

Implementation results on the integer Fibonacci matrix size 2×2 for key exchanging scheme

Abdalgabar K. Yahea [†]

Department of Mathematics

College of Computer Science and Mathematics

Tikrit University

Tikrit

Iraq

Ruma Kareem K. Ajeena ^{*}

Department of Computer Science

College of Education for Pure Science (Ibn Al-Haitham)

University of Baghdad

Baghdad

Iraq

and

Scientists Foundation for Development

NGO Directorate

General Secretariat of the Council of Ministers

Baghdad

Iraq

Abstract

In several encryption algorithms, the key exchange scheme (KES) type: Diffie-Hellman is used as a fundamental tool. In this paper, a new KES model has been proposed as an alternative contribution for using the matrix of Fibonacci numbers ($IFM_{2 \times 2}$). On the proposed model, the private keys are created as the $IFMs_{2 \times 2}$ through selecting the Fibonacci numbers (FNs) randomly over F_p , where p is a prime. The power $IFMs_{2 \times 2}$ from left (right) side is calculated ($LPIFM_{2 \times 2}$ ($RPIFM_{2 \times 2}$)). These matrices are also used to compute public keys. A new algorithm of the proposed scheme, namely $IFM_{2 \times 2}$ -KES, is presented in this work. New results are displayed for small parameter values, implemented in Python. The difficult computations

[†] E-mail: abdalgabark@gmail.com

^{*} E-mail: ruma.k.kh@ihcoedu.uobaghdad.edu.iq; (Corresponding Author)
scientists.ffd2019@gmail.com

of $\text{LPIFM}_{2 \times 2}$ and $\text{RPIFM}_{2 \times 2}$ simultaneously determine the security of the proposed algorithm. The proposed $\text{IFM}_{2 \times 2}$ -KES is considered a bright point for the communication scheme.

Subject Classification: Primary 94A60, Secondary 15A99.

Keywords: Cryptography, KES, Linear algebra, $\text{IFM}_{2 \times 2}$, $\text{RPIFM}_{2 \times 2}$, Fibonacci numbers, Security.

1. Introduction

In general, mathematics, with its multidisciplinary nature, has been used to solve many problems, for instance, in graph theory [1], in solving life problems in applied algebra [2], [3], and in computer science [4], [5], [6], [7], [8]. On the other hand, mathematical cryptography [9], especially ECC [10], has been widely used in several areas, depending on several mathematical problems to increase security.

Matrix algebra is also used to improve the key exchange scheme and to design several encryption algorithms. In 2012, the authors [11] used non-commutative rings to construct matrices to improve the Diffie-Hellman key exchange scheme. In 2013, authors [12] proposed an encrypted scheme based on DHKE using small matrices defined on a group ring.

In 2019, the authors [13] proposed a public-key cryptosystem using a subgroup of $\text{GL}(k, \mathbb{Z}_n)$, where $n, k \in \mathbb{Z}^+$. They also discussed the security issues of their proposed cryptosystem. The security is determined by solving nonlinear systems of integers, which is considered an NP-hard problem.

In 2023, the authors [14] presented an efficient version of the DHKE scheme using block matrices over elliptic curves to increase security. Also in the same year, author [15] proposed a new definition of integer matrix size 2×2 ($\text{IM}_{2 \times 2}$) to represent a scalar in a core operation of the ECCs through the integer sub-decomposition concept. Furthermore, Ajeena [15] presented an alternative DHKE version, called $\text{IM}_{2 \times 2}$ -DHKE. Left (right) power integer matrices size 2×2 have been generated, which are used to create a shared secret key (SSK) between two users in more secure way.

In this work, the $\text{IFM}_{2 \times 2}$ is used to develop a new KES model. A new $\text{IFM}_{2 \times 2}$ -KES algorithm has been presented. New results are discussed for small parameter values, implemented in Python. On the proposed algorithm, the security level has been determined.

The organization of this work is: The important concepts from mathematics are displayed in Section 2. Section 3 discusses the proposed

IFM $_{2 \times 2}$ -KES algorithm. New implemented results are discussed in Section 4. The security issues are determined in Section 5. The explanation of the conclusions is done in the final section.

2. Preliminaries

The integer matrix (IM $_{2 \times 2}$) has been used in many cryptographic applications [15]. In a more specific way, the integer matrix of Fibonacci numbers with size 2×2 (IFM $_{2 \times 2}$) is also defined by

$$\zeta_{IFM_{2 \times 2}} = \begin{bmatrix} \varepsilon_1 & \varepsilon_2 \\ \varepsilon_3 & \varepsilon_4 \end{bmatrix} (\text{mod } p) \quad (1)$$

where ζ is an element in a prime field F_p and

$$\text{Tr}_1(\zeta_{IFM_{2 \times 2}}) + \text{Tr}_2(\zeta_{IFM_{2 \times 2}}) = (\varepsilon_1 + \varepsilon_4) + (\varepsilon_2 + \varepsilon_3) = \zeta, \text{ where } \varepsilon_i, \text{ for } i=1, \dots, 4$$

are Fibonacci numbers have been selected randomly.

A power integer matrix size of FNs with size 2×2 from a right-side (RPIFM $_{2 \times 2}$) on F_p is expressed by a matrix $\zeta_{IFM_{2 \times 2}}$ defined in Equation (1) to the power by Fibonacci matrix of integer $r_{IFM_{2 \times 2}}$ which is also defined by

$$\begin{aligned} \zeta_{IFM_{2 \times 2}}^{r_{IFM_{2 \times 2}}} (\text{mod } p) &\equiv \begin{bmatrix} \varepsilon_1 & \varepsilon_2 \\ \varepsilon_3 & \varepsilon_4 \end{bmatrix} \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} (\text{mod } p) \equiv, \\ \begin{bmatrix} \varepsilon_1^{r_1} \varepsilon_3^{r_2} & \varepsilon_2^{r_1} \varepsilon_4^{r_2} \\ \varepsilon_1^{r_3} \varepsilon_3^{r_4} & \varepsilon_2^{r_3} \varepsilon_4^{r_4} \end{bmatrix} (\text{mod } p) &\equiv \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} (\text{mod } p) \equiv A_{IM_{2 \times 2}} (\text{mod } p). \end{aligned} \quad (2)$$

3. The IFM $_{2 \times 2}$ -KES Algorithm

The proposed IFM $_{2 \times 2}$ -KES to create the SSK is presented in the following algorithm.

Algorithm 1. The algorithm of IFM $_{2 \times 2}$ -KES.

Input. The elements p and g in F_p .

Output. Return SSK.

1. The integers a, b $[2, p-1]$ are selected secretly as private keys of two users.
2. For ζ, a , and b , the IFM $_{2 \times 2}$ are generated randomly.

3. The public keys $A_{IFM_{2 \times 2}}$ and $B_{IFM_{2 \times 2}}$ have been computed for both users.
4. The integers A and B are recovered from $A_{IFM_{2 \times 2}}$ and $B_{IFM_{2 \times 2}}$ and exchanged between two users.
5. The integer B reaches to first user and she/he computes the new $B_{IFM_{2 \times 2}}$. While the integer A reaches to second user, so he/she calculates new $A_{IFM_{2 \times 2}}$.
6. The matrices $A'_{IFM_{2 \times 2}}$ and $B'_{IFM_{2 \times 2}}$ are computed by two users respectively.
7. $A'_{IFM_{2 \times 2}} \equiv B'_{IFM_{2 \times 2}} \pmod{p} = \text{SSK}$.

4. Implemented Results on the IFM_{2×2}-KES Algorithm

Various numerical results are implemented in Python for various values of p . In Table 1, the private, public keys, and SSK are computed in this section.

Table 1
Shows the implemented results of IFM_{2×2}-KES algorithm.

p	g	$IFM_{g2 \times 2}$	L	$IFM_{L2 \times 2}$	R	$IFM_{R2 \times 2}$	A	$IFM_{A2 \times 2}$	B	$IFM_{B2 \times 2}$	SSK
59	34	$\begin{bmatrix} 2 & 3 \\ 8 & 21 \end{bmatrix}$	29	$\begin{bmatrix} 3 & 5 \\ 8 & 13 \end{bmatrix}$	43	$\begin{bmatrix} 3 & 5 \\ 34 & 1 \end{bmatrix}$	3	$\begin{bmatrix} 2 & 1 \\ 0 & 0 \end{bmatrix}$	25	$\begin{bmatrix} 20 & 4 \\ 1 & 0 \end{bmatrix}$	40
71	44	$\begin{bmatrix} 8 & 13 \\ 21 & 2 \end{bmatrix}$	16	$\begin{bmatrix} 1 & 2 \\ 5 & 8 \end{bmatrix}$	17	$\begin{bmatrix} 1 & 3 \\ 5 & 8 \end{bmatrix}$	4	$\begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix}$	24	$\begin{bmatrix} 18 & 2 \\ 3 & 1 \end{bmatrix}$	10
73	47	$\begin{bmatrix} 5 & 8 \\ 13 & 21 \end{bmatrix}$	18	$\begin{bmatrix} 2 & 3 \\ 5 & 8 \end{bmatrix}$	29	$\begin{bmatrix} 3 & 5 \\ 8 & 13 \end{bmatrix}$	37	$\begin{bmatrix} 29 & 17 \\ 63 & 1 \end{bmatrix}$	24	$\begin{bmatrix} 13 & 1 \\ 5 & 5 \end{bmatrix}$	39
97	71	$\begin{bmatrix} 34 & 21 \\ 13 & 3 \end{bmatrix}$	60	$\begin{bmatrix} 13 & 34 \\ 5 & 8 \end{bmatrix}$	18	$\begin{bmatrix} 8 & 5 \\ 3 & 2 \end{bmatrix}$	95	$\begin{bmatrix} 25 & 30 \\ 21 & 19 \end{bmatrix}$	89	$\begin{bmatrix} 72 & 7 \\ 10 & 2 \end{bmatrix}$	38
97	71	$\begin{bmatrix} 34 & 21 \\ 13 & 3 \end{bmatrix}$	60	$\begin{bmatrix} 13 & 34 \\ 5 & 8 \end{bmatrix}$	10	$\begin{bmatrix} 5 & 2 \\ 2 & 1 \end{bmatrix}$	95	$\begin{bmatrix} 25 & 30 \\ 21 & 19 \end{bmatrix}$	30	$\begin{bmatrix} 26 & 3 \\ 1 & 0 \end{bmatrix}$	79

5. Security Issue and Conclusion

In the proposed IFM_{2×2}-KES algorithm, creating the matrices IFM_{2×2}, LPIFM_{2×2}, and RPIFM_{2×2} randomly over a prime field F_p with a huge prime p is considered a strong point to compute the SSK. The probability to determine the correct private keys is

$$P_{\text{Secretkeys}} = P(a) + P(b) = 8/p.$$

Thus, generating IFMs_{2×2} to compute the SSK in the proposed algorithm provides a higher level of security for encryption schemes. With IFM sizes of 3×3 or 4×4 , the security level for computing the SSK has been increased.

References

- [1] M. H. Hashem and R. K. K. Ajeena, "The tensor product bipartite graph for symmetric encryption scheme," *AIP Conference Proceedings*, vol. 2591, no. 1, Art. no. 050003 (2023).
- [2] G. E. Arif, F. A. Abdullah, and Y. Al-Douri, "Modeling of the electronic properties of hexagonal semiconductors," *Advanced Materials Research*, vol. 925, pp. 364–368 (2014).
- [3] S. A. Khalaf and N. S. Jasim, "Calculation for the groups," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 25, no. 2, pp. 609–613 (2022).
- [4] B. J. Al-khafaji, M. Salih, S. Shnain, and Z. Nabat, "Improved technique for hiding data in a colored and a monochrome image," *Periodicals of Engineering and Natural Sciences*, vol. 8, no. 2, pp. 1000–1010 (2020).
- [5] W. N. Abdullah and S. A. Alagha, "A parallel adaptive genetic algorithm for job shop scheduling problem," *J. Phys. Conf. Ser.*, vol. 1879, no. 2, Art. no. 022078 (2021).
- [6] S. S. Hussei, S. S. Altyar, L. A. Tawfeeq, and E. S. Harba, "Reconstruction of three-dimensional object from two-dimensional images by utilizing distance regularized level set algorithm and mesh object generation," *Baghdad Science Journal*, vol. 17, no. 3 (2020).
- [7] G. I. Arb and K. Al-Majdi, "A freights status management system based on Dart and Flutter programming language," *J. Phys. Conf. Ser.*, vol. 1530, no. 1, Art. no. 012020 (2020).
- [8] W. H. Abdulsalam, S. Mashhadani, S. S. Hussein, and A. A. Hashim, "Artificial intelligence techniques to identify individuals through palm image recognition," *Int. J. Math. Comput. Sci.*, vol. 20, no. 1, pp. 165–171 (2020).
- [9] S. M. Suhael, Z. A. Ahmed, and A. J. Hussain, "Proposed hybrid cryptosystems based on modifications of Playfair cipher and RSA cryptosystem," *Baghdad Science Journal*, vol. 21, no. 1, pp. 151–160 (2024).

- [10] R. K. K. Ajeena and H. Kamarulhaili, "On the distribution of scalar k for elliptic scalar multiplication," *AIP Conference Proceedings*, vol. 1682, no. 1, Art. no. 020052 (2015).
- [11] M. Eftekhari, "A Diffie–Hellman key exchange protocol using matrices over noncommutative rings," *Groups Complex. Cryptol.*, vol. 4, no. 1, pp. 167–176 (2012).
- [12] D. Kahrobaei, C. Koupparis, and V. Shpilrain, "Public key exchange using matrices over group rings," *Groups Complexity Cryptology*, vol. 5, no. 1, pp. 97–115 (2013).
- [13] Z. Y. Karatas, E. Luy, and B. Gonen, "A public key cryptosystem based on matrices," *Int. J. Comput. Appl.*, vol. 182, pp. 47–50 (2018).
- [14] H. H. Hadi and A. A. Neamah, "Diffie–Hellman key exchange based on block matrices combined with elliptic curves," *Int. J. Intell. Syst. Appl. Eng.*, vol. 11, no. 5s, pp. 353–360 (2023).
- [15] R. K. K. Ajeena, "Integer matrix size 2×2 sub-decomposition method for elliptic curve cryptography," *Computer Science*, vol. 18, no. 4, pp. 599–606 (2023).

Received May, 2025