REFERENCES

1. *Alferov A. P., Zubov A. Y., Kuz'min A. S., and Cheremushkin A. V.* Osnovy kriptografii [Basics of Cryptography]. Moscow, Gelios ARV Publ., 2001. (in Russian)
2. *Matthew R. and Oliver B.* New Stream Ciphers Designs. Springer, 2008.
3. *Andreas K.* Stream Cipher. Springer, 2013.
4. *Bilyak I. B. and Kamlovskii O. V.* Chastotnye kharakteristiki tsiklov vykhodnykh posledovatel'nostey kombiniruyushchikh generatorov nad polem iz dvukh elementov [The frequency characteristics of cycle of output sequences combining generator over the field of two elements]. Prikladnaya Diskretnaya Matematika, 2015, no. 3(29), pp. 17–31. (in Russian)
5. *Lidl R. and Niederreiter H.* Finite Fields. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 1997.
6. *Fomichev V. M.* Fomichev V.M. Diskretnaya matematika i kriptologiya Diskretnaya matematika i kriptologiya [Discrete Mathematics and Cryptology. Moscow, Dialog-MEPhI Publ., 2010. (in Russian)
7. *Rueppel R. A.* Analysis and Design of Stream Ciphers. Springer Verlag, 1986.
8. *Kamlovskii O. V.* Kolichestvo poyavleniy elementov v vykhodnykh posledovatel'nostyakh fil'truyushchikh generatorov [Distribution properties of sequences produced by filtering generators]. Prikladnaya Diskretnaya Matematika, 2013, no. 3(21), pp. 11–25. (in Russian)
9. *Camion P. and Canteaut A.* Correlation-Immune and Resilient Function over a Finite Alphabet and Their Application in Cryptography. Springer, 1998.
10. *Niederreiter H.* Weights of cyclic codes. Information and Control, 1997, vol. 34, pp. 130–140.

UDC 003.26 DOI 10.17223/2226308X/12/44

DISCRETE LOGARITHM FOR NILPOTENT GROUPS AND CRYPTANALYSIS OF POLYLINEAR CRYPTOGRAPHIC SYSTEM[1]

V. A. Roman'kov

We present an efficient algorithm to compute a discrete logarithm in a finite nilpotent group, or more generally, in a finitely generated nilpotent group. Special cases of a finite p-group (p is a prime) and a finitely generated torsion free nilpotent group are considered. Then we show how the derived algorithm can be generalized to an arbitrary finite or finitely generated nilpotent group respectively. We suppose that group is presented by generating elements and defining relators or as a subgroup of a triangular matrix group over a prime finite field (in finite case) or over the ring of integers (in torsion-free case). On the base of the derived algorithm we give a cryptanalysis of some schemes of polylinear cryptography known in the literature.

Keywords: *discrete logarithm, nilpotent group, polylinear system, cryptanalysis.*

Introduction

Let G be a group. We say that the *discrete logarithm* is (efficiently) *computable* in G if there is an efficient algorithm that finds an exponent $x \in \mathbb{Z}$ for any expression of the form $f = g^x$, where $g, f \in G$. The problem of determining x given g and $f = g^x$ is called the *discrete logarithm problem* in G. The classical Diffie — Hellman exchange protocol, the ElGamal system and many other cryptographic schemes, protocols and systems are based

[1] The author is supported by RFBR, project No. 18-41-550001a.

on assumption about difficult solvability of the discrete logarithm problem in the groups chosen as platforms for them. See for examples [1 – 3].

Most of these schemes, protocols and systems use abelian groups as platforms. Multiplicative groups of finite fields and groups of elliptic curves over finite fields are most popular for this using. The security of currently popular algorithms relies on one of three hard mathematical problem: the integer factorization problem, the discrete logarithm problem on the multiplicative group of a finite field or the elliptic-curve discrete logarithm problem.

It turned out that main of public-key algorithms can be efficiently broken by a sufficiently strong hypothetical quantum computer. Shor [4] and Grover [5] algorithms provided a quantum way to break a many of public-key protocols. Even though current, publicly known, quantum computers lack processing power to break any real cryptographic algorithm, the cryptographic community take a great attention on constructing of new so-called *post-quantum* cryptographic algorithms that based on non-commutative algebraic structures. Now the *Post-Quantum Cryptography* is a specific area for investigation. Most popular cryptographic platforms in this new area are: matrix groups, nilpotent and polycyclic groups, Artin braid groups, some other infinite abstract groups, and so on. See [6, 7] for survey of the current state of this area. Cryptographic analysis of the main algorithms of algebraic cryptography can be found in [8 – 13].

In this paper, we consider the discrete logarithm problem in a finite nilpotent group, specifically, in a group $\mathrm{UT}(n, \mathbb{F}_p)$ of unitriangular $n \times n$ matrices over a prime finite field $\mathbb{F}_p$ of characteristic p. We introduce an efficient algorithm that solves the problem by computing the discrete logarithm in any finite nilpotent group. This approach can be applied to computing of the discrete logarithm in any finitely generated nilpotent group, in particular, this algorithm can be applied to a group $\mathrm{UT}(n, \mathbb{Z})$ of unitriangular matrices over the ring $\mathbb{Z}$ of integers.

Since every finite nilpotent group G is a direct product of its Sylow p-subgroups for $p \in \pi(G)$, in the finite case, it is sufficient to describe an algorithm in the case when G is a finite p-group for a prime p. Then a corresponding version the Chinese Remainder Theorem allows to compute the discrete logarithm in any finite nilpotent group. Any finitely generated torsion free nilpotent group has a finite normal central series with free abelian of a finite rank quotients, also it embeds into $\mathrm{UT}(n, \mathbb{Z})$ for suitable n. All elements of finite orders in a finitely generated nilpotent group G forms a finite subgroup $T = T(G)$ (*torsion subgroup*). Then $G_0 = G/T$ is torsion-free, and we can use G_0 and T to obtain a generalization of the constructed algorithm to any finitely generated nilpotent group. Fundamentals of the theory of nilpotent groups see, for example, in [14 – 16], a short introduction can be found in [17].

Note that matrix groups, as one of the most widely studied classes of non-abelian groups, were considered as suitable platforms for algorithms of the group-based cryptography from the very begiinning. In [18] and in some of other papers, different authors proposed (using the Jordan theory) to reduce the discrete logarithm problem for a matrices to the simultaneous discrete logarithm problem for some extension of the underlined field. This approach does not work in the case when all characteristic numbers are 1, as in the case of unitriangular matrices. So we need in different approaches to solve this specific case.

1. The discrete logarithm in a nilpotent group

Let G be a finite p-group. Consider a normal series

$$G = G_0 > G_1 > \ldots > G_k = 1, \qquad (1)$$

where $G_{i+1} = G_i^p G_i'$, $i = 0, \ldots, k-1$. Here $G_i^p = \mathrm{gp}(g^p : g \in G_i)$ and G_i' is the derived subgroup of G_i generated by all commutators of the form $[g, f] = g^{-1}f^{-1}gf$, $g, f \in G_i$. Any quotient $B_i = G_i/G_{i+1}$ is an elementary abelian p-group of a rank r_i, i.e., is a direct product $\prod\limits_{j=1}^{r_i} C_j(p)$, $C_j(p) \simeq C_p$, where C_p is a cyclic group of order p.

For any $g \in G$, we have that $g^p \in G_1$, and inductively, that $g^{p^l} \in G_l$, hence $g^{p^k} = 1$. Suppose that

$$g^x = f, \tag{2}$$

where g, f are known elements of G and x ($x \in \mathbb{N}$, $1 \leqslant x < |g|$) is unknown exponent. Here $|g|$ denotes an order of g. We'll compute x in the form

$$x = x_0 + x_1 p + \ldots + x_{k-1}p^{k-1}, \text{ where } 0 \leqslant x_i \leqslant p,\ i = 0, 1, \ldots, k-1.$$

Algorithm

1) For any $h \in G$, $\bar{h}$ means a standard image of h in B_0. Suppose that $\bar{f} \neq 1$, then $\bar{g} \neq 1$, and $\bar{g}^{x_0} = \bar{f}$. This exponent x_0 is uniquely computed by usual computation with vectors in B_0. Then we set $g_1 = g^p$, $f_1 = g^{-x_0}f \in G_1$ and reduce our computation to equation
$$g_1^{(x-x_0)/p} = f_1$$
in G_1.
If $\bar{f} = 1$ and $\bar{g} = 1$, then $g, f \in G_1$ from the beginning and we continue with equation
$$g^{x - x_{k-1}p^{k-1}} = f$$
in G_1 because in this case $g^{p^{k-1}} = 1$.
If $\bar{f} = 1$ ($f \in G_1$) and $\bar{g} \neq 1$, then we have $x_0 = 0$, we set $g_1 = g^p \in G_1$ and continue with equation
$$g_1^{x/p} = f$$
in G_1.
2) Continuing this process we obtain a solution $x = \log_g(f)$.

In a specific case, when $G = \mathrm{UT}(n, \mathbb{F}_p)$ series (1) is as follows: G_i ($i = 1, \ldots, n-1$) consists of all matrices with zero first i diagonals above the main diagonal. Since each finite p-group embeds into $\mathrm{UT}(n, \mathbb{F}_p)$ for suitable n one can apply the described above algorithm to the corresponding matrix group $\mathrm{UT}(n, \mathbb{F}_p)$. Note that we compute the minimal discrete logarithm x.

Now let G be a finite nilpotent group. Then G is a direct product $\prod\limits_{p \in \pi(G)} G_p$, where G_p denotes Sylow p-subgroup of G. Let $g = \prod\limits_{p \in \pi(G)} g_p$ and $f = \prod\limits_{p \in \pi(G)} f_p$ be expressions of g and f respectively as elements of this direct product. Let x_p be a solution of $g_p^{x_p} = f_p$ in G_p, $p \in \pi(G)$. A solution x of (2) can be efficiently computed by the Chinese Remainder Theorem as a solution of the following system of equations:

$$x = x_p \pmod{p^{t_p}}, \text{ where } p^{t_p} \text{ is order of } g_p,\ p \in \pi(G).$$

Similar algorithm works for any group $\mathrm{UT}(n, \mathbb{Z})$, and so for every finitely generated torsion free nilpotent group G, because every such group embeds into $\mathrm{UT}(n, \mathbb{Z})$ for sufficiently large n. Also, we can use a central series of G with torsion free quotients, that are free abelian groups of finite ranks.

Let G be a finitely generated nilpotent group and let $T = T(G)$ be its the torsion subgroup consisting of all elements of finite order, which is known is finite. The elements g and f in (2) simultaneously lie or not in T. If $g, f \in T$, we apply the algorithm to compute x in finite group T. If $g, f \notin T$, then exponent x is uniquely determined for the corresponding equation $\bar{g}^x = \bar{f}$ in torsion free group $\bar{G} = G/T$. Hence we succeeded again.

2. Applications

In recent years polylinear (in other words, multilinear) maps attracted attention of cryptographers. Now it is a new hot topic in cryptography because they offer a significant number of applications. The main open problem in this area is constructing a secure and efficiently computable polylinear map. The idea has been first proposed by D. Boneh and A. Silverberg [19], see also [20–22]. In [23], the authors proposed two polylinear protocols using finite p-groups as platforms, in which the security is based on the chosen discrete logarithm problem. Below we describe these two protocols and give a cryptanalysis to show a vulnerability of them.

At first, we will introduce the idea of a *cryptographic polylinear map.* Let $C_p(1)$ and $C_p(2)$ be two cyclic groups of prime order p. Let

$$\alpha : C_1(p) \times \ldots \times C_1(p) \to C_2(p)$$

be a non-degenerate polylinear map. Here non-degenerate means that if $g(1)$ is generator for $C_p(1)$, then $\alpha(g(1), \ldots, g(1))$ is a generator $g(2)$ for $C(2)$. Polylinear means that

$$\alpha(g_1^{k_1}, \ldots, g_n^{k_n}) = \alpha(g_1, \ldots, g_n)^{k_1 \ldots k_n} \text{ for any } g_1, \ldots, g_n \in C_p(1).$$

More generally, we can define a polylinear map as

$$\alpha : G_1 \times \ldots \times C_n \to G,$$

where $G_1, \ldots, G_n, G$ are arbitrary groups such that

$$\alpha(g_1^{k_1}, \ldots, g_n^{k_n}) = \alpha(g_1, \ldots, g_n)^{k_1 \ldots k_n} \text{ for any } g_i \in G_i,\ i = 1, \ldots, n,$$

with some natural non-degeneracy property.

Obviously, that a polylinear map with good cryptographic properties, namely, efficient computability of main operations in both the groups $C_p(i)$, $i = 1, 2$, efficient computability of α and difficult the discrete logarithm problem in $C_p(1)$, can be used in constructing cryptographic schemes. For example, a version of the famous Diffie — Hellman protocol can be based on a polylinear map.

Now we will consider two protocols proposed in [23].

Protocol 1.

Let $A_1, \ldots, A_{n+1}$ be the users. They choose a public nilpotent group G of nilpotency class $n > 1$. Denote inductively simple commutators on elements of G as follows. An usual commutator $[g_1, g_2]$ is said to be *simple of length* 2. Suppose that $[g_1, \ldots, g_q]$ is a simple commutator of length q, then $[[g_1, \ldots, g_q], g_{q+1}]$ is *simple commutator of length* $q+1$. A group G is *nilpotent of nilpotency class* n if every simple commutator of length $n+1$ is 1 and n is minimal with this property. Then the following identity is true.

For any $l_i \in \mathbb{N}$, $i = 1, \ldots, n$, and any tuple $(g_1, \ldots, g_n)$ of elements of G

$$[g_1^{l_1}, \ldots, g_n^{l_n}] = [g_1, \ldots, g_n]^l \text{ for } l = \prod_{i=1}^{n} l_i.$$

The key exchange works as follows:

- The users A_j's choose in random positive integers k_j, $j = 1, \ldots, n+1$, respectively, and transmit in public channel elements $g_i^{k_j}$ for $i = 1, \ldots, n$.
- The user A_j computes $[g_1^{k_1}, \ldots, g_{j-1}^{k_{j-1}}, g_{j+1}^{k_{j+1}}, \ldots, g_n^{k_n}]^{k_j} = [g_1, \ldots, g_n]^k$, $k = \prod\limits_{j=1}^{n+1} k_j$.
- $K = [g_1, \ldots, g_n]^k$ is the exchanged-key.

Cryptanalysis. By any pair of public elements $g_j, g_j^{k_j}$ we efficiently compute $\tilde{k}_j$ such that $g_i^{\tilde{k}_j} = g_i^{k_j}$ by the algorithm described in Section 1. Then we can compute K as A_j's does. A possible difference between k_j and $\tilde{k}_j$ obviously does not matter.

Protocol 2.

Let the users $A_1, \ldots, A_{n+1}$ choose a public nilpotent group G of nilpotency class $n > 1$ as above. In addition, G should be non-n-Engel group. It means that there are elements f and g such that the simple commutator $[f, g; n] = [f, g, \ldots, g]$ of length $n+1$ is not 1.

The key exchange works as follows.

- The users A_j's choose in random elements k_j, respectively, $j = 1, \ldots, n+1$, and transmit in public channel elements g^{k_j} for $j = 1, \ldots, n+1$.
- The user A_j computes

$$[f^{k_j}, g^{k_1}, \ldots, g^{k_{j-1}}, g^{k_{j+1}}, \ldots, g^{k_{n+1}}] = [f, g; n]^k, \; k = \prod_{j=1}^{n+1} k_j.$$

- $K = [f, g; n]^k$ is the exchanged-key.

Cryptanalysis. By any pair of elements g, g^{k_j} we efficiently compute $\tilde{k}_j$ such that $g^{\tilde{k}_j} = g^{k_j}$ by the algorithm described in Section 1. Then we can compute K as A_j's does. A possible difference between k_j and $\tilde{k}_j$ obviously does not matter in this case too.

Remark 1. Considering the Protocols 1 and 2 above we supposed that elements of the plaform group are written either as words on given generators, or as matrices in the matrix setting. In [23], the authors do not explain what is the form of expression of an element. Note, that we assume that we can efficiently compute an exponent in any expression of the form $g^x = f$ in an elementary abelian p-group. Obviously, we can if elements of this group are written as vectors over $\mathbb{F}_p$. It is possible for both of the forms of expressing of elements we talk about.

In [23], the authors proposed the following group as platform. Take $q = 2p^3 + 1$ where p and q are large primes. Let $X = \mathrm{gp}(x)$ and $Y = \mathrm{gp}(y)$ be the subgroups of $\mathbb{F}_q^*$ of orders p^3 and p^2, respectively. Selecting a nontrivial automorphism α of X amounts to choose a positive integer $m < p^3$, relatively prime to p, such that $\alpha(x) = x^m$. Define $G = Y \rtimes_\alpha X$, that is a semidirect product of X by Y. We identify x with $(1, x)$ and y with $(y, 1)$. Suppose that $m = p + 1$. Then we have for G the following presentation:

$$G = \langle x, y : x^{p^3} = y^{p^2} = 1, x^y = x^{p+1} \rangle.$$

Then G is a finite p-group of order p^5 and nilpotency class 3, which is not 2-Engel.

The group G is suggested as a platform for Protocols 1 and 2 for 4 and 3 users, respectively.

Consider for example Protocol 2. Then one can take $f = x$ and $g = y$. Indeed, $[x, y] = x^{-1}x^y = x^p$, $[x, y; 2] = x^{p^2}$, and $[x, y; 3] = 1$. The algorithm constructing above works if we can efficiently solve the discrete logarithm problem in $\mathbb{F}_q^*$. Unfortunately, the authors of [23] do not explain details of expressions of the elements. Anyway, our the approach reduces the problem to the computations in abelian groups, hence Protocols 1 and 2 cannot be considered as pure post-quantum protocols.

There are other approach as follows. Let $\tilde{\mathbb{F}}_q(z)$ be an extension of $\mathbb{F}_q$, where $z^p = x$. Then we define $z^y = z^{p+1}$ and $z^x = z$ and obtain group $\tilde{G}$ that contains G as a subgroup. We see that

$$[z, y^{k_1}, y^{k_2}, y^{k_3}] = [x, y; 2]^k, \; k = \prod_{j=1}^{3} k_j,$$

that is the exchanged key.

REFERENCES

1. *Menezes A. J., van Oorchot P. C., and Vanstone S. A.* Handbook of Applied Cryptography. N.Y., CRC Press, 1997.
2. *Koblitz N.* A Course in Number Theory and Cryptography. N.Y., Springer, 1987.
3. Roman'kov V. A. Vvedenie v kriptografiyu [Introduction to Cryptography]. Moscow, Forum Publ., 2012 (in Russian).
4. *Shor P.* Polynomial-time algorithm for prime factorization and discrete logarithms on a quantum computer. SIAM J. Comput., 1997, no. 5, pp. 1484–1509.
5. *Grover L. K.* A fast quantum mechanical algorithm for database search. Proc. 28th Ann. ACM Symp. on Theory of Comput., 1997, no. 5, pp. 212–219.
6. *Myasnikov A., Shpilrain V., and Ushakov A.* Group-Based Cryptography. Barselona-Basel, CRM, 2008 (Advances Courses in Math.).
7. *Myasnikov A., Shpilrain V., and Ushakov A.* Non-commutative Cryptography and Complexity of Group-Theoretic Problems. With Appendix by Natalia Mosina. Math. Surveys and Monographs, 2011, vol. 177, Providence RI, AMS.
8. *Roman'kov V. A.* Algebraicheskaya kriptografiya [Algebraic cryptography]. Omsk, OmSU Publ., 2013. (in Russian)
9. *Myasnikov A. and Roman'kov V.* A linear decomposition attack. Groups, Complexity, Cryptology, 2015, vol. 7, pp. 81–94.
10. *Roman'kov V.* A non-linear decomposition attack. Groups, Complexity, Cryptology, 2015, vol. 8, pp. 197–207.
11. *Roman'kov V. A.* Essays in Algebra and Cryptology. Algebraic Cryptanalysis. Omsk, OmSU Publ., 2018.
12. *Tsaban B.* Polynomial-time solutions of computational problems in noncommutative-algebraic cryptography. J. Cryptology, 2015, vol. 28, pp. 601–622.
13. *Ben-Zvi A., Kalka A., and Tsaban B.* Cryptanalysis via algebraic spans. LNCS, 2018, vol. 109991, pp. 1–20.
14. *Kargapolov M. I. and Merzlyakov Y. I.* Fundamentals of the Theory of Groups. N.Y., Springer Verlag, 1979.
15. *Hall P.* Nilpotent Groups. Edmonton Notes on Nilpotent Groups. Queen Mary College Math. Notes Math. Dept., London, Queen Mary College, 1969.
16. *Lennox J. C. and Robinson D. J. S.* The Theory of Infinite Soluble Groups. Oxford, Clarendon Press, 2004 (Oxford Math. Monographs).
17. *Roman'kov V. A. and Khisamiev N. G.* Nil'potentnye grruppy [Nilpotent Groups]. Ust-Kamenogorsk, EKSTU Publ., 2013. (in Russian)
18. *Menezes A. J. and Vanstone S. A.* A note on cyclic groups, finite fields and discrete logarithm problem. AAECC, 1992, vol. 3, pp. 67–74.

19. *Boneh D. and Silverberg A.* Applications of multilinear forms in cryptography. Contemporary Math., 2003, vol. 324, pp. 71–90.

20. *Lin H. and Tessaro S.* Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs. Cryptology ePrint Archive, Report 2017/250, 2017. `https://eprint.iacr.org/2017/250`

21. *Huang M. A.* Trilinear Maps for Cryptography. arXiv: 1803.10325, 2018.

22. *Mahalanobis A.* The Diffie — Hellman key exchange protocol and non-abelian nilpotent groups. Israel J. Math., 2008, vol. 165, pp. 161–187.

23. *Kahrobaei D., Tortora A., and Tota M.* Multilinear Cryptography Using Nilpotent Groups. arXiv: 1902.08777v1 [cs. CR] 23 Feb 2019. 8 p.