AAECC (2012) 23:143–149
DOI 10.1007/s00200-012-0170-z

ORIGINAL PAPER

Cryptanalysis of a key exchange protocol based on the endomorphisms ring End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$)

Abdel Alim Kamal · Amr M. Youssef

Received: 2 November 2011 / Revised: 15 March 2012 / Accepted: 15 March 2012 /
Published online: 5 April 2012

Abstract Climent et al. (Appl Algebra Eng Commun Comput 22:91–108, 2011) identified the elements of the endomorphisms ring End($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$) with elements in a set, E_p, of matrices of size 2×2, whose elements in the first row belong to $\mathbb{Z}_p$ and the elements in the second row belong to $\mathbb{Z}_{p^2}$. By taking advantage of matrix arithmetic, they proposed a key exchange protocol using polynomial functions over E_p defined by polynomials in $\mathbb{Z}[X]$. In this note, we show that this protocol is insecure; it can be broken by solving a set of 10 consistent homogeneous linear equations in 8 unknowns over $\mathbb{Z}_{p^2}$.

Keywords Cryptanalysis · Key exchange protocol · Endomorphism · Noncommutative ring

1 Introduction

Climent et al. [1] identified the elements of the endomorphisms ring End ($\mathbb{Z}_p \times \mathbb{Z}_{p^2}$) [2] with elements in a new set, denoted by E_p, of matrices of size 2×2, whose elements in the first row belong to $\mathbb{Z}_p$ and the elements in the second row belong to $\mathbb{Z}_{p^2}$. The following results were established in [1]:

A. A. Kamal
Department of Electrical and Computer Engineering (ECE), Concordia University,
1455 De Maisonneuve Blvd. W., Montreal, QC H3G 1M8, Canada
e-mail: a_kamala@encs.concordia.ca

A. M. Youssef (✉)
Concordia Institute for Information Systems Engineering(CIISE), Concordia University,
1455 De Maisonneuve Blvd. W., Montreal, QC H3G 1M8, Canada
e-mail: youssef@ciise.concordia.ca

The set

$$E_p = \left\{ \begin{bmatrix} a & b \\ pc & d \end{bmatrix} | a, b, c \in \mathbb{Z}_p \text{ and } d \in \mathbb{Z}_{p^2} \right\}$$

is a noncommutative unitary ring where addition is defined by

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 + a_2) \bmod p & (b_1 + b_2) \bmod p \\ p(c_1 + c_2) \bmod p^2 & (d_1 + d_2) \bmod p^2 \end{bmatrix},$$

and multiplication is defined by

$$\begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix} = \begin{bmatrix} (a_1 a_2) \bmod p & (a_1 b_2 + b_1 d_2) \bmod p \\ p(c_1 a_2 + d_1 c_2) \bmod p^2 & (pc_1 b_2 + d_1 d_2) \bmod p^2 \end{bmatrix}.$$

The additive and multiplicative identities of E_p are given by

$$O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \text{ and } I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \text{ respectively.}$$

Let $M = \begin{bmatrix} a & b \\ pc & pu + v \end{bmatrix} \in E_p$ with $a, b, c, u, v \in \mathbb{Z}_p$. Then M is invertible if and only if $a \neq 0$ and $v \neq 0$, and in this case we have

$$M^{-1} = \begin{bmatrix} a^{-1} & (-a^{-1}bv^{-1}) \bmod p \\ p[(-a^{-1}cv^{-1}) \bmod p] & p\left[\left(ca^{-1}b(v^{-1})^2 - u(v^{-1})^2 - \lfloor \frac{vv^{-1}}{p} \rfloor v^{-1}\right) \bmod p\right] + v^{-1} \end{bmatrix}.$$

Climent et al. [1] proved that the ring End $(\mathbb{Z}_p \times \mathbb{Z}_{p^2})$ is isomorphic to the ring E_p. Furthermore, they proved that the fraction of invertible elements in E_p is given by

$$\left(\frac{p-1}{p}\right)^2 \approx 1 \text{ for large } p. \tag{1}$$

Thus, for large values of p, almost all elements in E_p are invertible.

During the last decade, several cryptographic primitives using algebraic systems rather than traditional finite cyclic groups or finite fields have been proposed (e.g., see [3,4]).

In this context, and by trying to take advantage of matrix arithmetic, Climent et al. proposed a key exchange protocol using polynomial functions over E_p defined by polynomials in $\mathbb{Z}[X]$. In this note, we show that this protocol is not secure. In particular, we show that this protocol can be broken by solving a set of 10 consistent homogeneous linear equations in 8 unknowns over $\mathbb{Z}_{p^2}$.

2 Description of the key exchange scheme

For completeness, in this section, we briefly review the relevant details of the Climent et al. key exchange scheme. For further details, the reader is referred to [1].

Let $f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{Z}[X]$. For an element $M \in E_p$, the element

$$f(M) = a_0 I + a_1 M + a_2 M^2 + \cdots + a_n M^n \in E_p$$

where I is the multiplicative identity of E_p. The key exchange protocol proposed in [1] can be summarized as follows:

1. Alice and Bob agree on the public parameters $r, s \in \mathbb{N}$ and $M, N \in E_p$ for a large prime p.
2. Alice and Bob choose their private keys $f(X)$ and $g(X) \in \mathbb{Z}[X]$, respectively.
3. Alice computes her public key $P_A = f(M)^r N f(M)^s$ and sends it to Bob.
4. Bob computes his public key $P_B = g(M)^r N g(M)^s$ and sends it to Alice.
5. Alice and Bob compute $S_A = f(M)^r P_B f(M)^s$ and $S_B = g(M)^r P_A g(M)^s$ respectively.
6. Finally, Alice and Bob share the secret key $S_A = S_B$.

3 The proposed attack

The main idea of the attack is based on the following lemma.

Lemma 1 *Let*

$$W_1 = \begin{bmatrix} a_1 & b_1 \\ pc_1 & d_1 \end{bmatrix} \text{ and } W_2 = \begin{bmatrix} a_2 & b_2 \\ pc_2 & d_2 \end{bmatrix}$$

be two matrices in E_p such that

$$W_1 M = M W_1 \tag{2}$$

$$W_2 M = M W_2 \tag{3}$$

$$P_B W_2 = W_1 N. \tag{4}$$

Then we have

$$S_A = S_B = W_1 P_A W_2^{-1}.$$

Proof Note that $W_i, i = 1, 2$, commutes with M implies that W_i commutes with $f(M)$ and consequently W_i commutes with $f(M)^h$ for any $h \in \mathbb{N}$. Also W_i commutes with M implies that W_i^{-1} commutes with M (This follows by noting that $W_i M = M W_i \Rightarrow W_i M W_i^{-1} = M \Rightarrow M W_i^{-1} = W_i^{-1} M$). Thus we have

$$\begin{aligned} W_1 P_A W_2^{-1} &= W_1 f(M)^r N f(M)^s W_2^{-1} \\ &= f(M)^r W_1 N W_2^{-1} f(M)^s \\ &= f(M)^r P_B f(M)^s \\ &= S_A. \end{aligned}$$

□

It is easy to verify that $W_1 = g(M)^r$ and $W_2 = g(M)^{-s}$ is a valid solution to the system of equations in Lemma 1. Thus, this linear system of equations is consistent and consequently the attacker is guaranteed to find at least one solution for it. In what follows we show how the attacker can solve this system of equations. Let

$$M = \begin{bmatrix} m_1 & m_2 \\ pm_3 & m_4 \end{bmatrix} \in E_p.$$

Because of the structure of the elements in E_p, it is easy to verify that the equation resulting from equating the top left element on both sides of the resulting matrices products in (2) does not add any constraints to the system of equations and hence it can be eliminated (In other words, $(a_1m_1 + pb_1m_3) \equiv (a_1m_1 + pm_2c_1) \bmod p$ is always satisfied for all choices of a_1 and b_1). Consequently, (2) leads to the following three equations:

$$\begin{aligned} &a_1m_2 + b_1m_4 - b_1m_1 - d_1m_2 &&\equiv 0 \bmod p \\ &p(c_1m_1 + d_1m_3 - a_1m_3 - c_1m_4) &&\equiv 0 \bmod p^2 \\ &p(c_1m_2 - b_1m_3) &&\equiv 0 \bmod p^2 \end{aligned} \tag{5}$$

with unknowns $a_1, b_1, c_1 \in \mathbb{Z}_p$ and $d_1 \in \mathbb{Z}_{p^2}$. Similar argument applies to (3) (note, however, that (4) leads to 4 equations).

The solution for the above system of equations can be obtained by solving it over $\mathbb{Z}_{p^2}$ and then reducing the obtained solution for a_i, b_i and c_i modulo p, $i = 1, 2$ (recall that, for any multivariate polynomial f, $f(x_1, \ldots, x_n) \equiv 0 \bmod p^2 \Rightarrow f(x_1, \ldots, x_n) \equiv 0 \bmod p$.)

Thus the solution for the system of $3 + 3 + 4 = 10$ equations corresponding to Lemma 1 can be obtained by solving all equations over $\mathbb{Z}_{p^2}$ and then reducing the obtained solution for a_i, b_i and c_i modulo $p, i = 1, 2$. Based on our experimental results, this system of equations is always under-determined and many solutions exist for W_1 and W_2. Choosing any solution such that W_2 is invertible leads to the right key. Note that for large p, which is the case of interest for this cryptosystem, our experimental results confirmed this condition practically holds for almost all valid solutions (also see (1)). We illustrate our attack using the same toy example that was provided in [1] to explain the steps of the protocol.

Example 1 Assume that Alice and Bob agree on $p = 11, r = 3, s = 5$,

$$M = \begin{bmatrix} 5 & 8 \\ 44 & 102 \end{bmatrix} \text{ and } \begin{bmatrix} 10 & 3 \\ 77 & 37 \end{bmatrix}.$$

Alice chooses her secret key as $f(X) = 3 + 3X + 9X^2 + 5X^3 \in \mathbb{Z}[X]$ and Bob chooses his secret key as $g(X) = 9 + 6X + 5X^2 \in \mathbb{Z}[X]$. Thus we have

$$f(M) = 3 + 3M + 9M^2 + 5M^3 = \begin{bmatrix} 10 & 8 \\ 44 & 19 \end{bmatrix},$$

$$g(M) = 9 + 6M + 5M^2 = \begin{bmatrix} 10 & 5 \\ 88 & 72 \end{bmatrix}.$$

Alice computes her public key, P_A, as

$$P_A = f(M)^3 N f(M)^5 = \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix}$$

and sends it to Bob. Bob computes his public key, P_B, as

$$P_B = g(M)^3 N g(M)^5 = \begin{bmatrix} 10 & 10 \\ 11 & 16 \end{bmatrix}$$

and sends it to Alice. Alice computes her secret key $S_A = f(M)^3 P_B f(M)^5$ and Bob computes his secret key $S_B = g(M)^3 P_A g(M)^5$ to obtain

$$S_A = S_B = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix}.$$

As explained above, the solution for the system of equations in Lemma 1 can be obtained by solving

$$\begin{bmatrix} 8 & 9 & 0 & 3 & 0 & 0 & 0 & 0 \\ 77 & 0 & 22 & 44 & 0 & 0 & 0 & 0 \\ 0 & 77 & 88 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 2 & 0 & 8 \\ 0 & 0 & 0 & 0 & 44 & 0 & 99 & 77 \\ 0 & 0 & 0 & 0 & 0 & 44 & 33 & 0 \\ 10 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 4 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 110 & 77 & 110 & 0 & 66 & 0 \\ 0 & 0 & 33 & 37 & 0 & 110 & 0 & 105 \end{bmatrix} \begin{bmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \\ a_2 \\ b_2 \\ c_2 \\ d_2 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{bmatrix} \mod 121$$

and then reducing the obtained solution for a_i, b_i and c_i, $i = 1, 2$, modulo p. Solving this system of linear equations, we obtain

$$\begin{bmatrix} a_1 \\ b_1 \\ c_1 \\ d_1 \\ a_2 \\ b_2 \\ c_2 \\ d_2 \end{bmatrix} \equiv \begin{bmatrix} 41z_1 + z_2 & \mod 11 \\ 3z_1 + 65z_2 & \mod 11 \\ 7z_1 + 5z_2 + 11z_3 & \mod 11 \\ 43z_1 + 4z_2 & \mod 121 \\ 74z_1 + 111z_2 & \mod 11 \\ 99z_1 + 88z_2 & \mod 11 \\ 11z_4 & \mod 11 \\ 8z_1 + 12z_2 & \mod 121 \end{bmatrix}$$

where z_1, z_2, z_3, z_4 can assume any arbitrary values in $\mathbb{Z}_{121}$. The attacker chooses any random values for z_1, z_2, z_3, z_4 such that W_2 is invertible (which happens with probability ≈ 1 for large values of p). In this example, suppose that the attacker randomly chooses $[z_1, z_2, z_3, z_4]^T = [1, 1, 10, 7]^T$, then we have $[a_1, b_1, c_1, d_1, a_2, b_2, c_2, d_2]^T = [9, 2, 1, 47, 9, 0, 0, 20]^T$ and consequently we have

$$W_1 = \begin{bmatrix} 9 & 2 \\ 11 & 47 \end{bmatrix} \text{ and } W_2 = \begin{bmatrix} 9 & 0 \\ 0 & 20 \end{bmatrix} \Rightarrow W_2^{-1} = \begin{bmatrix} 5 & 0 \\ 0 & 115 \end{bmatrix}.$$

Finally, the attacker recovers the secret key by calculating

$$W_1 P_A W_2^{-1} = \begin{bmatrix} 9 & 2 \\ 11 & 47 \end{bmatrix} \begin{bmatrix} 10 & 5 \\ 110 & 119 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 115 \end{bmatrix} = \begin{bmatrix} 10 & 7 \\ 22 & 113 \end{bmatrix} = S_A = S_B.$$

4 Discussion and conclusion

The key exchange protocol proposed by Climent et al. is not secure. In fact, as noted by one of the anonymous reviewers, Climent's scheme can be seen as a partial generalization of Stickel's key agreement scheme [5] which was broken by Shpilrain in [6] (see also [7–9]). In particular, Shpilrain [6] deployed the same linearization approach used in our attack. Shpilrain [6] also suggested to use non-invertible matrices to foil such linear algebra attacks and to repair Stickel's scheme but his proposal has also been broken [8]. The fact that there are so few non-invertible elements in E_p is a weakness of the scheme since it makes the attacker's job easier.

It should also be noted that Stickel's scheme is only an instance of the group Diffie–Hellman scheme [10] which generalizes the original Ko et al. [11] braid group based protocol. Later on, several braid groups were suggested as platform groups. Linear algebra attacks on these braid-based schemes using the same techniques were also deployed (e.g., see [12–15]).

Acknowledgments The authors would like to thank the anonymous reviewers for the valuable comments and suggestions that helped improve the quality of the paper.

References

1. Climent, J.J., Navarro, P.R., Tortosa, L.: On the arithmetic of the endomorphisms ring $End(\mathbb{Z}_p \times Z_p^2)$. Appl. Algebra Eng. Commun. Comput. **22**, 91–108 (2011)
2. Bergman, G.M.: Examples in PI ring theory. Israel J. Math. **18**, 257–277 (1974)
3. Myasnikov, A., Shpilrain, V., Ushakov, A.: Non-Commutative Cryptography and Complexity of Group-Theoretic Problems in Mathematical, Surveys and Monographs. Vol. 177, American Mathematical Society, Providence (2011)
4. Tsaban, B.: Combinatorial Group Theory and Cryptography Bulletin (CGC Bulletin). http://u.cs.biu.ac.il/~tsaban/CGC/cgc.html
5. Stickel, E.: A new method for exchanging secret keys. In: Proceedings of the thrid International Conference on Information Technology and Applications (ICITA'05), pp. 426–430. Sidney (2005)
6. Shpilrain, V.: Cryptanalysis of Stickel's key exchange scheme. In: Computer Science in Russia-CSR'08, Lecture Notes in Computer Science, vol. 5010, pp. 283–288. Springer, Berlin (2008)
7. Sramka, M.: On the security of Stickel's key exchange scheme. Comb. Math. Comb. Comput. **66**, 151–159 (2008)

8. Mullan, C.: Cryptanalysing variants of Stickel's key agreement protocol. Math. Crypt. **4**(4), 365–373 (2011)
9. Mullan, C.: Some Results in Group-Based Cryptography, Thesis submitted to the University of London for the Degree of Doctor of Philosophy (2011)
10. Cha, J.C., Ko, K.H., Lee, S., Han, J.W., Cheon, J.H.: An efficient implementation of braid groups. In: Advances in Cryptology-ASIACRYPT'01, Lecture Notes in Computer Science, vol. 2248, pp. 144–156. Springer, Berlin (2001)
11. Ko, K.H., Lee, S., Cheon, J.H., Han, J.W., Kang, J.S., Park, C.: New public-key cryptosystem using braid groups. In: Bellare, M. (ed.) Advances in Cryptology-CRYPTO'00, Lecture Notes in Computer Science, vol. 1880, pp. 166–183. Springer, Berlin (2000)
12. Hughes, J.: A linear algebraic attack on the AAFG1 braid group cryptosystem. In: Australian Conference on Information Security and Privacy-ACISP'02, Lecture Notes in Computer Science, vol. 2384, pp. 176–189. Springer, Berlin (2002)
13. Cheon, J.H., Jun, B.: A Polynomial Time Algorithm for the Braid Diffie-Hellman Conjugacy Problem. In: Advances in Cryptology-CRYPTO'03, Lecture Notes in Computer Science, vol. 2729, pp. 212–225. Springer, Berlin (2003)
14. Lee, E., Park, J.H.: Cryptanalysis of the public-key encryption based on braid groups. In: Advances in cryptology-EUROCRYPT'03, Lecture Notes in Computer Science, vol. 2656, pp. 477–490. Springer, Berlin (2003)
15. Kalka, A.G.: Representation attacks on the braid Diffie-Hellman public key encryption. Appl. Algebra Eng. Commun. Comput. **17**, 257–266 (2006)