CRYPTANALYSIS OF TWO SCHEMES OF BABA ET AL. BY LINEAR ALGEBRA METHODS

VITALIĬ ROMAN'KOV

ABSTRACT. We show that the attacks based on the linear decomposition method introduced by the author and the span-method introduced by Tsaban allow one to find the transmitted message in the cryptosystem and the exchanged key in the protocol which are proposed in [1].

1. Introduction

In [1], S. Baba, S. Kotyada and R. Teja demonstrate how to define an approximate one-way function FACTOR in a non-Abelian group. As examples of a platform for realization of FACTOR they suggest one of groups like $GL_n(\mathbb{F}_q)$, $UT_n(\mathbb{F}_q)$, or Braid Groups B_n , $n \in \mathbb{N}$. Here \mathbb{F}_q denotes the finite field of order q. They believe that the function FACTOR is one-way. It means that the inverse to the FACTOR is easy to compute, while the function itself is hard to compute.

Then, using FACTOR function as a primitive the authors of [1] therefore define a public key cryptosystem which is comparable to the classical El-Gamal system based on the discrete logarithm problem. Recall, that the El-Gamal system can be described as follows: Let G be a public finite cyclic group with generator g, and let $x \in \mathbb{Z}$ is Alices private key. The element g^x is public. To send a message $m \in G$, Bob picks a random integer g and sends the cipher text $g = (g^y, g^{xy}m)$ to Alice. To decrypt, Alice calculates $g^y)^x = g^{xy}$ and inverts it to retrieve g.

In [1], the authors also propose a key exchange, analagous to the Diffie-Hellman key exchange protocol in a non-Abelian setting using FACTOR. Recall, that the classical Diffie-Hellman protocol can be described as follows: Let G be a public finite cyclic group with generator g, and let $x \in \mathbb{Z}$ is Alices private key, as well as $y \in \mathbb{Z}$ is Bobs private key. Alice publishes g^x and Bob publishes g^y . Then each of them computes the exchanged key $g^{xy} = (g^x)^y = (g^y)^x$.

In this paper, we apply and compare two methods of algebraic cryptanalysis via linear algebra, namely, the linear decomposition method invented and developed by the author in [2] - [4] and in [5] (with A. Myasnikov), and the span-method invented and developed by B. Tsaban in [6] and in [7]

¹Supported by RFBR, project 18-41-550001.

(with A. Ben-Zvi and A. Kalka), to show vulnerability of the proposed in [1] cryptosystem and protocol.

2. The ElGamal-type cryptosystem based on FACTOR [1]

Let G be any public group. Let $g,h \in G$ be two private elements of Alice, and let $\langle g \rangle$ and $\langle h \rangle$ be the cyclic subgroups generated by these elements, respectively. In order to define the FACTOR problem one assume that $\langle g \rangle \cap \langle h \rangle = \{1\}$. Let $f : \langle g \rangle \times \langle h \rangle \to G$ be a function defined as follows: $f(g^x, h^y) = g^x \cdot h^y$, where $x, y \in \mathbb{Z}$. Obviously, that f is injective. Then FACTOR $(g^x h^y) = f^{-1}(g^x h^y)$.

Cryptosystem. Let G be a non-Abelian group and let $g, h \in G$ be two non commuting elements. We assume that $\langle g \rangle \cap \langle h \rangle = \{1\}$. We suppose that Alice is the recipient of the messages and Bob is communicating with Alice. Let $m \in G$ be the message.

Alice picks arbitrary integers $x, y \in \mathbb{Z}$ and sets a public key $(G, g, h, g^x h^y)$. Alice has a private key (g^x, h^y) for decryption.

To send the message m, Bob picks arbitrary integers x^{\prime},y^{\prime} and sends cipher text

$$c = (g^{x+x'}h^{y+y'}, g^{x'}h^{y'}m)$$

to Alice.

To decrypt the text, Alice uses her private key and calculates

$$(g^x)^{-1}(g^{x+x'}h^{y+y'})(h^y)^{-1} = g^{x'}h^{y'}.$$

Then she inverts it to retrieve m.

The authors of this scheme hoped that the security of the crypto system described above reduces to solving FACTOR problem in the underlying group. Below we'll show that the system is vulnerable against linear algebra attacks.

Cryptanalysis.

We will show that any intruder can efficiently compute $g^{x'}h^{y'}$ and then retrieve m.

I. First we will use the Tsaban's span-method. We suppose that G is a finite group presented as a matrix group over a finite field. So, let $G ext{ } ext$

We can efficiently construct a basis $1, g, g^2, ..., g^k$ of V by checking for every succesive l = 1, 2, ... either g^{l+1} lies in $\operatorname{Lin}_{\mathbb{F}_q}(1, g, g^2, ..., g^l)$, or not. Then k is the least l such that this happens. Such verification is carried out by the Gauss elimination method which is known as efficient.

Consider the equation

$$(2.1) f(g^x h^y)h = hf(g^x h^y) \sim fg^x h = hfg^x,$$

that is linear with respect to n^2 unknown entries of matrix f. We will seek f in the form

$$f = \sum_{i=0}^{k} \alpha_i g^i,$$

i.e., we seek a solution f in V. We know that there is a non-degenerate solution $f = g^{-x}$. We can efficiently construct a basis $e_1, ..., e_p$ of the subspace of all solutions of (2.1) in V. Then we can use the following statement:

Invertibility Lemma [6] (see also [7]).

For a finite field \mathbb{F}_q , $e_1, ..., e_p \in \mathrm{M}_n(\overline{\mathbb{F}}_q)$), such that some linear combination of these matrices is invertible, if $\beta_1, ..., \beta_p$ are chosen uniformly and independently from \mathbb{F}_q , then the probability that the linear combination $f = \sum_{i=1}^p \beta_i e_i$ is invertible is at least $1 - \frac{n}{q}$.

Let element f be found. Then

$$f(g^x h^y) = h(fg^x), f(g^{x+x'} h^{y+y'}) = (g^{x'} h^{y'}) h^y (fg^x))$$

and

$$(g^{x'}h^{y'})h^y(fg^x))f^{-1}(g^xh^y)^{-1} = g^{x'}h^{y'}.$$

So

$$(g^{x'}h^{y'})^{-1}(g^{x'}h^{y'}m) = m.$$

The message m is recovered.

II. Now we will use the author's linear decomposition method. Let $G \leq M_n(\mathbb{F})$ be a matrix group over arbitrary (constructive) field \mathbb{F} . Let $V = \text{Lin}_{\mathbb{F}}(\langle g \rangle (g^x h^y) \langle h \rangle)$ be the linear subspace of $M_n(\mathbb{F})$ generated by all matrices of the form $g^i(g^x h^y)h^j$, $i, j \in \mathbb{Z}$. Then $\dim(V) \leq (n-1)^2$.

Let $e_1, e_2, ..., e_r$ be a basis of V that can be efficiently obtained in the same way as described above. Let $e_i = g^{u_i}(g^x h^y) h^{v_i}, u_i, v_i \in \mathbb{Z}, i = 1, ..., r$.

Since, $g^{x+x'}h^{y+y'} \in V$, we can efficiently obtain a presentation of the form

(2.2)
$$g^{x+x'}h^{y+y'} = \sum_{i=1}^{r} \alpha_i e_i, \ \alpha_i \in \mathbb{F}, \ i = 1, ..., r.$$

The right side of (2.2) is equal to

$$(2.3) g^x(\sum_{i=1}^r \alpha_i g^{u_i} h^{v_i}) h^y,$$

it follows by (2.2), that

(2.4)
$$g^{x'}h^{y'} = \sum_{i=1}^{r} \alpha_i g^{u_i}h^{v_i}.$$

The message m is recovered as above.

Remark. Remind, that the authors of [1] suggest as a platform for their cryptosystem one of the groups $GL_n(\mathbb{F}_q)$, $UT_n(\mathbb{F}_q)$, or Braid Groups B_n , $n \in \mathbb{N}$. In our cryptanalysis, we consider only matrix groups. Any group B_n admits a faithful matrix representation [9], [10]. The braid group

 B_n is linear via the so-called Lawrence-Krammer representation LK: $B_n \to \operatorname{GL}_m(\mathbb{Z}[t^{\pm 1}, 1/2])$, where m = n(n-1)/2, is injective. The Lawrence-Krammer representation of a braid can be computed in polynomial time. This representation is also invertible in (similar) polynomial time (see [10], [11]).

3. The Diffie-Hellman-type key exchange protocol based on FACTOR [1]

Suppose Alice and Bob want to exchange keys. Suppose G, g, h are as in FACTOR. Let Alice pick a pair of integers (x_1, y_1) , and Bob pick two integers (x_2, y_2) .

Then Alice sends the element $g^{x_1}h^{y_1}$ to Bob.

Independently Bob sends the element $g^{x_2}h^{y_2}$ to Alice.

Both Alice and Bob can recover the element $K = g^{x_1+x_2}h^{y_1+y_2}$. This is their private key.

Cryptanalysis.

Now we will apply and describe only the author's linear decomposition method. Let $G \leq \mathrm{M}_n(\mathbb{F})$ be a matrix group over arbitrary (constructive) field \mathbb{F} . Let $V = \mathrm{Lin}_{\mathbb{F}}(\langle g \rangle \langle h \rangle)$ be the linear subspace of $\mathrm{M}_n(\mathbb{F})$ generated by all matrices of the form $g^i h^j, i, j \in \mathbb{Z}$. Then $\dim(V) \leq (n-1)^2$.

Let $e_1, e_2, ..., e_r$ be a basis of V that can be efficiently obtained in the same way as described above. Let $e_i = g^{u_i} h^{v_i}, u_i, v_i \in \mathbb{Z}, i = 1, ..., r$.

Since, $q^{x_1}h^{y_1} \in V$, we can efficiently obtain a presentation of the form

(3.1)
$$g^{x_1}h^{y_1} = \sum_{i=1}^r \alpha_i e_i, \ \alpha_i \in \mathbb{F}, \ i = 1, ..., r.$$

Then

(3.2)
$$\sum_{i=1}^{r} \alpha_i g^{u_i} (g^{x_2} h^{y_2}) h^{v_i} = g^{x_2} (\sum_{i=1}^{r} \alpha_i e_i) h^{y_2} = K.$$

We succeeded again.

Of course, the Tsaban's span-method can be applied too.

The described cryptanalysis has many analogues, presented in [2]-[7]. In [8], a general scheme based on multiplications is presented. It corresponds to a number of cryptographic systems known in the literature, which are also vulnerable to attacks by the linear decomposition method. Note that the Tsaban's span-method allows him to show the vulnerability of the well-known schemes of Anshel et al. [12], and the Triple Decomposition Key Exchange Protocol of Peker [13].

A protection against linear algebra attacks is invented in [14]. It is described in the case of the Anshel et al. cryptographic scheme but can be applied to the Diffie-Hellman-type and some other schemes too.

References

[1] S. Baba, S. Kotyada and R. Teja, A non-Abelian factorization problem and an associated cryptosystem, IACR. Cryptology e-Print Archive, 48 (2011).

- [2] V. A. Roman'kov, *Algebraic cryptography*, Omsk: OmSU Publisher House, 2013, 135 pp. (in Russian).
- [3] V. A. Roman'kov, Cryptanalysis of some schemes applying automorphisms, Prikladnaya Discretnaya Matematika, 3 (2013), 35–51 (in Russian).
- [4] V. A. Roman'kov, Essays in algebra and cryptology: Algebraic cryptanalysis, Omsk: Omsu Publisher House, 2018, 207 p.
- [5] V. Roman'kov, A. Myasnikov, A linear decomposition attack, Groups Complexity Cryptology, 7, No. 1 (2015), 81–94.
- [6] B. Tsaban, Polynomial time solutions of computational problems in noncommutative-algebraic cryptography, Journal of Cryptology, 28 (2015), 601– 622
- [7] A. Ben-Zvi, A. Kalka, and B. Tsaban, Cryptanalysis via algebraic spans, In: Advances in Cryptology CRYPTO 2018. 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings Part I, 255–274 (Shacham, Hovay, Boldyreva, Alexandra (Eds.)).
- [8] V. A. Roman'kov, Two general schemes of algebraic cryptography, Groups, Complex., Cryptol. 10, No. 2 (2018), 83–98.
- [9] S. Bigelow, Braid groups are linear, J. Amer. Math. Soc. 14 (2001), 471–486.(2001)
- [10] D. Krammer, Braid groups are linear, Ann. Math. 155 (2002), 131–156 (2002)
- [11] J. H. Cheon, B. A. Jun, A polynomial time algorithm for the braid Diffie-Hellman conjugacy problem, In: CRYPTO 2003. LNCS, vol. 2729 (2003). Springer, Heidelberg (2003). 212–225 (Boneh, D. (Ed.))
- [12] I. Anshel, M. Anshel, and D. Goldfeld, An algebraic method for public-key cryptography, Math. Res. Lett. 6 (1999), 287–291.
- [13] Y.K. Peker, A new key agreement scheme based on the triple decomposition problem, Int. J. Netw. Secur. 16 (2014), 340–350.
- [14] V. Roman'kov, An improved version of the AAG cryptographic protocol, Groups, Complex., Cryptol, 11, No. 1 (2019), 35–42.

DOSTOEVSKY OMSK STATE UNIVERSITY E-mail address: romankov48@mail.ru