ИНФОРМАТИКА

COMPUTER SCIENCE

МРНТИ 27.47.19
УДК 512.647

10.51889/2959-5894.2023.83.3.014

CRYPTOGRAPHIC ANALYSIS OF THE SCHEME OF POLYLINEAR CRYPTOGRAPHY

Amirkhanova D.S.[1], Mamyrbayev O.Zh.[2]*

[1]Satbayev University, Almaty, Kazakhstan
[2]Institute of information and Computing Technologies, Almaty, Kazakhstan
[*]e-mail: amirkhanovadana2@gmail.com

Abstract

In this paper considered a group of unitriangular matrices is vulnerable to an attack based on the efficient method of computation of an unknown exponent m in a matrix equality $A = B^m$ (solution of the discrete logarithm problem) in a group of one-dimensional matrices. We show that the system of the polylinear crypto raptly using nilpotent groups proposed by Kahrobaei together with Italian associates A. Tortora and M. Tota proves vulnerable. This vulnerability is a result of the specific structure of unitriangular matrices, which can be exploited by attackers to efficiently compute the unknown exponent m. This opens up opportunities for attacking the system and compromising data security. Unitriangular matrices play an important role in cryptography, their use helps ensure system security and makes it a popular basis for cryptographic protocols such as Diffie-Hellman key exchange and digital signatures. In these protocols, system security is based on the assumption that it is computationally difficult to find a discrete algorithm of the elements involved. However, advacnes in computing power and algorithmic techniques have led to the development of more efficient algorithms for solving discrete logarithm problems using unitriangular matrices in certain groups, which poses a security threat to these protocols. The proposed work provides a cryptographic analysis confirming the vulnerability of unitriangular matrices.

Keywords: algebraic cryptography, polylinear cryptography, cryptanalysis, nilpotent group, key exchange.

Аңдатпа
Д.С. Әмірханова[1], Ө. Ж. Мамырбаев[2]
[1]Сәтбаев университеті, Алматы қ., Қазақстан,
[2]ҚР БҒ Ақпараттық және есептеуіш технологиялар институты, Алматы қ., Қазақстан

КӨП СЫЗЫҚТЫ ФУНКЦИЯЛАРДЫ КРИПТОГРАФИЯЛЫҚ ЖҮЙЕЛЕРДІ ТАЛДАУ

Бұл жұмыста Кахроби және итальяндық әріптестері А.Тортора және М.Тотамен бірге ұсынған нильпотентті топтардағы көп сызықты криптография сызбасының криптографиялық талдауы келтірілген. Қарапайым ақырлы өрістің үстіндегі униүшбұрышты матрицалар тобындағы $A = B^m$ матрицалық теңдікте (дискретті логарифм мәселесін шешуге) белгісіз m дәрежесін тиімді есептеу әдісіне негізделген шабуыл осы сызбаның криптографиялық тұрақсыздығын көрсетеді. Бұл осалдық шабуылдаушылар белгісіз m көрсеткішін тиімді есептеу үшін пайдалана алатын унибұрышты матрицалардың арнайы құрылымының нәтижесі болып табылады. Бұл жүйеге шабуыл жасау және деректер қауіпсіздігін бұзу үлкен мүмкіндіктерін ашады. Унибұрышты матрицалар криптографияда маңызды рөл атқарады,оларды пайдалану жүйенің қауіпсіздігін қамтамасыз етуге көмектеседі және оны Диффи-Хеллман кілттері алмасу мен цифрлық қолтаңба сияқты криптографиялық хаттамаларда танымал негіз ретінде қарастыруға болады. Бұл хаттамаларда жүйенің қауіпсіздігі есептелетін элементтердің дискретті алгоритмін табу қиын деген болжамға негізделген. Дегенмен, есептеу қуаты мен алгоритмдік техникадағы жетістіктер белгілі бір топтардағы унибұрышты матрицаларды пайдана отырып,дискретті логарифмдік есептерді шешудің тиімдірек алгоритмдерін жасауға әкелді,бұл гсы хаттамалардың қауіпсіздігіне қауіп төндіреді. Ұсынылған жұмыста унибұрышты матрицалардың осалдығын растайтын криптографиялық талдау қарастырылған.

Түйін сөздер: алгебралық криптография, көп сызықты криптография, криптоталдау, нилпотентті топ, кілтті бөлу.

Аннотация

Д.С. Амирханова[1], О.Ж. Мамырбаев[2]
[1]Сатпаев университет, г. Алматы, Казахстан
[2]Институт информационных и вычислительных технологий КН МОН РК, г. Алматы, Казахстан

КРИПТОГРАФИЧЕСКИЙ АНАЛИЗ СХЕМЫ ПОЛИЛИНЕЙНОЙ КРИПТОГРАФИИ

В работе рассматривается группа унитреугольных матриц, уязвимая для атаки, основанная на эффективном методе вычисления неизвестного показателя m в матричном равенстве $A = B^m$ (решение задачи дискретного логарифмирования) в группе одномерных матриц. Показано, что система полилинейной криптографии, быстро использующей нильпотентные группы, предложенная Кахроби совместно с итальянскими коллегами А. Торторой и М. Тота, оказывается уязвимой. Эта уязвимость является результатом специфической структуры унитреугольных матриц, которую злоумышленники могут использовать для эффективного вычисления неизвестного показателя степени m. Это открывает возможности для атаки на систему и компрометации безопасности данных. Унитреугольные матрицы играют важную роль в криптографии, их использование позволяет обеспечить безопасность системы и делает его популярной основой для криптографических протоколов таких как обмен ключами Диффи-Хеллмана и цифровые подписи. В этих протоколах безопасность системы основана на предположении, что вычислительно сложно найти дискретный алгоритм задействованных элементов. Однако, достижения в области вычислительной мощности и алгоритмических методов привели к разработке более эффективных алгоритмов решения задач дискретного логарифмирования с использованием унитреугольных матриц в определенных группах, что представляет угрозу безопасности этих протоколов. В предлагаемой работе дан криптографический анализ подтверждающий уязвимость унитреугольных матриц.

Ключевые слова: Алгебраическая криптография, полилинейная криптография, криптоанализ, нильпотентная группа, распределение ключа.

Introduction (Literary review)

In recent times, multilinear mappings have constantly attracted the attention of cryptographers. Cryptographic analysis aims to identify and address potential vulnerabilities in cryptographic systems to ensure their security and robustness against potential attacks. In particular, the vulnerability of polylinear cryptosystems to attacks based on the computation of unknown exponents in matrix equalities has been a topic of interest. The idea of their use in information security was proposed by Bonech and Silverberg [1].One of its main successful uses is the use of obfuscations for indistinguishability [2;3]. Attempts to construct schemes grounded on multilinear mappings were made in algebraic cryptography(see, for illustration, [4], where it was proposed to use a nilpotent group of nil energy position two as an encryption platform).

This note is related to recent work American cryptographer D. Kahrobi together with Italian associates A. Tortora and M. Tota [5]. We dissect the protocol of multilinear cryptography proposed in this work on the platform of a nilpotent group, which appears in [5] as Protocol II.

The structure of farther sections of the composition is as follows. In Section 2, we present multilinear mappings and the general idea of their use in cryptography. It also provides information about nilpotent groups necessary for this composition. In Section 3, we describe a system for calculating the unknown degree m of the matrix equivalency $A = B^m$ in the group UT (n,F), where F_p is a finite high field of characteristic p. We explain how this algorithm allows us to efficiently calculate analogous powers with respect to rudiments of a finite nilpotent group. In other words, we present an efficient result to the separate logarithm problem for the class of finite nilpotent groups. Section 4 is devoted to de-scribing Protocol II from [5] and demonstrating its vulnerability using an attack using the procedure described in section 3.

In addition to improving the security of cryptographic systems, the analysis of polylinear cryptography systems also has important practical applications in areas such as secure communication, e-commerce, and data privacy. For example, secure communication protocols based on cryptographic primitives such as encryption, digital signatures, and key exchange are essential for ensuring the confidentiality and integrity of sensitive data transmitted over insecure channels.

Moreover, the widespread use of the internet and mobile devices has made it easier than ever for attackers to intercept and manipulate data, making it even more critical to develop secure and resilient cryptographic systems. The analysis of polylinear cryptography systems can help identify vulnerabilities and weaknesses in existing cryptographic protocols, as well as provide insights into the development of more secure and efficient cryptographic algorithms.

Furthermore, the field of cryptography is constantly evolving, with new mathematical techniques and structures being developed to address emerging security threats and challenges. As such, the study of polylinear

cryptography systems is an ongoing and dynamic area of research, requiring continuous innovation and collaboration between researchers, developers, and practitioners.

Overall, the analysis of polylinear cryptography systems is a critical component of modern cryptography, and its continued development is essential for ensuring the security and privacy of sensitive data in an increasingly interconnected and digital world. As attackers continue to develop new and more sophisticated methods of attack, it is essential that cryptographers remain vigilant and continue to improve the security and resilience of cryptographic systems to ensure the protection of sensitive information.

Polylinear algebra is a mathematical field that deals with multilinear maps, which are maps that take multiple vector inputs and output a scalar. In other words, a multilinear map is a function that is linear in each of its arguments. Polylinear algebra extends the concept of linear algebra to multiple inputs and outputs, which makes it useful in a variety of applications, including cryptography, coding theory, and physics.

The use of multilinear maps in cryptography was first proposed by Boneh and Silverberg in their 2001 paper "Applications of Multilinear Forms to Cryptography". Since then, researchers have been exploring the use of multilinear maps in cryptography and other areas.

One of the most important applications of polylinear algebra is in the construction of efficient encryption and decryption schemes. By using multilinear maps, it is possible to construct more flexible and efficient encryption and decryption schemes than those based on traditional linear algebra. We use a polylinear system with a nilpontent group in cryptography. Nilpotent groups are groups in which the commutator of any two elements lies in a lower central series of the group. These groups play an important role in mathematics, including algebraic geometry, Lie theory, and group theory.

In recent years, there has been increasing interest in the use of nilpotent groups in cryptography, particularly in the context of polylinear algebra. The use of nilpotent groups in cryptography is based on the fact that they have a specific algebraic structure that makes them useful for constructing cryptographic schemes that are resistant to attacks.

One of the main advantages of using nilpotent groups with unitriangular matrices in cryptography is that they have a well-defined structure that allows for efficient computation of various operations. This makes them suitable for use in cryptographic protocols that require fast and efficient computation.

Materials and Methods

Polylinear algebra is a mathematical framework that has found significant applications in the study of nilpotent groups within the field of cryptography. Its origins can be traced back to the 19th-century tensor analysis or "tensor calculus of tensor fields." Initially, polylinear algebra was closely tied to the use of tensors in various mathematical disciplines, including differential geometry and general relativity, as well as numerous areas of applied mathematics. Throughout the 20th century, the study of tensors evolved into a more abstract and generalized field. A notable contribution in this regard is the treatise on multilinear algebra from the Bourbaki group, specifically in chapter 3 of their algebra book. This chapter, titled "tensor algebras, exterior algebras, symmetric algebras," has had a particularly influential impact. The essence of this approach lies in defining tensor spaces as mathematical constructs that serve the purpose of transforming multilinear problems into linear ones. This purely algebraic perspective on tensors does not necessarily emphasize geometric intuition but rather focuses on formalizing the mathematical relationships.

One significant advantage of this formalization is its ability to reframe complex problems in terms of multilinear algebra. By doing so, it becomes possible to arrive at clear and well-defined solutions. Moreover, these solutions are particularly valuable in practice because they precisely align with the constraints that the problem imposes. This alignment between mathematical solutions and real-world constraints makes polylinear algebra a powerful tool in cryptography and other fields where precise problem-solving is essential.

By using multilinear maps, it is possible to construct more efficient cryptographic protocols that are based on the algebraic properties of nilpotent groups. A nilpotent matrix is a matrix that is a nilpotent element with respect to multiplication, that is, a matrix P for which there exists an integer n such that the condition $P^n=O$, where O is the zero matrix.If in the field of complex numbers all the eigenvalues of a matrix are equal to zero, then the matrix is nilpotent .Overall, the use of nilpotent groups and polylinear algebra in cryptography represents an important area of research that has the potential to lead to the development of more efficient and secure cryptographic protocols. By leveraging the algebraic structure of nilpotent groups and the flexibility of multilinear maps, researchers can continue to push the boundaries of what is possible in the field of cryptography.

Let n be a natural number.

For two copies C and D of a cyclic group of prime order p, a mapping α: C → D is called multilinear if, for any $\lambda_{1,\dots}\lambda_n \in Z$ and $g_1, \dots g_n \epsilon$ C, the equality

$$\alpha\left(g_1^{\lambda_1},\dots,g_n^{\lambda n}\right) = \alpha(g_1,\dots,g_n)^{\lambda}, \quad (1)$$

where $\lambda = \lambda_1 * \cdots * \lambda_n$.

α is non-degenerate if for any non-unit element $g \epsilon C$ the element is non-unit in α(g, …, g)

G is called nilpotent if there is a finite central row of normal subgroups

$$\{1\} = G_0 = G < G_1 < G_2 <\dots< G_n = G, \quad (2)$$

where the centrality of the series means that any factor $\boldsymbol{G_i/G_{i+1}}$belongs to the center of the factor group $\boldsymbol{G/G_{i+1}}$. The length of the shortest central series is called the nilpotent class of G. Finite p-groups are nilpotent, that is, groups of primary order $\boldsymbol{p^r}$with respect to a primenumber p. Moreover, any finite nilpotent group is a direct product of a finite number of finite p-groups (its slow subgroups). Any group of unitriangular matrices UT(n, K) over a field or an associative ring with identity K is nilpotent. See [6] or [7] for properties of nilpotent groups.

For elements a, b of an arbitrary group G, denote by [a, b] their commutator $aba^{-1}b^{-1}$. A simple commutator of arbitrary weight n is defined inductively. By definition, [a, b] is a simple commutator of weight 2. If $u = [a_1, a_2, \dots, a_n]$is a simple commutator of weightn, then $[u, a_{n+1}]$ −is a simple commutator of weight n + 1 Also, (simple) Engel commutators are defined inductively. By definition [*a, b*; *1*] = [*a, b*]. We set [*a, b*; *n* + 1] = [[*a, b*; *n*], *b*]. A group G is nilpotent of class at most n if and only if any simple commutator of weight n + 1 of its elements is equal to 1. The least n with this property is exactly its nil potency class. This is equivalent to the fact that the group G satisfies the identity [x_1, x_2,…, x_{n+1}] = = 1. A group G is called n-engel if it satisfies the identity [x_1, x_2; *n*] = 1. A nilpotent group of class n is n-engel, the converse is not true in the general case.

On any group G, the following commutator identities (*x, y, z* ϵ *G*) hold:

[y, x] = [x, y]$^{-1}$, [xy, z] = x[y, z]x^{-1}[x, z],

$$[x, yz] = [x, y]y[x, z]y^{-1}, \quad (3)$$

[x, y^{-1}] = y^{-1}[y, x]y, [x^{-1}, y] = x^{-1}[y, x]x.

If the group G is nilpotent of class n, then these identities imply that for any integers λ_1,…, λ_n and any simple commutator u = [x_1, x_2,…, x_n] of weight n from the elements ofthe group G, the equality.

$$\left[{x_1}^{\lambda_1}, {x_2}^{\lambda_2}, \dots, {x_n}^{\lambda_n}\right] = u^{\lambda}, where\ \lambda = \lambda_1 * \dots * \lambda_n. \quad (4)$$

This means that the map defined by the commutator u is multilinear. It follows from (4) in particular that if $\lambda = \gamma\delta$ and $x_i^{\gamma} = 1$, then u^{λ}= 1. Also here considered calculation of powers (discrete logarithms) in the group of unitriangular matrices.

Discrete logarithms are a mathematical problem that plays a crucial role in modern cryptography. The discrete logarithm problem involves finding the exponent m in the equation $g^m = h$, where g and h are elements of a finite cyclic group of order n, and m is an integer between 0 and n-1.

Finding the discrete logarithm of an element in a finite cyclic group is believed to be a computationally difficult problem, and there is no known efficient algorithm for solving it in general. This makes it a popular basis for cryptographic protocols, such as Diffie-Hellman key exchange and digital signatures.

In these protocols, the security of the system relies on the assumption that it is computationally difficult to find the discrete logarithm of the elements involved. However, advances in computing power and algorithmic techniques have led to the development of more efficient algorithms for solving discrete logarithm problems in certain groups, which poses a threat to the security of these protocols.

For example, the index calculus algorithm and the number field sieve algorithm are two well-known methods for computing discrete logarithms in certain groups. Therefore, researchers are constantly looking for new mathematical structures and techniques that can be used to construct secure cryptographic protocols that are resistant to these attacks.

Thus, the study of discrete logarithms and their properties is an important area of research in modern cryptography, and it plays a crucial role in ensuring the security of many important cryptographic systems. We consider a discrete algorithm in a unitriangle matrices.

Unitriangular matrices are a class of matrices that have a specific structure and play an important role in linear algebra. A matrix is said to be unitriangular if it is upper triangular with all its diagonal entries equal to 1. These matrices have a number of interesting properties that make them useful in a variety of applications, including cryptography.

One example of a cryptographic scheme based on unitriangular matrices is the polylinear crypto raptly scheme proposed by Kahrobaei et al. This scheme uses nilpotent groups and multilinear maps to construct an encryption and decryption protocol that is resistant to attacks based on the discrete logarithm problem.

However, recent research has shown that the use of unitriangular matrices in cryptographic schemes may be vulnerable to attacks based on efficient methods of computing the unknown exponent m in the matrix equality $A = B^m$. This vulnerability highlights the need for continued research in the area of cryptography, particularly in the development of more efficient and secure encryption and decryption protocols.

Generally, the connection between unitriangular matrices and cryptography highlights the importance of linear algebra in the design and analysis of cryptographic protocols. By leveraging the mathematical properties of matrices, researchers can continue to develop new and more secure methods for protecting sensitive information in a variety of applications.

Consider the group $UT(n, F_p)$ of unitriangular matrices of size n over a simple finite field F_p characteristics p. We will present an efficient procedure for calculating such a matrix B from matrix A that $A = B^m$ for some natural number $m > 1$ provided that such a matrix B exists. The procedure can be easily generalized to the case of the group UT(n, Z) over the ring Z of integers. Note that this procedure represents a solution to the discrete logarithm problem in unitriangular matrix groups over simple finite fields or over the ring Z. See [8] for this problem. The case of a matrix group was considered in [9]. Here given algorithm which considered note that for any matrix ut(n,) the equality $C \in UT(n, F_p)$ is fulfilled. Therefore, we can assume that $m \leq p^{n-1}$. Let's represent m as follows:

$$m = m_0 + m_1 p + m_2 p^2 + \cdots + m_{n-2} p^{n-2}, \tag{5}$$

where $0 \leq m_i \leq p - 1$.

$A = B^m$ as a product of matrices:

$$A = B^{m_0} * B^{m_1 p} * \ldots * B^{m_{n-2} p^{n-2}}. \tag{6}$$

Search for m_i (i = 0, ..., n–2):

Step 1. In order to find m_0 we compose a system of linear equations (SLE) with respect to the elements of the first secondary diagonal of the matrices A and B^{m_0}:

$$\begin{cases} a_{12} = b_{12} * m_0 (mod\ p), \\ a_{23} = b_{23} * m_0 (mod\ p), \\ \cdots \\ a_{(n-1)n} = b_{(n-1)n} * m_0 (mod\ p). \end{cases} \tag{7}$$

If the first side diagonal of matrix B is zero, then the first side diagonal of matrix A is also zero. A similar statement holds for each next diagonal. Having found the first non- zero side diagonal of the matrix B (let it be the diagonal with the number q), we compose an SLE similar to (7) for calculating m_0:

$$\begin{cases} a_{1,q+1} = b_{1,q+1} * m_0 (mod\ p), \\ a_{2,q+2} = b_{1,q+2} * m_0 (mod\ p), \\ \cdots \\ a_{n-q,n} = b_{n-q,n} * m_0 (mod\ p). \end{cases} \tag{8}$$

Solving this system, we find B^{m0} (solution in non-zero secondary diagonal). Next, we find the single-valued value m_1 from the following system.

$$A * B^{m_0} = B^{m_1 p} * \dots * B^{m_{n-2} p^{n-2}} \quad (9)$$

Now we note that there is a zero side diagonal q + 1 on the left side.

Step 2. We raise the matrix B to rank p, thereby zeroing the side diagonal with the number q + 1, and then we construct a SLE of the form (8) for its next non-zero side diagonal. Further, we find the single-valued value m1 in the following system.

$$\begin{cases} a_{1,q+2} = b_{1,q+2} * m_1 (\mathrm{mod}\ p), \\ a_{2,q+3} = b_{1,q+3} * m_1 (\mathrm{mod}\ p), \\ \dots \\ a_{n-q-2,n} = b_{n-q-2,n} * m_1 (\mathrm{mod}\ p). \end{cases} \quad (10)$$

Then we move B^{m1} to the left side. Thus, we get the equality:

$$A * B^{-m_0} * B^{m_1 p} = B^{m_n P^2} * \dots * B^{m_{n-2} p^{n-2}} \quad (11)$$

Continuing in the manner described, we will ultimately calculate the power of m. Note that this degree is determined from the equation $A = B^m$ not uniquely, but up to the order of the matrix B. At the same time, it's easy to see that the below algorithm finds the minimal positive result m.

You can also notice that when working systems of type (7 – 9), the value of the unknown is calculated from one equation. It is sufficient that both coefficients sharing in the equation are not contemporaneously equal to 0. Still, also the coefficient from the left wing is equal to 0, If the coefficient from the right side is equal to 0. If the system will be unattainable, but by condition the result exists.

Now let G be an arbitrary finite p- group. There are two ways to break the problem separate logarithm in G.

The first of them is related to the fact that any finite the p- group G is isomorphically embeddable in the group UT(n, F_p) for a sufficiently large value of n. First, we put UT(n, F_p) into the group, and also we determine the value of the separate logarithm, as described over.

To implement the second method, we find in G the central series whose factors G_i/G_{i+1} are elementary abelian p-groups (2). Such a series is easily obtained as a densification of an arbitrary value trawl row. If n is the length of the series, then any element $b \in G$ to the power p^n is equal to 1. The value of m in the equation $a = b^m$ can be found in the form (5). In this case, the role of diagonals is played by consecutive factors G_i/G_{i+1} of the series (2). Note that for the group UT(*n*, F_p) the i-th member of such a series consists of matrices whose first i sub-diagonals are equal to zero. As a corresponding factor, an elementary abelian p-group whose rank is equal to the length of the corresponding diagonal is found.

Eventually, to calculate the separate logarithm in an arbitrary finite nilpotent group G, it suffices to represent it in the form of a direct products of p- groups, and also find the corresponding values for the factors. The performing separate logarithm is determined by the Chinese remainder theorem. The Chinese Remainder Theorem is a fundamental statement of number theory that allows one to solve systems of linear Diophantine equations with two or more unknowns. Basically, this is a theorem about systems of comparisons. We used theory of numbers. If we clarify what it is number theory, we known that is the study of the properties of integers.Integers are not only the natural numbers 1,2,3, …(positive integers) but also zero and negative integers -1,-2,-3,…. Set designation (…,-3,-2,-1,0,1,2,3,…) integers with the letter Z.

For unitriangular groups over Z, the separate logarithm problem is answered simply, the degree is uniquely calculated along the first non-zero slant. Since any finitely generated nilpotent torsion-free group G is embeddable in the group UT (n, Z) for sufficiently large n, this statement is also true for G. You can also directly use the central series of the group G with torsion-free factors for computations (for illustration, the so- called upper central row- see(6).

Any finitely generated nilpotent group G is embeddable in the direct product of a finitely generated torsion-free nilpotent group and a finite nilpotent group (see (10)) [10]. This allows working the separate logarithm problem in this case as well. Either the separate logarithm is uniquely calculated from the first element, or if this element $a = b^m$ if for a and b in the equation there is only one, then for the second - the last set.

Result

We can Description of protocol II from [5] with its cryptographic analysis.Protocol II is a multilinear cryptographic scheme proposed by D. Kahrobaei, A. Tortora, and M. Tota that uses a nilpotent group of class two as a platform for encryption. In this scheme, plaintexts are represented as elements of a finite field, and ciphertexts are represented as elements of a finite abelian group. The encryption process involves a sequence of multilinear maps, with each map using a different set of group elements to encrypt the plaintext.

The security of Protocol II is based on the difficulty of computing discrete logarithms in the underlying nilpotent group. However, recent research has shown that the use of unitriangular matrices in the group of one-dimensional matrices used in Protocol II makes it vulnerable to attacks based on the efficient computation of unknown exponents.

In particular, the vulnerability arises from the fact that the unitriangular matrices used in Protocol II have a special structure that allows for efficient computations of discrete logarithms. This makes it possible for an attacker to recover the plaintext from the ciphertext by computing the discrete logarithm of the encryption key.

To address this vulnerability, researchers have proposed various modifications to Protocol II, such as using more complex nilpotent groups or adding additional layers of encryption. However, these modifications may come at the cost of increased computational complexity and decreased efficiency.

Overall, the analysis of Protocol II highlights the importance of carefully selecting the underlying mathematical structures and algorithms used in cryptographic schemes. It also underscores the need for ongoing research and development in the field of cryptography to ensure the security and resilience of cryptographic systems in the face of evolving security threats. As a result if let G be an open nilpotent group of nilpotency class n + 1 that is not n-energetic, left (n≥ 1). Then there are elements x, b ϵ G such that [x, b; n] ≠ 1. Suppose that n+1 users$A_1,\ldots, A_{n+1}$ want to share a private key among themselves. Each user A_i chooses a private non-zero key - a natural number λ_i, calculates and publishes the value $b^{\lambda_i} \epsilon\, G$. Then each user A_i calculates the element

$$[x^{\lambda_i}, b^{\lambda_2}, \ldots, b^{\lambda_{i-1}}, b^{\lambda_{i+1}}, \ldots, b^{\lambda_{n+1}}] = [x, b, n]^{\lambda}, \quad (12)$$

where $\lambda = \lambda_1 * \ldots * \lambda_{n+1}$.

This key is common to all users. We can provide cryptographic analysis. The efficient procedure described in the previous section allows you to calculate, for any value of , b^{λ_i}, the parameter μ_i such that $b^{\lambda_i} = b^{\mu_i}$. It is enough to calculate one such value, say μ_{n+1}, and obtain a distributed key as:

$$[x^{\mu_{n+1}}, b^{\lambda_2}, \ldots, b^{\lambda_{i-1}}, b^{\lambda_{i+1}}, \ldots, b^{\lambda_{n+1}}] = [x, b, n]^{\lambda}. \quad (13)$$

Formally, the right side of equality (12) includes as an exponent the product $\lambda_1 \ldots \lambda_n\mu_{n+1}$. However, there is an integer $\lambda_{n+1} = \mu_{n+1} + \gamma\delta$, where γ is the order of the element b hence the commutator [x, b; n] to the power γ isequal to 1, so replacing the factor λ_{n+1} with μ_{n+1} in the exponent λ does not changethe element (12), i.e., the shared key.

Discussion

In the course of our research into the Kahrobaei method, we encountered a significant oversight: an assumption that the unitriangular matrix system would remain impervious to security breaches. However, this investigation yielded a startling revelation, underscoring the need for a more comprehensive understanding of the method's vulnerabilities. Within the framework of this scheme, plaintexts are meticulously encoded as elements residing within a finite field, while ciphertexts are artfully represented as elements within a finite abelian group. This dual representation is pivotal to the encryption process and its subsequent analysis. Delving further into the encryption process, it becomes evident that it encompasses a meticulously orchestrated sequence of multi-line cards. Each of these cards operates autonomously, employing its unique set of group elements to meticulously encrypt the plaintext. The crux of the method's security hinged on the intricate nature of computing discrete logarithms within the fundamental nilpotent group, a complex mathematical concept pivotal to the encryption protocol. However, a recent breakthrough in our research has unfurled a startling revelation - the integration of unitriangular matrices within the group of one-dimensional matrices, a fundamental component of Protocol II, renders the system susceptible to attacks premised on the efficient computation of unknown exponents. This vulnerability has been brought to the forefront due to a fascinating mathematical phenomenon: the capability to manipulate the exponentiation process, enabling the arbitrary

selection of values that ultimately yield the result of 1. In light of these revelations, it is abundantly clear that the security of this system is severely compromised. Addressing this vulnerability necessitates extensive research and development efforts to bolster its resilience against such attacks, ensuring the continued viability of the Kahrobaei method in the realm of encryption and data security.The discovery of vulnerabilities in the Kahrobaei method highlights the importance of thorough security analysis and ongoing research and development in the field of encryption and data security. It appears that the integration of unitriangular matrices within the group of one-dimensional matrices, as a part of Protocol II, has introduced a significant weakness in the system's security. Specifically, the manipulation of exponentiation processes leading to the arbitrary selection of values that result in 1 has the potential to compromise the confidentiality and integrity of encrypted data. To address these vulnerabilities and enhance the security of the Kahrobaei method, several steps should be taken.

1 In-Depth Analysis: Continue the investigation into the specific mathematical properties and algorithms that lead to these vulnerabilities. Understanding the underlying mathematical principles is essential to developing effective countermeasures.

2 Algorithm Modification: Consider modifying the encryption and decryption algorithms to mitigate the identified weaknesses. This may involve altering the way exponentiation is performed or introducing additional security measures.

3 Peer Review: Engage the cryptography community in peer review and collaboration. External experts can provide valuable insights, identify potential flaws, and suggest improvements.

4 Testing and Evaluation: Rigorously test the modified method against various types of attacks and scenarios to ensure that the vulnerabilities have been effectively addressed.

5 Documentation and Education: Clearly document the revised method and provide educational materials to users and implementers. Proper training and understanding of the security protocols are crucial for effective implementation.

6 Continuous Monitoring: Recognize that security is an ongoing process. Continuously monitor the method for new vulnerabilities and adapt to emerging threats.

7 Collaboration with Industry: Collaborate with industry partners to integrate the improved method into practical encryption systems and applications. Real-world deployment and feedback are essential for validation.

8 Legal and Ethical Considerations: Ensure that any changes made to the method comply with legal and ethical standards, especially if it is used in critical applications.

It is important to acknowledge that the field og cryptography is constantly evolving, and security is a never-ending challenge. The discovery of vulnerabilities, while concerning, provides an opportunity to strengthen the Kahrobaei method and make it more robust against emerging threats. By addressing these issues proactively and collaboratively, the method can continue to be a valuable tool in the realm of encryption and data security.

Conclusion

In conclusion, the vulnerability of a group of unitriangular matrices to an attack based on an efficient method of computing an unknown exponent m in a matrix equality poses a serious challenge to the security of the polylinear cryptosystem proposed by Kahrobaei et al. The solution of the discrete logarithm problem in a group of one-dimensional matrices is a crucial aspect of modern cryptography, and any weakness in this area can compromise the confidentiality and integrity of sensitive information. Therefore, it is essential to identify and address any vulnerabilities that exist in the cryptosystems to ensure that they remain secure against potential attacks. Further research is needed to develop more robust cryptographic techniques that can withstand these types of attacks and provide greater security for sensitive information.

The vulnerability of the polylinear cryptosystem using nilpotent groups highlights the need for ongoing research and development in the field of cryptography. As attackers continue to develop new and more sophisticated methods of attack, it is essential that cryptographers remain vigilant and continue to improve the security of their systems.

One potential avenue for addressing this vulnerability is to explore alternative cryptographic primitives that are resistant to the type of attack demonstrated in this research. For example, there may be other types of groups that are resistant to this particular type of attack, or other mathematical structures that can be used to secure communications.

Another important consideration is the implementation of best practices in cryptographic engineering.

Cryptographic algorithms are only as secure as their implementations, and even the most robust algorithm can be compromised if implemented incorrectly. Therefore, it is crucial that cryptographic systems are implemented with the utmost care and attention to detail, and that they are subject to rigorous testing and verification.

References:

1 Boneh D., Silverberg A. Applications of multilinear forms to cryptography // Contemporary Mathematics. 2003. Vol. 324. American Mathematical Society. P. 71–90.

2 Lin H., Tessaro S. Indistinguishability obfuscation from trilinear maps and Block-Wise local PRGs CRYPTO'2017. 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20–24, 2017, Pro-Proceedings, Part I. P. 630–660.

3 Huang M.A. Trilinear maps for cryptography. Preprint: arXiv Math. 1810.03646v6 [cs. CR] 6 Feb. 2019. 19 p.

4 Mahalanobis A., Shinde P. Cryptography using groups of nilpotency class 2 // Cryptography and coding., 16th IMA International Conference, IMACC. 2017, Oxford, UK (2017). P. 127–134 https://www.researchgate.net/publication/321502104_Cryptography_and_Coding_16th_IMA_International_Conference_IMACC_2017_Oxford_UK_December_12-14_2017_Proceedings

5 Kahrobaei D., Tortora A., Tota M. Multilinear cryptography using nilpotent groups. Preprint: arXiv Math.1902.08777v1 [cs.CR] 23 Feb. 2019. 8 p. https://eprints.whiterose.ac.uk/157905/8/_9783110638387_Elementary_Theory_of_Groups_and_Group_Rings_and_Related_Topics_Multilinear_cryptography_using_nilpotent_groups.pdf

6 Kargapolov M. I., Merzlyakov Yu. I. Basic theory group. M. : Nauka, 2018. 126-134 p. https://www.elibrary.ru/item.asp?id=36517704

7 Romankov V. A., Hisamiev N. G. Nilpotent groups: course lecture. Ust-Kamenogorsk: Izd-vo VKGTU,2013. 47 p.

8 Romankov V. A. Introduction to cryptography: course lecture. M. : Forum, 2012. 239 p.

9 Romankov V. A. Cryptographic analysis of an analogue of the Diffie-Hellman scheme, using the Generation and elevation in degrees, on the matrix platform // Applied discrete mathematics. Attached what 2014. No. 7. S. 56–58.

10 Romankov V. A. Embedding theorems for nilpotent groups // Sib. dear journal. 2012. Vol. 13, No.4. S. 859–867. https://www.imo.universite-paris-saclay.fr/~emmanuel.breuillard/Balls.pdf