International Journal of Mathematics and Computer Science
Volume **20,** Issue no. 1, (2025), 313–316
DOI: https://doi.org/10.69793/ijmcs/01.2025/ruma

Integer Fibonacci Matrix of Size 2×2 for Key Exchanging Scheme

Abdalgabar K. Yahea[1], **Ruma Kareem K. Ajeena**[2]

[1]Department of Mathematics
College of Computer Science and Mathematics
Tikrit University
Tikrit, Iraq

[2]Department of Computer Science
College of Education for Pure Science (Ibn Al- Haitham)
University of Baghdad &
Scientists Foundation for Development
Baghdad, Iraq

email: abdalgabarkh@gmail.com, ruma.k.kh@ihcoedu.uobaghdad.edu.iq

(Received August 22, 2024, Accepted October 23, 2024
Published October 28, 2024)

Abstract

Key exchanging scheme of Diffie-Hellman type (KES-DH) is a fundamental tool which can be employed for encryption algorithms. In this paper, we propose an alternative model of KES-DH as another contribution using the integer Fibonacci matrix of size 2×2 ($\text{IFM}_{2\times 2}$) which is inspired by Ajeena in [8]. In the proposed KES-DH, namely $\text{IFM}_{2\times 2}$-KES-DH, the private keys are converted into $\text{IFMs}_{2\times 2}$ through the random selections of the Fibonacci numbers over a prime field F_p. The left (right) side power $\text{IFMs}_{2\times 2}$ is computed ($\text{LPIFM}_{2\times 2}$($\text{RPIFM}_{2\times 2}$)). The public keys are computed using these matrices. The $\text{IFM}_{2\times 2}$-KES-DH is proved mathematically based on $\text{LPIFM}_{2\times 2}$ and $\text{RPIFM}_{2\times 2}$. Users shared secret key (SSK) is calculated. The security issue is determined based on the computations

Key words and phrases: Cryptography, KES-DH, $\text{IFM}_{2\times 2}$, $\text{IFM}_{2\times 2}$-KES-DH, Security.
AMS (MOS) Subject Classifications: 94A60, 15-XX, 15Bxx, 11B39.
ISSN 1814-0432, 2025, https://future-in-tech.net

of LPIFM$_{2\times2}$ and RPIFM$_{2\times2}$ simultaneously. The proposed model is useful in cryptographic applications.

1 Introduction

For more secure communication schemes, several mathematical problems [1]-[3] can be employed to design efficient encryption algorithms [4],[5]. The KES-DH is utilized to compute a SSK which is critical in encryption schemes. Various versions on the KES-DH have been proposed previously [6], [7] among others. Recently, Ajeena [8] presented another modified version of KES-DH. In the present work, we propose a specific version of KES-DH based on IFM$_{2\times2}$.

2 Integer Fibonacci Matrices of Size 2 × 2

Definition 2.1. *The sequence of Fibonacci numbers is defined by* $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5, F_6 = 8, ..., F_n = F_{n-1} + F_{n-2}$.

Definition 2.2. *Let* F_p *be a prime field and* $g \in F_p$*. The integer Fibonacci matrix of size 2 × 2 (IFM$_{2\times2}$) is expressed as*

$$g_{IFM_{2\times2}} = \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix}$$

such that $Tr_1(g_{IFM_{2\times2}}) + Tr_1(g_{IFM_{2\times2}}) = (F_1 + F_4) + (F_2 + F_3)$*, where* F_1, F_2, F_3, F_4 *are random Fibonacci numbers.*

Definition 2.3. *A left-side power integer Fibonacci matrix size* 2×2 *(LPIFM$_{2\times2}$) over* F_p *is given as an integer Fibonacci matrix* $[F]_{IFM_{2\times2}}$ *powered by an integer Fibonacci matrix* $[a]_{IFM_{2\times2}}$*:*

$$\begin{aligned} {}^{[a]_{IFM_{2\times2}}}[F]_{IFM_{2\times2}} (mod\ p) &\equiv {}^{\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}} \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix} (mod\ p) \\ &\equiv \begin{bmatrix} {F_1}^{a_1} \cdot {F_3}^{a_2} & {F_2}^{a_1} \cdot {F_4}^{a_2} \\ {F_1}^{a_3} \cdot {F_3}^{a_4} & {F_2}^{a_3} \cdot {F_4}^{a_4} \end{bmatrix} (mod\ p) \\ &\equiv \begin{bmatrix} A_1 & A_2 \\ A_3 & A_4 \end{bmatrix} (mod\ p) \equiv [A]_{IM_{2\times2}} (mod\ p) \end{aligned}$$

with $Tr_1([A]_{2\times2}) + Tr_2([A]_{2\times2}) (mod\ p) = A \in F_p$.

Definition 2.4. *A right-side power integer Fibonacci matrix size* 2×2 *(RPIFM$_{2\times2}$) over F_p is given to be an integer Fibonacci matrix $[F]_{IFM_{2\times2}}$ powered by an integer Fibonacci matrix $[b]_{IFM_{2\times2}}$:*

$$[F]_{IFM_{2\times2}}{}^{[b]_{IFM_{2\times2}}}(mod\ p) \equiv \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix}^{\begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}} (mod\ p)$$

$$\equiv \begin{bmatrix} {F_1}^{b_1} \cdot {F_2}^{b_3} & {F_1}^{b_2} \cdot {F_2}^{b_4} \\ {F_3}^{b_1} \cdot {F_4}^{b_3} & {F_3}^{b_2} \cdot {F_4}^{b_4} \end{bmatrix} (mod\ p)$$

$$\equiv \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix} (mod\ p) \equiv [B]_{IM_{2\times2}}(mod\ p)$$

with $Tr_1([B]_{2\times2}) + Tr_2([B]_{2\times2})(mod\ p) = B \in F_p$.

3 IFM$_{2\times2}$ for KES-DH

The IFM$_{2\times2}$-KES-DH can be explained by the following steps: The IFM$_{2\times2}$-KES-DH public domain parameters are: a prime number p and $g \in F_p$.

- Two users generated the IFM$g_{2\times2}$ and secret IFM$a_{2\times2}$, IFM$b_{2\times2}$ of g, a and b, where $a, b \in F_p$ which are selected secretly as their private keys.
- The user's public keys A and B are calculated using Definitions (2.3) and (2.4) respectively and exchanged between them.
- Two users receive B and A and convert them to IFM$_{B_{2\times2}}$ and IFM$_{A_{2\times2}}$, respectively.
- The first user computes A' using Definition (2.3) with input (IFM$_{B_{2\times2}}$, IFM$a_{2\times2}$). On the other hand, the second user computes B' using Definition (2.4) with input (IFM$_{A_{2\times2}}$, IFM$b_{2\times2}$).
- The SSK is $A' \equiv B'(mod\ p)$.

4 Security Issues and Conclusions

Using a huge prime number p, generating the matrices IFM$_{2\times2}$, LPIFM$_{2\times2}$, and RPIFM$_{2\times2}$ over F_p randomly is a strong point for computing the users secret keys. The correct values to generate the secret keys take the probability $P_{Secretkeys} = P(a) + P(b) = 8/p$. So, the proposed model to compute the

SSK using the $IFM_{2\times 2}$ is more secure for encryption algorithms, more secure $IFM_{2\times 2}$-KES-DH with $IFM_{3\times 3}$, $IFM_{4\times 4}$ and so on.

References

[1] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, Comparison Studies on Integer Decomposition Method for Elliptic Scalar Multiplication, Adv. Sci. Lett. **20,** no. 2, (2014), 526–530.

[2] R. K. K. Ajeena, H. Kamarulhaili, On the distribution of scalar k for elliptic scalar multiplication, AIP Conf. Pro. 1682, no. 1, 2015.

[3] Luma Naji Mohammed Tawfiq, Israa Najm Abood, Persons Camp Using Interpolation Method, J. Phys.: Conf. Series, 1003, no. 1, (2018), 012055.

[4] Karrar Taher R. Aljamaly, Ruma Kareem K. Ajeena, The kr-elliptic curve public key cryptosystem, J. of Phys.: Conf. Series, 1879, no. 3, (2021).

[5] Hashim Madlool Hashim, Ruma Kareem K. Ajeena, The Computational Complexity of the Elliptic Curve Factorization Algorithm over Real Field, J. Phys.: Conf. Series, 1897, no. 1, (2021), 012046.

[6] Eun-Jun Yoon, Il-Soo Jeon, An efficient and secure Diffie-Hellman key agreement protocol based on Chebyshev chaotic map, Communications in Nonlinear Science and Numerical Simulation **16,** no. 6, (2011), 2383–2389.

[7] Rachid Rimani, Naima Hadj Said, Adda Ali-Pacha, O. Özer, Key exchange based on Diffie-Hellman protocol and image registration, Indonesian Journal of Electrical Engineering and Computer Science, (2021).

[8] R. K. K. Ajeena, A proposed modification of Diffie-Hellman key exchange based on integer matrices, Int. J. Math. Comp. Sci., **19,** no. 1, (2024), 211–218.

[9] R. K. K. Ajeena, Integer matrix size 2×2 sub-decomposition method for elliptic curve cryptography, Comp. Sci., **18,** no. 4, (2023), 599–606.