International Journal of Computer Applications (0975 - 8887)
Volume 182 - No.42, February 2019

A Public Key Cryptosystem based on Matrices

Zekeriya Y. Karatas
University of Cincinnati Blue Ash College
Department of Mathematics, Physics, and Computer Science
Blue Ash, OH 45236 USA

Erkam Luy
Erciyes University
Department of Mathematics
Kayseri, 38039, TURKEY

Bilal Gonen
University of Cincinnati
School of Information Technology
Cincinnati, OH 45221 USA

ABSTRACT

In this article, a novel public key cryptosystem is introduced by using an abelian subgroup of $\mathrm{GL}(k, \mathbb{Z}_n)$ where n and k are positive integers. Instead of exponentiation, the conjugation automorphisms are mainly used to define the public and private keys. This allows the calculations to be fast and effective. The security analysis of the cryptosystem is discussed and it is shown that the cryptosystem is highly secure. Moreover, proposed scheme also generalizes the main scheme given in [1].

General Terms

Encryption, Decryption, Cryptosystems

Keywords

Lower Triangular Matrices, General Linear Group, Public Key Cryptosystems

1. INTRODUCTION

The concept of public key cryptography has a vast history starting with the scheme introduced by Deffie and Hellman [2] in 1976. Later, many different public key cryptosystems based on hard mathematical problems were introduced by different authors. The first practical public key cryptosystem (PKC) RSA was introduced in 1978 by Rivest, Shamir and Adleman in [3]. Another practical PKC was found by ElGamal in 1985 which was introduced in [4]. Many other PKCs were introduced by many authors which can be seen in [5], [6], [7], [8], [9], and [10]. In many of these PKCs, the integers modulo n was used where n is a certain integer. As a different idea, in [1], the authors introduced a novel public-key cryptosystem based on the abelian subgroup

$$K = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} \middle| \; a, b \in \mathbb{Z}_n \text{ with } a^2 - b^2 \in \mathbb{Z}_n^* \right\}$$

of the general linear group $GL(2, \mathbb{Z}_n)$ where $\mathbb{Z}_n^*$ denotes the set of the elements in $\mathbb{Z}_n$ with a multiplicative inverse. In this cryptosystem, the authors choose two random elements from K, and define the encryption and decryption by using these two matrices. This is one of the interesting cryptosystems which is based on a subgroup of matrices. The authors showed that the system is secure and, the executions of encryption and decryption are fast since they did not use any exponentiation of matrices.
The following is the original scheme given in [1] by which this paper was motivated.

2. ORIGINAL CRYPTOSYSTEM BY KHAN AND SHAH

Key Generation

(1) Select random prime numbers r and s such that $r \neq s$ and compute $n = rs$ or $n = r^l$ for $l \geq 2$.
(2) Select four random integers a, b, c and $d \in \mathbb{Z}_n$ such that $a^2 - b^2, c^2 - d^2 \in \mathbb{Z}_n^*$.
(3) Form two matrices in the subgroup K from four integers selected in step 2:
$A = \begin{bmatrix} a & b \\ b & a \end{bmatrix}$, $B = \begin{bmatrix} c & d \\ d & c \end{bmatrix}$ (Note that $A, B \in K \leq GL(2, \mathbb{Z}_n)$ by the choice of a, b, c, d.)
(4) Define two commutative inner product automorphisms of the ring of 2×2 matrices $M_2(\mathbb{Z}_n)$:
$\chi : V \longrightarrow A^{-1}VA$ and $\delta : V \longrightarrow B^{-1}VB$ for every $V \in M_2(\mathbb{Z}_n)$.
Note that since the matrices A and B commute, the automorphisms χ and δ commute.
(5) Compute the following automorphisms of $M_2(\mathbb{Z}_n)$:
$\rho = \chi^2\delta$ and $\sigma = \chi\delta^2$ which are given by
$\rho : V \longrightarrow (A^2B)^{-1}V(A^2B)$, $\sigma : V \longrightarrow (AB^2)^{-1}V(AB^2)$.
Note that the automorphisms ρ and σ commute, and we have $\rho = \chi\delta^{-1}\sigma$, $\sigma = \chi^{-1}\delta\rho$.
(6) Select a random invertible matrix $N \in GL(2, \mathbb{Z}_n)$, such that N does not belong to group K.
(7) Compute the matrices N^{-1}, $\rho(N)$ and $\sigma(N^{-1})$.
(8) The public key is $(n, \rho(N), \sigma(N^{-1}))$ and the private key is (A, B).

Encryption

(1) Represent the plaintext m as a 2×2 matrix over residue ring $\mathbb{Z}_n$: $m \in M_2(\mathbb{Z}_n)$.

(2) Choose a random matrix $X_m \in K$. (Note that for every plaintext, we choose a new random matrix.)
(3) Define the automorphism $\upsilon : V \longrightarrow X_m^{-1} V X_m$, where $V \in M_2(\mathbb{Z}_n)$.
(4) Compute the matrices $\upsilon(\rho(N))$, $\upsilon(\sigma(N^{-1}))$ and $m\upsilon(\rho(N))$.
(5) Choose a random unit $\mu \in \mathbb{Z}_n^*$ and send the ciphertext: $C = (C_1, C_2) = (\mu^{-1}\upsilon(\sigma(N^{-1})), \mu m\upsilon(\rho(N)))$.

Decryption

(1) Compute $d = \chi\delta^{-1}(C_1) = \chi\delta^{-1}(\mu^{-1}\upsilon(\sigma(N^{-1}))) = \mu^{-1}\upsilon(\rho(N^{-1}))$.
(2) Compute $C_2 d = (\mu m\upsilon(\rho(N)))(\mu^{-1}\upsilon(\rho(N^{-1}))) = m$.

In the following section, the main scheme, which forms the center of this paper, is proposed.

3. PROPOSED SCHEME

In the proposed PKC, the previous cryptosystem is generalized by using a subgroup of $GL(k, \mathbb{Z}_n)$ where k and n are any two positive integers. Note that in the previous scheme, the size of a matrix is 2×2 and n is a product of two primes or a power of only one prime. The proposed change will make a big improvement on the original scheme in terms of security. As a start, consider the abelian subgroup

$$H = \left\{ \begin{bmatrix} a_1 & 0 & 0 & 0 & \dots & 0 \\ a_2 & a_1 & 0 & 0 & \dots & 0 \\ a_3 & a_2 & a_1 & 0 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & 0 \\ a_{k-1} & \dots & a_3 & a_2 & a_1 & 0 \\ a_k & a_{k-1} & \dots & a_3 & a_2 & a_1 \end{bmatrix} \middle| \; a_i \in \mathbb{Z}_n,\ a_1^k \in \mathbb{Z}_n^*,\ 1 \leq i \leq k \right\}$$

of the general linear group $\mathrm{GL}(k, \mathbb{Z}_n)$. It is clear that H is a subset of lower triangular matrices as well. Thus, this cryptosystem can be formed similarly by using upper triangular matrices. It can be easily proved that H is abelian. Two random matrices will be chosen from H to define encryption. From the definition of the subgroup, such a matrix is in $\mathrm{GL}(k, \mathbb{Z}_n)$ if and only if $\gcd(a_1, n) = 1$. The following is the main scheme of the PKC proposed in this article.

Key Generation

(1) Choose two matrices A and B in the subgroup H with $A \neq B$. (Note here that the verification of A and B being in H is much more easier than the original scheme.)
(2) Define two commutative inner product automorphisms of the ring of $k \times k$ matrices $M_k(\mathbb{Z}_n)$:
$\chi : V \longrightarrow A^{-1}VA$ and $\delta : V \longrightarrow B^{-1}VB$ for every $V \in M_k(\mathbb{Z}_n)$.
Clearly χ and δ commute as A and B commute.
(3) Compute the following automorphisms of $M_k(\mathbb{Z}_n)$:
$\rho = \chi^2\delta$ and $\sigma = \chi\delta^2$ which are given by
$\rho : V \longrightarrow (A^2B)^{-1}V(A^2B)$, $\sigma : V \longrightarrow (AB^2)^{-1}V(AB^2)$.
Note that similar to the original scheme, ρ and σ commute, and $\rho = \chi\delta^{-1}\sigma$, $\sigma = \chi^{-1}\delta\rho$.
(4) Select a random invertible matrix $N \in GL(k, \mathbb{Z}_n)$ which does not belong to group H.
(5) Compute the matrices N^{-1}, $\rho(N)$ and $\sigma(N^{-1})$.
(6) The public key is $(n, \rho(N), \sigma(N^{-1}))$ and the private key is (A, B).

Encryption

(1) Represent the plaintext m as a $k \times k$ matrix over the ring $\mathbb{Z}_n$, that is, $m \in M_k(\mathbb{Z}_n)$.
(2) Choose a random matrix $X_m \in H$. (Similarly, we choose a new random matrix for every plaintext.)
(3) Define the automorphism $\upsilon : V \longrightarrow X_m^{-1} V X_m$, where $V \in M_k(\mathbb{Z}_n)$.
(4) Compute the matrices $\upsilon(\rho(N))$, $\upsilon(\sigma(N^{-1}))$ and $\upsilon(\rho(N))$.
(5) Send the ciphertext: $C = (C_1, C_2) = (\upsilon(\sigma(N^{-1})), m\upsilon(\rho(N)))$.

Decryption

(1) Compute $d = \chi\delta^{-1}(C_1) = \chi\delta^{-1}(\upsilon(\sigma(N^{-1}))) = \upsilon(\rho(N^{-1}))$.
(2) Compute $C_2 d = (m\upsilon(\rho(N)))(\upsilon(\rho(N^{-1}))) = m$.

Alternatively, someone can directly compute $m = C_2\chi\delta^{-1}(C_1)$.

THEOREM 1. *The algorithm given in Section 3 works.*

PROOF. Since the same automorphisms in [1] are used, the same proof in [1, Theorem 1] is valid for this theorem. It can also be clearly seen from part 2 of decryption algorithm.

□

Note that the unit μ is not included in the proposed scheme which was used in the original scheme. As it will be seen in Security Analysis section, using the unit μ in any of the schemes does not increase the security level.

4. AN EXAMPLE

The following is an example in the 3×3 case, that is, when $k = 3$.
Key Generation

(1) Let $k = 3, n = 26$. Choose $a_1 = 5, a_2 = 6, a_3 = 7, b_1 = 3, b_2 = 1$ and $b_3 = 6 \in \mathbb{Z}_{26}$ so that
$A = \begin{pmatrix} 5 & 0 & 0 \\ 6 & 5 & 0 \\ 7 & 6 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 0 & 0 \\ 1 & 3 & 0 \\ 6 & 1 & 3 \end{pmatrix}$.
Note that $\det A \equiv 125 \equiv 21 \pmod{26}$ and $\det B \equiv 27 \equiv 1 \pmod{26}$, hence $A, B \in H$.
(2) Define the following automorphisms of the ring $M_3(\mathbb{Z}_{26})$:
$\chi : V \longrightarrow A^{-1}VA$
$\delta : V \longrightarrow B^{-1}VB$ for every $V \in M_3(\mathbb{Z}_{26})$.
(3) Compute the following automorphisms:
$\rho = \chi^2\delta$, $\sigma = \chi\delta^2$ which are given by
$\rho : V \longrightarrow (A^2B)^{-1}V(A^2B)$
$\sigma : V \longrightarrow (AB^2)^{-1}V(AB^2)$.
(4) Choose a random invertible $N = \begin{pmatrix} 3 & 5 & 7 \\ 2 & 11 & 17 \\ 1 & 13 & 4 \end{pmatrix}$ which clearly does not belong to H.
(5) Compute the matrices $N^{-1} = \begin{pmatrix} 15 & 5 & 24 \\ 1 & 15 & 19 \\ 19 & 2 & 17 \end{pmatrix}$, $\rho(N) = \begin{pmatrix} 23 & 25 & 7 \\ 6 & 3 & 23 \\ 23 & 5 & 18 \end{pmatrix}$, $\sigma(N^{-1}) = \begin{pmatrix} 8 & 3 & 24 \\ 18 & 5 & 21 \\ 5 & 22 & 8 \end{pmatrix}$.
(6) Public key is $(n = 26, \rho(N), \sigma(N^{-1}))$ and the private key is (A, B).

Encryption

(1) Represent the plaintext $m = \begin{pmatrix} 11 & 3 & 7 \\ 9 & 3 & 6 \\ 6 & 5 & 19 \end{pmatrix}$.

(2) Choose a random matrix $X_m = \begin{pmatrix} 15 & 0 & 0 \\ 1 & 15 & 0 \\ 0 & 1 & 15 \end{pmatrix} \in H$. Note that for a different message, a different random matrix X_m can be used.

(3) Define the automorphism $\upsilon : V \longrightarrow X_m^{-1} V X_m$, where $V \in M_3(\mathbb{Z}_{26})$.

(4) Compute the matrices $\upsilon(\rho(N)) = \begin{pmatrix} 9 & 2 & 7 \\ 5 & 12 & 20 \\ 22 & 21 & 23 \end{pmatrix}$,

$\upsilon(\sigma(N^{-1})) = \begin{pmatrix} 19 & 17 & 24 \\ 1 & 3 & 7 \\ 21 & 12 & 25 \end{pmatrix}$.

(5) The ciphertext is $C = (C_1, C_2)$ where

$C_1 = \upsilon(\sigma(N^{-1})) = \begin{pmatrix} 19 & 17 & 24 \\ 1 & 3 & 7 \\ 21 & 12 & 25 \end{pmatrix}$,

$C_2 = m\upsilon(\rho(N)) = \begin{pmatrix} 8 & 23 & 12 \\ 20 & 24 & 1 \\ 3 & 3 & 6 \end{pmatrix}$.

Decryption

(1) Compute

$m = C_2 \chi \delta^{-1}(C_1) = \begin{pmatrix} 11 & 3 & 7 \\ 9 & 3 & 6 \\ 6 & 5 & 19 \end{pmatrix}$.

5. SECURITY ANALYSIS

5.1 A Chiphertext Only Attack

Assume that (C_1, C_2) is the ciphertext of the plaintext m. So, the attacker needs to solve the system
$C_1 = X_m^{-1}\sigma(N^{-1})X_m$
$C_2 = mX_m^{-1}\rho(N)X_m$.
In the original scheme given in [1], the authors used a unit μ to increase the security. However, attacker can compute $C_2C_1 = mX_m^{-1}\rho(N)\sigma(N^{-1})X_m$, and more conveniently, try to solve this system for X_m and m instead of solving two systems separately for X_m, μ and m as stated in [1]. Hence, in the proposed system, the unit μ is not used which has no effect on the security, but increases the computation time.
Note that there are $\phi(n)$ possibilities for the diagonal entry of X_m, and n^{k-1} possibilities for the remaining lower diagonal entries of X_m. Hence, there are $\phi(n)n^{k-1}$ possible tries for the solution of the system. Thus, if n and k are chosen large enough, then it is infeasible to compute X_m, and hence m.
Here, if it is compared with the scheme given in [1], the security in the proposed scheme increases significantly as any size of matrices can be chosen which will increase the dimension of the system.

5.2 A Known-Plaintext Attack

Note that for each plaintext m, a specific matrix X_m is used in the scheme. Hence, it does not matter how many pairs of plaintexts and ciphertexts someone knows, it is infeasible to obtain a plaintext from a corresponding ciphertext. Thus, this attack will not be efficient as well.

5.3 A Chosen Chiphertext Attack

By using this attack, someone can obtain an unknown plaintext. Assume that $C = (C_1, C_2)$ is the corresponding ciphertext of the desired plaintext m. The attacker can choose a random invertible matrix $\widetilde{m}$ and be given access to the plaintext of the ciphertext $(C_1, \widetilde{m}C_2)$ which is $\widetilde{m}m$. Then the attacker obtains $(\widetilde{m})^{-1}\widetilde{m}m = m$.
However, an elementary modification on the proposed system can be used in order to prevent this type of attack. It is the same idea given in [1]. This problem can be solved by the change $C_2 = X_m^{-1}\rho(N)X_m m X_m^{-1}\rho(N)X_m$. In decryption, the plaintext can be obtained by $m = dC_2d$ with $d = \chi\delta^{-1}(C_1)$. This change will prevent the proposed system from this type of attack since the matrices m and X_m do not commute in general.
Note that this type of attack could even brake famous systems such as RSA and ElGamal. In this case, an elementary modification can fix this problem which shows the significance of the proposed elementary change.

6. CONCLUSION

In this article, the public key cryptosystem given in [1] is generalized by using a bigger matrix group. It can clearly be seen that the generalized scheme is more secure than the original one with respect to various attacks as a result of the increase in the size of the matrices. Although the computation time will decrease, someone can choose the best size for the security and computation time depending on the needs. Also, since exponentiation is not used, the encryption and decryption will be more simple and faster. This system can be efficiently used in key exchange protocols for symmetric schemes. In this case, someone can choose large size matrices to keep the exchange secure. This can not be done for the scheme given in [1]. Moreover, a simple numerical example is given in Section 4.

7. REFERENCES

[1] M. Khan and T. Shah. A novel cryptosystem based on general linear group. *3D Res*, 6:2, 2015.

[2] W. Deffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[3] R. L. Rivest, A. Shamir, and L. A. Adleman. Method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM.*, 21(2):120–126, 1978.

[4] T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions on Information Theory*, 31:469–472, 1985.

[5] P. Pailler. Public-key cryptosystems based on composite degree residuosity classes. *Advances in Cryptology, EUROCRYPT*, pages 223–238, 1999.

[6] M. O. Rabin. Digitized signatures and public-key functions as intractible as factorization. *MIT Laboratory for Computer Science Technical Report*, LCS/TR-212, 1979.

[7] Z. Cao. A threshold key escrow scheme based on public key cryptosystem. *Science in China (E Series)*, 44(4):441–448, 2001.

[8] K. Komaya, U. Maurer, T. Okamoto, and S. Vanston. New public-key schemes bases on elliptic curves over the ring zn. in j. feigenbaum (ed.). *Crypto91*, LNCS 576:252–266, 1992.

[9] P. Smith and Lennon M. Luc: A newpublic key system. *Proceedings of the IFIP TC11 Ninth International Conference on Information Security*, IFIP/Sec 93:103–117, 1993.

[10] M. Thangavel, P. Varalakshmi, M. Murrali, and K. Nithya. An Enhanced and Secured RSA Key Generation Scheme (ES-RKGS). *J. Information Security and App.*, 20:3–10, 2015.