Cryptanalysis of Some Protocols Using Matrices over Group Rings

Mohammad Eftekhari(✉)

LAMFA, CNRS UMR 7352, Université de Picardie – Jules Verne,
33 rue Saint-Leu, 80039 Amiens, France
mohamed.eftekhari@u-picardie.fr

Abstract. We address a cryptanalysis of two protocols based on the supposed difficulty of discrete logarithm problem on (semi) groups of matrices over a group ring. We can find the secret key and break entirely the protocols.

Keywords: Key exchange · Symmetric groups · Representation of algebras

1 Introduction

The Diffie-Hellman key agreement protocol is the first published practical solution to the key distribution problem, allowing two parties that have never met to exchange a secret key over an open channel. It uses the cyclic group $\mathbb{F}_q^*$, where $\mathbb{F}_q$ is the finite field of q elements. The security of this protocol is based on the difficulty of computing discrete logarithms (DL) in the group $\mathbb{F}_q^*$. There are several algorithms for computing discrete logarithms, some of them are subexponential when applied to $\mathbb{F}_q^*$.

It is important to search for easily implementable groups, for which the DL problem is hard and there is no known subexponential time algorithm for computing DL. The group of points over $\mathbb{F}_q$ of an elliptic curve is such a group. In [8], the group of invertible matrices with coefficients in a finite field was considered for such a key exchange. In [6], using the Jordan form it was shown that the discrete logarithm problem on such matrices can be reduced to the same problem over some small extensions of the finite base field.

In [4], the authors consider the semigroup of matrices (3-by-3 matrices) over the group ring $\mathbb{F}_7[S_5]$, where S_5 is the group of permutation of $\{1, 2, 3, 4, 5\}$. The security of this protocol is based on the supposed difficulty of the discrete logarithm problem in the (semi) group of matrices with coefficients in $\mathbb{F}_7[S_5]$.

Moreover in [5], the authors propose the same semigroup as a platform for the Cramer-Shoup cryptosystem which is a generalization of ElGamal's protocol. Here the security is based on the supposed difficulty of the discrete logarithm problem in the group of invertible 3-by-3 matrices with coefficients in $\mathbb{F}_7[S_5]$.

In [1,2,7] a cryptanalysis of [4] is proposed. Their methods are somehow different. In [1], the problem of discrete logarithm in a semigroup is reduced

M. Joye and A. Nitaj (Eds.): AFRICACRYPT 2017, LNCS 10239, pp. 223–229, 2017.
DOI: 10.1007/978-3-319-57339-7_13

to the same problem in a subgroup of the same semigroup. In [2] one uses a slight modification of Shor's quantum algorithm to find the period of a singular matrix (there is no notion of order for such a matrix) and thereby solving the discrete logarithm problem in semigroups. In [7], $\mathrm{Mat}_3(\mathbb{F}_7[S_5])$ is embedded in $\mathrm{Mat}_{360}(\mathbb{F}_7)$ and then one uses the same procedure as in [6] (adapted to singular matrices). The conclusion of all three papers above is that using a quantum computer one can break the key exchange protocol of [4].

In contrast to the above analysis we use the irreducible representations of the group S_5; then using the fact that the algebra $\mathbb{F}_7[S_5]$ is semi-simple, we give an isomorphism between this algebra and an algebra of block matrices with coefficients in $\mathbb{F}_7$. Then we use this isomorphism to give an isomorphism between $\mathrm{Mat}_3(\mathbb{F}_7[S_5])$, and still another algebra of block matrices over $\mathbb{F}_7$. To do so, we combine the same blocks of the first isomorphism.

This way we reduce the discrete logarithm problem over $\mathrm{Mat}_3(\mathbb{F}_7[S_5])$, to the same problem over block matrices with coefficients in $\mathbb{F}_7$. The maximum size of a block is 18, reducing dramatically the computations. Now we can apply the same procedure (eventually modified for singular matrices) as in [4], to each block and resolve the problem of discrete logarithm entirely (using actual computers) and find the secret key. So the conclusion is that the platform proposed in [4] and [5] are simply insecure.

The rest of this paper is organized as follows. Section 2, will be devoted to the irreducible representations of S_5. In Sect. 3, we explain the isomorphism between matrices with coefficients in $\mathbb{F}_7[S_5]$, and block matrices with coefficients in $\mathbb{F}_7$, and show that the protocols proposed in [4,5] can be broken. In Sect. 4, we give an example to illustrate our analysis. Finally we conclude with some remarks in Sect. 5.

2 Irreducible Representations of S_5

For our purpose, it will be easier to use the following presentation of S_5. We note $W := (12)$ and $Z := (12345)$. The group S_5 is defined by generators W, Z and relations T, where T is the following set of relations:

$$\begin{gathered} W^2 = \mathrm{id} \\ Z^5 = \mathrm{id} \\ (ZW)^4 = \mathrm{id} \\ WZ^{-1}WZW = Z^{-1}WZWZ^{-1}WZ \\ [W, Z^{-2}WZ^2] = \mathrm{id} \\ [W, Z^{-3}WZ^3] = \mathrm{id} \end{gathered}$$

The group S_5 has two distinct representations of dimension one (namely the trivial one and the signature), two non isomorphic irreducible representations of dimension four, two non isomorphic irreducible representations of dimension five, and one irreducible representation of dimension six. We give the images of the

generators Z and W by these representations, and one can verify the relations T, for the images, thereby proving that one defines morphisms from S_5 to matrix groups. One can compare the trace of these morphisms with the character table of S_5 to be sure we obtain all the irreducible representations of S_5.

To construct these representations one can follow the general description of [3], using Young polytabloids, to construct the Specht modules which give the irreducible representation of S_5.

$$W = (12) \longmapsto A_1 \oplus A_1' \oplus A_4 \oplus A_4' \oplus A_5 \oplus A_5' \oplus A_6$$

where

$$A_1 = 1;\ A_1' = -1;\ A_4 = \begin{pmatrix} -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 1 \end{pmatrix};\ A_4' = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} -1 & 0 & 1 & 0 & -1 \\ 0 & -1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix};\ A_5' = \begin{pmatrix} 1 & 0 & -1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & -1 \end{pmatrix}$$

$$A_6 = \begin{pmatrix} -1 & 0 & 1 & 0 & 1 & 0 \\ 0 & -1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$Z = (12345) \longmapsto B_1 \oplus B_1' \oplus B_4 \oplus B_4' \oplus B_5 \oplus B_5' \oplus B_6$$

where

$$B_1 = 1;\ B_1' = 1;\ B_4 = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{pmatrix};\ B_4' = \begin{pmatrix} 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & -1 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & -1 \end{pmatrix}$$

$$B_5 = \begin{pmatrix} 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix};\ B_5' = \begin{pmatrix} 0 & 0 & -1 & -1 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 & -1 \\ 1 & 0 & -1 & -1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix};\ B_6 = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & -1 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

3 Cryptanalysis of Protocols

In [4] the authors propose the Diffie-Hellman key exchange using 3-by-3 matrices over $\mathbb{F}_7[S_5]$. So Alice and Bob, take a public matrix $M \in \mathrm{Mat}_3(\mathbb{F}_7[S_5])$ which

may be non-invertible. Alice chooses a secret integer n, computes M^n and sends it to Bob. Bob chooses a secret integer n', computes $M^{n'}$ and sends it to Alice. Every party can now compute the common key $M^{nn'}$.

In [5], they use the same platform for the Cramer-Shoup cryptosystem which we do not recall. We underline only that there is a public key M as above, and during the protocol among other data sent, there is M^n where n is the secret key. So if we are able to give a solution for the discrete logarithm problem in the case of $M \in \mathrm{Mat}_3(\mathbb{F}_7[S_5])$, in both cases the platform proposed is not secure. That is what we are going to explain.

As 7 does not divide $|S_5| = 120$, the algebra $\mathbb{F}_7[S_5]$ is semi-simple and Maschke's theorem asserts that this algebra is isomorphic to a direct sum of matrix algebras (over $\mathbb{F}_7$), in other words it is isomorphic to an algebra of block matrices over $\mathbb{F}_7$. Let us denote by f this isomorphism. To be of any use for our purpose, we have to make precise this isomorphism explicitly. The $\mathbb{F}_7$-linear extension (to $\mathbb{F}_7[S_5]$) of the morphism of S_5 using the irreducible representations of S_5 given on generators $W = (12), Z = (12345)$ in Sect. 2, gives the isomorphism f between $\mathbb{F}_7[S_5]$ and its image. So for any element $x = \sum_{i=1}^{120} a_i x_i \in \mathbb{F}_7[S_5]$, $a_i \in \mathbb{F}_7$ and $x_i \in S_5$ we can compute its image as a direct sum of matrices with coefficients in $\mathbb{F}_7$. Note that this decomposition is a special case of Wedderburn's theorem asserting that every semi-simple algebra can be decomposed as a direct sum of all its distinct simple submodules.

Up to now we have represented a matrix $M \in \mathrm{Mat}_3(\mathbb{F}_7[S_5])$ as a matrix with coefficients in $\mathbb{F}_7$ by replacing each coefficient M_{ij} of M by $f(M_{ij})$. For example M_{11} is replaced by

$$A = \begin{pmatrix} a_1 & & & & & & \\ & a_1' & & & & & \\ & & a_4 & & & & \\ & & & a_4' & & & \\ & & & & a_5 & & \\ & & & & & a_5' & \\ & & & & & & a_6 \end{pmatrix}$$

where a_i, a_i' are block matrices with coefficients in $\mathbb{F}_7$ and the indexes denote the size of the block.

Let us denote by $A, B, C, E, F, G, H, I, J$ the block matrices corresponding to $M_{11}, M_{12}, M_{13}, M_{21}, M_{22}, M_{23}, M_{31}, M_{32}, M_{33}$. Then B is a block matrix which we represent the same way as A by denoting $b_1, b_1', b_4, b_4', \ldots$ its blocks. We use the same notations for $C, D, \ldots$. It is an easy computation to prove that there is a natural isomorphism between matrices

$$\begin{pmatrix} A & B & C \\ D & E & F \\ H & I & J \end{pmatrix}$$

and the block matrix whose first block is obtained by composing (side by side) the first blocks of $A, B, C, D, \ldots$, namely

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ d_1 & e_1 & f_1 \\ h_1 & i_1 & j_1 \end{pmatrix},$$

which gives a 3×3 matrix over $\mathbb{F}_7$.

The second block is obtained by composing the second blocks of $A, B, C, D, \ldots$, namely

$$\begin{pmatrix} a'_1 & b'_1 & c'_1 \\ d'_1 & e'_1 & f'_1 \\ h'_1 & i'_1 & j'_1 \end{pmatrix},$$

and so on.

To sum up, we represent the matrix $M \in \mathrm{Mat}_3(\mathbb{F}_7[S_5])$ by a block matrix in $\mathbb{F}_7$ whose blocks are of size $3, 3, 12, 12, 15, 15, 18$. We represent also the matrix M^n by a block matrix with the same size $3, 3, 12, 12, 15, 15, 18$ in $\mathbb{F}_7$. Now we can apply the same techniques as in [6], namely write the Jordan form of each block in some small extension base $\mathbb{F}_{7^\alpha}$ and find the secret key n. Note that for singular blocks, we need a slight modification of the procedure of [6], as proposed in [7].

4 An Example

We use the notations of Sects. 2 and 3.

Let us denote e the identity element of S_5.

Let

$$M = \begin{pmatrix} 2e + W + S & 3e + WS & e + S^2 \\ 5e + 2SWS & e + W + S^3 & S \\ W + S^2 & 2e + S & e + W \end{pmatrix} \in \mathbb{F}_7[S_5]$$

and $N = M^n$ (n is unknown) two given matrices. Our goal is to find $l \in \mathbb{N}$ such that $M^l = N$.

We represent every coefficient of M as a block matrix as follows:

$2e + W + S = (2A_1) + (A_1 \oplus A'_1 \oplus A_4 \oplus A'_4 \oplus A_5 \oplus A'_5 \oplus A_6) + (B_1 \oplus B'_1 \oplus B_4 \oplus B'_4 \oplus B_5 \oplus B'_5 \oplus B_6) = (2A_1 + A_1 + B_1) \oplus (A'_1 + B'_1) \oplus (A_4 + B_4) \oplus A'_4 + B'_4) \oplus (A_5 + B_5) \oplus (A'_5 + B'_5) \oplus (A_6 + B_6) = (4) \oplus (0) \oplus (A_4 + B_4) \oplus (A'_4 + B'_4) \oplus (A_5 + B_5) \oplus (A'_5 + B'_5) \oplus (A_6 + B_6)$.

$3e + WS = (3A_1) + (A_1B_1 \oplus A'_1B'_1 \oplus (A_4B_4 \oplus A'_4B'_4 \oplus A_5B_5 \oplus A'_5B'_5 \oplus A_6B_6) = (3A_1 + A_1B_1) \oplus (A'_1B'_1) \oplus A_4B_4) \oplus (A'_4B'_4) \oplus (A_5B_5) \oplus (A'_5B'_5) \oplus (A_6B_6) = (4) \oplus (-1) \oplus (A_4B_4) \oplus (A'_4B'_4) \oplus (A_5B_5) \oplus (A'_5B'_5) \oplus (A_6B_6)$.

$e + S^2 = (2) \oplus (1) \oplus B_4^2 \oplus {B'}_4^2 \oplus B_5^2 \oplus {B'}_5^2 \oplus B_6^2.$

$5+2SWS = (0) \oplus (2) \oplus 2B_4A_4B_4 \oplus 2B'_4A'_4B'_4 \oplus 2B_5A_5B_5 \oplus 2B'_5A'_5B'_5 \oplus 2B_6A_6B_6.$

$e+W+S^3 = (3) \oplus (0) \oplus (A_4+B_4^3) \oplus (A'_4+{B'}_4^3) \oplus (A_5+B_5^3) \oplus (A'_5+{B'}_5^3) \oplus (A_6+B_6^3).$

$S = (1) \oplus (-1) \oplus B_4 \oplus B'_4 \oplus B_5 \oplus B'_5 \oplus B_6.$

$W+S^2 = (2) \oplus (2) \oplus (A_4+B_4^2) \oplus (A'_4+{B'}_4^2) \oplus (A_5+B_5^2) \oplus (A'_5+{B'}_5^2) \oplus (A_6+B_6^2).$

$2e + S = (3) \oplus (1) \oplus B_4 \oplus B'_4 \oplus B_5 \oplus B'_5 \oplus B_6.$

$e + W = (2) \oplus (1) \oplus A_4 \oplus A'_4 \oplus A_5 \oplus A'_5 \oplus A_6.$

So far we have represented M by a matrix whose coefficients are block matrices as above with coefficients in $\mathbb{F}_7$. It is straightforward that this matrix is isomorphic to the block matrix we form as follows:

Take the first component of each coefficients to form the matrix

$$M_1 = \begin{pmatrix} 4 & 4 & 2 \\ 0 & 3 & 1 \\ 2 & 3 & 2 \end{pmatrix},$$

then take the second component of each coefficient to form the matrix

$${M'}_1 = \begin{pmatrix} 2 & -1 & 1 \\ 2 & 0 & -1 \\ 2 & 1 & 1 \end{pmatrix}.$$

Take the third component of the coefficients to obtain

$$M_4 = \begin{pmatrix} A_4 + B_4 & A_4B_4 & B_4^2 \\ 2B_4A_4B_4 & A_4 + B_4^3 & B_4 \\ A_4 + B - 4^2 & B_4 & A_4 \end{pmatrix}$$

Note that this matrix is of size 12. Continuing this way we obtain another matrix of size 12 which we denote by ${M'}_4$, two matrices of size 15 denoted by M_5 and ${M'}_5$ and a last matrix of size 18 denoted by M_6. We have $M = M_1 \oplus {M'}_1 \oplus M_4 \oplus {M'}_4 \oplus M_5 \oplus {M'}_5 \oplus M_6$.

We do the same operation on matrix $N = M^n$ to express it as a block matrix of the same size as above. Now we can separately work on corresponding blocks of M and N of the same size, computing the characteristic polynomials, Jordan forms... as suggested in [6], and reduce the discrete logarithm problem to the one on some small extension of the field $\mathbb{F}_7$. It may happen that some block is not invertible. We can still compute the Jordan forms and with a slight modification as suggested in [7] finish the work.

Note that the size of blocks in the above decomposition of M are the product of the size of M as a matrix with coefficients in $\mathbb{F}_7[S_5]$ (namely 3) and the degrees

of irreducible representations of S_5. So if we replace the group S_5 by some other finite group G and the field $\mathbb{F}_7$ by $\mathbb{F}_p$, such that $\mathbb{F}_p[G]$ is a semi-simple algebra, the same procedure works. In fact representations of finite groups are very well known (techniques for constructing the irreducible representations will be different). If $n_1, n_2, \ldots, n_k$ are the degrees of all distinct irreducible representations of G we know that $|G| = n_1^2 + n_2^2 + \ldots n_k^2$ and each n_j divides $|G|$ and even more... (see [9]), such that these degrees are small enough comparing to $|G|$, and a matrix $M \in \mathbb{F}_p[G]$ of size 3 for example, will be decomposed in block matrices with coefficients in $\mathbb{F}_p$ and sizes $3n_1, 3n_2, \ldots, 3n_k$.

5 Conclusion

We showed that using matrices with coefficients in $\mathbb{F}_7[S_5]$ as a platform for Diffie-Hellman key exchange is not secure. One may wonder if replacing $\mathbb{F}_7$ by $\mathbb{F}_2, \mathbb{F}_3$ or $\mathbb{F}_5$ give something essentially different. In fact in these cases the group algebra is not semi-simple anymore and Wedderburn's theorem cannot be applied. But these new algebras are not far from being semi simple; in fact they differ from being semi simple by a nilpotent radical, and the quotient is semi simple and then the same procedure as explained in Sect. 2 can be applied. To sum up we believe that no secure cryptographic protocol can be based upon these algebras.

Furthermore replacing the group S_5 by some other finite group G, can be cryptanalyzed the same way using the irreducible representations of G.

References

1. Banin, M., Tsaban, B.: A reduction of semigroup DLP to classic DLP. Des. Codes Crypt. **81**, 75–82 (2006)
2. Childs, A., Ivanyos, G.: Quantum computation of discrete logarithms in semigroups. J. Math. Cryptology **8**(4), 405–416 (2014)
3. James, G.D.: The Representation Theory of the Symmetric Groups, vol. 682. Springer, Heidelberg (1978). SLN
4. Kahrobaei, D., Koupparis, C., Shpilrain, W.: Public key exchange using matrices over group rings. G.C.C. **5**(1), 97–115 (2013)
5. Kahrobaei, D., Koupparis, C., Shpilrain, W.: A CCA secure cryptosystem using matrices over group rings. Amer. Math. Soc. Contemp. Math. **633**, 73–80 (2015)
6. Menezes, A.J., Wu, Y.-H.: The discrete logarithm problem in $GL_n(\mathbb{F}_q)$. ARS Combinatorica **47**, 23–32 (1997)
7. Myasnikov, A., Ushakov, A.: Quantum algorithm for discrete logarithm problem for matrices over finite group rings.
8. Odonne, R., Varadharajan, D., Sanders, P.: Public key distribution in matrix rings. Electron. Lett. **20**, 386–387 (1984)
9. Serre, J.P.: Représentations linéaires des groupes finis. Hermann, Paris (1967)