thanks the University technical and financial support.

References

[1] D. Chaum and E. van Heyst, Group signatures, *Advances in Cryptology EUROCRYPT '91*, Vol. **547** of Lecture Notes in Computer Science, Springer-Verlag, pp. 257–265, 1991

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

[3] Oana Ticleanu, Nicolae Constantinescu, Daniel Ebanca, Intelligent data retrieval with hierarchically structured information, *KES-IIMS*, Vol. **254**, pp. 345–351, Jun 26-28, Portugal, 2013

[4] Oana Ticleanu, Differential operators over particular elliptic curves spaces with cryptographic applications. E. Journal of Differential Equations, Vol. 2015, No.303, pp. 19, 2015.

[5] Oana Ticleanu, Endomorphisms on elliptic curves for optimal subspaces and applications to differential equations and nonlinear cryptography. E. Journal of Differential Equations, Vol 2015, No.214, pp. 19, 2015.

[6] Alin Golumbeanu, Oana Ticleanu, Elliptic Curves Differentiation with Application to Group Signature Scheme, E. Journal of Differential Equations, Vol. 2017, No. 237, pp. 121, 2017.

[7] Nicolae Constantinescu, Oana Ticleanu, Alin Golumbeanu, Nonlinieearities on Cryptographic Shift Registers, Annals of the University of Craiova, Mathematics and Computer Science Series, Vol. 43(1), pp. 2732, 2016.

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

[9] Nicolae Constantinescu, Authentication ranks with identities based on elliptic curves, *Annals of the University of Craiova, Mathematics and Computer Science Series*, Vol. **XXXIV**(1), pp. 94–99, 2007

[10] Silisteanu Calina, Mitariu Loredana, Ranga Remus, Antonescu Elisabeta, Duica Lavinia, Racheriu Mihaela, Totan Maria and Manea Marinela, Potentiating the Effect of Treatment with Voltaren Gel Using Ultrasonic Frequencies of 1 MHz, Revista de Chimie, **69** (2018), no. 7, 1749–1751.

[11] Ramzi Alsaedi, Nicolae Constantinescu, Vicentiu Radulescu, Nonlinearities in Elliptic Curve Authentication, *Entropy*, Vol. **16**(9), pp. 5144–5158, 2014

[12] Montgomery, P.L. Modular Multiplication without Trial Division. *Math. Comput.* **1985**, *44*, 519–521.

[13] Nicolae Constantinescu, Security System Vulnerabilities, *Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science*, Vol. **13**(2), pp. 175–179, 2012

[14] Muller, V. Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two. *J. Cryptol.* **1998**, *11*, 219–234.

[15] Duica Lavinia, Antonescu Elisabeta, Pirlog Mihail, Purnichi Traian, Szakacs Julianna, Totan Maria, Vintila Bogdan, Mitariu Mihaela, Mitariu Sebastian, Cernusca and Stetiu Andreea, Clinical and Biochemical Correlations of Aggression in Young Patients with Mental Disorders, Revista de Chimie, **69** (2018), no. 6, 1544–1549.

[16] Ion Iancu, Nicolae Constantinescu and Mihaela Colhon, Fingerprints Identification using a Fuzzy Logic System, *International Journal of Computers, Communications & Control*, Vol. **5**(4), pp. 525–531, 2010

[17] Nicolae Constantinescu, George Stephanides, Mirel Cosulschi and Mihai Gabroveanu, RSA-Padding Signatures with Attack Studies, *International Conference on Web Information Systems and Technologies: Internet Technology/Web Interface and Applications*, Portugal, ISBN 978-972-8865-46-7, pp. 97–100, 2006

[18] Mutica M., Ciubara Anamaria, Duica Lavinia, Alexandru D., Plesea Condratovici, Pirlog Mihail and Cara M., Elderly schizophrenic patients - clinical and social correlations, European Neuropsychopharmacology, **26** (2016), no. 2, 5512-5512.

[19] Nicolae Constantinescu, Authentication hierarchy based on blind signature, *Journal of Knowledge Communication and Computing Technologies*, Vol. **1**(1), pp. 77–84, 2010.

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

[21] D. Yong, G. Feng, High speed modular divider based on GCD algorithm over GF(2m), *Journal on Communications*, Vol. **29**(10), pp. 199–204, oct. 2008

[22] Emil Simion and Nicolae Constantinescu, Complexity Computations in Code Cracking Problems, *Concurrent Engineering in Electronic Packaging, IEEE Communication*, may 05-09, pp. 225–232, ISSE 2001

[23] N. Smart, How secure are elliptic curves over composite extension fields?, *EUROCRYPT 2001*, Vol. **2045** of Lecture Notes in Computer Science, Springer-Verlag, pp. 30–39, 2001

Ramzi Alsaedi,
Department of Mathematics,
Faculty of Sciences, King Abdulaziz University,
P.O. Box 80203, Jeddah 21589, Saudi Arabia.
Email: ramzialsaedi@yahoo.co.uk.
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: rsalsaedi@uj.edu.sa

Abdelwahab Dhifli,
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: amdhifli@uj.edu.sa

Abdeljabbar Ghanmi,
Department of Mathematics,
University of Jeddah,
College of Sciences, Saudi Arabia.
Email: aaalghanmy1@uj.edu.sa