Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2026, Volume 32, Number 1, 96–111
DOI: 10.7546/nntdm.2026.32.1.96-111

Determinant-preserving blind signatures from Hadamard-type t-Jacobsthal–Leonardo sequences

Elahe Mehraban [1,*], **Reza Ebrahimi Atani** [2],
Ömür Deveci [3] **and Ghadir Golkarian** [4]

[1] Mathematics Research Center, Near East University TRNC
Mersin 10, 99138 Nicosia, Türkiye
e-mail: e.mehraban.math@gmail.com

[2] Department of Computer Engineering, Faculty of Engineering, University of Guilan
Rasht, Iran
e-mail: rebrahimi@guilan.ac.ir

[3] Department of Mathematics, Faculty of Science and Letters, Kafkas University
36100 Kars, Türkiye
e-mail: odeveci36@hotmail.com

[4] Art & Sciences Faculty, Eurasia Reserach Center, Near East University
Lefkosia, Cyprus
e-mail: ghadir.golkarian@neu.edu.tr

* *Corresponding author*

Received: 4 October 2025 **Revised:** 17 February 2026
Accepted: 22 February 2026 **Online First:** 24 February 2026

Abstract: In this paper, we introduce a new class of sequences called the termed Hadamard-type t-Jacobsthal Leonardo sequence which is generated by applying a Hadamard-type product to the characteristic polynomials of the t-Jacobsthal and Leonardo sequences. We derive fundamental algebraic properties of these sequences including determinant formulas, combinatorial identities, and exponential representations, and building on these mathematical results, we construct a novel blind signature scheme in which the public and secret keys are represented as companion matrices derived from the new sequences. The proposed scheme ensures correctness through determinant-preserving transformations and achieves blindness and unforgeability under matrix-based key assumptions. We provide security analysis within the standard cryptographic framework and discuss efficiency aspects compared with existing blind signature constructions. Our results demonstrate that Hadamard-type t-Jacobsthal–Leonardo matrices can serve as a new algebraic foundation for cryptographic protocols, thereby linking structured number-theoretic sequences with provably secure digital signature mechanisms.

Keywords: Jacobsthal sequence, Leonardo sequence, Blind signature.
2020 Mathematics Subject Classification: 11K31, 11C20, 68P25, 68R01, 68P30, 15A15.

1 Introduction

Blind signatures, introduced by Chaum [11], are a fundamental cryptographic primitive that enables a signer to authenticate a message without learning its content. This property has made blind signatures central to privacy-preserving applications such as electronic voting, anonymous credentials, and untraceable digital cash and payments. Over the past decades, numerous constructions have been proposed, ranging from RSA-based blind signatures [12, 26, 28] to identity-based and lattice-based schemes [17–20, 25, 34]. In [12], an identity-based restrictive partially blind signature scheme was proposed and shown to be provably secure in the random oracle model. A direct construction of an identity-based blind signature scheme was presented in [23], offering computational efficiency due to its short signature length. In [26], the authors proposed a scheme that applies the Fibonacci, Lucas, and Fibonacci–Lucas matrix coding to quantum digital signatures, leveraging a recently developed quantum key distribution (QKD) system. The main research directions have focused on improving security guarantees, computational efficiency, and resistance to quantum adversaries.

Beyond classical RSA-based constructions, researchers have explored stronger blind signature schemes. For example, cascade blind factors were introduced in [33] to increase resistance against forgery attacks. Studies on Lehmer–Pierce sequences [36] highlight how number-theoretic recurrences may share algebraic vulnerabilities, which is relevant for designing secure cryptographic primitives. On the other hand, provably secure blind signature schemes have been developed within formal frameworks, such as the partially blind signatures of Abe and Okamoto [1] and subsequent refinements [8], which emphasize rigorous security models. More recently, Lysyanskaya [27] has provided modern security analyses of RSA-based blind signatures, reinforcing the importance of precise unforgeability and blindness definitions.

Parallel to these developments, number-theoretic sequences have emerged as a source of structured algebraic constructions for cryptographic primitives. For example, Fibonacci and Lucas sequences have been applied to digital signatures and key distribution [29, 30]. Such approaches exploit the algebraic properties of recurrence relations and companion matrices to construct deterministic yet hard-to-invert transformations, which are attractive for cryptographic use.

In this work, we extend this line of research by introducing the Hadamard-type t-Jacobsthal–Leonardo sequences, obtained through a Hadamard-type product of the characteristic polynomials of t-Jacobsthal and Leonardo sequences. These sequences possess rich algebraic properties, including closed-form determinants and exponential generating functions, which make them suitable candidates for cryptographic constructions.

The Jacobsthal sequence $\{J_n\}$ is

$$J_n = J_{n-1} + 2J_{n-2},\ n \geq 0,$$

with $J_0 = 0$ and $J_1 = 1$ [22]. One of the generalizations of this sequence is For $t \geq 3$, the t-Jacobsthal sequence $\{J_n(t)\}_{n=0}^{\infty}$ is

$$J_n(t) = J_{n-1}(t) + 2J_{n-2}(t) + \cdots + J_{n-t}(t),\ n \geq t,$$

with $J_0(t) = J_1(t) = \cdots = J_{t-2}(t) = 0$ and $J_{t-1}(t) = 1$.

This sequence has been generalized in various directions, leading to structures with rich algebraic properties. These generalized sequences have been extensively studied in the context of matrix theory and group constructions [7, 13, 15]. The Gaussian Jacobsthal and Gaussian Jacobsthal– Lucas polynomials are discussed in [6]. Further developments in [31] explored the d-Gaussian Jacobsthal and d-Gaussian Jacobsthal–Lucas polynomials, along with their matrix representations. A broader generalization, known as the k-Jacobsthal numbers, was presented in [21]. Additionally, the Jacobsthal–Padovan p-sequences within group settings were discussed in [2].

The Leonardo sequence (see [10, 16, 24]) has also been studied recently, and it is defined as follows:

The Leonardo sequence is

$$Le(n) = Le(n-1) - Le(n-2) + 1,\ n \geq 2,$$

with $Le(0) = Le(1) = 1$. Also, another recurrence relation for Leonardo sequences exists as follows:

$$Le(n+1) = 2Le(n) - Le(n-2),\ n \geq 2,$$

(see [5, 35]). The characteristic polynomials of the t-Jacobsthal and Leonardo sequence are $x^t - x^{t-1} - 2x^{t-2} - x^{t-3} - \cdots - 1$ and $x^3 - 2x^2 + 1$, respectively.

Leonardo numbers were studied in [9]. In [14], the Jacobsthal–Padovan p-sequences are studied and some of their properties. In 2021, using the Binet formula for Leonardo numbers, new identities involving these numbers were established in [4]. A generalization of the Leonardo numbers was proposed in [5], where infinite lower triangular matrices with Leonardo number entries were also defined. In [32], the Gaussian Leonardo numbers were investigated, leading to the introduction of new families of these Gaussian forms. In this work, we introduce a new sequence based on the Leonardo and t-Jacobsthal sequences.

The Hadamard-type product of polynomials f and g is defined as follows [3].

Definition 1.1. *The Hadamard-type product of polynomials f and g is $f * g = \sum_{i=0}^{\infty}(a_i * b_i)x^i$ where*

$$a_i * b_i = \begin{cases} a_ib_i, & \text{if } a_ib_i \neq 0, \\ a_i + b_i, & \text{if } a_ib_i = 0, \end{cases}$$

and $f(x) = a_mx^m + \cdots + a_1x + a_0$ and $g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$.

Our main contribution is a blind signature scheme built on these new sequences. Specifically:

- We define the Hadamard-type t-Jacobsthal–Leonardo sequences and establish their companion matrices.
- We prove algebraic properties such as determinant preservation, which we exploit for signature verification.
- We design a blind signature protocol in which keys are represented as structured matrices, and correctness is guaranteed by determinant invariance.
- We analyze the scheme's security in terms of blindness, unforgeability, and resistance to forgery under matrix inversion assumptions.
- We discuss the computational aspects of the scheme and its relation to existing blind signature constructions.

This paper thereby bridges mathematical sequence theory with practical cryptographic design, contributing both to the development of generalized number sequences and to privacy-preserving digital signature mechanisms. The remainder of this paper is organized as follows. In Section 2, we introduce the Hadamard-type t-Jacobsthal–Leonardo sequences and establish several related results. In Section 3, we present a new blind signature scheme based on these sequences and in Section 4 we analyze its security. Finally the paper is concluded in Section 5.

2 The Hadamard-type t-Jacobsthal–Leonardo sequences

In this section, we define a new class of sequences by applying the Hadamard-type product to the characteristic polynomials of the t-Jacobsthal and Leonardo sequences.

Let us consider the case where $t = 3$. Using the characteristic polynomials of the 3-Jacobsthal and Leonardo sequences, along with Definition 1.1, we define the Hadamard-type product of these polynomials as follows:

Definition 2.1. *For integers $t=3$, the Hadamard-type 3-Jacobsthal–Leonardo sequences, denoted by $\{JL_n(3)\}_0^{\infty}$, are defined as*

$$JL_n(3) = -2JL_{n-1}(3) + 2JL_{n-2}(3) + JL_{n-3}(3),\ n \geq 0, \tag{1}$$

with initial conditions $JL_0(3) = JL_1(3) = 0$ and $JL_2(3) = 1$.

The Hadamard-type 3-Jacobsthal–Leonardo sequences have the following companion matrix

$$\tau(3) = \begin{bmatrix} -2 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \tag{2}$$

and is called the Hadamard-type 3-Jacobsthal–Leonardo matrix.

Theorem 2.1. *For $n \geq 3$, we have*

$$(\tau(3))^n = \begin{bmatrix} JL_{n+2}(3) & JL_{n+1}(3) + JL_n(3) & JL_{n+1}(3) \\ JL_{n+1}(3) & JL_n(3) + JL_{n-1}(3) & JL_n(3) \\ JL_n(3) & JL_{n-1}(3) + JL_{n-2}(3) & JL_{n-1}(3) \end{bmatrix},$$

Proof. We use induction on n. For $n = 3$ we have

$$(\tau(3))^3 = \begin{bmatrix} 13 & 7 & 5 \\ 5 & 3 & 2 \\ 2 & 1 & 1 \end{bmatrix} = \begin{bmatrix} JL_5(3) & JL_4(3) + JL_3(3) & JL_4(3) \\ JL_4(3) & JL_3(3) + JL_2(3) & JL_3(3) \\ JL_3(3) & JL_2(3) + JL_1(3) & JL_2(3) \end{bmatrix},$$

so the statement holds. Now, assume that the statement holds for $n = t$. Therefore, for $n = t + 1$ we have

$$\begin{aligned}(\tau(2))^{t+1} &= \begin{bmatrix} -2 & 2 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} JL_{t+2}(3) & JL_{t+1}(3) + JL_t(3) & JL_{t+1}(3) \\ JL_{t+1}(3) & JL_t(3) + JL_{t-1}(3) & JL_t(3) \\ JL_t(3) & JL_{t-1}(3) + JL_{t-2}(3) & JL_{t-1}(3) \end{bmatrix} \\ &= \begin{bmatrix} JL_{t+3}(3) & JL_{t+2}(3) + JL_{t+1}(3) & JL_{t+2}(3) \\ JL_{t+2}(3) & JL_{t+1}(3) + JL_t(3) & JL_{t+1}(3) \\ JL_{t+1}(3) & JL_t(3) + JL_{t-1}(3) & JL_t(3) \end{bmatrix},\end{aligned}$$

which completes the proof. □

Lemma 2.1. *Let $h(x)$ be the generating function of the Hadamard-type 3-Jacobsthal and Leonardo sequences. Then*

$$g(x) = \frac{x^2}{1 + 2x - 2x^2 - x^3}. \tag{3}$$

Proof. We have

$$\begin{aligned} h(x) &= \sum_{n=1}^{\infty} JL_n(3)x^n \\ &= JL_1(3)x^1 + JL_2(3)x^2 + \sum_{n=3}^{\infty} JL_n(3)x^n \\ &= JL_2(3)x^2 + \sum_{n=3}^{\infty} -2JL_{n-1}(3) + 2JL_{n-2}(3) + JL_{n-3}(3)x^n \\ &= x^2 - 2\sum_{n=3}^{\infty} JL_{n-1}(3)x^n + 2\sum_{n=3}^{\infty} JL_{n-2}(3)x^n + \sum_{n=3}^{\infty} JL_{n-3}(3)x^n \\ &= x^2 - 2x\sum_{n=1}^{\infty} JL_n(3)x^n + 2x^2\sum_{n=1}^{\infty} JL_n(3)x^n + x^3\sum_{n=1}^{\infty} JL_n(3)x^n \\ &= x^2 - 2xh(x) + 2x^2h(x) + x^3h(x). \end{aligned}$$

□

Theorem 2.2. *The Hadamard-type 3-Jacobsthal and Leonardo sequences $\{JL_n(3)\}$ have the following exponential representation*

$$g(x) = x^2 \exp\sum_{i=1}^{\infty} \frac{(x)^i}{i}(-2 + 2x + x^2)^i.$$

Proof. Using (3), we have

$$\ln h(x) = \ln x^2 - \ln(1 - 2x + 2x^2 + x^3).$$

Since

$$\begin{aligned} - \ln\left(1 - 2x + 2x^2 + x^3\right) &= -\Big[- x(2 - 2x - x^2) - \frac{1}{2}x^2(2 - 2x - x^2)^2 \\ &\qquad - \cdots - \frac{1}{i}x^i(2 - 2x - x^2)^i - \cdots \Big] \\ &= \sum_{i=1}^{\infty} \frac{(x)^i}{i}(2 - 2x - x^2)^i, \end{aligned}$$

the result follows. □

Corollary 2.1. *For $n \geq 3$, we have* $\det \tau(3)^n = 1$.

Proof. From (2), $\det \tau(3) = 1$, then $\det \tau(3)^n = 1$. □

Now, consider $t = 4$. By the characteristic polynomials of 4-Jacobsthal and Leonardo sequences and Definition 1.1, we define the Hadamard-type product of the characteristic polynomials of 4-Jacobsthal and Leonardo sequences as follows.

Definition 2.2. *For integer $t = 4$, the Hadamard-type 4-Jacobsthal–Leonardo sequences, denoted by $\{JL_n(4)\}_0^{\infty}$, are defined as*

$$JL_n(4) = JL_{n-1}(4) - 4JL_{n-2}(4) + JL_{n-3}(4) + JL_{n-4}(4),\ n \geq 0, \tag{4}$$

with initial conditions $JL_0(4) = JL_1(4) = JL_2(4) = 0$ and $JL_3(4) = 1$.

The Hadamard-type 4-Jacobsthal–Leonardo sequences have the following companion matrix

$$\tau(3) = \begin{bmatrix} 1 & -4 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, \tag{5}$$

which is called the Hadamard-type 4-Jacobsthal–Leonardo matrix.

Theorem 2.3. *For $n \geq 4$, we have*

$$(\tau(4))^n = \begin{bmatrix} JL_{n+3}(4) & JL_{n+4}(4) - JL_{n+3}(4) & JL_{n+2}(4) + JL_{n+1}(4) & JL_{n+2}(4) \\ JL_{n+2}(4) & JL_{n+3}(4) - JL_{n+2}(4) & JL_{n+1}(4) + JL_n(4) & JL_{n+1}(4) \\ JL_{n+1}(4) & JL_{n+2}(4) - JL_{n+1}(4) & JL_n(4) + JL_{n-1}(4) & JL_n(4) \\ JL_n(4) & JL_{n+1}(4) - JL_n(4) & JL_{n-1}(4) + JL_{n-2}(4) & JL_{n-1}(4) \end{bmatrix}.$$

Proof. We use induction on n. For $n = 4$ we have

$$(\tau(4))^4 = \begin{bmatrix} 8 & 22 & -9 & -6 \\ -6 & 14 & -2 & -3 \\ -3 & -3 & 2 & 1 \\ 1 & -4 & 1 & 1 \end{bmatrix} = \begin{bmatrix} JL_7(4) & JL_8(4) - JL_7(4) & JL_6(4) + JL_5(4) & JL_6(4) \\ JL_6(4) & JL_7(4) - JL_6(4) & JL_5(4) + JL_4(4) & JL_5(4) \\ JL_5(4) & JL_6(4) - JL_5(4) & JL_4(4) + JL_3(4) & JL_4(4) \\ JL_4(4) & JL_5(4) - JL_4(4) & JL_3(4) + JL_2(4) & JL_3(4) \end{bmatrix},$$

so the statement holds. Now, assume that the statement holds for $n = s$. Therefore, for $n = s + 1$ we have

$$\begin{aligned}(\tau(4))^{s+1} &= \begin{bmatrix}1 & -4 & 1 & 1\\ 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix} \times \begin{bmatrix} JL_{s+3}(4) & JL_{s+4}(4)-JL_{s+3}(4) & JL_{s+2}(4)+JL_{s+1}(4) & JL_{s+2}(4)\\ JL_{s+2}(4) & JL_{s+3}(4)-JL_{s+2}(4) & JL_{s+1}(4)+JL_{s}(4) & JL_{s+1}(4)\\ JL_{s+1}(4) & JL_{s+2}(4)-JL_{s+1}(4) & JL_{s}(4)+JL_{s-1}(4) & JL_{s}(4)\\ JL_{s}(4) & JL_{s+1}(4)-JL_{s}(4) & JL_{s-1}(4)+JL_{s-2}(4) & JL_{s-1}(4)\end{bmatrix}\\ &= \begin{bmatrix} JL_{s+4}(4) & JL_{s+5}(4)-JL_{s+4}(4) & JL_{s+3}(4)+JL_{s+2}(4) & JL_{s+3}(4)\\ JL_{s+3}(4) & JL_{s+4}(4)-JL_{s+3}(4) & JL_{s+2}(4)+JL_{s+1}(4) & JL_{s+2}(4)\\ JL_{s+2}(4) & JL_{s+3}(4)-JL_{s+2}(4) & JL_{s+1}(4)+JL_{s}(4) & JL_{s+1}(4)\\ JL_{s+1}(4) & JL_{s+2}(4)-JL_{s+1}(4) & JL_{s}(4)+JL_{s-1}(4) & JL_{s}(4)\end{bmatrix},\end{aligned}$$

which completes the proof. □

Lemma 2.2. *Let $g(x)$ be the generating function of the Hadamard-type 4-Jacobsthal and Leonardo sequences. Then*

$$g(x) = \frac{x^3}{1 - x + 4x^2 - x^3 - x^4}. \tag{6}$$

Proof. We have

$$\begin{aligned} g(x) &= \sum_{n=1}^{\infty} JL_n(4)x^n\\ &= JL_1(4)x^1 + JL_2(4)x^2 + JL_3(4)x^3 + \sum_{n=4}^{\infty} JL_n(4)x^n\\ &= JL_3(4)x^3 + \sum_{n=4}^{\infty} JL_{n-1}(4) - 4JL_{n-2}(4) + JL_{n-3}(4) + JL_{n-4}(4)x^n\\ &= x^3 + \sum_{n=4}^{\infty} JL_{n-1}(4)x^n - 4\sum_{n=4}^{\infty} JL_{n-2}(4)x^n + \sum_{n=4}^{\infty} JL_{n-3}(4)x^n + \sum_{n=4}^{\infty} JL_{n-4}(4)x^n\\ &= x^3 + x\sum_{n=1}^{\infty} JL_n(4)x^n - 4x^2\sum_{n=1}^{\infty} JL_n(4)x^n + x^3\sum_{n=1}^{\infty} JL_n(4)x^n + x^4\sum_{n=1}^{\infty} JL_n(4)x^n\\ &= x^3 + xg(x) - 4x^2g(x) + x^3g(x) + x^4g(x). \end{aligned}$$

□

Theorem 2.4. *The Hadamard-type 4-Jacobsthal and Leonardo sequences $\{JL_n(4)\}$ have the following exponential representation*

$$g(x) = x^3 \exp\sum_{i=1}^{\infty} \frac{(x)^i}{i}(1 - 4x + x^2 + x^3)^i.$$

Proof. Using (6), we have

$$\ln g(x) = \ln x^3 - \ln(1 - x + 4x^2 - x^3 - x^4).$$

Since

$$\begin{aligned} -\ln\left(1 - x + 4x^2 - x^3 - x^4\right) &= -\Big[- x(1 - 4x + x^2 + x^3) - \frac{1}{2}x^2(1 - 4x + x^2 + x^3)^2\\ &\qquad - \cdots - \frac{1}{i}x^i(1 - 4x + x^2 + x^3)^i - \cdots\Big]\\ &= \sum_{i=1}^{\infty} \frac{(x)^i}{i}(1 - 4x + x^2 + x^3)^i, \end{aligned}$$

the result follows. □

Corollary 2.2. *For $n \geq 4$, we have $\det\tau(4)^n = (-1)^n$.*

Proof. From (5), $\det\tau(4) = -1$, then $\det\tau(4)^n = (-1)^n$. □

3 Blind signatures using the Hadamard-type t-Jacobsthal–Leonardo matrix

In this section, we present a new blind signature using Hadamard-type t-Jacobsthal–Leonardo matrix and the security is studied. We now introduce the new blind signature.

In the algorithm, Alice is requesting the signature, Bob is the blind signer, and Charlie verifies the signature. Alice and Bob, Alice and Charlie, and Bob and Charlie establish the keys K_{AB}, K_{AC} and K_{BC}, respectively. These keys belong to the Hadamard-type 3-Jacobsthal–Leonardo matrix. The algorithm is conducted over classical channels.

Alice takes a message M which is a matrix $M = (m_{ij})_{3\times 3} 1 \leq i, j \leq 3$, and obtains the blind message $M' = M \times K_{AC}$. Alice encrypts the blind message M' with the key K_{AB} and gets $M'' = M' \times K_{AB}$. This is sent to Bob and the determinant of M is sent to Charlie. Then Bob uses K_{AB} to obtain $M' = \times M'' \times K_{AB}^{-1}$. He gets signature $S = M' \times K_{BC}$, and sends it Charlie. Charlie calculates the determinant of S. If $\det S = \det M$, he accepts the signature, otherwise he rejects it.

Algorithm

Alice requests the signature, Bob provides the blind signature, and Charlie verifies the signature. Alice and Bob, Alice and Charlie, and Bob and Charlie establish the keys K_{AB}, K_{AC} and K_{BC}, respectively. These keys are elements of $\tau(3)^n$. The algorithm steps are given below and illustrated in Fig. 1.

1. Alice takes a message $M = (m_{ij})_{3\times 3} 1 \leq i, j \leq 3$ and gets the blind message $M' = M \times K_{AC}$. Alice encrypts the blind message M' with the key K_{AB} and obtains $M'' = M' \times K_{AB}$. This is sent to Bob and the determinant of M is sent to Charlie.

2. Using K_{AB}, Bob obtains $M' = M'' \times K_{AB}^{-1}$.
   Then he gets the signature $S = M' \times K_{BC}$, and sends it to Charlie.

3. Charlie calculates the determinant of S.
   If $\det S = \det M$, he accepts the signature, otherwise he rejects it.

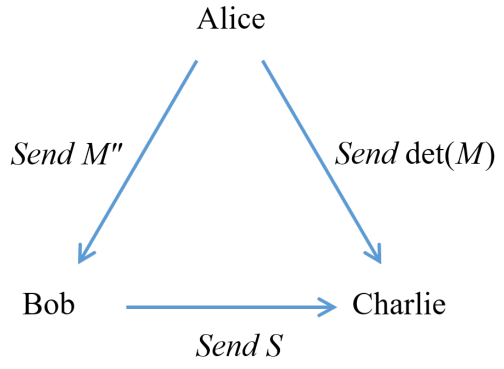

Figure 1. Scheme of the algorithim.

From Corollary 2.1, we have $\det(\tau(3)^n) = 1$. The verification is

$$\det S = \det(M^{'}) \times \det(K_{BC}) = \det(M) \times \det(K_{AC}) = \det M.$$

For $t = 4$, the algorithm is similar, only is used $\tau(4)^n$ instead of $\tau(3)^n$ and message M which is a matrix $M = (m_{ij})_{4\times 4} 1 \leq i, j \leq 4$. For the verification process, according to Corollary 2.2, the signature is accepted if $\det S = \pm \det M$; otherwise, it is rejected.

Example 3.1. i. Consider the keys K_{AB}, K_{AC}, and K_{BC}, and M as follows

$$\tau(3)^4 = \begin{bmatrix} 40 & -24 & -15 \\ -15 & 10 & 6 \\ 6 & -3 & -2 \end{bmatrix} := K_{AB},$$

$$\tau(3)^7 = \begin{bmatrix} -714 & 442 & 273 \\ 273 & -168 & -104 \\ -104 & 65 & 40 \end{bmatrix} := K_{AC}$$

$$\tau(3)^8 = \begin{bmatrix} 1870 & -1155 & -714 \\ -714 & 442 & 273 \\ 273 & -168 & -104 \end{bmatrix} := K_{BC}$$

and

$$M = \begin{bmatrix} 1 & 5 & 8 \\ 9 & 1 & 4 \\ 4 & 3 & 2 \end{bmatrix}.$$

Alice computes $M^{'}$ as

$$M^{'} = M \times K_{AC} = \begin{bmatrix} 1 & 5 & 8 \\ 9 & 1 & 4 \\ 4 & 3 & 2 \end{bmatrix} \times \begin{bmatrix} -714 & 442 & 273 \\ 273 & -168 & -104 \\ -104 & 65 & 40 \end{bmatrix} = \begin{bmatrix} -181 & 122 & 73 \\ -6569 & 4070 & 2513 \\ -2245 & 1394 & 860 \end{bmatrix}.$$

and encrypts the blind message $M^{'}$ with the key K_{AB} to obtain

$$\begin{aligned} M^{''} = M^{'} \times K_{AB} &= \begin{bmatrix} -181 & 122 & 73 \\ -6569 & 4070 & 2513 \\ -2245 & 1394 & 860 \end{bmatrix} \times \begin{bmatrix} 40 & -24 & -15 \\ -15 & 10 & 6 \\ 6 & -3 & -2 \end{bmatrix} \\ &= \begin{bmatrix} -8632 & 5345 & 3301 \\ -308732 & 190817 & 117929 \\ -105550 & 65240 & 40319 \end{bmatrix}. \end{aligned}$$

She sends this to Bob and sends $\det M = 164$ to Charlie. Using K_{AB}, Bob obtains

$$\begin{aligned} M^{'} = M^{''} \times K_{AB}^{-1} &= \begin{bmatrix} -8632 & 5345 & 3301 \\ -308732 & 190817 & 117929 \\ -105550 & 65240 & 40319 \end{bmatrix} \times \begin{bmatrix} -2 & -3 & 6 \\ 6 & 10 & -15 \\ -15 & -24 & 40 \end{bmatrix} \\ &= \begin{bmatrix} -181 & 122 & 73 \\ -6569 & 4070 & 2513 \\ -2245 & 1394 & 860 \end{bmatrix}. \end{aligned}$$

Then he gets the signature

$$S = M^{'} \times K_{BC} = \begin{bmatrix} -181 & 122 & 73 \\ -6569 & 4070 & 2513 \\ -2245 & 1394 & 860 \end{bmatrix} \times \begin{bmatrix} 1870 & -1155 & -714 \\ -714 & 442 & 273 \\ 273 & -168 & -104 \end{bmatrix}$$

$$= \begin{bmatrix} -405649 & 250715 & 154948 \\ -14503961 & 8963951 & 5540024 \\ -4958686 & 3064643 & 1894052 \end{bmatrix},$$

and sends it to Charlie. For verification, Charlie computes $\det S = 164$. Since $\det M = \det S$, he accepts a signature.

ii. Consider the keys K_{AB}, K_{AC}, and K_{BC}, and M as follows

$$\tau(4)^4 = \begin{bmatrix} 8 & 22 & -9 & -6 \\ -6 & 14 & -2 & -3 \\ -3 & -3 & 2 & 1 \\ 1 & -4 & 1 & 1 \end{bmatrix} := K_{AB},$$

$$\tau(4)^6 = \begin{bmatrix} -11 & -118 & 38 & 30 \\ 30 & -41 & 2 & 8 \\ 8 & 22 & -9 & -6 \\ -6 & 14 & -2 & -3 \end{bmatrix} := K_{AC}$$

$$\tau(4)^8 = \begin{bmatrix} -47 & 535 & -140 & -129 \\ -129 & 82 & 19 & -11 \\ -11 & -118 & 38 & 30 \\ 30 & -41 & 2 & 8 \end{bmatrix} := K_{BC}$$

and

$$M = \begin{bmatrix} 4 & 5 & 2 & 1 \\ 7 & 9 & 8 & 1 \\ 9 & 3 & 1 & 0 \\ 0 & 1 & 4 & 5 \end{bmatrix}.$$

Alice computes $M^{'}$ as

$$M^{'} = M \times K_{AC} = \begin{bmatrix} 4 & 5 & 2 & 1 \\ 7 & 9 & 8 & 1 \\ 9 & 3 & 1 & 0 \\ 0 & 1 & 4 & 5 \end{bmatrix} \times \begin{bmatrix} -11 & -118 & 38 & 30 \\ 30 & -41 & 2 & 8 \\ 8 & 22 & -9 & -6 \\ -6 & 14 & -2 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} 116 & -619 & 142 & 145 \\ 245 & -991 & 208 & 228 \\ -1 & -1163 & 339 & 288 \\ 32 & 117 & -44 & -31 \end{bmatrix}.$$

and encrypts the blind message $M^{'}$ with the key K_{AB} to obtain

$$M^{''} = M^{'} \times K_{AB} = \begin{bmatrix} 116 & -619 & 142 & 145 \\ 245 & -991 & 208 & 228 \\ -1 & -1163 & 339 & 288 \\ 32 & 117 & -44 & -31 \end{bmatrix} \times \begin{bmatrix} 8 & 22 & -9 & -6 \\ -6 & 14 & -2 & -3 \\ -3 & -3 & 2 & 1 \\ 1 & -4 & 1 & 1 \end{bmatrix}$$
$$= \begin{bmatrix} 4361 & -7120 & 623 & 1448 \\ 7510 & -10020 & 421 & 1939 \\ 6241 & -18473 & 3301 & 4122 \\ -345 & 2598 & -641 & -618 \end{bmatrix}.$$

She sends this to Bob and sends $\det M = 664$ to Charlie. Using K_{AB}, Bob obtains

$$M^{'} = M^{''} \times K_{AB}^{-1} = \begin{bmatrix} 4361 & -7120 & 623 & 1448 \\ 7510 & -10020 & 421 & 1939 \\ 6241 & -18473 & 3301 & 4122 \\ -345 & 2598 & -641 & -618 \end{bmatrix} \times \begin{bmatrix} 1 & -1 & 4 & -1 \\ -1 & 2 & -5 & 5 \\ 5 & -6 & 22 & -10 \\ -10 & 15 & -46 & 32 \end{bmatrix}$$
$$= \begin{bmatrix} 116 & -619 & 142 & 145 \\ 245 & -991 & 208 & 228 \\ -1 & -1163 & 339 & 288 \\ 32 & 117 & -44 & -31 \end{bmatrix}.$$

Then he gets the signature

$$S = M^{'} \times K_{BC} = \begin{bmatrix} 116 & -619 & 142 & 145 \\ 245 & -991 & 208 & 228 \\ -1 & -1163 & 339 & 288 \\ 32 & 117 & -44 & -31 \end{bmatrix} \times \begin{bmatrix} -47 & 535 & -140 & -129 \\ -129 & 82 & 19 & -11 \\ -11 & -118 & 38 & 30 \\ 30 & -41 & 2 & 8 \end{bmatrix}$$
$$= \begin{bmatrix} -19580 & 16845 & 1602 & -2759 \\ -32129 & 19489 & 5000 & -2510 \\ -33895 & 59291 & -5991 & -12232 \\ 2992 & -9975 & 1908 & 2253 \end{bmatrix},$$

and sends it to Charlie. For verification, Charlie computes $\det S = 664$. Since $\det M = \det S$, he accepts a signature.

4 Security analysis

In this section, we analyze the security of the proposed blind signature scheme according to the standard notions of blindness and unforgeability introduced in [1, 8], and more recently revisited in [27]. These properties are the cornerstone of blind signature protocols and are evaluated in both classical and modern frameworks [27]. Our analysis also introduces a new hardness assumption, the *Determinant Invariance Problem*, which underpins the security of our construction. For comparison, we note that cascade blind signatures [33] and RSA-based variants [27] follow similar formalization patterns. While our analysis is algebraic and determinant-based, the design goals parallel those in formal models of blind signature security. Furthermore, cascade-based strengthening techniques [33] represent another line of defense against forgery, complementing our determinant-preserving approach. At the same time, results such as [36] remind us that number-theoretic sequences may have hidden structural weaknesses, and thus the robustness of our Hadamard-type constructions deserves further scrutiny under more advanced attack models.

4.1 Security model

A blind signature scheme must satisfy two primary properties:

- **Blindness:** The signer should not be able to link a signature to the specific message for which it was requested, even if later shown the message-signature pair.
- **Unforgeability:** No probabilistic polynomial time adversary should be able to generate a valid signature on a new message without interacting with the legitimate signer.

Our scheme additionally benefits from *determinant-preservation*, which provides a simple algebraic invariant for verification.

4.2 Determinant Invariance Problem (DIP)

We introduce the Determinant Invariance Problem (DIP) in which the foundation of our scheme is based on its complex computational problem: Given a random invertible Hadamard-type t-Jacobsthal Leonardo matrix $\tau(t)^n$ and a message matrix M, it is computationally infeasible to produce a forged matrix S such that

$$\det(S) = \det(M)$$

without knowledge of the secret key matrices K_{AB}, K_{AC}, K_{BC}. This problem is analogous to classical hardness assumptions such as integer factorization (RSA) or the Short Integer Solution problem (SIS) in lattice-based schemes. The algebraic complexity of number-theoretic recurrences has been studied in the context of Lehmer–Pierce sequences [36], where structural vulnerabilities can emerge. In contrast, our construction relies on determinant invariance, which resists trivial algebraic inversions.

Unforgeability. To forge a valid signature, an attacker must correctly guess both the key K_{BC} and the message M. Suppose an adversary attempts to forge a signature on a message M without querying the signer. Verification requires that $\det(S) = \det(M)$. The adversary must therefore either:

1. guess the correct key K_{BC}, or
2. construct a forged M' consistent with the hidden transformations while preserving the determinant.

Both cases reduce to solving the DIP, which we assume infeasible. Compared to cascade blind signatures [36], where multiple blinding factors increase robustness, our scheme achieves security through structured determinant invariance.

Blindness. The proposed scheme ensures that Bob (the signer) can sign a message without learning its content. During the protocol, Bob observes only the blinded message $M'' = M' \times K_{AB}$, where $M' = M \times K_{AC}$. Since K_{AC} is secret and independent, Bob cannot derive M from M'' without solving DIP. Thus, blindness holds by semantic independence of the masking transformations. This definition aligns with the indistinguishability based blindness games introduced in [1, 8].

Repudiation Resistance. Charlie (the verifier) checks signatures using only determinant equality. Charlie verifies the signature using the determinant condition $\det(S) = \pm \det(M)$. If the condition holds, it confirms that Bob created the signature. Once a signature is validated, neither Alice (the requester) nor Bob (the signer) can repudiate their role in the transaction. This property is consistent with binding mechanisms analyzed in the RSA-based framework of [27].

Error Detection and Correction. Matrix-based encodings inherently support redundancy. Similar to Fibonacci-based error correction techniques achieving 99.8% reliability [30], our structured companion matrices provide error detection and correction capability. A similar approach can be applied here, resulting in equivalent error detection and correction performance.

Comparison with Related Work. Our determinant-based approach complements cascade blinding techniques [33] and highlights resilience against algebraic collapse, which has been observed in sequence-based cryptography [36]. While formal models of blindness and unforgeability [1, 8] serve as the benchmark for provable security, our construction provides a new algebraic foundation. Moreover, modern analyses such as [27] stress the importance of clearly defined hardness assumptions, which we provide via DIP.

5 Conclusions

In this work, we introduced the Hadamard-type t-Jacobsthal–Leonardo sequences and investigated their algebraic properties, including determinant invariance, companion matrices, and exponential generating functions. Building on these results, we proposed a blind signature scheme in which signing and verification are expressed through structured matrix transformations derived from these sequences. This construction demonstrates a novel connection between number-theoretic recurrences and privacy-preserving digital signature protocols. Generalizing the construction to Hadamard-type t-Jacobsthal–Leonardo sequences for $t \geq 5$ may yield richer algebraic structures and potentially stronger cryptographic primitives.

References

[1] Abe, M., & Okamoto, T. (2000). Provably secure partially blind signatures. In: Bellare, M. (Ed.), *Advances in Cryptology – CRYPTO 2000*, Santa Barbara, California, USA (LNCS Vol. 1880, pp. 271–286). Springer.

[2] Aküzüm, Y., & Deveci, Ö. (2017). On the Jacobsthal–Padovan p-sequences in groups. *Topology and Its Applications*, 5, 63–66.

[3] Aküzüm, Y., & Deveci, Ö. (2020). The Hadamard-type k-step Fibonacci sequences in groups. *Communications in Algebra*, 48(7), 2844–2856.

[4] Alp, Y., & Koçer, E. G. (2021). Some properties of Leonardo numbers. *Konuralp Journal of Mathematics*, 9(1), 183–189.

[5] Alp, Y., & Koçer, E. G. (2024). Leonardo and hyper-Leonardo numbers via Riordan arrays. *Ukrainian Mathematical Journal*, 76(3), 326–340.

[6] Asci, M., & Gurel, E. (2013). Gaussian Jacobsthal and Gaussian Jacobsthal Lucas polynomials. *Notes on Number Theory and Discrete Mathematics*, 19(1), 25–36.

[7] Bród, D., & Michalski, A. (2022). On generalized Jacobsthal and Jacobsthal–Lucas numbers. *Annales Mathematicae Silesianae*, 36(2), 115–128.

[8] Camenisch, J., & Lysyanskaya, A. (2003). A signature scheme with efficient protocols. In: *Security in Communication Networks (SCN 2002)* (LNCS Vol. 2576, pp. 268–289). Springer.

[9] Catarino, P., & Borges, A. (2019). On Leonardo numbers. *Acta Mathematica Universitatis Comenianae*, 89(1), 75–86.

[10] Catarino, P., & Borges, A. (2020). A note on incomplete Leonardo numbers. *Integers*, 20, Article 43.

[11] Chaum, D. (1983). Blind signatures for untraceable payments. In: Chaum, D., Rivest, R. L. & Sherman, A. T. (Eds.), *Advances in Cryptology* (pp. 199–203). Springer.

[12] Chen, W., Qin, B., Wu, Q., Zhang, L., & Zhang, H. (2009). ID-based partially blind signatures: A scalable solution to multi-bank e-cash. In: *Proceedings of the International Conference on Signal Processing Systems*, Singapore (pp. 433–437).

[13] Daşdemir, A. (2012). On the Jacobsthal numbers by matrix method. *SDU Journal of Science*, 7(1), 69–76.

[14] Deveci, Ö. (2019). The Jacobsthal–Padovan p-sequences and their applications. *Proceedings of the Romanian Academy, Series A, 20*(3), 215–224.

[15] Deveci, Ö., & Karaduman, E. (2012). The cyclic groups via the Pascal matrices and generalized Pascal matrices. *Linear Algebra and Its Applications*, 473, 2538–2545.

[16] dos Santos Mangueira, M. C., Vieira, R. P. M., Alves, F. R. V., & Catarino, P. M. M. C. (2022). Leonardo's bivariate and complex polynomials. *Notes on Number Theory and Discrete Mathematics*, 28(1), 115–123.

[17] Ebrahimi Atani, R., Ebrahimi Atani, S., & Hassani Karbasi, A. (2018). A provably secure variant of ETRU based on extended ideal lattices over direct product of Dedekind domains. *Journal of Computing and Security*, 5(1), 13–34.

[18] Ebrahimi Atani, R., Ebrahimi Atani, S., & Hassani Karbasi, A. (2018). NETRU: A non-commutative and secure variant of CTRU cryptosystem. *The ISC International Journal of Information Security*, 10(1), 45–53.

[19] Ebrahimi Atani, R., Ebrahimi Atani, S., & Hassani Karbasi, A. (2019). A new ring-based SPHF and PAKE protocol on ideal lattices. *The ISC International Journal of Information Security*, 11(1), 75–86.

[20] Ebrahimi Atani, R., Ebrahimi Atani, S., & Mirzakuchaki, S. (2008). Public key cryptography using semigroup actions and semirings. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(4), 437–445.

[21] Falcon, S. (2014). On the k-Jacobsthal numbers. *American Review of Mathematics and Statistics*, 2(1), 67–77.

[22] Horadam, A. F. (1988). Jacobsthal and Pell curves. *The Fibonacci Quarterly*, 26(1), 77–83.

[23] Hu, X., Wang, J., & Yang, Y. (2011). Secure ID-based blind signature scheme without random oracle. In: *Proceedings of the International Conference on Network Computing and Information Security*, Guilin, China (pp. 245–249).

[24] Karataş, A. (2022). On complex Leonardo numbers. *Notes on Number Theory and Discrete Mathematics*, 28(3), 458–465.

[25] Karbasi, A. H., Ebrahimi Atani, R., & Ebrahimi Atani, S. (2018). PairTRU: Pairwise non-commutative extension of the NTRU public key cryptosystem. *International Journal of Information Security Systems*, 7(1), 11–19.

[26] Lai, H., Luo, M., Pieprzyk, J., Qu, Z., Li, S., & Orgun, M. A. (2017). An efficient quantum blind digital signature scheme. *Science China Information Sciences*, 60, Article ID 082501.

[27] Lysyanskaya, A. (2023). Security analysis of RSA-BSSA. In: *Public-Key Cryptography – PKC 2023*, Atlanta, GA, USA (pp. 251–280). Springer.

[28] Mehraban, E., Gulliver, T. A., Ebrahimi Atani, R., & Hincal, E. (2024). A novel electronic voting system using a blind signature scheme and blockchain. In: *Proceedings of the 11th International Symposium on Telecommunications* (pp. 790–794).

[29] Mehraban, E., Gulliver, T. A., & Hincal, E. (2026). Blind signatures from the generalized (t, k)-Fibonacci p-sequences. *Journal of Dynamics and Games*, 13, 193–203.

[30] Mehraban, E., & Hashemi, M. (2023). Coding theory on the generalized balancing sequence. *Notes on Number Theory and Discrete Mathematics*, 29(3), 503–524.

[31] Özkan, E., & Uysal, M. (2022). d-Gaussian Jacobsthal, d-Gaussian Jacobsthal–Lucas polynomials and their matrix representations. *Electronic Journal of Mathematical Analysis and Applications*, 10(2), 124–140.

[32] Prasad, K., Mohanty, R., Kumari, M., & Mahato, H. (2024). Some new families of generalized k-Leonardo and Gaussian Leonardo numbers. *Communications in Combinatorics and Optimization*, 9(3), 539–553.

[33] Rahman, A. A. R. A., & Husain, A. K. (2016). A strong blind signature using cascade blind factors. *International Journal of Innovative Research in Computer Science & Technology*, 4(1), 7–9.

[34] Ramezanpour Naseri, A., Abbasi, A., & Ebrahimi Atani, R. (2023). A new public key cryptography using M_q matrix. *Journal of Mathematical Modeling*, 11(4), 681–693.

[35] Shannon, A. G. (2019). A note on generalized Leonardo numbers. *Notes on Number Theory and Discrete Mathematics*, 25(3), 97–101.

[36] Skałba, M. (2018). Note on Lehmer–Pierce sequences with the same prime divisors. *Bulletin of the Australian Mathematical Society*, 97(1), 11–14.