International Journal of Mathematics and
Computer Science, **19**(2024), no. 1, 211–218

A proposed modification of Diffie-Hellman key exchange based on integer matrices

Ruma Kareem K. Ajeena

Department of Mathematics
Education College for Pure Sciences
University of Babylon
Babil, Iraq

email: ruma.usm2015@gmail.com

(Received April 20, 2023, Revised May 18, 2023,
Accepted July 7, 2023, Published August 31, 2023)

Abstract

Diffie-Hellman key exchange (DHKE) protocol was published in 1976 by Whitfield Diffie and Martin Hellman. Several versions to improve the DHKE were presented by many researchers. In this work, an alternative version of DHKE is proposed as a new contribution. In the proposed version, which is called $IM_{2\times2}$-DHKE, the secret keys of users are represented by integer matrices size 2×2, ($IM_{2\times2}$), through a random selection of the integers modulo p. The power integer matrices size 2×2 are generated in left ($LPIM_{2\times2}$) and right ($RPIM_{2\times2}$) sides. The public keys are computed using these matrices. The $IM_{2\times2}$-DHKE is proved mathematically based on ($LPIM_{2\times2}$) and ($RPIM_{2\times2}$). A more secure shared secret key (SSK) between two users is created through the computations of ($LPIM_{2\times2}$) and ($RPIM_{2\times2}$) simultaneously. New experimental result of $IM_{2\times2}$-DHKE is presented with small parameters as a study case. This contribution is quite useful for symmetric and asymmetric encryption applications.

Key words and phrases: Cryptography, DHKE, $IM_{2\times2}$, $IM_{2\times2}$-DHKE, Security.
AMS (MOS) Subject Classifications: 94A60, 15-XX, 15Bxx.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

1 Introduction

Various mathematical problems are used to design several communication schemes [1], [2], [3], [4], [5]. The DHKE as a protocol is used to create a SSK that is utilized to encrypt the data and decrypt it. Many researchers presented various versions of DHKE. In 2011, Yoon and Jeon [6] proposed another version of DHKE through using the Chebyshev chaotic map. In 2017, Aryan [7] proposed two stages to generate a SSK, second key computed as a primitive root of the first one. In 2020, Mäurer et al. [8] used three different DHKE versions for digital aeronautical communication in term of security. In same year, Muth, Robert, and Florian Tschorsch [9] proposed the SmartDHX and implemented the DHKE on chain that gave authenticity and integrity of a plaintext. Several studies for improving the DHKE were proposed in [10], [11], [12], [13], [14], [15].
This work is organized as follows:
In Section 2, we display the basic facts of $IM_{2\times2}$ and the definitions of right and left sides power $IM_{2\times2}$. In Section 3, we discuss the $IM_{2\times2}$-DHKE protocol. In Section 4, we present an example of $IM_{2\times2}$-DHKE protocol with small parameters as a study case. The security issue is discussed in Section 5. Finally, our conclusions appear in Section 6.

2 The power integer matrices size 2×2

The $IM_{2\times2}$ has been defined as a new concept of linear algebra by Ajeena [16]. Some properties of these matrices are discussed as well. Depending on the right and left power matrices given in [17], special definitions of $IM_{2\times2}$ can be made as follows:

Definition 2.1. *A left-side power integer matrix size* 2×2 *(*$LPIM_{2\times2}$*) over a prime field* F_p *is defined to be a matrix* $[A]_{2\times2}$ *powered by a matrix* $[L]_{2\times2}$*:*

$$^{[L]_{2\times2}}[A]_{2\times2} \equiv \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \ (mod\ p) \equiv \begin{bmatrix} {a_1}^{l_1} \cdot {a_3}^{l_2} & {a_2}^{l_1} \cdot {a_4}^{l_2} \\ {a_1}^{l_3} \cdot {a_3}^{l_4} & {a_2}^{l_3} \cdot {a_4}^{l_4} \end{bmatrix} \ (mod\ p) = [B]_{2\times2}$$

where $b_{ij} = \prod_{k=1}^{m} a_{kj}^{l_{ik}} \in [B]_{2\times2}$ *and* $[A]_{2\times2}, [B]_{2\times2}, [L]_{2\times2}$ *are* $IM_{2\times2}$*.*

Definition 2.2. *A right-side power integer matrix size* 2×2 *(*$RPIM_{2\times2}$*)*

over F_p is defined to be a matrix $[A]_{2\times 2}$ powered by a matrix $[R]_{2\times 2}$:

$$[A]_{2\times 2}^{[R]_{2\times 2}} \equiv \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}^{\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}} (mod\ p) \equiv \begin{bmatrix} {a_1}^{r_1} \cdot {a_2}^{r_3} & {a_1}^{r_2} \cdot {a_2}^{r_4} \\ {a_3}^{r_1} \cdot {a_4}^{r_3} & {a_3}^{r_2} \cdot {a_4}^{r_4} \end{bmatrix} (mod\ p) = [C]_{2\times 2}$$

where $c_{ij} = \prod_{k=1}^{m} a_{ik}^{r_{kj}} \in [C]_{2\times 2}$ and $[A]_{2\times 2}, [C]_{2\times 2}, [R]_{2\times 2}$ are $IM_{2\times 2}$.

3 The $IM_{2\times 2}$-DHKE protocol

Let F_p be a prime field and let A be a generator element in F_p. The secret keys of users are L and R in F_p, respectively. These elements are represented by integer matrices size 2×2, $IM_{2\times 2}$ defined in [16]. So, the matrices that are corresponding to A, L, R are defined respectively by

$$[A]_{2\times 2} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \ni Tr_1([A]_{2\times 2}) + Tr_2([A]_{2\times 2}) = (a_1 + a_4) + (a_2 + a_3) = A,$$

$$[L]_{2\times 2} = \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix} \ni Tr_1([L]_{2\times 2}) + Tr_2([L]_{2\times 2}) = (l1 + l_4) + (l_2 + l_3) = L,$$

and

$$[R]_{2\times 2} = \begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix} \ni Tr_1([R]_{2\times 2}) + Tr_2([R]_{2\times 2}) = (r_1 + r_4) + (r_2 + r_3) = R.$$

The matrices $L_{M_{2\times 2}}$ and $R_{M_{2\times 2}}$ are generated secretly using the random way. First and second users compute their public keys B and C respectively depending on the proposed definition which is given in Definition 2.1.

$$\begin{aligned} {}^{[L]_{2\times 2}}[A]_{2\times 2}\ (mod\ p) &\equiv \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}\ (mod\ p) \\ &\equiv \begin{bmatrix} {a_1}^{l_1} \cdot {a_3}^{l_2} & {a_2}^{l_1} \cdot {a_4}^{l_2} \\ {a_1}^{l_3} \cdot {a_3}^{l_4} & {a_2}^{l_3} \cdot {a_4}^{l_4} \end{bmatrix}\ (mod\ p) \\ &\equiv \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}\ (mod\ p) \\ &\equiv [B]_{2\times 2}\ (mod\ p) \\ &\equiv Tr_1([B]_{2\times 2}) + Tr_2([B]_{2\times 2})\ (mod\ p) \\ &\equiv (B_1 + B_4) + (B_2 + B_3)\ (mod\ p) \equiv B\ (mod\ p). \end{aligned}$$

while computing C is done by

$$\begin{aligned}
[A]_{2\times 2}{}^{[R]_{2\times 2}} \ (mod\ p) &\equiv \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}^{\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}} \ (mod\ p) \\
&\equiv \begin{bmatrix} {a_1}^{r_1} \cdot {a_2}^{r_3} & {a_1}^{r_2} \cdot {a_2}^{r_4} \\ {a_3}^{r_1} \cdot {a_4}^{r_3} & {a_3}^{r_2} \cdot {a_4}^{r_4} \end{bmatrix} \ (mod\ p) \\
&\equiv \begin{bmatrix} C_1 & C_2 \\ C_3 & C_4 \end{bmatrix} \ (mod\ p) \\
&\equiv [C]_{2\times 2} \ (mod\ p) \\
&\equiv Tr_1([C]_{2\times 2}) + Tr_2([C]_{2\times 2}) \ (mod\ p) \\
&\equiv (C_1 + C_4) + (C_2 + C_3) \ (mod\ p) \equiv C \ (mod\ p).
\end{aligned}$$

The values of B and C are exchanged between two users. The first user sends B to the second user, thus he/she computes

$$\begin{aligned}
[B]_{2\times 2}{}^{[r]_{2\times 2}} \ (mod\ p) &\equiv \begin{bmatrix} B_1 & B_2 \\ B_3 & B_4 \end{bmatrix}^{\begin{bmatrix} r_1 & r_2 \\ r_3 & r_4 \end{bmatrix}} \ (mod\ p) \\
&\equiv \begin{bmatrix} {B_1}^{r_1} \cdot {B_2}^{r_3} & {B_1}^{r_2} \cdot {B_2}^{r_4} \\ {B_3}^{r_1} \cdot {B_4}^{r_3} & {B_3}^{r_2} \cdot {B_4}^{r_4} \end{bmatrix} \ (mod\ p) \\
&\equiv \begin{bmatrix} B'_1 & B'_2 \\ B'_3 & B'_4 \end{bmatrix} \ (mod\ p) \\
&\equiv [B']_{2\times 2} \ (mod\ p) \\
&\equiv Tr_1([B']_{2\times 2}) + Tr_2([B']_{2\times 2}) \ (mod\ p) \\
&\equiv (B'_1 + B'_4) + (B'_2 + B'_3) \ (mod\ p) \equiv B' \ (mod\ p).
\end{aligned}$$

The second user sends C to the first user, thus he/she computes

$$\begin{aligned}
{}^{[L]_{2\times 2}}[C]_{2\times 2} \ (mod\ p) &\equiv \begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix} \begin{bmatrix} C_1 & C_2 \\ C_3 & C_4 \end{bmatrix} \ (mod\ p) \\
&\equiv \begin{bmatrix} {C_1}^{l_1} \cdot {C_3}^{l_2} & {C_2}^{l_1} \cdot {C_4}^{l_2} \\ {C_1}^{l_3} \cdot {C_3}^{l_4} & {C_2}^{l_3} \cdot {C_4}^{l_4} \end{bmatrix} \ (mod\ p) \\
&\equiv \begin{bmatrix} C'_1 & C'_2 \\ C_3 & C'_4 \end{bmatrix} \ (mod\ p) \\
&\equiv [C']_{2\times 2} \ (mod\ p) \\
&\equiv Tr_1([C']_{2\times 2}) + Tr_2([C']_{2\times 2}) \ (mod\ p) \\
&\equiv (C'_1 + C'_4) + (C'_2 + C'_3) \ (mod\ p) \equiv C' \ (mod\ p).
\end{aligned}$$

The values B' and C' are equal and represent a SSK that is computed using the proposed $IM_{2\times 2} - DHKE$ as follows:

$$\begin{aligned} C' = [C']_{2\times 2} &\equiv {}^{[l]_{2\times 2}}[C]_{2\times 2} \ (mod\ p) \\ &\equiv {}^{[l]_{2\times 2}}([A]_{2\times 2}{}^{[r]_{2\times 2}}) \ (mod\ p) \\ &\equiv ({}^{[l]_{2\times 2}}[A]_{2\times 2}{}^{[r]_{2\times 2}}) \ (mod\ p) \\ &\equiv ({}^{[l]2\times 2}[A]_{2\times 2})\,{}^{[r]_{2\times 2}} \ (mod\ p) \\ &\equiv [B]_{2\times 2}{}^{[r]_{2\times 2}} \ (mod\ p) \equiv \ [B']_{2\times 2} \ (mod\ p) \equiv B' \ (mod\ p). \end{aligned}$$

4 A study case of the $IM_{2\times 2}$-DHKE protocol

Take the prime number $p = 11$ and let $A = 7 \in F_{11}$. The secret keys of first and second users are $L = 8$ and $R = 10$, respectively. The $IMs_{2\times 2}$ are determined randomly by

$$7_{M_{2\times 2}} = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \equiv Tr_1(7_{M_{2\times 2}}) + Tr_2(7_{M_{2\times 2}}) \ (mod\ 11) = 7,$$

$$8_{M_{2\times 2}} = \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix} \equiv Tr_1(8_{M_{2\times 2}}) + Tr_2(8_{M_{2\times 2}}) \ (mod\ 11) = 8$$

and

$$10_{M_{2\times 2}} = \begin{bmatrix} 3 & 2 \\ 3 & 2 \end{bmatrix} \equiv Tr_1(10_{M_{2\times 2}}) + Tr_2(10_{M_{2\times 2}}) \ (mod\ 11) = 10.$$

The first user computes his/her public key by

$$B \equiv {}^{[L]}[A] \ (mod\, 11) \equiv \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \ (mod\, 11) \equiv \begin{bmatrix} 2^3 \cdot 1^2 & 2^3 \cdot 2^2 \\ 2^1 \cdot 1^2 & 2^1 \cdot 2^2 \end{bmatrix} \ (mod\, 11) = 6.$$

The second user calculates his/her public key by

$$C \equiv \ [A]^{[R]} \ (mod\, 11) \equiv \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 3 & 2 \end{bmatrix} \ (mod\, 11) \equiv \begin{bmatrix} 2^3 \cdot 2^3 & 2^2 \cdot 2^2 \\ 1^3 \cdot 2^3 & 1^2 \cdot 2^2 \end{bmatrix} \ (mod\, 11) = 10.$$

The users exchange the computations of B and C, the second user receives $B = 6$ to compute a SSK B'. He/She first converts 6 into integer matrix size 2×2 by

$$6_{M_{2\times 2}} = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}.$$

Therefore,

$$B' \equiv [A]^{[r]} \,(mod\, 11) \equiv \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 3 & 2 \end{bmatrix} \,(mod\, 11) \equiv \begin{bmatrix} 2^3 \cdot 1^3 & 2^2 \cdot 1^2 \\ 1^3 \cdot 2^3 & 1^2 \cdot 2^2 \end{bmatrix} \,(mod\, 11) = 2.$$

On other hand, the first user receives $C = 10$. He/She converts it to $\mathrm{IM}_{2\times 2}$ as

$$10_{M_{2\times 2}} = \begin{bmatrix} 3 & 2 \\ 3 & 2 \end{bmatrix}.$$

Therefore,

$$C' \equiv {}^{[L]}[C] \,(mod\, 11) \equiv \begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} 3 & 2 \\ 3 & 2 \end{bmatrix} \,(mod\, 11) \equiv \begin{bmatrix} 3^3 \cdot 3^2 & 2^3 \cdot 2^2 \\ 3^1 \cdot 3^2 & 2^1 \cdot 2^2 \end{bmatrix} \,(mod\, 11) = 2.$$

Therefore, $B' \equiv C' \,(mod\, 11) = 2$ which is a SSK of two users.

5 The security issue

The DHKE has been improved using the $\mathrm{IM}_{2\times 2}$, $\mathrm{LPIM}_{2\times 2}$ and $\mathrm{RPIM}_{2\times 2}$ as given in Definitions 2.1 and 2.2, respectively. The random generation of these matrices over F_p with a huge prime number p gives strong generating of the secret keys for users. The choice of each element in any matrix here needs the probability 1 from possible values p. In other words, generating the secret key L as $\mathrm{IM}_{2\times 2}$ needs the probability $P(L) = 4/p$. Similarly, for a second secret key R, the probability is $P(R) = 4/p$. So the total probability of correct values for generating the secret keys is

$$P_{Secret\ keys} = P(L) + P(R) = \frac{8}{p}.$$

Thus the determination of these secret keys by the attackers is more difficult.

6 Conclusions

In this paper, the $\mathrm{IM}_{2\times 2}$-DHKE protocol was proposed as an alternative protocol to use for computing the SSK that is a fundamental tool for encryption in the symmetric and asymmetric schemes. The $\mathrm{IM}_{2\times 2}$-DHKE protocol depends on the random represented $\mathrm{IM}_{2\times 2}$ of secret keys which also by certain

types of matrices, their elements are in F_p. The security on $\mathrm{IM}_{2\times2}$-DHKE is determined based on the difficulty to recover the secret keys $[L]_{2\times2}$ and $[R]_{2\times2}$. Many cases of these representations need to compute by Attackers to determine the correct choices of the secret keys. The modification of DHKE with $\mathrm{IMs}_{2\times2}$ increases the security since the random creation of matrices that corresponded to ISD sub-scalars are difficult to recover that cannot help the attackers to recover the original scalar k which represents the ECDLP. Therefore, the $\mathrm{IM}_{2\times2}$-DHKE protocol is a secure scheme to generate a SSK for cryptographic applications. In spite of increasing the security of DHKE with integer matrices size 2×2, with large sizes 3×3 and 4×4 and so on of matrices, more levels of the security can be accrued.

References

[1] Ruma Kareem K. Ajeena, Hailiza Kamarulhaili, Point multiplication using integer sub-decomposition for elliptic curve cryptography, Applied Mathematics and Information Sciences, **8,** no. 2, (2014), 5–17.

[2] Hashim Madlool Hashim, Ruma Kareem K. Ajeena, The Computational Complexity of the Elliptic Curve Factorization Algorithm over Real Field, Journal of Physics: Conference Series **1897,** no. 1, (2021), 012046.

[3] Muna Haider Hashem, Ruma Kareem K. Ajeena, The tensor product bipartite graph for symmetric encryption scheme, AIP Conference Proceedings, **2591,** no. 1, (2023).

[4] Ali Hussein, Ali Marwah, Ahmed A. Omran, Ruma Kareem K. Ajeena, The Cartesian product graph for encryption schemes, AIP Conference Proceedings, **2591,** no. 1, (2023).

[5] Ruma Kareem K. Ajeena, Shatha Mohammed Hashim, Firas A. Abdullatif, Mersenne Weighted Graph for Increasing the Symmetric Encryption Schemes Security, Second International Conference on Electrical, Electronics, Information and Communication Technologies, (2023), 1-4.

[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] Chaithanya Kumar, PM Durai Raj Vincent, Enhanced Diffie-Hellman algorithm for reliable key exchange, IOP Conference Series: Materials Science and Engineering **263,** no. 4, (2017), 042015.

[8] Nils Mäurer, Thomas Gräupl, Christoph Gentsch, Corinna Schmitt, Comparing different Diffie-Hellman key exchange flavors for LDACS, DASC-IEEE, (2020), 1-10.

[9] Robert Muth, Florian Tschorsch, Smartdhx: Diffie-hellman key exchange with smart contracts, DAPPS-IEEE, (2020), 164–168.

[10] 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).

[11] Adoté François-Xavier Ametepe, Arnaud SRM Ahouandjinou, Eugène C. Ezin, Robust encryption method based on AES-CBC using elliptic curves DiffieHellman to secure data in wireless sensor networks, Wireless Networks, **28,** no. 3, (2022), 991–1001.

[12] Jiaxin Pan, Chen Qian, Magnus Ringerud, Signed (Group) DiffieHellman Key Exchange with Tight Security, Journal of Cryptology, **35,** no. 4,(2022), 26.

[13] Nawal Khudhair Abbas, Ruma Kareem K. Ajeena, More secure on the DL-encryption schemes using the TFM function, AIP Conference Proceedings, **2398,** no. 1, (2022).

[14] Huda K. Aljader, Ruma Kareem K. Ajeena, The optimized Diffie-Hellman key exchange using the graphical method, Journal of Discrete Mathematical Sciences and Cryptography, (2022), (accepted).

[15] Huda K. Aljader, Ruma Kareem K. Ajeena, The optimized Diffie-Hellman Key Exchange using the Simplex Method, journal of Solid State Phenomena, 2022. (accepted).

[16] Ruma Kareem K. Ajeena, Integer matrix size 2×2 sub-decomposition method for elliptic curve cryptography, International Journal of Mathematics and Computer Science **18,** no. 4, (2023), 599–606.

[17] Eligijus Sakalauskas, Enhanced matrix power function for cryptographic primitive construction, Symmetry, **10,** no. 2, (2018), 43.