Electronic Journal of Differential Equations, Vol. 2015 (2015), No. 214, pp. 1–9.
ISSN: 1072-6691. URL: http://ejde.math.txstate.edu or http://ejde.math.unt.edu
ftp ejde.math.txstate.edu

ENDOMORPHISMS ON ELLIPTIC CURVES FOR OPTIMAL SUBSPACES AND APPLICATIONS TO DIFFERENTIAL EQUATIONS AND NONLINEAR CRYPTOGRAPHY

OANA ADRIANA ŢICLEANU

Abstract. Finite spaces are used on elliptic curves cryptography (ECC) to define the necessary parameters for nonlinear asymmetric cryptography, and to optimize certain solutions of differential equations. These finite spaces contain a set of "cryptographic points" which define the strengthens of the chosen field. One of the current research areas on ECC is choosing optimal subspaces which contains most of the interesting points. The present work presents a new way to define the cryptographic strengthens of a particular field, by constructing an endomorphism between the classically studied subspaces and a certain subspace.

1. Introduction

Recent research in the area of elliptic curves revels that the main applications are about cryptography, mostly about the classical Rivest, Shamir and Adleman encryption algorithm (RSA). The lack of mathematical foundations in the special area of cryptographic subspaces, and the incomplete proofs of parts of it, generates brakes on the implementation, testing and reliability of such methods. There have been proposed and developed a lot of key sessions in authentication with the basic model of elliptic curves, which have become standard tools. Parallel to this, the study of isomorphisms on elliptic spaces has lead us to the theory of space reduction, which is used for obtaining a low dimensional approach. In this study we show a new method for reconstructing a larger space with cryptographic properties for a certain amount of points; this space is called extended multi field (EMF).

2. Mathematical foundations on ECC maps construction

We start with the most important parts of the computing principle: adding points, and multiplying by a scalar selected points for elliptic curves cryptography (ECC). This is necessary for constructing reduced spaces.

Let $r \in \mathbb{R}$ and $P \in E$, where E is an elliptic curve as defined in [2], were r should be represented on 160 or more bits. There are many methods to do computations (see for example [1, 12, 14, 21]). In the present work, we adopt the

2010 *Mathematics Subject Classification.* 12H20, 35R03, 11G05.
Key words and phrases. Elliptic curves cryptography; endomorphism of elliptic curves; Frobenius endomorphism.

Submitted April 9, 2015. Published August 17, 2015.

classical construction, starting from the Weierstrass equation, and using Koblitz adapted proofs [19].

Definition 2.1. An elliptic curve E defined on a K field is given by the equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_i \in K$. This equation is called the Weierstrass equation.

Definition 2.2. The discriminant of the elliptic curve given by the Weierstrass equation has the form

$$\Delta = d_2^2d_8 - 8d_4^3 - 27d_6^2 + 9d_2d_4d_6,$$

where $\Delta \neq 0$ and:

$$d_2 = a_1 + 4a_2, \quad d_4 = 2a_4 + a_1a_3, \quad d_6 = a_3^2 + 4a_6$$
$$d_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_3^2\,.$$

In the case: $K = F_q$, where $q > 3$ is a prime number, the Weierstrass equation can be simplified to

$$E : y^2 = x^3 + ax + b$$

The discriminant in this case is $\Delta = -16(4a^3 + 27b^2)$.

Elliptic curves defined over a binary field are given by the equation

$$E : y^2 = x^3 + ax + b,$$

and have discriminant $\Delta = b$. For a point $P(x, y)$ its reverse is $-P(x, x + y)$. The addition and the doubling operations of the points are calculated in the same way as the prime curves case: If we have the point $P(x, y)$, its reverse will be $-P(x, -y)$. If we have two points P and Q with $P(x_2, y_1)$ and $Q(x_2, y_2)$ then their addition will be

$$P + Q = R(x_3, y_3),$$

where

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

and $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$. For the doubling operation, there are the formulas

$$x_3 = \lambda^2 - 2x_1$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

where $\lambda = \frac{3x_1^2 + a}{2y_1}$.

The only difference between the curves defined on a K field and the curves defined on a $K = F_q$ binary field, is that for a point $P(x, y, z)$ the inverse of it is $P(x, x + y, z)$. More details about implementation can be found in [4].

3. Koblitz mathematical infrastructure

Let E be an elliptic curve defined over the filed F_q, by

$$E_a : Y^2 + XY = X^3 + aX^2 + 1, \quad \text{with } a = 0 \text{ or } a = 1$$

which is called Koblitz multiplication curve with its properties presented for the first time in [19].

A Koblitz curve E has coefficients in F_q and a point from $E(F_q)$ with $q = 2^k$ and k is a large number, for the efficiency of the security it can be even a prime number $k \geq 160$, [8].

Koblitz formed the equation which makes the calculation of the number of points on an elliptic curve easier :

$$\#E(F_{2^k}) = 2^k - \big(\frac{-1+\sqrt{-7}}{2}\big)^k - \big(\frac{-1-\sqrt{-7}}{2}\big)^k + 1.$$

The calculation on Koblitz curves has the advantage of using the homomorphism groups:

$$\tau : E(F_q) \to E(F_q), \quad \tau(x,y) = (x^2, y^2).$$

In the calculation of the points on an elliptic curve, there are endomorphisms allowed [5], under the form of a ring, $\operatorname{End}(E)$, which include:

- a scalar multiplicative group;
- Frobenius endomorphism ψ (on a limited field);
- $\mathbb{Z}[\psi] \subseteq \operatorname{End}(E)$.

Examples of computing points on an elliptic curve using the endomorphisms can be found in [5, 6, 19]. According to these, we have the following statement.

Theorem 3.1. $\operatorname{End}(E)$ *is isomorphic to an order in an imaginary quadratic field, for an integer D called discriminant,*

$$\mathcal{O}(D) := \mathbb{Z} + \frac{D+\sqrt{D}}{2}\mathbb{Z}.$$

Frobenius endomorphism ψ has the trace t and norm n, therefore $\mathbb{Z}[\psi] \cong \mathcal{O}(t^2 - 4n)$.

Let E be an elliptic curve on the finite field F_q, and ψ a Frobenius endomorphism E. In an integer ring with imaginary quadratic field $K = \mathbb{Q}(\sqrt{D_k})$, an element τ with norm q is equal with:

$$\tau = \frac{t + z\sqrt{D_k}}{2} \quad \text{with } 4q = t^2 - z^2 D_k.$$

The trace of τ is $q + 1 - \#E$, according to [2].

Definition 3.2. Let $\operatorname{End}(E)$ be a endomorphisms ring on an elliptic curve, where $\operatorname{End}(E)$ is either $\mathbb{Z}$, or an isomorphism with a quadratic imaginary order, or an order in a quaternion algebra.

Now, there can be formulated, starting from [2], the next theorems.

Theorem 3.3. $\operatorname{End}(E)$ *is a ring where the multiplication is resulted from the composition.*

Proof. The only point which is required for the verification is the distribution law. Let the endomorphism α, β and γ, where

$$\begin{aligned}(\alpha\circ(\beta+\gamma))(P) &= \alpha((\beta+\gamma)(P))\\ &= \alpha(\beta(P)+\gamma(P)) \quad \text{(by [10, Theorem 3.2])}\\ &= \alpha(\beta(P))+\alpha(\gamma(P)) \quad \text{(because } \alpha \text{ is an homomorphism)}\\ &= (\alpha\circ\beta)(P)+(\alpha\circ\gamma)(P).\end{aligned}$$

Furthermore we obtain $\alpha\circ(\beta+\gamma)=\alpha\circ\beta+\alpha\circ\gamma$ or $(\alpha+\gamma)\circ\gamma=\alpha\circ\gamma+\beta\circ\gamma$. □

Theorem 3.4. End(E) *is a* $\mathbb{Z}$ *algebra, where the multiplication by* m*, and* $m\in\mathbb{Z}$ *is resulted from the composition with* $[m]$*. If* End(E) *contains another endomorphism than the multiples of* m*, then* E *will have a complex multiplication.*

Proof. It has already been demonstrated in Theorem 3.3 that End(E) is a ring, and the multiplication given by m shows that $\mathbb{Z}$ is a subring.

If $p=F_q$ is a finite filed, then E has a complex multiplication, so Frobenius endomorphism $\alpha=(X^k,Y^k)$. Let $P=(a,b)$ be a point in E, then $E(\alpha(P))=E(a^k,b^k)=E(a,b)^k=0$, so $\alpha(P)\in E$. □

3.1. **Frobenius endomorphism.** Let K be a finite field with q elements, and the group $G(K_*/K)$, also called the group of Galois, is generated by the Frobenius automorphism β relative to K, defined by $\beta(\alpha)=\alpha^q$ for any α from K_*. For any finite extension of k/K, the automorphism $k\overset{\beta}{\hookleftarrow}k$ determines a morphism $M(k)\to M(k)$. So, for any X in $M(k)$ it can be defined $X^\beta=X\times_\beta k$. Let O_X be the contact with the function from X and for any subset $Y\subseteq X$, it makes $X\to M(k)$ to be an homeomorphism determined by the map $X\to M(k)$.

Furthermore we define $w_1:O_X(Y)\to O_X(Y)\otimes_\beta k$ and $w_2:k\to O_X(Y)\otimes_\beta k$, two injections $f\mapsto f\otimes 1$ and $\gamma\mapsto 1\otimes\gamma$, and we define the map ψ^* by

$$\begin{gathered}O_X(Y)\otimes_\beta k\xrightarrow{\psi^*}O_X(Y)\otimes_\beta k,\\ f\otimes\gamma\mapsto f^2\otimes\gamma^2.\end{gathered}$$

Thus it can be said that we have defined a Frobenius morphism. If we replace X with an elliptic curve E defined on a k filed and we define $\psi(O)$ being the identity of E^β, then the Frobenius morphism determines Frobenius isogeny $\psi:E\to E^\beta$.

For the particular case when $k=K$, we take it that $E^\beta=E$ and ψ is called Frobenius endomorphism.

If the elliptic curve E is given by the Weierstrass equation

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,$$

then the elliptic curve E^β will be

$$y^2+a_1^qxy+a_3^q=x^3+a_2^qx^2+a_4^qx+a_6^q,$$

and Frobenius isogeny is given by the map

$$\begin{gathered}E\xrightarrow{\psi}E^\beta\\ (x_0,y_0)\mapsto(x_0^q,y_0^q)\end{gathered}$$

We take it that E/K is an elliptic curve defined over a K field. Frobenius endomorphism relative to K checks the equation $\psi^2+t\psi+q=0$ in the endomorphism ring. For any extension k/K of r grade, Frobenius endomorphism relative to k is ψ^r.

4. On site map construction

In this section we define and prove the optimization maps on elliptic curves particular subspaces with cryptographic properties.

4.1. **Frobenius based maps.**

Let be K a filed of characteristic p and E an elliptic curve over K. Let ψ be a Frobenius endomorphism relative to K. From it we define a ring of endomorphism $\mathrm{End}(E)$, a grade in a quaternion algebra.

If $E[p^r] = 0$ for all $r \geq 1$, according with [26] we can prove that a ring of endomorphism $\mathrm{End}(E)$ is the grade in a quadratic imaginary extension of $\mathbb{Q}$.

From this point, we construct an extension of the endomorphism in the following manner:

$$E_1[\Phi^t] = Q/\Phi^t\mathbb{Q}, \quad \text{where } t \in \mathbb{Z},\ t > r$$

These represents an iteration of the basic Koblitz Curve, where Φ is an integer by enough to respect the condition $|E_1| >> |E|$.

We named E_1 as an EMF, as previously defined. This condition ensure the existence of all included subspace generated by $E[p^r]$ from Koblitz theorem [26].

From these, we have E_1 is a supersingular curve and is ordinary, but it is not compulsory for the extension of $End_K(E)$, otherwise it is not a grade in a quaternion algebra [30].

Let be $F_q = F_\Phi t$. We will define our map as follows:

$$\phi : F_q \to F_q :\ x \mapsto x^\Phi \text{ in all subspaces,}$$

it means that for any element x, will be constructed an image of it in any extension of basic Frobenius construction (which represent that any point x has an image on $E_1[\Phi^t]$, previous defined).

It can be noticed that $\phi(0) = 0$, $\phi(1) = 1$ and for all $x, y \in F_q$, $\phi(x, y) = \phi(x)\phi(y)$. The classic Frobenius relation is

$$\begin{aligned} \phi(x+y) = (x+y)^p &= \sum_{i=0}^{p} \binom{p}{i} x^{p-i} y^i \\ &= x^p + \binom{p}{p-1} x^{p-1} y + \dots + \binom{p}{1} x y^{p-1} + y^p \end{aligned} \tag{4.1}$$

for any $x, y \in F_q$. So, $\phi : F_q \to F_q$ is a fields homomorphism. This relation will become

$$\phi(x+y) = (x+y)^\phi = \sum_{i=0}^{\Phi} \binom{\Phi}{i} \prod_{j=1}^{t} x^j,$$

where x^j represents the transformation of x in the subspace j.

From it, is deducted that to construct F_Φ, we will have

$$F_\Phi = \{a \in F_q : \phi(x) = x \text{ in all subspaces}\}$$

It is a tough condition which increase the complexity computation on brute force attack.

4.2. **Example on exposed map construction.** Let $E : y^2 = x^2 + ax$ be an elliptic curve defined over F_Φ field and $t \equiv 1(mod\ 4)$ a prime number. Let be an α element by grade 4 which belongs to the $F_\Phi t$ fields extensions.

From these, the map $\phi : E_1 \to E_1$ (as before defined E_1) will have stated $\phi : (x, y) \mapsto \left(-\frac{x}{4}, \alpha y\right)$, and $\phi : \infty \to \infty$ is an endomorphism of E_1, defined on field $F_\Phi t$.

The endomorphism rings for will become

$$E_1/F_\Phi t : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in F_\Phi t$, where $E(F_\Phi t)$ is a rational point set $F_\Phi t$ over E together with a common point $\mathcal{O}$, for all subspaces.

4.3. **Using extended map of elliptic curves.** In the following we present an application of the extended map construction based on extension of classical solution [2].

Proposition 4.1. *Let* $\operatorname{End}(E_1) = Hom(E_1, E_1)$ *be the ring for an elliptic curve* E_1*, as defined at subsection 4.2. This ring* $\operatorname{End}(E_1)$ *certain completeness subspaces with cryptographic points.*

Proof. The assertion state that ring $\operatorname{End}(E_1)$ has no zero divisors, because it means that the mathematical model is correct defined. Let ν_i and ϑ_i two elements (i is the index of the chosen subspaces). The proof is extended from one subspace, in the same manner, to all other subspaces.

If $\nu_i\vartheta_i = 0$, then $0 = deg(\nu_i\vartheta_i) = deg(\nu_i) \cdot \deg(\vartheta_i)$ and therefore $\deg(\nu_i) = 0$ results that $\nu_i = 0$ respectively $\deg(\vartheta_i) = 0$ which conclude $\vartheta_i = 0$, because otherwise in the formula (4.1) we will have a nonzero point which generates $\mathcal{O}$. □

5. Further applications of elliptic curves to differential equations

In this section we point out the relevance of elliptic curves into the framework of differential equations. Hence, it can be easily seen that the results from our paper can be successfully used to develop the study of some particular classes of differential equations.

Elliptic curves may not be quite as well known circles, but they are really very famous and useful in number theory, and constitute a major area of current research. The elliptic curves were fundamentally used by Wiles and Taylor in order for proving the famous Fermat Last Theorem.

It is also shown that the elliptic curves arise very naturally in the context of KdV Equation. In fact, Korteweg and de Vries showed that the long-wave limit of the periodic waves from elliptic functions is the solitary wave. The discovery of solitary wave solutions to a nonlinear PDE was a surprise in the 19th century. The KdV equation looks like the equation for an elliptic curve when one assumes the solution is a traveling wave. Of course, much more complicated solution equations are connected to algebraic geometry.

The general picture is the following: choose any algebraic curve with an associated Jacobian Variety. Then there exists a solution to a solution equation associated to each choice of a curve and an element of the associated group. If the curve is a hyper-elliptic curve, then it is a solution of KdV Equation.

Recently, in [16] it has been studied some connections between elliptic curves and Mathieu's equation, which represents a model for vibrating elliptical membranes.

Its canonical form is

$$\frac{d^2u}{dz^2} + (\lambda - 2q\cos(2z))u = 0.$$

The Mathieu equation is useful in various mathematics and physics problems. As an example, the separation of variables for the wave equation in the elliptical coordinates leads to the Mathieu equation.

It was shown that the Floquet exponent of the Mathieu equation can be obtained from the integral of a differential form along the two homology cycles of an elliptic curve. According to the Floquet theory, the solution of the Mathieu equation can be written as

$$u_\nu(z) = e^{\omega z} f(z),$$

where $f(z)$ is a function of period π, and in general ν is a constant independent of z.

The exponent ν is called the Floquet characteristic exponent, it is a function of the constants λ and q. A classical result is that the Floquet exponent can be obtained through the Hill's determinant.

Moreover, if ν is an even integer, then the solution $u(z)$ is a periodic function of period π; if ν is an odd integer, then the solution $u(z)$ is a periodic function of period 2π.

The relation between the Mathieu equation and the elliptic curve naturally arise in the integrable theory. The Mathieu equation is the Schrödinger equation of the two body Toda system, while the elliptic curve is just the spectral curve of the classical Toda system.

For instance, let us consider the Mathieu operator

$$\mathcal{L} = d_z^2 + \lambda - q\left(e^{-2iz} + e^{-2iz}\right) = (x^2 + \lambda) \pm \sqrt{y^2 + 4q^2},$$

where $x = d_z$ and $y = q\left(e^{-2iz} + e^{-2iz}\right)$, and it follows the elliptic curve

$$y^2 = (x^2 + \lambda)^2 - 4q^2.$$

We remark that there is a geometric structure for the Mathieu equation which is not captured by asymptotic analysis. Of course, it is possible that the relation we present here is just a particular case of a general picture.

Moreover, in [9] it is treated difference equations on elliptic curves. Some general properties of the difference Galois groups of equations of order two are studied. Interesting connections with the class of discrete Lame equations was also treated. In the context of difference equations, interesting further applications and open problems can be considered. More precisely, our results could be applied for studying difference equations by using the recent Mountain Pass discrete theory used in [20, 23, 24].

Finally, we recall the connection of elliptic curves with the Picard-Fuchs equation, which is a linear ordinary differential equation whose solutions describe the periods of elliptic curves. For more details, see [15]. This equation can be viewed as a hypergeometric differential equation. It has two linearly independent solutions, called the periods of elliptic functions. The ratio of two solutions of the hypergeometric equation is also known as a Schwarz triangle map. Moreover, note that the Picard-Fuchs equation belongs also to the class of Riemann differential equations.

Conclusion. The present work illustrates the construction of an extended map for ECC, with increased complexity against brute force attack, through particular subspaces which define the way to raise the security of the real time implementation for authenticated key exchange algorithms, based on particular supersingular elliptic curves. The theory developed here can be used to study the solutions of some classes of differential equations with substantial relevance in this field, as presented in section 5.

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] R. Alsaedi, N. Constantinescu, V. Rădulescu; Nonlinearities in elliptic curve authentication, *Entropy*, **16** (2014), 5144–5158.

[2] G. Bisson, A. V. Sutherland; Computing the endomorphism ring of an ordinary elliptic curve over a finite field, *J. Number Theory*, **131** (2011), 815-831.

[3] M. Ciet, T. Lange, F. Sica, J. J. Quisquater; Improved algorithms for efficient arithmetic on elliptic curves using fast endomorphisms, Advances in Cryptology - EUROCRYPT 2003, Lecture Notes in Computer Science, 2656, Springer, Berlin, 2003, pp. 387-400.

[4] N. Constantinescu; *Criptography*, Ed. Romanian Academy, ISBN: 978-973-27-1871-1 (2009), 197–220.

[5] N. Constantinescu; Elliptic curve cryptosystems and scalar multiplication, *Annals of the University of Craiova, Mathematics and Computer Science Series*, XXXVII (2010), 27–34.

[6] N. Constantinescu; Elliptic curves-based algorithms in cryptography, Annals of University of Bucharest, XXXI (2004), 149–159.

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

[8] N. Constantinescu; Authentication protocol based on elliptic curve cryptography, *Annals of the University of Craiova, Mathematics and Computer Science Series*, XXXVII (2010), 83–91.

[9] T. Dreyfus, J. Roques; Galois groups of difference equations of order two on elliptic curves, *SIGMA Symmetry Integrability Geom. Methods Appl.*, **11** (2015), Paper 003, 23 pp.

[10] A. Enge; *Elliptic Curves and Their Applications to Cryptography. An Introduction*, Kluwer Academic Publishers, Boston/Dordrecht/London, 2001.

[11] R. P. Gallant, R. J. Lambert, S. A. Vanstone; *Faster point multiplication on elliptic curves with efficient endomorphisms*, In J. Kilian (ed.), CRYPTO 2001, Springer LNCS 2139, 2001.

[12] D. Gordon; A survey of fast exponentiation methods, *Journal of Algorithms*, **27** (1998), 129–146.

[13] G. Gordon; Face recognition based on depth maps and surface curvature, In *Geometric Methods in Computer Vision, SPIE*, July 1991, 1–12.

[14] D. Hankerson, J. Hernandez, A. Menezes; Software implementation of elliptic curve cryptography over binary fields, *Proceedings of CHES 2000*, LNCS 1965.

[15] J. Harnad; *Picard-Fuchs Equations, Hauptmoduls and Integrable Systems*, Chapter 8 (Pgs. 137–152) of Integrability: The Seiberg-Witten and Witham Equation (Eds. H. W. Braden and I. M. Krichever, Gordon and Breach, Amsterdam, 2000.

[16] W. He, Y.-G. Miao; *Mathieu equation and elliptic curve*, arXiv: 1006.5185v3.

[17] K. Ireland, M. Rosen; *A classical introduction to modern number theory*, Graduate Texts in Mathematics, vol 84 (1982), Springer-Verlag.

[18] N. Ishii; Trace of Frobenius endomorphism of an elliptic curve with complex multiplication, *Bull. Austral. Math. Soc.*, **70** (2004), 125–142.

[19] N. Koblitz; CM curves with good cryptographic properties, *Proc. Crypto '91*, Springer-Verlag (1992), 279–288.

[20] M. Mălin; Multiple solutions for a class of oscillatory discrete problems, *Adv. Nonlinear Anal.*, **4** (2015), 221-233.

[21] A. Menezes, P. van Oorschot, S. Vanstone; *Handbook of Applied Cryptography*, CRC Press, Boca Raton, 1996.

[22] Y-H. Park, S. Jeong, C. Kim, J. Lim; *An alternate decomposition of an integer for faster point multiplication on certain elliptic curves*, Advances in Cryptology - Proceedings of PKC 2002, volume 2274 of Lecture Notes in Computer Science, Springer (2002), 323–334.

[23] V. Rădulescu; Nonlinear elliptic equations with variable exponent: old and new, *Nonlinear Analysis: Theory, Methods and Applications*, **121** (2015), 336-369.

[24] V. Rădulescu, D. Repovš; *Partial Differential Equations with Variable Exponents: Variational Methods and Qualitative Analysis*, CRC Press, Taylor & Francis Group, Boca Raton, 2015.

[25] F. Sica, M. Ciet, J. J. Quisquater; *Analysis of the Gallant-Lambert-Vanstone method based on efficient endomorphisms: elliptic and hyperelliptic curves*, Conference: Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, 2002.

[26] J. H. Silverman; *The Arithmetic of Elliptic Curves*, 2nd Edition, Spinger, 1986.

[27] J. A. Solinas; *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology - Proceedings of CRYPTO 1997, volume 1294 of Lecture Notes in Computer Science, Springer (1997), 357–371.

[28] G. Stephanides, N. Constantinescu; The GN-authenticated key agreement, *Journal of Applied Mathematics and Computation*, **170** (2005), 531–544.

[29] W. Waterhouse; Abelian varieties over finite fields, *Ann. Sci. École Norm. Sup.*, **4** (1969), 521–560.

[30] R. Bröker; Constructing supersingular elliptic curves, *Journal of Combinatorics and Number Theory*, **1** (2009), 269–273.

Oana Adriana Ţicleanu
University of Craiova, Street: A. I. Cuza 13, 200585 Craiova, Romania
E-mail address: oana.ticleanu@inf.ucv.ro