UDC 512.54

V.A. Roman'kov

F.M. Dostoevsky Omsk State University, Russia
(E-mail: romankov48@mail.ru)

A polynomial algorithm for the braid double shielded public key cryptosystems

We propose new provable practical deterministic polynomial time algorithm of cryptographic analysis for the braid Wang, Xu, Li, Lin and Wang «Double shielded public key cryptosystems», where the authors recommended the Artin braid groups B_n as platforms for proposed protocols. We show that a linear decomposition attack based on the decomposition method introduced by the author works for the image of braids under the Lawrence-Krammer representation by finding the exchanging keys in the both two main protocols by Wang et. al. These keys can be effectively computed in their original form too. Thus the protocols proposed by Wang et. al. are vulnerable.

Key words: cryptography, protocol, braid group, cryptanalysis, attack, linear decomposition, representation.

Introduction

In this paper we discuss, following [1, 2], a new practical attack on the two main protocols proposed in [3]. This attack works when the platform groups are linear. We show that in this case, contrary to the common opinion (and some explicitly stated security assumptions), one does not need to solve the underlying algorithmic problems to break the scheme, i.e., there is another algorithm that recovers the private keys without solving the principal algorithmic problem on which the security assumptions are based. This changes completely our understanding of security of these schemes. The efficacy of the attack depends on the platform group, so it requires a specific analysis in each particular case. In general one can only state that the attack is in polynomial time in the size of the data, when the platform and related groups are given together with their linear representations. In many other cases we can effectively use known linear representations of the groups under consideration. The braid groups are among them in view of the Lawrence-Krammer representation. The monography [1] solves uniformly protocols based on the conjugacy search problem (Ko et. al. [4], Wang et. al. [5]), protocols based on the decomposition and factorization problems (Stickel [6], Alvares et. al. [7], Shpilrain and Ushakov [8]), protocols based on actions by automorphisms (Mahalanobis [9], Habeeb, Kahrobaei et. al. [10], Markov, Mikhalev et.al. [11]), and a number of other protocols. In this paper we apply our method to the double shielded key exchange protocols 1 and 2 proposed in [3].

Construction of a basis

Let V be a finite dimensional vector space over a field F with basis $B = \{v_1, \dots, v_r\}$. Let $\mathrm{End}(V)$ be the semigroup of endomorphisms of V. We assume that elements in V are given as vectors relative to B, and endomorphisms in End (V) are given by their matrices relative to B. Let $< W >$ denotes submonoid generated by W.

For an endomorphism $a \in \mathrm{End}(V)$ and an element $v \in V$ we denote by v^a the image of v under a. Also, for any subsets W of V and A of $\mathrm{End}(V)$ we put $W^A = \{w^a | w \in W, a \in A\}$, and denote by $\mathrm{Sp}(W)$ the subspace of V generated by W. We assume that elements of the field F are given in some constructive form and the «size» of the form is defined. Furthermore, we assume that the basic field operations in F are efficient, in particular they can be performed in polynomial time in the size of the elements. In all the particular protocols considered in this paper the field F satisfies all these conditions.

There is an algorithm that for given finite subsets $W \subseteq V$ and $U \subseteq \mathrm{End}(V)$ finds a basis of the subspace $\mathrm{Sp}(W^{<U>})$ in the form $\{w_1^{a(1)}, \dots, w_t^{a(t)}\}$, where $w_i \in W$ and $a(i)$ is a product of elements from U. Furthermore, the number of field operations used by; the algorithm is polynomial in $r = \dim_F(V)$ and the cardinalities $|W|$ and $|U|$ of W and U, respectively.

Using Gauss elimination one can effectively find a maximal linearly independent subset L_0 of W. Notice that $\mathrm{Sp}(L_0^{<U>}) = \mathrm{Sp}(W^{<U>})$. Adding to the set L_0 one by one elements v^a, where $v \in L_0$, $a \in U$ and checking every time linear independence of the extended set, one can effectively construct a maximal linearly independent subset L_1 of $L_0 \cup L_0^U$ which extends the set L_0. Notice that $\mathrm{Sp}(L_0^{<U>}) = =\mathrm{Sp}(L_1^{<U>})$ and the elements in L_1 are of the form w^a, where $w \in W$ and $a = 1$ or $a \in U$. It follows that if $L_0 = L_1$ then L_0 is a basis of $\mathrm{Sp}(W^{<U>})$. If $L_0 \neq L_1$ then we repeat the procedure for L_1 and find a maximal linearly independent subset L_2 of $L_1 \cup L_1^U$ that extends L_1. Keep going one constructs a sequence of strictly increasing subspaces $L_0 < L_1 < \ldots < L_i$ of V. Since the dimension r of V is finite the sequence stabilizes for some $i \leq r$. In this case L_i is a basis of $\mathrm{Sp}(W^{<U>})$ and its elements are in the required form.

To estimate the upper bound of the number of the field operations used by the algorithm, observe first that the number of the field operations in Gauss elimination performed on a matrix of size $n \times r$ is $\mathrm{O}(n^2 r)$. Hence it requires at most $\mathrm{O}(n^2 r)$ steps to construct L_0 from W, where $n = |W|$ is the number of elements in W. Notice that $|L_j| \leq r$ for every j. So to find L_{j+1} it suffices to perform Gauss elimination on the matrix corresponding to $L_j \cup L_j^U$ which has size at most $r + r|U|$. Thus the upper estimate on this number is $\mathrm{O}(r^3|U|^2)$. Since there are at most r iterations of this procedure one has the total estimate as $\mathrm{O}(r^3|U|^2 + r|W|^2)$.

In this paper V is underlying linear space of a matrix algebra $\mathrm{Mat}_t(F)$ of all matrices of size $t \times t$ over F. Let G be a subgroup of the multiplicative group of $\mathrm{Mat}_t(F)$, and A and B are two subgroups of G. Every pair of elements $a \in A$ and $b \in B$ define an automorphism $\varphi(a, b)$ of V such that for every $v \in V$ one has $v^{\varphi(a,b)} = avb$. Let U be submonoid generated by all such automorphisms. Thus for every subset $W \subseteq V$ one can effectively construct a basis of subspace W^U.

The double shielded key exchange protocol 1 from [3]

At first we describe the protocol 1 from [3]. Recall that in [3] the Artin braid groups B_n were recommended as platforms for the proposed protocols constructing.

In view of the Lawrence-Krammer representation of the braid group B_n we can assume that the group G below is given as a linear group over a field F. So, we assume that G is a part of a finite dimensional vector space V.

Alice and Bob agree on a non-abelian group G, and randomly chosen element $h \in G$ and two subgroups A and B of G, such that $ab = ba$ for any $a \in A$ and any $b \in B$. We assume that A and B are finitely generated and are given by the fixed generating sets $\{a_1, ..., a_n\}$ and $\{b_1, ..., b_m\}$, respectively.

Alice chooses four elements $c_1, c_2, d_1, d_2 \in A$, computes $x = d_1 c_1 h c_2 d_2$ and then sends x to Bob.

Bob chooses six elements $f_1, f_2, g_1, g_2, g_3, g_4 \in B$, computes $y = g_1 f_1 h f_2 g_2$ and $w = g_3 f_1 x f_3 g_4$, and then sends (y, w) to Alice.

Alice chooses two elements $d_3, d_4 \in A$, computes $z = d_3 c_1 y c_2 d_4$ and $u = d_1^{-1} w d_2^{-1}$, and then sends (z, u) to Bob.

Bob sends $v = g_1^{-1} z g_2^{-1}$ to Alice.

Alice computes $K_A = d_3^{-1} v d_4^{-1} = c_1 f_1 h f_2 c_2$.

Bob computes $K_B = g_3^{-1} u g_4^{-1} = c_1 f_1 h f_2 c_2$ which is equal to K_A and then $K = K_A = K_B$ is Alice and Bob's common secret key.

Now we show how the common secret key can be computed. Let BzB be subspace of V generated by all elements of the form fzg where $f, g \in B$. We can construct a basis $\{e_i z l_i (e_i, l_i \in B, i = 1, ..., r)\}$ of BzB in a polynomial time as it is explained in the previous section. Since $v \in BzB$, we can effectively write it in the form

$$v = \sum_{i=1}^{r} \alpha(i) e_i z l_i, \tag{1}$$

where $\alpha(i) \in F$ for $i = 1, ..., r$. In a similar way we construct bases $\{e_j^{'} h l_j^{'} (e_j^{'}, l_j^{'} \in B, j = 1, ..., s)\}$ of BhB, and $\{e_k^{''} w l_k^{''} (e_k^{''}, l_k^{''} \in B, k = 1, ..., q)\}$ of BwB. Then we get presentations

$$y = \sum_{j=1}^{s} \beta(j) e_j^{'} h l_j^{'}, \tag{2}$$

where $\beta(j) \in F$ for $j = 1, ..., s$, and

$$x = \sum_{k=1}^{q} \gamma(k) e_k^{''} w l_k^{''}, \tag{3}$$

where $\gamma(k) \in F$ for $k = 1, ..., q$.

Now we swap w by u in the right hand side of (3). By direct computation we obtain

$$\sum_{k=1}^{q} \gamma(k) e_k^{''} u l_k^{''} = \sum_{k=1}^{q} \gamma(k) e_k^{''} d_1^{-1} w d_2^{-1} l_k^{''} = d_1^{-1} (\sum_{k=1}^{q} \gamma(k) e_k^{''} w l_k^{''}) d_2^{-1} = d_1^{-1} x d_2^{-1} = c_1 h c_2. \quad (4)$$

Then we swap h by $c_1 h c_2$ in the right hand side of (2) and get

$$\sum_{j=1}^{s} \beta(j) e_j^{'} c_1 h c_2 l_j^{'} = c_1 (\sum_{j=1}^{s} \beta(j) e_j^{'} h l_j^{'}) c_2 = c_1 y c_2 = c_1 g_1 f_1 h f_2 g_2 c_2. \quad (5)$$

At last we swap z by $c_1 g_1 f_1 h f_2 g_2 c_2$ in the right hand side of (1) and get

$$\sum_{i=1}^{r} \alpha(i) e_i c_1 g_1 f_1 h f_2 g_2 c_2 l_i = d_3^{-1} (\sum_{i=1}^{r} \alpha(i) e_i z l_i) d_4^{-1} = c_1 f_1 h f_2 c_2 = K. \quad (6)$$

The double shielded key exchange protocol 2 from [3]

Now we describe the protocol 2 from [3].

As before we assume that the group G below is given as a linear group over a field F. So, we assume that G is a part of a finite dimensional vector space V.

Alice and Bob agree on a non-abelian group G, and randomly chosen element $h \in G$ and two subgroups A and B of G, such that $ab = ba$ for any $a \in A$ and any $b \in B$. We assume that A and B are finitely generated and are given by the fixed generating sets $\{a_1, ..., a_n\}$ and $\{b_1, ..., b_m\}$, respectively.

Alice chooses four elements $c_1, d_1 \in A$ and $f_2, g_2 \in B$, computes $x = d_1 f_1 h_2 d_2$ and then sends x to Bob.

Bob chooses six elements $c_2, d_2, d_3 \in A$ and $f_1, g_1, g_3 \in B$, computes $y = g_1 f_1 h c_2 d_2$ and $w = g_3 f_1 x c_2 d_3$, and then sends (y, w) to Alice.

Alice chooses two elements $d_4 \in A$ and $g_4 \in B$, computes $z = d_4 c_1 y f_2 g_4$ and $u = d_1^{-1} w g_2^{-1}$, and then sends (z, u) to Bob.

Bob sends $v = g_1^{-1} z d_2^{-1}$ to Alice.

Alice computes $K_A = d_4^{-1} v g_4^{-1}$. Bob computes $K_B = g_3^{-1} u d_3^{-1} = c_1 f_1 h f_2 c_2$ which is equal to K_A and then $K = K_A = K_B$ is Alice and Bob's common secret key.

Now we show how the common secret key can be computed. Let BzA be subspace of V generated by all elements of the form fzd where $f \in B, d \in A$.

We can construct a basis $\{e_i z l_i (e_i \in B, l_i \in A, i = 1, ..., r)\}$ of BzA in a polynomial time as it is explained in the previous section. Since $v \in BzA$, we can effectively write it in the form

$$v = \sum_{i=1}^{r} \alpha(i) e_i z l_i, \quad (7)$$

where $\alpha(i) \in F$ for $i = 1, ..., r$.

In a similar way we construct bases $\{e_j^{'} h l_j^{'} (e_j^{'} \in B, l_j^{'} \in A, j = 1, ..., s)\}$ of BhA, and $\{e_k^{''} w l_k^{''} (e_k^{''} \in \in B, l_k^{''} \in A, k = 1, ..., q)\}$ of BwA.

Then we get presentations:

$$y = \sum_{j=1}^{s} \beta(j) e_j^{'} h l_j^{'}, \quad (8)$$

where $\beta(j) \in F$ for $j = 1, ..., s$, and

$$x = \sum_{k=1}^{q} \gamma(k) e_k^{''} w l_k^{''}, \quad (9)$$

where $\gamma(k) \in F$ for $k = 1, ..., q$.

Now we swap w by u in the right hand side of (9). By direct computation we obtain

$$\sum_{k=1}^{q}\gamma(k)e_k^{''}ul_k^{''}=\sum_{k=1}^{q}\gamma(k)e_k^{''}d_1^{-1}wg_2^{-1}l_k^{''}=d_1^{-1}(\sum_{k=1}^{q}\gamma(k)e_k^{''}wl_k^{''})g_2^{-1}=d_1^{-1}xg_2^{-1}=c_1hf_2. \quad (10)$$

Then we swap h by $c_1hf_2$in the right hand side of (8) and get

$$\sum_{j=1}^{s}\beta(j)e_j^{'}c_1hf_2l_j^{'}=c_1(\sum_{j=1}^{s}\beta(j)e_j^{'}hl_j^{'})f_2=c_1yf_2=c_1g_1f_1hc_2d_2f_2. \quad (11)$$

At last we swap z by $c_1g_1f_1hc_2d_2f_2$ in the right hand side of (7) and get

$$\sum_{i=1}^{r}\alpha(i)e_ic_1g_1f_1hc_2d_2f_2l_i=d_4^{-1}(\sum_{i=1}^{r}\alpha(i)e_izl_i)g_4^{-1}=c_1f_1hc_2f_2=K. \quad (12)$$

Two other, the shielded public key encryption protocol and the shield digital signature protocol in [3] completely based on the protocols 1 and 2. They can be attacked by the procedures that has been just described.

The Lawrence-Krammer representation

Let B_n denotes the Artin braid group on n strings, $n \in N$, where N denotes the set of natural numbers. R. Lawrence described in 1990 a family of so called *Lawrence representations* of B_n. Around 2001 S. Bigelow [11] and D. Krammer [12] independently proved that all braid groups B_n are linear. Their work used new the *Lawrence-Krammer representations* $\rho_n : B_n \to \mathrm{GL}_{n(n-1)/2}(Z[t^{\pm 1}, s^{\pm 1}])$ that has been proved faithful for every $n \in N$. One can effectively find the image $\rho_n(g)$ for every element $g \in B_n$.

Moreover, there exists an effective procedure to recover a braid $g \in B_n$ from its image $\rho_n(g)$. It was shown in [13] that it can be done in $\mathrm{O}(m^3 log d_t)$ multiplications of entries in $\rho_n(g)$. Here $m = n(n-1)/2$ and d_t is a parameter that can be effectively computed by $\rho_n(g)$. See [13] for details.

Complexity of the proposed cryptanalysis

In this paper we proposed a polynomial time deterministic algorithm to recover secret; keys established by the protocols 1 and 2 in [3]. We assumed that the group G in this protocols is linear. The authors of [3] suggested that the infinite nonabelian groups B_n with $n \geq 12$ can be taken as the platform groups for the protocols 1 and 2 in [3]. By the Lawrence-Krammer representations the groups B_n are linear. Moreover, this representations are effective computable and invertible. Unfortunately, in this setting the proposed protocols are not secure. Our cryptanalysis in the above sections shows that the linear decomposition attack works effectively in this case.

We present a cryptanalysis such that all used tools consist of only classical Gauss elimination process. It is well known that the Gauss elimination process is a polynomial procedure. To estimate the upper bound of the number of the field operations used by the algorithm, observe first that the number of the field operations in Gauss elimination performed on a matrix of size $n \times r$ is $\mathrm{O}(n^2r)$. Hence it requires at most $\mathrm{O}(n^2r)$ steps to construct L_0 from W, where $n = |W|$ is the number of elements in W. Notice that $|L_j| \leq r$ for every j. So to find L_{j+1} it suffices to perform Gauss elimination on the matrix corresponding to $L_j \cup L_j^U$ which has size at most $r + r|U|$. Thus the upper estimate on this number is $\mathrm{O}(r^3|U|^2)$. Since there are at most r iterations of this procedure one has the total estimate as $\mathrm{O}(r^3|U|^2 + r|W|^2)$. When we derive solutions in (1)–(3) and in (7)–(9) we can estimate the time complexity by a polynomial function depending of the dimension r of the space V and the parameter $m = max\{|A|, |B|\}$ as $\mathrm{O}(r^3m^2)$. With this estimation we can compute the secret keys in the form of matrices. If the platform B_n is given by an abstract presentation, we can use the Lawrence-Krammer's representation, and then its inverse. It was shown in [14] that both these procedures are polynomial in time. Details can be found in [14].

Similar cryptanalysis can be applied to many other protocols based on (semi) groups presented as linear (semi)groups. Moreover, in a number of other cases we can firstly transform our platform to the linear form, and then apply our cryptanalysis. But in this latter case we should care about dimension of representation. Moreover, we need in tractable inverse map. All such topics open new area of pure theoretical investigations

in the representation theory. Fortunately, studying of algebraic algorithms with a point of view of its possible practical application are led by many mathematicians. There are a lot of interesting and useful results in this direction.

Supported by Russian Foundation for Basic Research, project 15-41-04312.

References

1 *Романьков В.А.* Алгебраическая криптография. — Омск: ОмГУ, 2013. — С. 135.

2 *Романьков В.А.* Криптоанализ некоторых схем, использующих автоморфизмы // Прикладная дискретная математика. — 2013. — № 3. — С. 35–51.

3 *Wang X., Xu C., Li G., Lin H., Wang W.* Double shielded public key cryptosystems // Cryptology ePrint Archive Report 2014/588. — 2014. — P. 1–14.

4 *Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J., Park C.* New public-key cryptosystem using braid groups // Advances in Cryptology. CRYPTO 2000. — Vol. 1880 (Lecture Notes Comp. Sc.) — Berlin: Springer, 2000. — P. 166–183.

5 *Wang L., Wang L., Cao Z., Okamoto E., Shao J.* New constructions of public-key encryption schemes from conjugacy search problems // Information security and cryptology. (Lecture Notes Comp. Sc.) — Berlin: Springer, 2010. — Vol. 6584. — P. 1–17.

6 *Stickel E.* A New Method for Exchanging Secret Keys // Proc. of the Third Intern. Conf. on Information Technology and Applications (ICITA 05). Contemp. Math. (IEEE Computer Society). — 2005. — Vol. 2. — P. 426–430.

7 *Alvarez R., Martinez F.-M., Vicent J.F., Zamora A.* A Matricial Public Key Cryptosystem with Digital Signature // WSEAS Trans. on Math. — 2008. — Vol. 4(7). — P. 195–204.

8 *Shpilrain V., Ushakov A.*A new key exchange protocol based on the decomposition problem // Algebraic Methods in Cryptography Contemp. Math. — 2006. — Vol. 418. — P. 161–167.

9 *Mahalanobis A.* The Diffie-Hellman key exchange protocol and non-abelian nilpotent groups // Israel Math. Journal. — 2008 — Vol. 165. — P. 161–187.

10 *Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V.* Public key exchange using semidirect product of (semi)groups. — [ER]. Access mode: arXiv math.: 1304.6572v1[cs.CR]. 24 Apr. 2013. — P. 1–12.

11 *Марков В.Т., Михалев А.В., Грибов А.В., Золотых П.А., Скаженик С.С.* Квазигруппы и кольца в кодировании и построении криптосхем // Прикладная дискретная математика. — 2012. — № 4. — С. 35–52.

12 *Bigelow S.* Braid groups are linear // Amer. Math. Soc. Journal. — 2001. — Vol. l. — P. 471–486.

13 *Krammer D.* Braid groups are linear // Ann. Math. — 2002. — Vol. 155. — P. 131–156.

14 *Cheon J.H., Jun B.* A Polynomial Time Algoritm for the Braid Diffie-Hellman Conjugacy Problem // Advances in Cryptology. CRYPTO-2003. Lect. Notes in Comput. Sci. — 2003. — Vol. 2729. — P. 212–225.

В.А. Романьков

Өрімге негізделген ашық кілті бар қос панельдік шифрлау жүйесі үшін полиномиалды алгоритм

Мақалада ашық кілтпен кемерлер шифрлау жүйесінде негізделген криптографиялық талдау үшін алгоритм уақыты бойынша детерминдік полиномдық практикалық жаңа дәлелденетін Ванга, Ксу, Ли, Лин және Вана «Double shielded public key eryptosystems» ұсынылды. Автор платформа орнына B_n Артина кемер группасын қолдануға кеңес берді. Осы жұмыста автордың жүргізген сызықтық декомпозициялық бағыты бөліктелген әдіске негізделген Лоуренс-Крамер түсінігіне қатысты кемер бейнесіне қолданылып көрсетілген. Нәтижесінде [3] хаттамаға негізделген қос бөлінген кілттер табылды. Бұл кілттер оларды айқын түрде де белсенді есептейді. Осылайша [3] хаттамада осалдығы орнатылған.

В.А. Романьков

Полиномиальный алгоритм для основанной на косах системы шифрования с открытым ключом двойного щита

В статье предложен новый доказуемый практический детерминистский полиномиальный по времени алгоритм для криптографического анализа, основанный на косах системы шифрования с открытым ключом Ванга, Ксу, Ли, Лин и Ванга «Double shielded public key cryptosystems». Рекомендованы к использованию в качестве платформ группы кос Артина B_n. Показана, линейной декомпозиционной атаки, основанной на методе разложения, введенном автором, применимость к образам кос относительно представления Лоуренс-Крамера. В результате найдены разделенные ключи в обоих основных протоколах из [3]. Эти ключи эффективно вычисляются и в их оригинальном виде. Тем самым установлена уязвимость протоколов из [3].

References

1 Roman'kov V.A. *Algebraic cryptography,* Omsk: Omsk State University, 2013, p. 135.

2 Roman'kov V.A. *Discrete Applied Mathematics,* 2013, 3, p. 35–51.

3 Wang X., Xu C., Li G., Lin H., Wang W. *Cryptology ePrint Archive Report* 2014/588, 2014, p. 1–14.

4 Ko K.H., Lee S.J., Cheon J.H., Han J.W., Kang J., Park C. *Advances in Cryptology. CRYPTO 2000. Vol. 1880 (Lecture Notes Comp. Sc.)*, Berlin: Springer, 2000, p. 166–183.

5 Wang L., Wang L., Cao Z., Okamoto E., Shao J. *Information security and cryptology,* (Lecture Notes Comp. Sc.), Berlin: Springer, 2010, 6584, p. 1–17.

6 Stickel E. *Proc. of the Third Intern. Conf. on Information Technology and Applications (ICITA 05),* Contemp. Math. (IEEE Computer Society), 2005, 2, p. 426–430.

7 Alvarez R., Martinez F.-M., Vicent J.F., Zamora A. *WSEAS Trans. on Math.,* 2008, 4 (7), p. 195–204.

8 Shpilrain V., Ushakov A. *Algebraic Methods in Cryptography. Contemp. Math.,* 2006, 418, p. 161–167.

9 Mahalanobis A. *Israel Math. Journal,* 2008, 165, p. 161–187.

10 Habeeb M., Kahrobaei D., Koupparis C., Shpilrain V. [ER]. Access mode: arXiv math.: 1304.6572v1 [cs.CR], 24 Apr. 2013, p. 1–12.

11 Markov V.T., Mihalyov A.V., Gribov A.V., Zolotyh P.A., Skazhenik S.S. *Discrete Applied Mathematics,* 2012, 4, p. 35–52.

12 Bigelow S. *Amer. Math. Soc. Journal,* 2001, l, p. 471–486.

13 Krammer D. Ann. *Math. Journal,* 2002, 155, p. 131–156.

14 Cheon J.H., Jun B. *Advances in Cryptology. CRYPTO-2003,* Lect. Notes in Comput. Sci., 2003, 2729, p. 212–225.