MATHEMATICS AND COMPUTATIONAL SCIENCES

Vol 1(2), 2021, pp:71-77

DOI:10.30511/mcs.2021.522222.1015

ISSN:2717-2708

http://mcs.qut.ac.ir/

Qom University of Technology

Bilinear cryptography using Lie algebras from p-groups

Elaheh Khamseh [1]

Abstract: Pairings are particular bilinear maps, and they have been defined based on elliptic curves which are abelian groups. In cryptography and security problems use these pairings. Mrabet et al. proposed pairings from a tensor product of groups in 2013. Also Mahalanobis et al. proposed bilinear cryptography using groups of nilpotency class two in 2017. In this paper, I develop a novel idea of a bilinear cryptosystem using Lie algebras from p-groups. First the researcher proposes pairing on Lie algebras from elliptic curves, and then pairings that can be constructed on Lie algebras from some of the non-abelian p-groups.

Keywords: Lie algebra; Bilinear map; P-group.
2020 Mathematics Subject Classification: 11-01; 11Gxx, 11G05.
Receive: 15 December 2020, **Accepted:** 20 February 2021

1 Introduction

Pairing-based cryptography is a major area of research in public key cryptography. The security of pairing-based cryptosystems relies on the difficulty of solving various computational problems [23, 32]. Some of these computational problems have only been very recently proposed, and there have been little security in the literature of whether they are truly difficult. Bilinear maps were originally introduced in cryptography in order to solve the discrete logarithm problem. Bilinear or pairing based cryptosystems are used in many practical situations such as identity based encryption, see [10], short singnatures, see [6] and tripartite Diffie-Hellman key exchange, [14, 2].
I am not going to survey all of pairing-based cryptographic protocols but will refer the reader to [3]. Developments in mathematical and computational cryptanalysis (see [5, 34, 16]) have renewed interest in developing new cryptographic methods. These methods include public-key cryptography based on hidden monomial systems, combinatorial-algebraic systems, and the theories of elliptic and hyperelliptic curves (see [18]). Many pairings considered in the literature are naturally associated with some objects arising in algebraic (projective) geometry such as elliptic curves and some generally abelian varieties.

More recently pairings over more general abelian varieties have been proposed [20] and even based on dot-product [29] for homomorphic encryptions. Also group theorist proposed pairings from a tensor product point of view in [22, 31], and bilinear cryptography using groups of nilpotency class 2, [21]. In this paper I propose a new construction of pairing, which is based on Lie algebras from p-groups.

[1]Department of Mathematics, Shahr-e-Qods Branch, Islamic Azad University, Tehran, Iran. Email:elahehkhamseh@gmail.com

2 An Introduction to Pairing-based Cryptography

In this section, I describe the bilinear pairing assumptions. We begin with the abstract pairing requirements and bilinear maps used in cryptographic protocols.

Let $(G_1, +)$ and $(G_2, +)$ be two additive cyclic groups of prime order q, with $G_1 = \langle p_1 \rangle$ and $G_2 = \langle p_2 \rangle$, $(G_T, .)$ a multiplicative cyclic group of order q with $G_T = \langle g \rangle$. We write as usual 0 for the identity elements of G_1, G_2 and 1 for G_T.

A pairing or a bilinear map is a map $\widehat{e} : G_1 \times G_2 \to G_T$ with the following properties:
1) bilinearity: For all $p_1, p_1^{'} \in G_1$, $p_2, p_2^{'} \in G_2$, $\widehat{e}$ is a group homomorphism in each component, i.e.
a) $\widehat{e}(p_1 + p_1^{'}, p_2) = \widehat{e}(p_1, p_2).\widehat{e}(p_1^{'}, p_2)$.
b) $\widehat{e}(p_1, p_2 + p_2^{'}) = \widehat{e}(p_1, p_2).\widehat{e}(p_1, p_2^{'})$.
2) non-degeneracy: $\widehat{e}$ is non-degenerate in each component. i.e.
a) For all $p_1 \in G_1$, $p_1 \neq 0$, there is an element $p_2 \in G_2$ such that $\widehat{e}(p_1, p_2) \neq 1$,
b) For all $p_2 \in G_2$, $p_2 \neq 0$, there is an element $p_1 \in G_1$ such that $\widehat{e}(p_1, p_2) \neq 1$,
3) computability: There is an efficient algorithm to compute $\widehat{e}(p_1, p_2)$ for all $p_1 \in G_1$, $p_2 \in G_2$.

I remind here the basic facts and definitions of pairing over elliptic curves. Let E be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic p. The integer r is chosen to be a prime divisor of $|E(\mathbb{F}_q)|$, co-prime with p. A pairing is usually defined over the points of r-torsion of E : $E[r] = \{P \in E(\bar{\mathbb{F}_q}) : rP = \infty\}$, where ∞ is the point at infinity of the elliptic curve. We know that $E[r] \cong \frac{\mathbb{Z}}{r\mathbb{Z}} \times \frac{\mathbb{Z}}{r\mathbb{Z}}$ [31, Chap III, Cor 6.4]. The embedding degree k of E relatively to r is the smallest integer such that r divides $q^k - 1$. A result of Balasubramanian and Koblitz [31] ensures that, when $k > 1$, all the points of $E[r]$ are rational over the extension $\mathbb{F}_{q^k}$ of degree k, i.e. $E[r] = E(\mathbb{F}_{q^k})$. The group G_1 is then the subgroup generated by a point $P \in E(\mathbb{F}_q)$ of order r. The subgroup G_2 is chosen as another subgroup of order r of $E[r]$, a popular choice is the subgroup generated by a point Q of order r over $E(\mathbb{F}_{q^k})$ such that $\pi(Q) = qQ$, where π represents the Frobenius endomorphism over $\mathbb{F}_q$, the group G_T is the unique subgroup of order r of $\mathbb{F}_{q^k}^*$ (it exists and is unique because r divides $(q^k - 1)$ and $\mathbb{F}_{q^k}^*$ is a cyclic group.) This choice of subgroups may be seen as the restriction to $G_1 \times G_2$ of the Weil pairing on $E[r] \times E[r]$, or the Tate pairing, or one of its variant (reduced Tate, Ate, twisted Ate, optimal pairing or pairing lattices). The Miller algorithm is used to compute all these pairings [11].

The original objective of pairing in cryptography was to solve the discrete logarithm problem. The pairing shifts the discrete problem from a subgroup over an elliptic curve to a discrete logarithm problem over a finite field. The interest is that the discrete logarithm problem is easier on finite fields compared to elliptic curves [23]. Also in pairing based cryptosystems we have MOV attack [23] on the elliptic curve discrete logarithm problem. The attack was first envisioned by Gerhard Frey. The idea was to use the bilinear properties of the Weil pairing to reduce a discrete logarithm problem in an elliptic curve over a finite field $\mathbb{F}_q$ to a discrete logarithm problem in $\mathbb{F}_{q^k}$. It is known [24] that most of the time for non supersingular curves, this k, the embedding degree is very large. Later, the pairings were used to compose the tripartite Diffie-Hellman key exchange [14]. It was a simplification of the Diffie-Hellman key construction between three entities. Let A, B and C be three users who want to set up a common secret key among themselves. Then choose three integers α, β and γ respectively and keep it a secret. They then compute $\alpha g, \beta g$ and γg respectively from the public information $G = \langle g \rangle$ and broadcast this information over the public channel. The user A on receiving βg and γg can compute $\widehat{e}(\beta g, \gamma g)^{\alpha}$ using his private key α. The same thing can be computed by B and C by using the public information of the other two users and his private information. The common key becomes $\widehat{e}(g, g)^{\alpha\beta\gamma}$. All is well and nice in what we just said, except that $\widehat{e}$ being an alternate (skew-symmetric) map, $\widehat{e}(g, g) = 1$. There are many approaches to solve that problem, one was proposed by Joux [14] and others using a distortion map. In the interest of brevity of this paper I won't go into further details of pairing based cryptosystems using elliptic curves. I will propose Lie algebras from

p-groups instead of elliptic curves. Nowadays, pairings are used for several protocols such as identity based cryptography [7] or short signature schemes [15]. The security of pairing-based cryptography lays on the discrete logarithm problem over the three groups $G_1,\ G_2$ and G_T, (see [8]).

3 Lie algebra

A Lie algebra is a vector space L over a field $\mathbb{F}$ with an operation $[.,.] : L \times L \to L$, which we call a Lie bracket, such that the following axioms are satisfied:
1) It is bilinear,
2) It is skewed symmetric: $[x, x] = 0$ which implies $[x, y] = -[y, x]$ for all $x,\ y \in L$,
3) It satisfies the Jacobi Identity: $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$.
If you want to know more about Lie algebra, you can see [12].

3.1 Lie algebras from p-groups

A group G is said to be a finite p-group if G has p^k elements, where $p > 0$ is a prime. For a group H, we denote H^p the subgroup generated by all h^p for $h \in H$. Let G be a p-group. We define a series $G = k_1(G) \geq k_2(G) \geq ...$ by $k_n(G) = (k_{n-1}(G), G)k_m(G)^p$, where m is the smallest integer such that $pm \geq n$. This series is called the Jennings series of G. You can see [17] for more information about the construction of this series.

Theorem 3.1. *[17] We have*
1) $(k_m(G), k_n(G)) \leq k_{n+m}(G)$
2) $k_n(G)^p \leq k_{np}(G)$.

Set $G_m = \frac{k_m(G)}{k_{m+1}(G)}$. Then by Theorem (3.1), all elements of G_m have order p, and G_m is abelian. Now since any abelian group the direct product of cyclic group of order p, i.e., $G_m = H_1 \times ...H_k$ where $H_k \cong \frac{\mathbb{Z}}{p\mathbb{Z}}$. Now fix a generator h_i of H_i. Then any element in G_m can be written as $h_1^{n_1} \times ... \times h_k^{n_k}$, where $0 \leq n_i \leq p-1$. Set $V_m = \mathbb{F}_p^k$. Then we have an isomorphism $\sigma_m : G_m \to V_m$ of G_m onto the additive group of V_m. It is given by $\sigma_m(h_1^{n_1} \times ... \times h_k^{n_k}) = (n_1, ..., n_k)$. For $j \geq 1$, we let $T_j : k_j(G) \to^{\pi_j} G_j \to^{\sigma_j} V_j$, where π_j is the projection map.
Set $L = V_1 \oplus V_2 \oplus ....$ Then L is a vector space over $\mathbb{F}_p$. We fix a basis B of L that is the union of bases of the components V_m. Let $x,\ y \in B$ be such that $x \in V_i$ and $y \in V_j$. Furthermore, let $g \in k_i(G)$ and $h \in k_j(G)$ be such that $T_i(g) = x$ and $T_j(h) = y$ respectively. Then we define $[x, y] = T_{i+j}((g, h))$.
This product is well-defined, i.e. $[x, y]$ does not depend on the choice of $g,\ h$. This follows from the identity $(g, fh) = (g, h)(g, f)((g, f), h)$, which holds for all elements f, g, h in any group.

Lemma 3.2. *[17] For $x,\ y \in B$, we have that $[x, x] = 0$ and $[x, y] + [y, x] = 0$.*

Proof. Let $x \in V_i$ and $y \in V_j$. Let $g \in k_i(G)$ and $h \in k_j(G)$ be pre-images of respectively x under T_i and y under T_j. Then
$[x, x] = T_{2i}((g, g)) = T_{2i}(1) = 0$ and
$[x, y] + [y, x] = T_{i+j}((g, h)) + T_{i+j}((h, g)) = T_{i+j}((g, h)(h, g)) = T_{i+j}(1) = 0$ □

Lemma 3.3. *[17] For $x_1, x_2, x_3 \in B$, we have*
$[x_1, [x_2, x_3]] + [x_2, [x_3, x_1]] + [x_3, [x_1, x_2]] = 0$

Proof. Suppose that $x_i \in V_{m_i}$ for $i = 1, 2, 3$. Let $g_i \in k_{m_i}(G)$ be a pre image of x_i under T_i for $i = 1, 2, 3$. Then
$[x_1, [x_2, x_3]] + [x_2, [x_3, x_1]] + [x_3, [x_1, x_2]] = T_{m_1+m_2+m_3}((g_1, (g_2, g_3))(g_2, (g_3, g_1))(g_3, (g_1, g_2))$.

Now the result follows from the fact that
$(g_1,(g_2,g_3))(g_2,(g_3,g_1))(g_3,(g_1,g_2)) \in k_{m_1+m_2+m_3+1}(G)$. □

Corollary 3.4. *[17] With the product* $[\ ,\ ]: L \times L \to L$ *the vector space* L *becomes a Lie algebra.*

Example 3.1. *[17]: Let* G *be the group generated by three elements* $g_1,\ g_2,\ g_3$ *subject to the relations* $(g_2,g_1) = g_3,\ (g_3,g_1) = (g_3,g_2) = 1,\ g_1^2 = g_2^2 = g_3$ *and* $g_3^2 = 1$. *The first relation is the same as* $g_2g_1 = g_1g_2g_3$, *whereas the second and third relations allow us to rewrite any word in the generators to an expression of the form* $g_1^{i_1}g_2^{i_2}g_3^{i_3}$ *(*).*
Using the remaining relations, we can rewrite this to be a word of the form (*) where $0 \le i_k \le 1$. *Hence* G *contains* $2^3 = 8$ *elements. The Jennings series of* G *is* $k_1(G) = G,\ k_2(G) = \langle g_3\rangle$, *and* $k_3(G) = 1$. *So* $G_1 = \frac{G}{\langle g_3\rangle} = \langle \bar{g}_1, \bar{g}_2\rangle$, *where* $\bar{g}_2.\bar{g}_1 = \bar{g}_1.\bar{g}_2$. *Therefore* $G_1 = \{1,\ \bar{g}_1,\ \bar{g}_2,\ \bar{g}_1\bar{g}_2\}$. *Let* V_1 *be a 2-dimensional vector space over* $\mathbb{F}_2$ *spanned by* $\{e_1,\ e_2\}$. *Let* $\sigma_1 : G_1 \to V_1$ *be the morphism given by* $\sigma_1(\bar{g}_i) = e_i$, $i = 1,\ 2$ *(so* $\sigma(\bar{g}_1\bar{g}_2) = e_1 + e_2$*). Also we have that* $G_2 = \frac{\langle g_3\rangle}{1} = \{1,\ g_3\}$. *Let* V_2 *be a 1-dimensional vector space over* $\mathbb{F}_2$ *spanned by* e_3. *Then* $\sigma_2 : G_2 \to V_2$ *is given by* $\sigma_2(g_3) = e_3$. *Now let* $L = V_1 \oplus V_2$. *We calculate the Lie product of* e_1 *and* e_2*:*

$$[e_1, e_2] = T_2((g_1, g_2)) = T_2(g_3) = e_3.$$

Similarly it can be seen that $[e_1, e_3] = [e_2, e_3] = 0$.

4 The central idea

In the previous section, we explained the Lie algebra that can be constructed from p-groups. In this section I propose two pairings that can be defined on Lie algebras.

4.1 The First Proposed pairing On Lie algebra From P-groups

Let $\mathbb{F}$ be any field. Let L be a d-dimensional Lie algebra over $\mathbb{F}$. Its (algebraic) dual L^* is the Lie algebra $Hom_{\mathbb{F}}(L, \mathbb{F}) = gl(L)$ of all linear forms. We observe that L separates the points of L^* since if $a \in L$ is non-zero, then it belongs to some basis of L over $\mathbb{F}$ so that we may choose a linear map $l : L \to \mathbb{F}$ such that $l(a) \neq 0$ and l takes any value for the other elements of the basis. Therefore the $\mathbb{F}$-bilinear form $\langle . \mid . \rangle : L \times L^* \to \mathbb{F}$ given by $\langle a \mid l\rangle = l(a)$ is a pairing. Moreover, if $(e_i)_{i=1}^d$ is a basis of L over the base field, then for each $j = 1, ..., d$, we may define a linear form $e^j \in L^*$ by the relations $e^j(e_i) = 1$, if $j = i$, and 0 otherwise. It turns that $(e^i)_{i=1}^d$ is a basis of L^* over $\mathbb{F}$ called the dual basis of $(e_i)_{i=1}^d$ and that $L \cong L^*$ (as Lie algebras). Under the isomorphism $e^i \to e_i$, the pairing becomes $\langle a|b\rangle = \Sigma_{i=1}^d a_i b_i$, where $a_i = e^i(a)$, $b_i = e^i(b)$ for each $i = 1, ..., d$, and we recover the usual dot-product of $\mathbb{F}^d$.

Remark. The above construction works in particular when $\mathbb{F}$ is the finite field $\mathbb{F}_{p^n}$ with p^n elements of characteristic p. In this case, any finite-dimensional vector space is actually finite, and we obtain a pairing between finite Lie algebras (and therefore finite abelian groups). When $n = 1$, we recover the construction of "dual pairing vector space" from [29, 30].

Let L be a Lie algebra from a p-group that defined in section 3. There are plenty finite p-groups. So, it is a natural choice to investigate p-groups that the discrete logarithm problem is hard. Let E be an elliptic curve over the finite field $\mathbb{F}_q$ of characteristic p, i.e. $q = p^n$. The embedding degree k of E relatively to r is the smallest integer such that r divides $q^k - 1$. A result of Balasubramanian and Koblitz [31] ensures that, when $k > 1$, all the points of $E[r]$ are rational over the extension $\mathbb{F}_{q^k}$ of degree k, i.e. $E[r] = E(\mathbb{F}_{q^k})$. We can consider the subgroup $E[r]$ of the elliptic curve. It is a p-group and we can use the process of section 3 to build Lie algebra from it. In fact we can use $\mathbb{F}_{p^{kn}}$-bilinear form $\langle . \mid . \rangle : L \times L^* \to \mathbb{F}_{p^{kn}}^*$.

4.2 The Second Proposed Pairing On Lie Algebras From non-abelian P-groups

We consider $\widehat{e} : L \times L \to L$, where L is a Lie algebra from p-groups of section 3, and for every $x,\ y \in L$, $(x, y) \to [x, y]$, is a bilinear map. For p-groups we consider non-abelian p-groups such as non-abelian groups of order p^n, $n = 3,\ 4,\ 5$ and 6 where the construction have found up to now, you can see [13, 9]. Also there are papers for construction of groups $p^7,\ p^8$ and p^9 in special cases [28, 35, 19].
Different types of non-abelian groups of order p^n, p an odd prime:
I. $n = 3$, two types:
(i) $x^{p^2} = e,\ y^p = e,\ y^{-1}xy = x^{1+p}$,
(ii) $x^p = e,\ y^p = e,\ z^p = e,\ z^{-1}yz = yx,\ z^{-1}xz = x,\ y^{-1}xy = x$.
Non-abelian groups of order 2^3, two types:
(i) identical with I (i), writing 2 for p,
(ii) $x^4 = e,\ y^4 = e,\ y^{-1}xy = x^{-1},\ y^2 = x^2$.
II. $n = 4$, ten types, p an odd prime:
(i) $x^{p^3} = e,\ y^p = e,\ y^{-1}xy = x^{1+p^2}$,
(ii) $x^{p^3} = e,\ y^p = e,\ z^p = e,\ z^{-1}yz = yx^p,\ y^{-1}xy = x,\ z^{-1}xz = x$,
(iii) $x^{p^2} = e,\ y^{p^2} = e,\ y^{-1}xy = x^{1+p}$,
(iv)$x^{p^2} = e,\ y^p = e,\ z^p = e,\ z^{-1}xz = x^{1+p},\ x^{-1}yx = y,\ z^{-1}yz = y$,
this group (iv) being the direct product of $\{y\}$ and $\{x, z\}$,
(v) $x^{p^2} = e,\ y^p = e,\ z^p = e,\ z^{-1}xz = xy,\ y^{-1}xy = x,\ z^{-1}yz = y$,
(vi), (vii), (viii),
$x^{p^2} = e,\ y^p = e,\ y^{-1}xy = x^{1+p},\ z^{-1}xz = xy,\ z^{-1}yz = y,\ z^p = x^{ap}$,
where for (vi) $a = 0$, for (vii) $a = 1$, for (viii) $a =$ any non-residue, $(mod p)$,
(ix) $x^p = e,\ y^p = e,\ z^p = e,\ t^p = e,\ t^{-1}zt = zx,\ t^{-1}yt = y,\ t^{-1}xt = x,\ z^{-1}yz = y,\ z^{-1}xz = x,\ y^{-1}xy = x$,
this group (ix) being the direct product of $\{y\}$ and $\{x, z, t\}$,
Non-abelian groups of order 2^4, nine types:
(i), (ii), (iii), (iv) and (v) identical with II (i), (ii), (iii), (iv) and (v) respectively, writing 2 for p,
(vi) $x^4 = e,\ y^4 = e,\ z^2 = e,\ y^{-1}xy = x^{-1},\ y^2 = x^2,\ z^{-1}yz = y,\ z^{-1}xz = x$,
this group (vi) being the direct product of $\{z\}$ and $\{x, y\}$,
(vii) $x^3 = e,\ y^2 = e,\ y^{-1}xy = x^{-1}$,
(viii) $x^3 = e,\ y^2 = e,\ y^{-1}xy = x^2$,
(ix) $x^3 = e,\ y^4 = e,\ y^{-1}xy = x^{-1},\ y^2 = x^4$.
We refer the construction of groups p^5 and p^6 to [13]. More recently, practical algorithms have been developed to construct the groups of a given order, such as the p-group generation algorithm of Newman [26] and O'Brien [27]. We can construct the Lie algebra from these p-groups similar example (3.5). So these pairings are computable. Also they are bilinear, from the bilinearity of Lie algebras. Since the pairing have to be non-degeneracy, we should select the non-abelian p-groups that no two elements commutate with each other. For example the group $x^{p^2} = e,\ y^p = e,\ y^{-1}xy = x^{1+p}$, for the groups of order p^3.

5 conclusion

Pairing is an important concept in security communications and cryptography. There are many papers that have defined on elliptic curves. Recently some researchers have proposed pairing on tensor products of groups [22] and groups of nilpotency class 2 [21]. In this paper I propose bilinear pairings on the Lie algebras form p-groups instead of groups. These pairings are bilinear and computable. The implementation of them should be checked out by computer scientification. I hope that they will be useful in security problems

and cryptography.

Acknowledgement: I would like to thank Islamic Azad University of Shahr-e-Qods for supporting this work.

References

[1] R. Balasubramanian, N.Koblitz, The improbability than an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm, Journal of Cryptology 11(2) 1998, 141-145.

[2] R. Barua, R. Dutta, P. Sarkar, Extending Jouxs protocol to multi party key agreement, International Conference on Cryptology in India, Springer, Berlin, Heidelberg, 2003.

[3] R. Dutta, R. Barua, P. Sarkar, Pairing based cryptographic protocols: A survey, IACR Cryptol. ePrint Arch. 2004, 64

[4] I.F. Blake, G. Seroussi, N.P. Smart, Advances in elliptic curve cryptography. London Mathematical Society, Lecture Note Series, Cambridge University Press 2005.

[5] D. Boneh, Twenty years of attacks on the RSA cryptosystem, Notices Amer. Math. Soc. 46 1999, 203-213.

[6] D. Boneh, H. Shacham, B. Lynn, Short signatures from theWeil pairing. Journal of Cryptology, 17(4) 2004, 297-319.

[7] D. Boneh, M. K. Franklin, Identity-based encryption from the Weil pairing. SIAM Journal of Computing, 32(3) 2003, 586-617.

[8] J. Boxall, A. Enge, Some security aspects of pairing-based cryptography. Technical report of the ANR Project PACE, 2009, 243-258.

[9] W. Burnside, Theory of Groups of Finite Order, second ed, Cambridge Univ. Press, 1911.

[10] S. Chatterjee, P. Sarkar, Identity-Based Encryption, Springer, 2011.

[11] C. Costello, Pairing for beginners, A Note, 2013.

[12] W.A. Graff, Lie algebras: theory and algorithms, Elsevier, 2000.

[13] R. James, The groups of order p6 (p an odd prime), Math. Comput. 34 1980, 613-637.

[14] A. Joux, A one round protocol for Diffie-Hellman, Proceedings of the 4th International Symposium on Algorithmic Number Theory, 2000, 385394.

[15] M. Joye, G. Neven, Identity-based cryptography, 2 of Cryptology and Information Security Series, IOS Press, 2009.

[16] MD. Huang, W. Raskind , A multilinear Generalization of the Tate Pairing. Contemporary Mathematics, 2010, 225-263.

[17] B. Huppert, N. Blackbum, Finite Groups II, Springer-Verlag Berlin Heidelberg New York, 1982.

[18] N. Koblitz, Algebraic aspects of cryptography, Algorithms and Computation in Mathematics, Algorithms and Computation in Mathematics, 1998.

[19] S. Lee, A class of descendant p-groups of order p^9 and Higmans PORC conjecture, Journal of Algebra, 468 2016 440-447.

[20] D. Lubicz, D. Robert, Efficient pairing computations with theta functions, Proceedings of the 9th International Symposium in Algorithmic Number Theory, Nancy, France, July 19-23. Lecture Notes in Computer Science 6197 2010, 251-269.

[21] A. Mahalanobis, P. Shinde, Bilinear cryptography using groups of nilpotency class 2, IMA International Conference on Cryptography and Coding, 2017, 127-134.

[22] N.E. Mrabet, L. Poinsot,, Pairings from a tensor product point of view, arXiv preprint arXiv:1304.5779, 2013.

[23] A. Menezes, T. Okamoto, S.A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transactions on Information Theory 39(5)1993, 163-1646.

[24] N.E. Mrabet, L. Poinsot, Elementary group-theoretic approach to pairings, Liebniz International Proceeding Informatics, 2012, 1-13.

[25] N.E. Mrabet, A. Guillevi, Sorina Ionica, Efficient Multiplication in Finite Field Extensions of Degree 5, International Conference on Cryptology in Africa. Springer, Berlin, Heidelberg, 2011.

[26] M.F. Newman, Determination of groups of prime-power order, in Group Theory, Lecture Notes in Mathematics 573, Canberra, 1975, Springer-Verlag, Berlin, Heidelberg, New York, 1977, 7–84.

[27] E.A. O'Brien, The p-group generation algorithm, Journal of symbolic computation, 9(5-6) 1990, 677-698.

[28] E.A. O'Brien, M.R. Vaughan-Lee, The groups with order p7 for odd prime p, Journal of Algebra 292(1) 2005, 243-258.

[29] T. Okamoto, K. Takashima, Homomorphic encryption and signatures from vector decomposition, International conference on pairing-based cryptography. Springer, Berlin, Heidelberg, 2008.

[30] T. Okamoto, K. Takashima, Hierarchical predicate encryption for inner-products, International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2009.

[31] V.A. Roman kov, Discrete logarithm for nilpotent group and cryptanalysis of polylinear cryptographic system, Prikle. Mat. Suppl, 2019(12) 2019, 154-160.

[32] V.A. Roman kov, Algebraic cryptanalysis and new security enhancements, Moscow Journal of combinatorics and Number Theory, 9(2) 2020, 123-146.

[33] J.H. Silverman, The arithmetic of elliptic curves, Volume 106 of Graduate Texts in Mathematics, Springer, 1986.

[34] P.C. Van Oorschot, M.J. Wiener, Parallel collision search with cryptanalytic applications, Journal of cryptology, 12(1) 1999, 1-28.

[35] M.R. Vaughan-Lee, Groups of order p^8 and exponent p, International Journal of Group Theory, 4(4) 2015, 25-42.