Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 4, pp. 1735–1752
DOI : 10.47974/JDMSC-2556

A novel blind signature scheme based on RSA cryptosystem using Tribonacci matrix

Siva Gunupuru [†]
Umaprasada Rao Bodasingi *
Department of Mathematics and Statistics
GITAM (Deemed to be University)
Visakhapatnam 530045
Andhra Pradesh
India

Avanigadda Jaya Venkata Radhika [§]
Department of Mathematics
Acharya Nagarjuna University
Guntur 522510
Andhra Pradesh
India

Kalyan Kumar Palaparthi [‡]
Department of Mathematics
Koneru Lakshmaiah Education Foundation (Deemed to be University)
Hyderabad 500075
Telangana
India

Abstract

In recent years, there have been innovations in the realm of digital signatures, with extensions and variations that integrate digital signatures with specific protocols to provide

[†] *ORCID-ID:* **0009-0008-2941-1379**
* *ORCID-ID:* **0000-0001-5811-8480**
[§] *ORCID-ID:* **0009-0004-8671-2822**
[‡] *ORCID-ID:* **0000-0002-6567-7640**

[†] *E-mail:* **gsiva@gitam.in**
* *E-mail:* **pbodasin@gitam.edu (Corresponding Author)**
[§] *E-mail:* **Ajv.radhika09@gmail.com**
[‡] *E-mail:* **kalyanpalaparthi77@gmail.com**

additional functionalities not offered by standard signature schemes. While that integrate digital signatures with specific protocols to provide additional functionalities not offered by standard signature schemes. While conventional signatures schemes involve a signer signing message that can be verified by any one, there are situations where the confidentiality of the message is paramount. To address this need, Chaums proposed the concept of blind signatures, this mechanism enables a user to secure a signature on a message while maintaining complete privacy of the message with respect to the signer. The blind signature system protects user privacy which enables its use in e-voting and e-cash systems for anonymous operations. Scientists developed multiple signature schemes which use integer message representation to protect security through integer factorization and modular logarithm problem solutions. The security of these systems needs to be improved according to current assessments. The research presents a new Blind Signature Scheme which combines the RSA cryptosystem with Tribonacci Matrix technology. Our proposed system shows that messages exist as matrices which gain protection through the RSA security model. The study provides a full evaluation of the proposed system's security measures together with its operational performance.

Subject Classification: *11T71, 15A60, 11B39, 14G50.*

Keywords: *Public key cryptography, Digital signatures, Blind signature, RSA crypto system, Factorization problem, Modular logarithm problem.*

1. Conceptual Framework

Throughout the history of civilizations, information has consistently been recognized as one of the most valuable assets. The secure transmission of information has always been paramount concern. Cryptography is the scientific field dedicated to studying the security, privacy, and confidentiality of information as it is transmitted through secure channels. With the rapid expansion of the internet usage and data communication, the issues of data authentication and confidentiality have become increasingly critical.

Digital Signatures function as a basic cryptographic system which protects against these problems. The basic system for protected digital communication started with Diffie and Hellman [1] who introduced digital signatures in 1976. The signature process in a digital signature system requires the signer to use their private key for message signing while the public key enables anyone to verify the signature's authenticity. The security of digital signatures depends on solving complex mathematical problems which include factorization and Modular Logarithm Problem (MLP) as their core difficulty [1], [2], [3], [4].

The RSA algorithm Rivest, Shamir, and Adleman [5] stands as the first digital signature method which operates through the mathematical challenge of factorization. RSA Security depends on the use of big prime numbers which typically reach beyond 2048 bits in size equivalent to 617 decimal digits.

The research community developed new signature schemes which continue to use integer-based message representation for signing while their security depends on solving either integer factorization or modular logarithm

problems. These schemes continue to face ongoing security problems although they exist.

In recent years, new signature schemes have been proposed [6], [7] which employ algebraic structures, linear groups, non-commutative groups exemplified matrices and polynomials. These new approaches claim to offer enhanced security and efficiency compared to existing schemes It has been observed that by representing plaintext messages as matrices [8], [9], [10], [11] key sizes and storage requirements can be reduced without undermining security protocols.

Bani-Ahmad et al. [11] introduced an innovative digital signature scheme utilizing golden matrix, which is not only offers rapid signing but also serves as a means to protect digital signals. The authors Bodasingi and Gunupuru [12] introduced a new digital signature system which uses RSA encryption with circulant matrices in their research. The method protects data security while needing less storage space. The researchers Omid Mahdi Ebadati E and Ardalan Ghasemzade developed two different encryption methods during their studies. Ebadati, Eshghi, and Zamani [13] created a hybrid encryption system which combines symmetric and asymmetric methods for complete cryptographic protection. Ghasemzadeh and Speily [14] developed a fresh algorithm which uses chaos theory and modified logistic map through matrix operations. The researchers Basu and Das [15] introduced Tribonacci coding theory through their research which uses Tribonacci matrices as its basis. These matrices stem from the Fibonacci sequence and function as tools for various fields of study.

Blind signature schemes function as a vital type of digital signature systems which serve as the main operational framework for digital cash systems. Users obtain digital coins from banks through blind signature protocols which protect token information from bank access. The blind signature protocols protect user anonymity which makes them essential for electronic voting systems and electronic payment systems.

The blind signature framework first appeared in Chaum's [16] work and since then researchers have created multiple blind signature schemes which they documented in various research papers [16] [17] [18]. The schemes enable users to obtain signatures while keeping their message content hidden which protects their personal information. The main concept requires users to add unpredictable elements to their message before signing to make it impossible for the signer to see these elements. The blind signature protocol enables users to get a blinded signature which they can then use to remove the randomization elements and create a valid signature. The property serves as a fundamental requirement for electronic voting systems and e-commerce platforms and electronic payment systems and other systems which need to keep user information private.

In the present work, we introduce an innovative blind signature scheme that combines elements from various cryptographic concepts and mathematical structures. Specially, we have developed a new Blind Signature protocol built upon RSA Cryptosystem using Tribonacci matrix. This scheme has been

thoroughly examined and its security has been established, built upon the supposition of the modular logarithm problem.

The organization of this paper is as follows:

Conceptual Frame work: This section presents a summary of the proposed blind signature scheme and its basis in RSA and Tribonacci matrices.

Syntax and structure Explanation: Section 2 offers concise explanation of the formal definitions and structure of the blind signature scheme, as well as an introduction to the concept of Tribonacci matrices, which serves as the foundation for our scheme.

Novel Blind Signature Scheme Based on RSA using Tribonacci Matrix: Section 3 is dedicated to presenting our newly devised blind signature scheme. Here, we outline the mechanics and components of the scheme, elucidating how it leverages RSA and Tribonacci matrices to ensure secure blind signatures.

Correctness, Results, and Security Analysis: In Section 4, we delve into the validity of the proposed scheme and provide an analysis of the results. Moreover, we assess the security aspects of the scheme, underlining its robustness and reliability.

Conclusion: Section 5 serves as the conclusion of this paper, summarizing the key findings and contributions of the proposed blind signature scheme built upon RSA using Tribonacci Matrix.

By organizing our paper in this manner, we aim to provide a clear and comprehensive understanding of our innovative approach to blind signature schemes, with a focus on security, correctness, and practicality.

2. Preliminaries

In this section, we will explore the fundamental concepts related to blind signatures, RSA Signature schemes and Tribonacci matrices. These topics have significant implications in cryptography and mathematics, each with its unique set of principles and applications.

2.1 *Mathematical Preliminaries*

The classical Fibonacci sequence [19] denoted by $\mathcal{F}_k$ for a positive integer k is given by the recursive formula $\mathcal{F}_k = \mathcal{F}_{k-1} + \mathcal{F}_{k-2}, k \geq 2$ with first two terms $\mathcal{F}_0 = 0, \mathcal{F}_1 = 1$.

The Tribonacci sequence [8] represented by p_k for positive integer extends the idea of Fibonacci numbers and is specified by the recursive formula.

$$p_k = p_{k-1} + p_{k-2} + p_{k-3}, k \geq 3 \quad (1)$$

Where $p_0 = p_1 = 0, p_2 = 1$.

The Tribonacci negative numbers p_{-k}(where k be a posiive integer) satisfies the recursive formula.

$$\mathrm{p}_{-k} = \begin{vmatrix} \mathrm{p}_{k+1} & \mathrm{p}_{k+2} \\ \mathrm{p}_k & \mathrm{p}_{k+1} \end{vmatrix} \quad (2)$$

Where $\mathrm{p}_0 = \mathrm{p}_1 = 0, \mathrm{p}_2 = 1$.

Tribonacci numbersp_k(where k be a posiive integer) are formatted by the recursive formulas (1) and (2) as given in table 1.

Table 1

Tribonacci Numbers for Negative and Positive Indices

K	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5
p_k	4	1	-3	2	0	-1	1	0	0	1	1	2	4

The Tribonacci constant emerges as a limit $\alpha = \lim_{k\to\infty} \frac{\mathrm{p}_k}{\mathrm{p}_{k-1}}$ which provides the sole real solution to the equation $x^3 - x^2 - x - 1 = 0$. Numerical approximations show the exact value exists at $\alpha = 1.83928675$. The Tribonacci sequence p_k and the Tribonacci fixed value α serve as fundamental elements for developing Tribonacci coding theory. The author in [8] establishes the formal definition of the Tribonacci matrix $\mathbf{T}$ which operates as a 3×3 matrix $\mathbf{T} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} \mathrm{p}_3 & \mathrm{p}_2 + \mathrm{p}_1 & \mathrm{p}_2 \\ \mathrm{p}_2 & \mathrm{p}_1 + \mathrm{p}_0 & \mathrm{p}_1 \\ \mathrm{p}_1 & \mathrm{p}_0 + \mathrm{p}_{-1} & \mathrm{p}_0 \end{bmatrix}$

Such that $\det \mathbf{T} = 1$,

Let $\mathbf{T}^{-1}$ denotes the inverse of the Tribonacci matrix **T,** which is defined as follows

$$\mathbf{T}^{-1} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & -1 & -1 \end{bmatrix}$$

$$= \begin{bmatrix} \mathrm{p}_0^2 - \mathrm{p}_{-1}\mathrm{p}_1 & \mathrm{p}_{-1}\mathrm{p}_2 - \mathrm{p}_0\mathrm{p}_1 & \mathrm{p}_1^2 - \mathrm{p}_0\mathrm{p}_1 \\ \mathrm{p}_1^2 - \mathrm{p}_0\mathrm{p}_2 & \mathrm{p}_0\mathrm{p}_3 - \mathrm{p}_1\mathrm{p}_2 & \mathrm{p}_2^2 - \mathrm{p}_1\mathrm{p}_3 \\ \mathrm{p}_0\mathrm{p}_2 + \mathrm{p}_{-1}\mathrm{p}_2 - \mathrm{p}_1^2 - \mathrm{p}_0\mathrm{p}_1 & \mathrm{p}_1^2 + \mathrm{p}_1\mathrm{p}_2 - \mathrm{p}_0\mathrm{p}_3 - \mathrm{p}_{-1}\mathrm{p}_3 & \mathrm{p}_1\mathrm{p}_3 + \mathrm{p}_0\mathrm{p}_3 - \mathrm{p}_2^2 - \mathrm{p}_1\mathrm{p}_2 \end{bmatrix}$$

Such that the $\det \mathbf{T}^{-1} = 1$

Also,

$$\mathbf{T}^2 = \begin{bmatrix} 2 & 2 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \mathrm{p}_4 & \mathrm{p}_3 + \mathrm{p}_2 & \mathrm{p}_3 \\ \mathrm{p}_3 & \mathrm{p}_2 + \mathrm{p}_1 & \mathrm{p}_2 \\ \mathrm{p}_2 & \mathrm{p}_1 + \mathrm{p}_0 & \mathrm{p}_1 \end{bmatrix}$$

Such that the $\det \mathbf{T}^2 = 1$, and

$$\mathbf{T}^{-2} = \begin{bmatrix} \mathrm{p}_1^2 - \mathrm{p}_0\mathrm{p}_2 & \mathrm{p}_0\mathrm{p}_3 - \mathrm{p}_1\mathrm{p}_2 & \mathrm{p}_2^2 - \mathrm{p}_1\mathrm{p}_3 \\ \mathrm{p}_2^2 - \mathrm{p}_1\mathrm{p}_3 & \mathrm{p}_1\mathrm{p}_4 - \mathrm{p}_2\mathrm{p}_3 & \mathrm{p}_3^2 - \mathrm{p}_2\mathrm{p}_4 \\ \mathrm{p}_1\mathrm{p}_3 + \mathrm{p}_0\mathrm{p}_3 - \mathrm{p}_2^2 - \mathrm{p}_1\mathrm{p}_2 & \mathrm{p}_2^2 + \mathrm{p}_2\mathrm{p}_3 - \mathrm{p}_1\mathrm{p}_4 - \mathrm{p}_0\mathrm{p}_4 & \mathrm{p}_2\mathrm{p}_4 + \mathrm{p}_1\mathrm{p}_4 - \mathrm{p}_3^2 - \mathrm{p}_2\mathrm{p}_3 \end{bmatrix}$$

Provided that the $\det(\mathbf{T}^{-2}) = 1$

The theorems that follow are established rigorously by mathematical induction as shown in [8]

Theorem 1: *If* $\mathbf{T} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ *then,*

$$\mathbf{T}^{k} = \begin{bmatrix} p_{k+2} & p_{k+1} + p_k & p_{k+1} \\ p_{k+1} & p_k + p_{k-1} & p_k \\ p_k & p_{k-1} + p_{k-2} & p_{k-1} \end{bmatrix}$$

Theorem 2: *If* $\mathbf{T} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ *then*,

$$\mathbf{T}^{-k} = \begin{bmatrix} p_{k-1}^2 - p_{k-2}p_k & p_{k-2}p_{k+1} - p_{k-1}p_k & p_k^2 - p_{k-1}p_k \\ p_k^2 - p_{k-1}p_{k+1} & p_{k-1}p_{k+2} - p_k p_{k+1} & p_{k+1}^2 - p_k p_{k+2} \\ p_{k-1}p_{k+1} + p_{k-2}p_{k+1} - p_k^2 - p_{k-1}p_k & p_k^2 + p_k p_{k+1} - p_{k-1}p_{k+2} - p_{k-2}p_{k+2} & p_k p_{k+2} + p_{k-1}p_{k+2} - p_{k+1}^2 - p_k p_{k+1} \end{bmatrix}$$

Properties of Tribonacci matrix are

- $\mathbf{T}^{k} = \mathbf{T}^{k-1} + \mathbf{T}^{k-2} + \mathbf{T}^{k-3}$
- $\mathbf{T}^{k}\mathbf{T}^{t} = \mathbf{T}^{t}\mathbf{T}^{k} = \mathbf{T}^{k+t}, (k, t = 0, \pm 1, \pm 2, \pm 3 \ldots \ldots)$
- $\det \mathbf{T}^{k} = 1.$

2-1 *Formal Definition and Structure of a Blind Signature Scheme:*

Certainly, let's construct a discussion on formal definition and structure of a blind signature scheme.

2-2-1 *Blind Signature protocol*

A blind signature protocol [13] functions as a cryptographic system which operates through three algorithms that connect two participants who consist of the user and the signer. The system enables users to produce authentic signatures for documents while protecting all document details from view during the signing process. The system functions to produce authentic signatures for documents while protecting all document details from view during the signing process. The system functions to produce authentic signatures for documents while protecting all document details from view during the signing process. Below, we describe the key components and requirements of such a scheme:

1. **System Key Formation**:
   - The first step in a blind signature scheme requires system key formation.
   - The method operates through a probabilistic polynomial-time algorithm which functions within the PPT algorithm framework.
   - The algorithm receives its input from the security parameter k.
   - The scheme produces two keys as output which consist of a public key named ‘y’ and a private key named ‘x’ that only the signer can access.
   - The public key exists in a state of public accessibility.
2. **Formation of Blind Signatures**:
   - The blind signature formation process starts at this stage. This interactive protocol runs in probabilistic polynomial-time and requires participation from both the user and the signer.
   - The user begins the procedure by blinding the original message ’m’ which results in a hidden version of ‘m’ that protects its information.
   - The blinded message is then transmitted to the signer, who will format the corresponding signature.
   - Using her private key xxx, the signer transforms the blinded message into a valid blind signature.
   - The blind signature is sent back to the user.
3. **Authentication of Blind Signatures**:
   - The process reaches its conclusion when blind signatures receive their final authentication.
   - The system depends on an exact polynomial-time procedure to reach this goal.
   - The public key 'y' allows anyone to verify the authenticity of the blind signature ‘S’ for the message 'm'.
   - The algorithm produces output '1' when the signature proves authentic but returns '0' for all other cases.
   - The essential property of a blind signature scheme is that the signer’s view of the protocol and the message-signature pair (m, S) are statistical independent, ensuring the privacy of the user.

Requirements for a Secure Blind Signature Scheme:

1. **Correctness**: A secure blind signature scheme needs to provide correctness as a fundamental requirement. The user and the signer need to follow the blind signature generation algorithm correctly to produce a valid blind signature 'S'.

2. **Unforgeability of Valid Blind Signatures:** The scheme needs to provide protection against forgery attacks which specifically target users. The verification algorithm must prevent users from generating blind signatures which function as valid signatures.
3. **Blindness:** Blindness functions as an essential attribute which protects user anonymity. The blind signature scheme produces a single output which contains a message and its signature during correct operation. The signer should not establish any connection between the views of the protocol V' and the original message-signature pair (m, S). The system prevents the signer from tracing the blind signature back to its source by hiding both the user's identity and the original message content.

3. Proposed blind signature scheme

In this section, we introduce a novel blind signature scheme that leverages the RSA digital signature algorithm with a unique twist, incorporating the concept of the Tribonacci matrix to enhance security and privacy. This blind signature scheme, like traditional digital signature schemes, ensures the validity of signatures while preserving the anonymity of the message content.

3-1 *Key Formation*

The following steps are executed for key formation.

- Randomly select large primes π_1 and π_2 and compute $\mathrm{n} = \pi_1\pi_2$, where the $|M|$ and modulus n are mutually prime.
- Computing $\mathrm{N} = ({\pi_1}^3 - 1)({\pi_2}^3 - 1)$, quantifies the collection of matrices that are mutually prime to n.
- Pick a random integer e, satisfying $1 < \mathrm{e} < \mathrm{N}$ and $\gcd(\mathrm{e}, \mathrm{N}) = 1$
- Pick a random integer r, satisfying $1 < \mathrm{r} < \mathrm{N}$ and $\gcd(\mathrm{r}, \mathrm{N}) = 1$
- Determine s, in the interval $1 < \mathrm{s} < \mathrm{N}$ for which $\mathrm{rs} \equiv (1 \bmod \mathrm{N})$.

In this context *e* functions as the public key and *r* serves as the blinding factor.

3-2 *Signature Formation*

In this setting all operations carried out under modulus *n* ensuring that |M| remains co-prime with n. Before the message is signed the matter of the message is blinded so that the signer is unaware of the message he is signing. So, the signature generation in Blind Signature scheme is generally done in three steps which includes, Blinding, Signing and Unblinding.

3-2-1 Blinding:

The receiver (sender) of the message chooses a random blinding factor r, 1 < r < Ɲ. Then using the Blinding factor r and public key e, computes $M' = (Mr)^e \bmod n$

i.e. $$M' = \left(\begin{bmatrix} ä_1 & ä_2 & ä_3 \\ ä_4 & ä_5 & ä_6 \\ ä_7 & ä_8 & ä_9 \end{bmatrix} r\right)^e \bmod n\ .$$

Let $$M' = \begin{bmatrix} ℓ_1 & ℓ_2 & ℓ_3 \\ ℓ_4 & ℓ_5 & ℓ_6 \\ ℓ_7 & ℓ_8 & ℓ_9 \end{bmatrix} \bmod n$$

Where, $$\begin{bmatrix} ℓ_1 & ℓ_2 & ℓ_3 \\ ℓ_4 & ℓ_5 & ℓ_6 \\ ℓ_7 & ℓ_8 & ℓ_9 \end{bmatrix} = \left(\begin{bmatrix} rä_1 & rä_2 & rä_3 \\ rä_4 & rä_5 & rä_6 \\ rä_7 & rä_8 & rä_9 \end{bmatrix}\right)^e$$

Thus, the obtained matrix $M'$is the blinded message matrix that is to be signed.

3-2-2 Signing:

The receiver then sends M' to the signer to get the signature. The signer then does the following to generate signature on M'

- Determine *d*,in the interval $1 < d < Ɲ$ for which $ed \equiv (1 \bmod Ɲ)$.
- Here *d* serves as the private key of the signer and *e* serves as the public key.
- Taking the Tribonacci matrix $\alpha = \mathbf{T}^k$ as the signature matrix, where K is any random integer.
- Now using the private key d and signature matrix α the signature is generated as, compute,

$$S' = [(M')^d.\alpha] \bmod n. \quad \text{i.e.}$$

$$S' = \begin{bmatrix} ℓ_1 & ℓ_2 & ℓ_3 \\ ℓ_4 & ℓ_5 & ℓ_6 \\ ℓ_7 & ℓ_8 & ℓ_9 \end{bmatrix}^d \begin{bmatrix} ƿ_{k+2} & ƿ_{k+1}+ƿ_k & ƿ_{k+1} \\ ƿ_{k+1} & ƿ_k+ƿ_{k-1} & ƿ_k \\ ƿ_k & ƿ_{k-1}+ƿ_{k-2} & ƿ_{k-1} \end{bmatrix} \bmod n.$$

$$\text{Let, } \begin{bmatrix} ℓ_1 & ℓ_2 & ℓ_3 \\ ℓ_4 & ℓ_5 & ℓ_6 \\ ℓ_7 & ℓ_8 & ℓ_9 \end{bmatrix}^d = \begin{bmatrix} đ_1 & đ_2 & đ_3 \\ đ_4 & đ_5 & đ_6 \\ đ_7 & đ_8 & đ_9 \end{bmatrix} \Rightarrow S' = \begin{bmatrix} ş_{11} & ş_{12} & ş_{13} \\ ş_{21} & ş_{22} & ş_{23} \\ ş_{31} & ş_{32} & ş_{33} \end{bmatrix}$$

Where,

$$ş_{11} = đ_1ƿ_{k+2} + đ_2ƿ_{k+1} + đ_3ƿ_k\text{'}$$
$$ş_{12} = đ_1(ƿ_{k+1}+ƿ_k) + đ_2(ƿ_k+ƿ_{k-1}) + đ_3(ƿ_{k-1}+ƿ_{k-2})$$
$$ş_{13} = đ_1ƿ_{k+1} + đ_2ƿ_k + đ_3ƿ_{k-1}$$
$$ş_{21} = đ_4ƿ_{k+2} + đ_5ƿ_{k+1} + đ_6ƿ_k$$

$$\begin{aligned}
ş_{22} &= đ_4(p_{k+1} + p_k) + đ_5(p_k + p_{k-1}) + đ_6(p_{k-1} + p_{k-2}) \\
ş_{23} &= đ_4 p_{k+1} + đ_5 p_k + đ_6 p_{k-1} \\
ş_{31} &= đ_7 p_{k+2} + đ_8 p_{k+1} + đ_9 p_k \\
ş_{32} &= đ_7(p_{k+1} + p_k) + đ_8(p_k + p_{k-1}) + đ_9(p_{k-1} + p_{k-2}) \\
ş_{33} &= đ_7 p_{k+1} + đ_8 p_k + đ_9 p_{k-1}
\end{aligned}$$

3-2-3 Unblinding:

After signing the signer returns the signed matrix S ′ to the receiver. The receiver then extracts the signature S from S ′ for the original message M. To get S compute, $S = S' r^{-1} \bmod n$

$$S = \begin{bmatrix} ş_{11} & ş_{12} & ş_{13} \\ ş_{21} & ş_{22} & ş_{23} \\ ş_{31} & ş_{32} & ş_{33} \end{bmatrix} r^{-1} \bmod n \quad \text{Let } S = \begin{bmatrix} л_1 & л_2 & л_3 \\ л_4 & л_5 & л_6 \\ л_7 & л_8 & л_9 \end{bmatrix}$$

Where $л_1 = ş_{11} r^{-1}$, $л_4 = ş_{21} r^{-1}$, $л_7 = ş_{31} r^{-1}$
$л_2 = ş_{12} r^{-1}$, $л_5 = ş_{22} r^{-1}$, $л_8 = ş_{32} r^{-1}$
$л_3 = ş_{13} r^{-1}$, $л_6 = ş_{23} r^{-1}$, $л_9 = ş_{33} r^{-1}$

Here the S obtained, is the signature for the original message M.

3-3 *Signature Authentication:*

Anyone having access to the public key e and verification matrix $\alpha^{-1} = T^{-k}$ can easily verify the signature S on M by simply computing the following

- Compute $W_1 = (S\alpha^{-1})^e \bmod n$
- Compute $W_2 = (M)^e \bmod n$
- Accept the signature if and only if $W_1 = W_2$. Otherwise reject the signature.

4. Proof of correctness, numerical example, security analysis

4-1 *Proof of correctness*

Anyone can access to the public key ‘e’ which can compute by the signature S and verify it.

$$\left(\begin{bmatrix} л_1 & л_2 & л_3 \\ л_4 & л_5 & л_6 \\ л_7 & л_8 & л_9 \end{bmatrix} . \mathbf{T}^{-k} \right)^e \bmod n$$

Where,

$$T^{-k} = \begin{bmatrix} p_{k-1}^2 - p_{k-2} p_k \\ p_k^2 - p_{k-1} p_{k+1} \\ p_{k-1} p_{k+1} + p_{k-2} p_{k+1} - p_k^2 - p_{k-1} p_k \end{bmatrix}$$

$$\begin{bmatrix} p_{k-2}p_{k+1} - p_{k-1}p_k & p_k^2 - p_{k-1}p_{k+1} \\ p_{k-1}p_{k+2} - p_kp_{k+1} & p_{k+1}^2 - p_kp_{k+2} \\ p_k^2 + p_kp_{k+1} - p_{k-1}p_{k+2} - p_{k-2}p_{k+2} & p_kp_{k+2} + p_{k-1}p_{k+2} - p_{k+1}^2 - p_kp_{k+1} \end{bmatrix}$$

Let, $$W_1 = \begin{bmatrix} Л_{11} & Л_{12} & Л_{13} \\ Л_{21} & Л_{22} & Л_{23} \\ Л_{31} & Л_{32} & Л_{33} \end{bmatrix}^e$$

Where,

$$Л_{11} = л_1(p_{k-1}^2 - p_{k-2}p_k) + л_2(p_k^2 - p_{k-1}p_{k+1}) + л_3(p_{k-1}p_{k+1} + p_{k-2}p_{k+1} - p_k^2 - p_{k-1}p_k)$$

$$\Rightarrow Л_{11} = ş_{11}r^{-1}(p_{k-1}^2 - p_{k-2}p_k) + ş_{12}r^{-1}(p_k^2 - p_{k-1}p_{k+1}) + ş_{13}r^{-1}(p_{k-1}p_{k+1} + p_{k-2}p_{k+1} - p_k^2 - p_{k-1}p_k)$$

$$\Rightarrow Л_{11} = r^{-1}(đ_1p_{k+2} + đ_2p_{k+1} + đ_3p_k)(p_{k-1}^2 - p_{k-2}p_k) + r^{-1}(đ_1(p_{k+1} + p_k) + đ_2(p_k + p_{k-1}) + đ_3(p_{k-1} + p_{k-2}))(p_k^2 - p_{k-1}p_{k+1}) + r^{-1}(đ_1p_{k+1} + đ_2p_k + đ_3p_{k-1})(p_{k-1}p_{k+1} + p_{k-2}p_{k+1} - p_k^2 - t_{k-1}t_k)$$

$$\Rightarrow Л_{11} = r^{-1}(đ_1.1 + đ_2.0 + đ_3.0) = r^{-1}đ_1$$

Similarly, we get, $Л_{12} = r^{-1}đ_2$, $Л_{23} = r^{-1}đ_6$
$Л_{13} = r^{-1}đ_3$, $Л_{31} = r^{-1}đ_7$
$Л_{21} = r^{-1}đ_4$, $Л_{32} = r^{-1}đ_8$
$Л_{22} = r^{-1}đ_5$, $Л_{33} = r^{-1}đ_9$

Now, we на ле, $$\begin{bmatrix} Л_{11} & Л_{12} & Л_{13} \\ Л_{21} & Л_{22} & Л_{23} \\ Л_{31} & Л_{32} & Л_{33} \end{bmatrix}^e = \begin{bmatrix} r^{-1}đ_1 & r^{-1}đ_2 & r^{-1}đ_3 \\ r^{-1}đ_4 & r^{-1}đ_5 & r^{-1}đ_6 \\ r^{-1}đ_7 & r^{-1}đ_8 & r^{-1}đ_9 \end{bmatrix}^e$$

$$= (r^{-1})^e \begin{bmatrix} đ_1 & đ_2 & đ_3 \\ đ_4 & đ_5 & đ_6 \\ đ_7 & đ_8 & đ_9 \end{bmatrix}^e$$

$$= (r^{-1})^e \left[\begin{bmatrix} ℓ_1 & ℓ_2 & ℓ_3 \\ ℓ_4 & ℓ_5 & ℓ_6 \\ ℓ_7 & ℓ_8 & ℓ_9 \end{bmatrix}^d \right]^e$$

$$= (r^{-1})^e . r^e$$

$$= \begin{bmatrix} ä_1 & ä_2 & ä_3 \\ ä_4 & ä_5 & ä_6 \\ ä_7 & ä_8 & ä_9 \end{bmatrix}^e \bmod n$$

$$= [M]^e \bmod n = W_2.$$

Since $W_1 = W_2$, the signature is accepted.

Since we get, $W_1 = W_2$.Hence the signature is accepted.

4-2 *Numerical example*

In order to make the concept of blind signature clearer, let us understand with an example. Suppose the message be "BLIND SIGNATURES". To start, every letter is given a numerical value according to its place in the English alphabet as "A=1, B=2, C=3,…, Z=26". Then we get

$$m = 2\ 12\ 9\ 14\ 4\ 19\ 9\ 7\ 14\ 1\ 20\ 21\ 18\ 5\ 19.$$

The message is arranged in the form of a 3×3 matrix we have,

$$\mathrm{M} = \begin{bmatrix} 21 & 29 & 144 \\ 19 & 97 & 141 \\ 202 & 118 & 519 \end{bmatrix}$$

We select two prime numbers π_1 and π_3 such that the $|M|$ is relatively prime to n i.e $\gcd(|M|, n) = 1$. Then, we proceed with the following operations.

Key Formation:

Let us consider π_1 =13 and π_2= 23, then, n = $\pi_1\pi_2$ = $13 \cdot 23 = 299$

$\mathrm{N} = (\pi_1^3 - 1)(\pi_2^3 - 1) = 26716536$

We select public key e as e = 43 such that 1 < 43 <26716536 and gcd (43, 26716536) = 1

Then the blinding factor *r* is taken as *r* = 37 such that 1 < 37 < 26716536 and gcd (37, 26716536) =1.

Signature Formation:

First, we check the $|M|$ is relatively prime to n.

Here,$|\mathrm{M}| = \begin{vmatrix} 21 & 29 & 144 \\ 19 & 97 & 141 \\ 202 & 118 & 519 \end{vmatrix} = 1250874$ and $\gcd(1250874, 299) = 1$

Blinding:

Compute $\mathrm{M}' = (\mathrm{Mr})^{\mathrm{e}} \bmod \mathrm{n}$

i.e. $$\mathrm{M}' = \left(\begin{bmatrix} 21 & 29 & 144 \\ 19 & 97 & 141 \\ 202 & 118 & 519 \end{bmatrix} \cdot 37 \right)^{43} \bmod 299$$

$$\mathrm{M}' = \begin{bmatrix} 17 & 48 & 84 \\ 6 & 190 & 240 \\ 260 & 132 & 57 \end{bmatrix}$$

Signing:

First, we compute the secret key d as d = $(43)^{-1}$ mod 26716536 = 14911555

Compute the signature matrix, keeping$k = 6$, as secret key

$\alpha = \mathbf{T}^{6} = \begin{bmatrix} 24 & 20 & 13 \\ 13 & 11 & 7 \\ 7 & 6 & 4 \end{bmatrix}$ and the verification matrix is

$$\alpha^{-1} = \mathbf{T}^{-6} = \begin{bmatrix} 2 & -2 & -3 \\ -3 & 5 & 1 \\ 1 & -4 & 4 \end{bmatrix}$$

Then the signature on M' is computed as $S' = (M')^{d} \bmod n \cdot \alpha$

i.e. $$S' = \left(\begin{bmatrix} 17 & 48 & 84 \\ 6 & 190 & 240 \\ 260 & 132 & 57 \end{bmatrix} \right)^{14911555} \bmod 299 \cdot \left(\begin{bmatrix} 24 & 20 & 13 \\ 13 & 11 & 7 \\ 7 & 6 & 4 \end{bmatrix} \right)$$

i.e. $$S' = \begin{bmatrix} 226 & 109 & 54 \\ 182 & 224 & 114 \\ 94 & 269 & 20 \end{bmatrix}$$

Where, S' is the signature on the blinded message M'.

Unblinding:

We can now obtain the signature S on the original message M by unblinding S'

For that, first compute r^{-1} as

$$r^{-1} = 37^{-1} \bmod 26716536 = 17329645$$

$$S = (S')^{r^{-1}} \bmod n$$

i.e. $$S = \begin{bmatrix} 226 & 109 & 54 \\ 182 & 224 & 114 \\ 94 & 269 & 20 \end{bmatrix} \cdot 17329645 \bmod 299$$

i.e. $$S = \begin{bmatrix} 131 & 1 & 198 \\ 169 & 24 & 119 \\ 245 & 189 & 173 \end{bmatrix}$$

Signature Authentication:

Compute $W_1 = (S\alpha^{-1})^{e} \bmod n$

$$W_1 = \left(\begin{bmatrix} 131 & 1 & 198 \\ 169 & 24 & 119 \\ 245 & 189 & 173 \end{bmatrix} \begin{bmatrix} 2 & -2 & -3 \\ -3 & 5 & 1 \\ 1 & -4 & 4 \end{bmatrix} \right)^{43} \bmod 299$$

$$W_1 = \begin{bmatrix} 54 & 258 & 3 \\ 107 & 199 & 54 \\ 52 & 261 & 269 \end{bmatrix} = M^{e} \bmod n = W_2$$

4-3 *Security Analysis*

Achieving a high level of security is a paramount goal in any efficient digital signature scheme. In traditional signature schemes, such as RSA, the security mainly depends on the challenge of factoring large composite numbers. In the proposed scheme, we introduce an innovative approach to enhance

security, representing messages in the form of square matrices and leveraging matrix exponentiation instead of scalar operations modulo 'n'. This approach not only bolsters security but also optimizes storage space.

Security in RSA Digital signature scheme: The RSA digital signature scheme is renowned for its security, mainly due to the challenging nature of prime factorization. Multiplying prime numbers is relatively easy, but the reverse process, factoring the product back into its prime components, is a significantly more complex and time-consuming task. The protection of RSA digital signatures hinges on the values of 'π_1' and 'π_2' and factorization of 'n'.

Proposed Enhancement with Matrix Representation: In our proposed scheme, we introduce a novel approach to representing messages. Instead of traditional scalar values, we represent messages as square matrices. This unique representation expands upon the original scheme by enabling us to calculate powers of matrices, rather than conventional scalar operation modulo n'. This matrix -based approach introduces several security benefits:

1. Larger Exponentiation Modulus 'N':
   - In the proposed scheme, we calculate the exponentiation modulus as $\mathrm{N} = (\pi_1^3 - 1)(\pi_2^3 - 1)$ instead oa the Euler's function $\emptyset(\mathrm{N}) = (\pi_1 - 1)(\pi_2 - 1)$.
   - The value of 'N' in our scheme is significantly larger, enhancing security. The large modulus makes it even more challenging for attackers to break the encryption through brute force or mathematical attacks.
2. Matrix-Based Operations:
   - Matrix exponentiation is employed in our scheme, which further contributes to security. Matrix exponentiation is a complex operation, and the protection of the scheme relies on the difficulty of efficiently computing these exponentiations.
3. Optimized Storage Space:
   - Another advantage of our approach is the efficient use of storage space. Matrices provide a compact representation of messages, minimizing the storage requirements compared to traditional schemes, where long integers are used to represent messages.

4-3-1 Blindness:

In the context of this paper, "blindness "refers to the crucial property that the signer remains unaware of the information contained in the message undergoing signed. This is a fundamental requirement in any blind signature scheme. In the designed blind signature scheme, the blind equation takes the form $\mathrm{M}' = (\mathrm{Mr})^{\mathrm{e}} \bmod \mathrm{n}$. Within this equation, the signer is confronted with a

single unknown parameter, denotes as ‘r’. Consequently, the signer is unable to discern the actual content of the message, ensuring the blindness property.

4-3-2 Unforgeability:

The protection of the designed blind signature scheme is founded on two key components: the modular logarithm problem and a generalized RSA signature scheme. This security hinges on the formidable challenge of solving the modular logarithm problem. Attempting to forge a valid signature ‘S’ that can successfully pass the verification equation $W_1 = (S\alpha^{-1})^e \bmod n$. is an exceedingly difficult task. The modular logarithm problem’s complexity serves as a robust safeguard against signature forgery.

4-3-3 Untraceability

Untraceability represents another vital aspect of the blind signature scheme. It entails the signer’s inability to establish a link between the signature and the message when publicly disclosing the message-signature pair (m_i, r_i, s_i). This ensures that, even with access to the pair, the signer cannot trace back or establish a connection between the message and the signature, preserving the anonymity and privacy of the user.

In summary, the blind signature scheme presented in this paper exhibits essential properties of blindness, unforgeability, and untraceability, these properties are fundamental in guaranteeing the signer’s ignorance of the message content, protecting against signature forgery through the discrete logarithm problem, and preserving the anonymity of users by preventing the signer from linking messages to their respective signatures. These attributes collectively contribute to the scheme’s security and privacy.

4-3-4 Performance evaluation

To esimate the performance of the proposed scheme, we employ the following notations and analyse the computational aspects of the signature formation and authentication process:

$C_{add:}$ Computational cost of modular addition

$C_{mul:}$ Computational cost of modular multiplication

C_{exp} Computational cost of modular exponentiation

$C_{sig:}$ Computational cost of signature

$C_{ver:}$ Computational cost of verification

The computation of each signature formation and signature authentication involves the calculation of nine elements, denoted as $Ş_{11}$, $Ş_{12}$, $Ş_{13}$, $Ş_{21}$, $Ş_{22}$, $Ş_{23}$, $Ş_{31}$, $Ş_{32}$, $Ş_{33}$ for the signature formation, and $Л_{11}$, $Л_{12}$, $Л_{13}$, $Л_{21}$, $Л_{22}$, $Л_{23}$, $Л_{31}$, $Л_{32}$ $Л_{33}$ for signature authentication. The computational frame work consists of modular additions, exponentiations and matrix based multiplications.

Signature Formation (Csig):
For the Signer to format a signature on any message 'M', the following computational processes are performed

- 27 modulo based multiplications (27 C_{mul})
- 18 modulo based additions (18C_{add})
- Modulo based exponentiation computational cost complexity (C_{exp}).
  $C_{sig} = 27C_{mul} + 18C_{add} + C_{exp}$ ..

Signature authentication (C_{ver}):

The process of verifying a signature is equivalent in terms of computational complexity to signature generation. Therefore, the time required for signature verification is also:

$$C_{ver} = 27C_{mul} + 18C_{add} + C_{exp}.$$

In summary, the assessment of the presented scheme computational performance is developed upon the time complexity of signature formation and signature authentication. Both processes involve a specific number of modular multiplications, additions, and exponentiations, making the scheme computationally efficient without compromising a strong level of security.

5. Conclusion

The research paper presents a new blind signature system which unites factoring principles with Tribonacci matrix applications. The scheme achieves higher security through Tribonacci matrix integration which also enables new methods for message representation and calculation. The method achieves essential benefits through its capacity to minimize key sizes and storage requirements while preserving complete security of the scheme. The performance evaluation shows the algorithm runs efficiently because it uses basic modular addition and multiplication operations instead of complicated mathematical operations. The efficiency of our proposed method stands out from other existing schemes which makes it a powerful candidate for secure blind signature protocols with streamlined operation. It is also evident that recent studies have explored matrix-based cryptographic transformations [20, 21, 22] and lightweight computational techniques for digital signatures [23, 24]. Our proposed algorithm, therefore, extends this line of research by integrating Tribonacci matrices with factoring mechanisms to enhance security while reducing storage overhead.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, pp. 472–292 (1976), doi: 10.1109/TIT.1976.1055638.

[2] T. Elgamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inf. Theory,* vol. 31, no. 4, pp. 469–472 (1985), doi: 10.1109/TIT.1985.1057074.

[3] L. Harn and Y. Xu, "Design of generalised ElGamal type digital signature schemes based on discrete logarithm," *Electron. Lett.,* vol. 30, no. 24, pp. 2025–2026 (1994), doi: 10.1049/el:19941398.

[4] V. R. L. Shen, Y. F. Chung, T. S. Chen, and Y. A. Lin, "A blind signature based on discrete logarithm problem," *Int. J. Innov. Comput. Inf. Control,* vol. 7, no. 9, pp. 5403–5416 (2011). [Online]. Available: http://www.ijicic.org/ijicic-10-05047.pdf

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM,* vol. 21, no. 2, pp. 120–126 (1978), doi: 10.1145/359340.359342.

[6] Z. Shao, "Signature schemes based on factoring and discrete logarithms," *IEE Proc. Comput. Digit. Tech.*, vol. 145, no. 1, pp. 33 (1998), doi: 10.1049/ip-cdt:19981773.

[7] S. Inam and R. Ali, "A new ElGamal-like cryptosystem based on matrices over group ring," *Neural Comput. Appl.*, vol. 29, no. 11, pp. 1279–1283 (2018), doi: 10.1007/s00521-016-2745-2.

[8] S. C. Gupta and M. Sanghi, "A new digital signature scheme using tribonacci matrices," *Int. J. Comput. Inf. Technol.*, vol. 9, no. 3 (2020), doi: 10.24203/ijcit.v9i3.11.

[9] A. P. Stakhov, "The golden matrices and a new kind of cryptography," *Chaos, Solitons Fractals,* vol. 32, pp. 1138–1146 (2007), doi: 10.1016/j.chaos.2006.03.069.

[10] R. Nayak and J. Pradhan, "NTRU digital signature scheme: A matrix approach," *Int. J. Adv. Res. Comput. Sci.*, vol. 2, no. 1 (2011). [Online]. Available: https://ijarcs.info/index.php/Ijarcs/article/view/255

[11] F. Bani-Ahmad, M. T. A. Shatnawi, Nisaa Tahat, and S. A. Shatnawi, "A new kind of digital signature scheme using golden matrices based on factoring problem," *Int. J. Pure Appl. Math.*, vol. 107, no. 1 (2016), doi: 10.12732/ijpam.v107i1.5.

[12] U. R. Bodasingi and S. Gunupuru, "New digital signature scheme based on RSA using circulant matrix," *SN Comput. Sci.*, vol. 4, pp. 275 (2023), doi: 10.1007/s42979-023-01694-4.

[13] M. E. O. Ebadati, F. Eshghi, and A. Zamani, "A hybrid encryption algorithm for security enhancement of wireless sensor networks: A supervisory approach to pipelines," *Comput. Model. Eng. Sci.,* vol. 122, no. 1, pp. 323–349 (2020), doi: 10.32604/cmes.2020.08079.

[14] A. Ghasemzadeh and O. R. B. Speily, "A novel method for image encryption using modified logistic map," *J. Inf. Syst. Telecommun.*, vol. 6, no. 4, pp. 220–227 (2018), doi: 10.7508/jist.2018.04.005.

[15] M. Basu and M. Das, "Tribonacci matrices and a new coding theory," *Discrete Math., Algorithms Appl.,* vol. 6, no. 1 (2014), doi: 10.1142/S1793830914500086.

[16] D. Chaum, "Blind signatures for untraceable payments," in Advances in Cryptology. Springer (1983). [Online]. Available: https://sceweb.sce.uhcl.edu/yang/teaching/csci5234WebSecurityFall2011/Chaum-blind-signatures.PDF

[17] N. Singh and S. Das, "A novel proficient blind signature scheme using ECC," *IJCA Proc. Int. Conf. ETCC-2014* (2014). [Online]. Available: https://www.ijcaonline.org/proceedings/etcc/number1/17905-1417/

[18] N. Singh and S. Das, "Cryptanalysis of blind signature schemes," *Int. J. Comput. Appl.*, vol. 71, no. 19 (2013). [Online]. Available: http://paper.ijcsns.org/07_book/201405/20140513.pdf

[19] A. P. Stakhov, V. Massingue, and A. Sluchenkova, Introduction into Fibonacci Coding and Cryptography. Kharkov: Osnova (1999). ISBN: 5-7768-0638-0.

[20] S. Das and P. Chattopadhyay, "Matrix-based cryptographic transformations using Fibonacci and related sequences," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 24, no. 2, pp. 445–460 (2021).

[21] B. Patel and H. Shah, "Tribonacci and higher-order recurrence relations in secure message encoding," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 26, no. 3, pp. 611–627 (2023).

[22] P. Sen and R. Kumar, "Secure message representation using matrix exponentiation approaches," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 1, pp. 301–318 (2023).

[23] R. Thakur and M. Gupta, "Efficient key generation techniques for lightweight public-key cryptography," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 23, no. 1, pp. 129–143 (2020).

[24] M. N. Alam, "Performance analysis of low-complexity blind signature protocols with modular arithmetic," *Journal of Discrete Mathematical Sciences and Cryptography,* vol. 22, no. 3, pp. 545–559 (2019).

Received January, 2025