Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 1, pp. 193–198
DOI : 10.47974/JDMSC-2324

Right power integer Fibonacci matrix size 2×2 for digital signature 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 & Scientists Foundation for Development
Baghdad
Iraq

Abstract

A new version of digital signature scheme (DSS) has been proposed in this work. This version has used a new concept of linear algebra which is called the integer matrix of Fibonacci numbers with size 2×2 ($IFM_{2\times2}$). The main point is to use the $IFM_{2\times2}$ with its right power ($RPIFM_{2\times2}$) for creating the digital signature. The verification is done of this signature using the computations of the $RPIFM_{2\times2}$ as well. New implemented results on the proposed DSS-$RPIFM_{2\times2}$ have been done using Python programming. The issue of the security has been determined based on the randomization for generating the $IFM_{2\times2}$ of the elements over a field Fp of prime numbers secretly. The DSS- $PRIFM_{2\times2}$ version is proposed to be a more secure for sending the signed messages and to avoid forging the signature of them. Thus, the proposed version of DSS- $RPIFM_{2\times2}$ considers as a bright point for more authenticity, integrity and non-repudiation in compare to the previous communication schemes.

Subject Classification: *Primary 94A60, Secondary 15Bxx.*

Keywords: *Cryptography, Linear algebra, $IFM_{2\times2}$, $RPIFM_{2\times2}$, Fibonacci numbers, Security.*

† *E-mail:* **abdalgabark@gmail.com**
* *E-mail:* **ruma.k.kh@ihcoedu.uobaghdad.edu.iq (Corresponding Author)**

1. Introduction

Several problems in elliptic curve theory [1], graph theory [2, 3] and others [4, 5, 6] from mathematics are employed to build encryption schemes or DS S. The DSS is proposed in 1991 [7] by the NIST as a strategy to generate and validate the DSs. The integrity and non-repudiation of the data are provided using this strategy. Various studies for using the DSs are presented.

In 2014, Alrehily et al. [8] introduced improved versions of the DSSs that applied to the RSA, DSA and ECDSA. Recently, in 2022, Kumar and Sharma [9] studied various kinds of digital signature methods, such as ECDSA, RSA, OTS, Lightweight digital signature and others. Also, they compared the proposed methods based on the key sizes, computational and energy cost. In 2023, Lalem et al. [10] proposed a DSS based on the encryption algorithms.

The structure to this work is organized by: Section 2 presents the preliminaries about the $IFM_{2\times2}$ and the right power of it. In Section 3, the proposed version of the DSS based on the $RPIFM_{2\times2}$ has been discussed. While, on Section 4, the numerical results of proposed DSS- $RPIFM_{2\times2}$with small values of parameters are discussed. Finally, Section 5 comes to draw the security issues and conclusions.

2. Preliminaries

The DS [11] is a mathematical technique has been employed for validating the authenticity and integrity of the digital plaintext and other documents.

The integer matrix size 2×2 ($IM_{2\times2}$) has been defined for many cryptographic applications [12]. In more specific way, the $IFM_{2\times2}$ is also defined by

$$g_{IFM_{2\times2}} \equiv \begin{bmatrix} g_1 & g_2 \\ g_3 & g_4 \end{bmatrix} (\mathrm{mod}\, p), \tag{1}$$

where g is an element in a prime field F_p and $\mathrm{Tr}_1\ (g_{IFM_{2\times2}}) + \mathrm{Tr}_2(g_{IFM_{2\times2}}) = (g_1 + g_4) + (g_2 + g_3) = g$, with g_i are random Fibonacci numbers, for i =1,…,4.

A right-side power of $IFM_{2\times2}$ ($RPIFM_{2\times2}$) over F_p has expressed by $g_{IFM_{2\times2}}$ to power $r_{IFM_{2\times2}}$ which is $IFM_{2\times2}$ as well that defined by

$$g_{IFM_{2\times2}}{}^{r_{IFM_{2\times2}}}(\mathrm{mod}\,p)\equiv\begin{bmatrix}g_1 & g_2\\ g_3 & g_4\end{bmatrix}^{\begin{bmatrix}r_1 & r_2\\ r_3 & r_4\end{bmatrix}}(\mathrm{mod}\,p)\equiv\begin{bmatrix}g_1^{\,r_1}\cdot g_3^{\,r_2} & g_2^{\,r_1}\cdot g_4^{\,r_2}\\ g_1^{\,r_3}\cdot g_3^{\,r_4} & g_2^{\,r_3}\cdot g_4^{\,r_4}\end{bmatrix}(\mathrm{mod}\,p)$$
$$\equiv\begin{bmatrix}a_1 & a_2\\ a_3 & a_4\end{bmatrix}(\mathrm{mod}\,p)\equiv A_{IM_{2\times2}}(\mathrm{mod}\,p) \tag{2}$$

3. The RPIFM$_{2\times2}$ for New Version of DSS

Suppose g, r F_p. The IFMs$_{2\times2}$ of them are created using Equations (1) and (2). The $r_{IM_{2\times2}}$ formed as a private key of the first user. Her/His public key A is calculated as IM$_{2\times2}$ that is computed in Equation (2).

(3)

A plaintext M has been signed through choosing firstly an integer t randomly. The IFM$_{2\times2}$ of t is created by

$$t_{IFM_{2\times2}}\equiv\begin{bmatrix}t_1 & t_2\\ t_3 & t_4\end{bmatrix}(\mathrm{mod}\,p),\ \text{with}\ Tr_1(t_{IFM_{2\times2}})+Tr_2(t_{IFM_{2\times2}})=(t_1+t_4)+(t_2+t_3).$$

For i =1,…,4, the elements t_i are Fibonacci numbers which are selected randomly.

The signature $(\delta_{1IM_{2\times2}},\delta_{2IM_{2\times2}})$ is computed by first user by

$$\delta_{1IM_{2\times2}}\equiv g_{IFM_{2\times2}}{}^{t_{IFM_{2\times2}}}(\mathrm{mod}\,p)\equiv\begin{bmatrix}\varsigma_{11} & \varsigma_{12}\\ \varsigma_{13} & \varsigma_{14}\end{bmatrix}(\mathrm{mod}\,p)$$

and

$$\delta_{2IM_{2\times2}}\equiv\begin{bmatrix}t_1 & t_2\\ t_3 & t_4\end{bmatrix}^{-1}\left(\begin{bmatrix}h_1 & h_2\\ h_3 & h_4\end{bmatrix}-\begin{bmatrix}r_1 & r_2\\ r_3 & r_4\end{bmatrix}\times\begin{bmatrix}\varsigma_{11} & \varsigma_{12}\\ \varsigma_{13} & \varsigma_{14}\end{bmatrix}\right)(\mathrm{mod}\,p-1)\equiv\begin{bmatrix}\varsigma_{21} & \varsigma_{22}\\ \varsigma_{23} & \varsigma_{24}\end{bmatrix}$$

where $h_{IFM_{2\times2}}$ is a hash IFM$_{2\times2}$ of M. The signature $(\delta_{1IM_{2\times2}},\delta_{2IM_{2\times2}})$ has reaches to second user. So, he/she verifies the signature $(\delta_{1IM_{2\times2}},\delta_{2IM_{2\times2}})$ by computing

$$v_{1IM_{2\times2}}\equiv g_{IFM_{2\times2}}{}^{h_{IFM_{2\times2}}}(\mathrm{mod}\,p)\equiv\begin{bmatrix}g_1 & g_2\\ g_3 & g_4\end{bmatrix}^{\begin{bmatrix}h_1 & h_2\\ h_3 & h_4\end{bmatrix}}(\mathrm{mod}\,p)\equiv\begin{bmatrix}\upsilon_{11} & \upsilon_{12}\\ \upsilon_{13} & \upsilon_{14}\end{bmatrix}(\mathrm{mod}\,p)$$

And

$$v_{2IM_{2\times2}} \equiv A_{IM_{2\times2}}{}^{\delta_{1IM_{2\times2}}} \times \delta_{1IM_{2\times2}}{}^{\delta_{2IM_{2\times2}}} (\mathrm{mod}\, p)$$
$$\equiv \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}^{\begin{bmatrix} \varsigma_{11} & \varsigma_{12} \\ \varsigma_{13} & \varsigma_{14} \end{bmatrix}} \times \begin{bmatrix} \varsigma_{11} & \varsigma_{12} \\ \varsigma_{13} & \varsigma_{14} \end{bmatrix}^{\begin{bmatrix} \varsigma_{21} & \varsigma_{22} \\ \varsigma_{23} & \varsigma_{24} \end{bmatrix}} (\mathrm{mod}\, p)$$
$$\equiv \begin{bmatrix} \upsilon_{21} & \upsilon_{22} \\ \upsilon_{23} & \upsilon_{24} \end{bmatrix} (\mathrm{mod}\, p).$$

In case, v_1 and v_2 have same value, the signature is valid and acceptable, otherwise is not.

4. Implemented Results on the DSS Based on RPIFM$_{2\times2}$

With different values of p, some various numerical results are implemented using the Python programming language. In Table (1), the sign private and verification public keys, signature and verification process are computed.

5. Security Issue and Conclusion

On the DSS- RPIFM$_{2\times2}$ that has been proposed in this work, the security level is increased. A main point for this increasing is the random generating of the IFMs$_{2\times2}$ that are utilized to form the key to sign the plaintext which is stay secretly and the public key to verify the signature. For recovering the signature, the attackers need to know the private key. The correct key requires the probability is $4/p$, where p is a large prime. Thus, forging the signature of a plaintext is more complicated.

Table 1

The proposed DSS-RPIFM$_{2\times2}$ with various values of primes p.

p	13	23	31	59
g, r	5,3	17,15	8,13	34,55
$g_{IFM_{2\times2}}$, $r_{IFM_{2\times2}}$	$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 8 & 5 \\ 3 & 1 \end{bmatrix}, \begin{bmatrix} 8 & 3 \\ 2 & 2 \end{bmatrix}$	$\begin{bmatrix} 3 & 2 \\ 2 & 1 \end{bmatrix}, \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$	$\begin{bmatrix} 13 & 8 \\ 8 & 5 \end{bmatrix}, \begin{bmatrix} 21 & 13 \\ 13 & 8 \end{bmatrix}$
$A_{IM_{2\times2}}$	$\begin{bmatrix} 3 & 1 \\ 0 & 2 \end{bmatrix}$	$\begin{bmatrix} 6 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 3 \\ 4 & 8 \end{bmatrix}$	$\begin{bmatrix} 18 & 7 \\ 6 & 4 \end{bmatrix}$

Contd...

$t_{IFM_{2\times2}}$, $t^{-1}_{IFM_{2\times2}}$	$\begin{bmatrix}3&2\\2&1\end{bmatrix}, \begin{bmatrix}4&3\\2&3\end{bmatrix}$	$\begin{bmatrix}1&2\\3&5\end{bmatrix}, \begin{bmatrix}13&5\\2&1\end{bmatrix}$	$\begin{bmatrix}8&5\\5&3\end{bmatrix}, \begin{bmatrix}9&8\\7&5\end{bmatrix}$	$\begin{bmatrix}5&3\\3&2\end{bmatrix}, \begin{bmatrix}5&3\\2&1\end{bmatrix}$
$M_{IFM_{2\times2}}$	$\begin{bmatrix}5&3\\2&1\end{bmatrix}$	$\begin{bmatrix}5&3\\2&1\end{bmatrix}$	$\begin{bmatrix}8&5\\5&3\end{bmatrix}$	$\begin{bmatrix}6&4\\2&1\end{bmatrix}$
$(S_{1IM_{2\times2}}, S_{2IM_{2\times2}})$	$\left(\begin{bmatrix}1&1\\0&0\end{bmatrix}, \begin{bmatrix}1&0\\1&0\end{bmatrix}\right)$	$\left(\begin{bmatrix}5&3\\2&5\end{bmatrix}, \begin{bmatrix}1&1\\1&0\end{bmatrix}\right)$	$\left(\begin{bmatrix}6&7\\3&4\end{bmatrix}, \begin{bmatrix}5&6\\1&3\end{bmatrix}\right)$	$\left(\begin{bmatrix}20&16\\9&10\end{bmatrix}, \begin{bmatrix}9&19\\0&7\end{bmatrix}\right)$
$(V_{1IM_{2\times2}}, V_{2IM_{2\times2}})$	$\left(\begin{bmatrix}6&8\\1&1\end{bmatrix}, \begin{bmatrix}0&3\\0&0\end{bmatrix}\right) = 3$	$\left(\begin{bmatrix}9&7\\13&4\end{bmatrix}, \begin{bmatrix}5&5\\0&0\end{bmatrix}\right) = 10$	$\left(\begin{bmatrix}20&22\\8&1\end{bmatrix}, \begin{bmatrix}0&0\\14&6\end{bmatrix}\right) = 20$	$\left(\begin{bmatrix}36&40\\57&7\end{bmatrix}, \begin{bmatrix}1&4\\13&4\end{bmatrix}\right) = 22$
Signature is Valid	Yes	Yes	Yes	Yes

References

[1] Ruma Kareem Kadhim Ajeena and Hailiza Kamarulhaili, "On the distribution of scalar *k* for elliptic scalar multiplication," in *AIP Conference Proceedings*, vol. 1682, no. 1, Art. no. 020052 (Oct. 2015).

[2] Muna Haider Hashem and Ruma Kareem Kadhim Ajeena, "The tensor product bipartite graph for symmetric encryption scheme," in *AIP Conference Proceedings*, vol. 2591, no. 1, Art. no. 050003 (Mar. 2023).

[3] Takaaki Fujita, "Ultrafilter in digraph: Directed tangle and directed ultrafilter," *Journal of Advances in Mathematics and Computer Science*, vol. 39, no. 3, pp. 37–42 (2024).

[4] Sami Mohammed Suhael, Zaid Abbas Ahmed, and Ali Jassim Hussain, "Proposed hybrid cryptosystems based on modifications of Playfair cipher and RSA cryptosystem," *Baghdad Science Journal*, vol. 21, no. 1, pp. 151–160 (2023).

[5] Wisal Hashim Abdulsalam, Salah Mashhadani, Sura Saeed Hussein, and Ali Abbas Hashim, "Artificial intelligence techniques to identify individuals through palm image recognition," *International Journal of Mathematics and Computer Science*, vol. 20, no. 1, pp. 165–171 (2025).

[6] Israa Sattar Ahmed, Ahmed Al-Fayadh, Hassan Hadi Ebrahim, and Luma Sabah Abdalbaqi, "Implementation of the neutrosophic sets in measurable space with respect to neutrosophic ring," *International Journal of Neutrosophic Science*, vol. 25, no. 3, pp. 187–193 (2025), doi: 10.54216/IJNS.250317.

[7] David K. Black, "The digital signature standard: Overview and current status," *Computers & Security*, vol. 12, no. 5, pp. 437–446 (1993).

[8] Alaa Dakhil Alrehily, Asmaa Fahad Alotaibi, Suzan Badr Almutairy, Mashael Saleh Alqhtani, and Jayaprakash Kar, "Conventional and improved digital signature scheme: A comparative study," *Journal of Information Security*, vol. 6, no. 1, pp. 59–67 (2014).

[9] Pankaj Kumar and Saurabh Kumar Sharma, "An empirical evaluation of various digital signature schemes in wireless sensor networks," *IETE Technical Review*, vol. 39, no. 4, pp. 974–984 (2022).

[10] Farid Lalem, Abdelkader Laouid, Mostefa Kara, Mohammed Al-Khalidi, and Amna Eleyan, "A novel digital signature scheme for advanced asymmetric encryption techniques," *Applied Sciences*, vol. 13, no. 8, Art. no. 5172 (2023).

[11] Darrel Hankerson, Alfred J. Menezes, and Scott Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer Science & Business Media (2004).

[12] Ruma Kareem Kadhim Ajeena, "Integer matrix size 2×2 sub-decomposition method for elliptic curve cryptography," *Computer Science*, vol. 18, no. 4, pp. 599–606 (2023).

Received March, 2025