RESEARCH PAPER DOI: 10.22080/cste.2026.31071.1113

Contributions of Science and Technology for Engineering

Journal Home page: https://cste.journals.umz.ac.ir/

Matrix-Based Digital Signatures Using the Generalized k-Chebyshev p−Sequences

Reza Ebrahimi Atani [1]*, Elahe Mehraban [2]

[1] *Associated Professor, Department of Computer Engineering, University of Guilan, Rasht, Iran,*
ORCID: 0000-0001-9180-8707.

[2] *Associated Professor, Mathematics Research Center, Near East University, Mersin 10 99138, Nicosia, Turkey,*
ORCID: 0000-0001-8544-9592.

**Corresponding Author: rebrahimi@guilan.ac.ir*

Article Info

Received 18 January 2026
Accepted 03 November 2026
Available online 08 November 2026

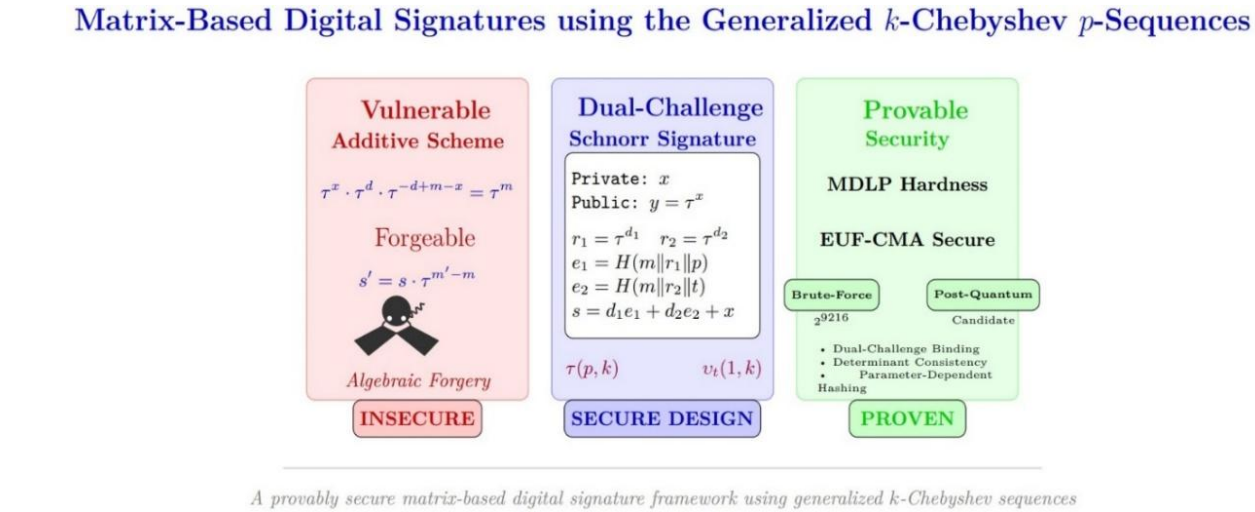
Keywords:

k-Chebyshev Sequences;
Digital Signature;
Public Key Cryptosystem;
EUF-CMA;
Matrix Discrete Logarithm Problem.

Abstract:

Digital signatures are a fundamental cryptographic primitive ensuring integrity, authenticity, and non-repudiation in digital communications. This paper introduces two novel generalizations of the classical *k-Chebyshev* sequences: the *k*-Chebyshev *p*-sequences and the *(k,t) -Chebyshev p-sequences*. These generalizations yield companion matrices of dimension $p+1$ and $p+t$, respectively, providing a flexible algebraic framework with tunable security parameters. Applying the cyclic subgroup structure of these matrices, we propose a matrix-based digital signature scheme that follows a dual-challenge Fiat-Shamir construction and extends the Schnorr paradigm. Unlike naive matrix exponentiation signatures, our scheme employs parameter-dependent hashing to cryptographically bind the message to the nonce, preventing algebraic forgeries. We formally analyze the scheme within the standard *EUF-CMA* security framework and prove its existential unforgeability under adaptive chosen-message attacks in the random oracle model, reducing its security to the hardness of the Matrix Discrete Logarithm Problem (MDLP). The security analysis demonstrates resistance to brute-force, index-calculus, Pohlig--Hellman, and linear recurrence attacks. The results establish generalized Chebyshev sequence theory as a fertile foundation for designing provably secure public-key cryptosystems, extending the landscape of algebraic methods in digital signatures.

Graphical Abstract



A provably secure matrix-based digital signature framework using generalized k-Chebyshev sequences

© 2026 University of Mazandaran

Copyright © 2026 by the authors. Licensee CSTE, Babolsar, Mazandaran. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC-BY) license (https://creativecommons.org/licenses/by/4.0/deed.en)

ISSN 3060-6578

Please cite this paper as: R. Ebrahimi Atani, E. Mehraban, "Matrix-Based Digital Signatures Using the Generalized k-Chebyshev p−Sequences". Contrib. Sci. Technol. Eng, vol. 3, no. 3, pp. 46-60, 2026, doi:10.22080/cste.2026.31071.1113.

1. Introduction

Digital signatures are a cornerstone of modern cryptography, providing authenticity, integrity, and non-repudiation in electronic communications. Their security typically rests on the intractability of number-theoretic problems, most notably the Discrete Logarithm Problem (DLP) and the Integer Factorization Problem. However, the advent of sub-exponential algorithms (e.g., index calculus) and, more critically, quantum algorithms (e.g., Shor's algorithm) threatens the long-term viability of classical DLP-based systems over finite fields and elliptic curves [1, 2]. Consequently, cryptographers have explored alternative algebraic structures, including matrix groups, non-abelian groups, and sequence-based constructions, to achieve post-quantum resistance or at least diversify the underlying hardness assumptions. One notable type of digital signature is the blind signature, originally proposed by Chaum [3]. A computationally efficient construction of identity-based blind signatures with short signature lengths was presented by Hu [4]. Further advancements were made by Rahman and Husain [5], who extended traditional blind signature schemes by embedding multiple random variables, known as blind factors, at different positions in the original message. More recently, blind RSA signatures were constructed using t-generalized Lehmer sequences in finite groups [6]. These sequences were 789used to develop new digital signature algorithms [7, 8, 9], offering a compelling example of their application in cryptography.

Sequences have historically played a pivotal role in cryptography, from stream ciphers to pseudorandom number generation and error-correcting codes [10, 11, 12]. In the context of public-key cryptography, the use of recursive sequences—such as Fibonacci, Pell, Lucas, and Chebyshev has gained traction due to their inherent algebraic structure and ease of matrix representation [13, 14]. In the study by Viswanath and Kumar [15], a public-key cryptosystem was developed using the Affine Hill Cipher, enhancing security by incorporating two or more digital signatures over a prime modulus. In Mehraban et al.'s study [16], new sequences called k-division L-Lehmer-Pell sequences were introduced and subsequently applied in a novel Affine Hill cipher algorithm. Specifically, the k-Chebyshev sequences possess a semigroup property that mimics scalar exponentiation, making them attractive for DLP-based protocols. Early works applied Chebyshev polynomials to chaotic map-based encryption [17], while more recent studies investigated geometric circulant matrices whose entries are Chebyshev polynomials [18]. Despite these advances, most sequence-based cryptosystems remain confined to finite fields or simple scalar recurrences, leaving them exposed to generic DLP attacks.

To mitigate these vulnerabilities, several researchers have turned to matrix-based cryptography. The Matrix Discrete Logarithm Problem (MDLP) generalizes the classical DLP by replacing scalar exponentiation with matrix exponentiation, offering a potentially richer algebraic landscape and a larger key space [19]. Matrix groups over finite fields are known to provide subexponential resistance to standard attacks, provided the matrices are carefully chosen to avoid reductions to finite-field DLP instances [20, 21]. Recent works have explored companion matrices for the Fibonacci [22], Pell [23], and Lehmer [24] sequences in Diffie-Hellman key exchange and encryption. In the study by Mehraban et al. [25], sequences based on generalized Lehmer and Jacobsthal sequences were introduced, leading to the definition of Hadamard-type generalized Jacobsthal-Lehmer sequences in finite groups. These sequences were applied to develop new digital signature algorithms, offering a compelling example of group theory's application in cryptography. However, applying these matrices to digital signatures introduces a non-trivial challenge: the algebraic structure often allows for straightforward forgeries (e.g., exponent manipulation) unless the signature is cryptographically bound to the message via a hash function. The literature lacks a systematic treatment of matrix-based signatures that combine (i) a rich family of recursively-defined matrices, (ii) rigorous EUF-CMA security, and (iii) explicit resistance to both algebraic and quantum attacks.

In this paper, we address this gap by introducing two novel generalizations of the classical k-Chebyshev sequences. Our first generalization, the k-Chebyshev p-sequences $\{C_n\^p\ (k)\}$, introduces a delay parameter p to the recurrence, yielding companion matrices of dimension $p+1$. This increased dimension directly increases the entropy of the private key space and complicates linear-relation attacks. Our second generalization, the (k,t)-Chebyshev p-sequences $\{C_n\^p\ (k,t)\}$, further extends the recurrence with a parameter t, providing even greater flexibility and mixing properties. For both families, we derive explicit matrix-power formulas (including negative powers), determinant identities, and generating functions that are essential for cryptographic implementation.

Based on these algebraic foundations, we design a matrix-based digital signature scheme that follows the Fiat–Shamir paradigm (or a Schnorr-like structure) to prevent algebraic forgeries. Unlike naive exponentiation-based proposals, our scheme employs a cryptographic hash function to bind the message to the nonce, ensuring that an adversary cannot trivially adjust exponents to forge a signature on a different message. We formally prove that the resulting scheme achieves Existential Unforgeability under Adaptive Chosen-Message Attack (EUF-CMA) in the random oracle model, under the hardness of the MDLP. To the best of our knowledge, this is the first signature scheme to leverage the generalized Chebyshev matrix structure and achieve a provable security reduction.

In summary, our main contributions are:

- The definition and algebraic characterization of two new families of sequences: the k-Chebyshev p-sequences and the (k,t)-Chebyshev p-sequences, including closed-form matrix powers, determinants, and generating functions.
- A secure digital signature framework that integrates these matrices with a challenge-response mechanism, preventing the algebraic forgeries that plague naive matrix exponentiation signatures.
- A formal security proof in the random oracle model, reducing EUF-CMA security of the scheme to the intractability of the MDLP.
- Numerical examples and a preliminary efficiency analysis, demonstrating the feasibility of the approach and highlighting its resistance to brute-force and algebraic attacks.

Related Work and Positioning: Our work intersects with several active research directions. Lattice-based signatures (e.g., Dilithium, Falcon) are among the leading post-quantum candidates and offer strong security guarantees. Yet, they rely on distinct hard problems (LWE, NTRU) and require careful parameter tuning for compactness. Matrix-based signatures offer a middle ground: they are conceptually simpler than lattice schemes, yet more versatile than scalar DLP systems. Compared to recent matrix schemes using Fibonacci [22] or Pell sequences [23], our Chebyshev-based construction provides a richer recurrence structure and, importantly, a formal security treatment. Moreover, our parameters p and t allow the key space to scale exponentially with the matrix dimension, offering a tunable trade-off between security and performance.

The paper is organized as follows. Section 2 presents the definitions and structural properties of the generalized k-Chebyshev sequences and the two new sequence families. Section 3 describes our proposed digital signature schemes and discusses practical implementation. Section 4 presents a comprehensive security analysis, including a formal reduction to MDLP, a discussion of quantum resilience, and an analysis of resistance to algebraic attacks. Finally, Section 5 concludes the paper and outlines future research directions.

2. The Generalized k-Chebyshev Sequences

In this section, we introduce two new families of sequences derived from the classical *k-Chebyshev* sequences. Unlike scalar recurrences, the matrix representation of these sequences enables efficient exponentiation via repeated squaring, which is essential for public-key operations. More importantly, the parameters we introduce serve cryptographic purposes:

- The parameter p determines the dimension *(p+1)* of the companion matrix, directly expanding the private key space from $\mathcal{O}(q\hat{}2)$ to $\mathcal{O}(q\hat{}(p+1))$.
- The parameter *t* introduces a longer memory into the recurrence (Definition 2.2), which complicates linear algebra attacks that exploit low-order relations among sequence terms.
- The parameter k modulates the growth rate and mixing properties of the sequence, affecting the distribution of matrix entries modulo q.

These properties collectively provide a flexible algebraic framework for constructing cryptosystems with tunable security levels.

Definition 2.1. The Chebyshev polynomials of the first and second kinds are defined as follows, respectively:

$$\begin{aligned} &T(n+2)(x) = 2xT(n+1)(x) - T(n)(x), \ \ n \geq 1, \\ &\text{with } T(0)(x) = 0 \text{ and } T(1)(x) = 1. \text{ And,} \\ &U(n+2)(x) = 2xU(n+1)(x) - U(n)(x), \ \ n \geq 1, \\ &\text{with } U(0)(x) = 0 \text{ and } U(1)(x) = 1 \text{ (see [29])} \end{aligned} \tag{1}$$

The first and second kinds of $h(x)$-Chebyshev polynomials, denoted by T_n and U_n, respectively, were introduced by Abchiche and Belbachir [26], where $h(x)$ is a non-constant polynomial with rational coefficients. Kishore and Verma [27] derived explicit formulas for Chebyshev polynomials of the third and fourth kinds for both odd and even indices using a combinatorial approach27. According to Ozkan and Akku's study [28], the k-Chebyshev sequences are defined as follows:

Definition 2.2. For a positive real number k, the *k-Chebyshev* sequences $C_n(k)$ are:

$$\begin{aligned} &C_{n+1}(k) = 2kC_n(k) - C_{n-1}(k), \ \ n \geq 1, \\ &\text{with } C_0(k) = 0 \text{ and } C_1(k) = k \end{aligned} \tag{2}$$

Subsequent work examined the relationships between the terms of the k-Chebyshev sequence and its generating function. Pucanović and Pešović [14] constructed geometric circulant matrices whose entries are Chebyshev polynomials of the first or second kind. The generalized k-Chebyshev sequences exhibit unique recursive relations that offer a solid foundation for constructing cryptographic primitives, particularly in digital signature schemes.

2.1. First Generalization: The *k*-Chebyshev *p*-Sequences

Definition 2.3. *For integers $p \geq 1$ and $k \geq 2$, the k-Chebyshev $p-$sequences denoted $\{C_n^p(k)\}$ are defined as:*

$$\begin{aligned} &C_n^p(k) = 2kC_{n-1}^p(k) - C_{n-p-1}^p(k), \ n \geq p+1, \\ &\textit{where } C_0^p(k) = C_1^p(k) = \cdots = C_{p-1}^p(k) = 0, \ C_p^p(k) = 1 \end{aligned} \tag{3}$$

This recurrence generalizes the classical *k-Chebyshev* sequence (which corresponds to p=1) by introducing a delay p. The sequence's behavior is influenced by both k and p, providing a more versatile tool for cryptographic schemes.

Example 2.1. As an example, we have:

- *If $p = k = 2$, we have* $\{C_n^2(2)\} = \{0,0,1,4,16,63,248,976, \dots\}$.
- *If $k = 3$ and $p = 2$, we have* $\{C_n^2(3)\} = \{0,0,1,6,36,215,1284,7668, \dots\}$.
- *If $k = 2$ and $p = 3$, we have* $\{C_n^3(2)\} = \{0,0,0,1,4,16,64,255,1016,4048, \dots\}$.
- *If $k = 3$ and $p = 3$, we have* $\{C_n^3(3)\} = \{0,0,0,1,6,36,216,1295,7764, \dots\}$.

A key feature of the generalized k-Chebyshev sequences is their ability to be represented using matrices. For example $\tau(p,k)$ is called k-Chebyshev $p-$sequences' companion matrix, which is a $(p+1) \times (p+1)$ matrix.

$$\tau(p,k)=\begin{bmatrix} 2k & 0 & 0 & \cdots & 0 & 0 & -1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_{(p+1)\times(p+1)}. \tag{4}$$

This matrix acts as a shift register, and its powers $\tau(p,k)^n$ encode the sequence terms, enabling efficient computation via modular matrix exponentiation.

Lemma 2.1. For $p=2,\ k\geq 2$ and $n\geq 3$, we have:

$$(\tau(2,k))^n=\begin{bmatrix} C_{n+2}^2(k) & -C_n^2(k) & -C_{n+1}^2(k) \\ C_{n+1}^2(k) & -C_{n-1}^2(k) & -C_n^2(k) \\ C_n^2(k) & -C_{n-2}^2(k) & -C_{n-1}^2(k) \end{bmatrix}. \tag{5}$$

Proof. Let $k=2$. The proof is by induction on n. Clearly the result holds for $n=3$ which gives

$$(\tau(2,2))^3=\begin{bmatrix} 63 & -4 & -16 \\ 16 & -1 & -4 \\ 4 & 0 & -1 \end{bmatrix}=\begin{bmatrix} C_5^2(2) & -C_3^2(2) & -C_4^2(2) \\ C_4^2(2) & -C_2^2(2) & -C_3^2(2) \\ C_3^2(2) & -C_1^2(2) & -C_2^2(2) \end{bmatrix}. \tag{6}$$

Assume the lemma holds for $3\leq n\leq i$. Then for $n=i+1$ we have

$$\begin{aligned}(\tau(2,k))^{i+1}&=\begin{bmatrix} 4 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}\begin{bmatrix} C_{i+2}^2(k) & -C_i^2(k) & -C_{i+1}^2(k) \\ C_{i+1}^2(k) & -C_{i-1}^2(k) & -C_i^2(k) \\ C_i^2(k) & -C_{i-2}^2(k) & -C_{i-1}^2(k) \end{bmatrix} \\ &=\begin{bmatrix} C_{i+3}^2(k) & -C_{i+1}^2(k) & -C_{i+2}^2(k) \\ C_{i+2}^2(k) & -C_i^2(k) & -C_{i+1}^2(k) \\ C_{i+1}^2(k) & -C_{i-1}^2(k) & -C_i^2(k) \end{bmatrix},\end{aligned} \tag{7}$$

which gives the result. For $k\geq 3$ is similar, we can prove.

In general, for $p\geq 3$ and $k\geq 2$, by induction on n the n −th power of the k-Chebyshev p −sequences matrix is

$$(\tau(p,k))^n=\begin{bmatrix} C_{n+p}^p(k) & -C_n^{\mathrm{p}}(k) & \cdots & -C_{n+p-2}^p(k) & -C_{n+p-1}^p(k) \\ C_{n+p-1}^p(k) & -C_{n-1}^{\mathrm{p}}(k) & \cdots & -C_{n+p-3}^p(k) & -C_{n+p-2}^p(k) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C_{n+1}^p(k) & -C_{n-p+1}^{\mathrm{p}}(k) & \cdots & -C_{n-1}^p(k) & -C_n^p(k) \\ C_n^p(k) & -C_{n-p}^{\mathrm{p}}(k) & \cdots & -C_{n-2}^p(k) & -C_{n-1}^p(k) \end{bmatrix}. \tag{8}$$

Lemma 2.2. For $k\geq 2$ we have $det(\tau(p,k))^n=\begin{cases}-1, & \text{if } p \text{ is even}, n \text{ is odd},\\ 1, & \text{otherwise.}\end{cases}$

Proof. By (2.2) we have

$$det\tau(p,k)=\begin{cases}-1, & \text{if } p \text{ is even.}\\ 1, & \text{otherwise.}\end{cases} \tag{9}$$

and the result follows.

Cryptographic implication: Since $\det(\tau(p,k))=\pm 1$, the matrix is unimodular over $\mathbb{Z}$ and therefore invertible modulo any prime q. This guarantees that $\tau(p,k)$ generates a cyclic subgroup of $\mathrm{GL}_{p+1}(\mathbb{F}_q)$, a necessary condition for the hardness of the MDLP.

From Definition 2.1, we have the following:

$$C_n^p(k)=C_{n+p+1}^p(k)-2kC_{n+p}^p(k),\ n<0, \tag{10}$$

Lemma 2.3. For $p=2,\ k\geq 2$ and $n\geq 3$, we have

$$(\tau(2,k))^{-n}=\begin{bmatrix} C^2_{-n+2}(k) & -C^2_{-n}(k) & -C^2_{-n+1}(k) \\ C^2_{-n+1}(k) & -C^2_{-n-1}(k) & -C^2_{-n}(k) \\ C^2_{-n}(k) & -C^2_{-n-2}(k) & -C^2_{-n-1}(k) \end{bmatrix}. \tag{11}$$

Proof. Let $k=2$. The proof is by induction on n. Clearly the result holds for $n=3$ which gives

$$(\tau(2,2))^{-3}=\begin{bmatrix} -1 & 4 & 0 \\ 0 & -1 & 4 \\ -4 & 16 & -1 \end{bmatrix}=\begin{bmatrix} C^2_{-1}(2) & -C^2_{-3}(2) & -C^2_{-2}(2) \\ C^2_{-2}(2) & -C^2_{-4}(2) & -C^2_{-3}(2) \\ C^2_{-3}(2) & -C^2_{-5}(2) & -C^2_{-4}(2) \end{bmatrix}. \tag{12}$$

Assume the lemma holds for $3\le n\le d$. Then for $n=d+1$ we have

$$\begin{aligned}(\tau(2,k))^{-(d+1)}&=\begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & 4 & 0 \end{bmatrix}\begin{bmatrix} C^2_{-d+2}(k) & -C^2_{-d}(k) & -C^2_{-d+1}(k) \\ C^2_{-d+1}(k) & -C^2_{-d-1}(k) & -C^2_{-d}(k) \\ C^2_{-d}(k) & -C^2_{-d-2}(k) & -C^2_{-d-1}(k) \end{bmatrix}\\ &=\begin{bmatrix} C^2_{-d+3}(k) & -C^2_{-d+1}(k) & -C^2_{-d+2}(k) \\ C^2_{-d+2}(k) & -C^2_{-d}(k) & -C^2_{-d+1}(k) \\ C^2_{-d+1}(k) & -C^2_{-d-1}(k) & -C^2_{-d}(k) \end{bmatrix},\end{aligned} \tag{13}$$

which gives the result. For $k\ge 3$ the proof is analogous.

In general, for $p\ge 3$ and $k\ge 2$, by induction on n, we have

$$(\tau(p,k))^{-n}=\begin{bmatrix} C^p_{-n+p}(k) & -C^p_{-n}(k) & \cdots & -C^p_{-n+p-2}(k) & -C^p_{-n+p-1}(k) \\ C^p_{-n+p-1}(k) & -C^p_{-n-1}(k) & \cdots & -C^p_{-n+p-3}(k) & -C^p_{-n+p-2}(k) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ C^p_{-n+1}(k) & -C^p_{-n-p+1}(k) & \cdots & -C^p_{-n-1}(k) & -C^p_{-n}(k) \\ C^p_{-n}(k) & -C^p_{-n-p}(k) & \cdots & -C^p_{-n-2}(k) & -C^p_{-n-1}(k) \end{bmatrix}. \tag{14}$$

2.2. Second Generalization: The (k,t)-Chebyshev p-Sequences

To further enrich the algebraic structure and complicate linear recurrence attacks, we introduce a second generalization that incorporates an additional memory parameter t.

Definition 2.4. For integers $p\ge 1, t\ge 2$ and $k\ge 2$, the (k,t)-Chebyshev $p-$sequences denoted $\{C^p_n(k,t)\}$ are defined as:

$$C^p_n(k,t)=2kC^p_{n-1}(k,t)-C^p_{n-p-1}(k,t)+\cdots+C^p_{n-t-p}(k,t),\ n\ge t+p, \tag{15}$$

where

$$C^p_0(k,t)=C^p_1(k,t)=\cdots=C^p_{t+p-2}(k,t)=0, C^p_{t+p-1}(k,t)=1 \tag{16}$$

The inclusion of t sums over the previous t terms, increasing the order of the recurrence and thus the dimension of the companion matrix to $(p+t)$. This expanded state space provides a larger keyspace and greater resistance to attacks that attempt to derive the secret exponent from linear dependencies.

Example 2.2. As an example, we have:

- For $p=1,\ t=2$ and $k=2$, we have $\{C^1_n(2,2)\}_0^\infty=\{0,0,1,4,15,57,217,826,\cdots\}$.
- For $p=1,\ t=2$ and $k=3$, we have $\{C^1_n(3,2)\}_0^\infty=\{0,0,1,6,3,205,1201,7036,41220,\cdots\}$.
- For $p=1,\ t=2$ and $k=4$, we have $\{C^1_n(4,2)\}_0^\infty=\{0,0,1,8,63,497,3921,\cdots\}$.

Lemma 2.4. Let $g_{C^p_n(k,t)}$ be the generating function of the (k,t)-Chebyshev $p-$sequences, then

$$g_{C^p_n(k,t)}=\frac{x^{t+p-1}}{1-2kx+x^{p+1}-x^{p+2}-\cdots-x^{t+p}}. \tag{17}$$

Proof. We have

$$\begin{aligned} g_{C_n^p(k,t)} &= \sum_{n=1}^{\infty} C_n^p(k,t)x^n \\ &= C_1^p(k,t)x + C_2^p(k,t)x^2 + \cdots + C_{t+p-1}^p(k,t)x^{t+p-1} + \sum_{n=t+p}^{\infty} C_n^p(k,t)x^n \\ &= x^{t+p-1} + \sum_{n=t+p}^{\infty} 2\,kC_{n-1}^p(k,t) - C_{n-p-1}^p(k,t) + C_{n-p-2}^p(k,t) + \cdots + C_{n-t}^p(k,t)x^n \\ &= x^{t+p-1} + \sum_{n=t+p+1}^{\infty}(\,2kC_{n-1}^p(k,t)x^n - \sum_{n=t+p+1}^{\infty} C_{n-p-1}^p(k,t)x^n + \sum_{n=t+p+1}^{\infty} C_{n-p-2}^p(k,t)x^n \\ &+ \cdots + \sum_{n=t+p+1}^{\infty} C_{n-t-p}^p(k,t))x^n \\ &= x^{t+p-1} + 2kx\sum_{n=1}^{\infty} C_n^p(k,t)x^n - x^{p+1}\sum_{n=1}^{\infty} C_n^p(k,t)x^n + \cdots + x^{t+p}\sum_{n=1}^{\infty} C_n^p(k,t)x^n \\ &= x^{t+p-1} + x2kg_{C_n^p(k,t)} - x^{p+1}g_{C_n^p(k,t)} + \cdots + x^{t+p}g_{C_n^p(k,t)}, \end{aligned} \tag{18}$$

so

$$g_{C_n^p(k,t)} = \frac{x^{t+p-1}}{1-2kx+x^{p+1}-x^{p+2}-\cdots-x^{t+p}}. \tag{19}$$

Lemma 2.5. The generating function of the (k,t)-Chebyshev p −sequences has the following exponential representation:

$$g_{C_n^p(k,t)} = x^{t+p-1}\exp\sum_{i=1}^{\infty}\frac{x^i}{i}(2k - x^{p-2} + x^{p-3} + \cdots + x^{t+p-1})^i, \tag{20}$$

where $t \geq 2$.

Proof. From (2.6) we have

$$\begin{aligned} &\ln\frac{g_{C_n^p(k,t)}}{x^{t+p-1}} = -\ln(1 - 2kx + x^{p+1} - x^{p+2} - \cdots - x^{t+p}). \\ &-\ln(1 - 2kx + x^{p+1} - x^{p+2} - \cdots - x^{t+p}) = -[-x(2k - x^p + \cdots + x^{t+p-1}) \\ &-\frac{1}{2}x^2(2k - x^p + \cdots + x^{t+p-1})^2 - \cdots - \frac{1}{n}x^n(2k - x^p + \cdots + x^{t+p-1})^n - \cdots], \end{aligned} \tag{21}$$

which gives the result.

From the recurrence relation (2.5), we obtain the companion matrix $v_t(1,k)$ of dimension $(p+t)\times(p+t)$ (which is also called the (k,t)-Chebyshev p −sequences matrix):

$$\begin{bmatrix} C_n^p(k,t) \\ C_{n-1}^p(k,t) \\ C_{n-p-1}^p(k,t) \\ \vdots \\ C_{n-t-p+1}^p(k,t) \\ C_{n-t-p}^p(k,t) \end{bmatrix} = \begin{bmatrix} 2k & -1 & 1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} C_{n-1}^p(k,t) \\ C_{n-p-1}^p(k,t) \\ C_{n-p-2}^p(k,t) \\ \vdots \\ C_{n-t-p}^p(k,t) \\ C_{n-t-p-1}^p(k,t) \end{bmatrix}, \tag{22}$$

which has a companion matrix

$$v_t(1,k) = \begin{bmatrix} 2k & -1 & 1 & \cdots & 1 & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix}_{(p+t)\times(p+t)} \tag{23}$$

$v_t(1,k)$ is called the (k,t)-Chebyshev p −sequences matrix. This matrix generalizes the previous construction and provides an even richer group structure.

Lemma 2.6. For $p = 1,\ t = 2, k \geq 2$ and $n \geq 3$ we have

$$(v_2(1,k))^n = \begin{bmatrix} C_{n+2}^1(k,2) & C_n^1(k,2) - C_{n+1}^1(k,2) & C_{n+1}^1(k,2) \\ C_{n+1}^1(k,2) & C_{n-1}^1(k,2) - C_n^1(k,2) & C_n^1(k,2) \\ C_n^1(k,2) & C_{n-2}^1(k,2) - C_{n-1}^1(k,2) & C_{n-1}^1(k,2) \end{bmatrix} \tag{24}$$

Proof. Let $k = 2$. The proof is by induction on n. Clearly the result holds for $n = 3$ which gives

$$(v_2(1,2))^3 = \begin{bmatrix} 57 & -11 & 15 \\ 15 & -3 & 4 \\ 4 & -1 & 1 \end{bmatrix} = \begin{bmatrix} C_5^1(2,2) & C_3^1(2,2) - C_4^1(2,2) & C_4^1(2,2) \\ C_4^1(2,2) & C_2^1(2,2) - C_3^1(2,2) & C_3^1(2,2) \\ C_3^1(2,2) & C_1^1(2,2) - C_2^1(2,2) & C_2^1(2,2) \end{bmatrix}. \tag{25}$$

Assume the lemma holds for $3 \leq n \leq s$. Then for $n = s + 1$ we have

$$(v_2(1,k))^{s+1} = \begin{bmatrix} 4 & -1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} C^1_{s+2}(k,2) & C^1_s(k,2) - C^1_{s+1}(k,2) & C^1_{s+1}(k,2) \\ C^1_{s+1}(k,2) & C^1_{s-1}(k,2) - C^1_s(k,2) & C^1_s(k,2) \\ C^1_s(k,2) & C^1_{s-2}(k,2) - C^1_{s-1}(k,2) & C^1_{s-1}(k,2) \end{bmatrix}$$
$$= \begin{bmatrix} C^1_{s+3}(k,2) & C^1_{s+1}(k,2) - C^1_{s+2}(k,2) & C^1_{s+2}(k,2) \\ C^1_{s+2}(k,2) & C^1_s(k,2) - C^1_{s+1}(k,2) & C^1_{s+1}(k,2) \\ C^1_{s+1}(k,2) & C^1_{s-1}(k,2) - C^1_s(k,2) & C^1_s(k,2) \end{bmatrix}. \quad (26)$$

which gives the result. For $k \geq 3$, , the proof is analogous.

In general, for $p = 1, k \geq 2$ and $t \geq 2$, by induction on n the n-th power of the (k,t)-Chebyshev p-sequence matrix is given by the block form below (note the corrected alignment to avoid ambiguous column counts):

$$(v_t(1,k))^n = \begin{bmatrix} C^1_{n+t}(k,t) & (C^1_{n+t-2}(k,t) + C^1_{n+t-3}(k,t) + \cdots + C^1_n(k,t)) - C^1_{n+t-1}(k,t) \\ C^1_{n+t-1}(k,t) & (C^1_{n+t-3}(k,t) + C^1_{n+t-4}(k,t) + \cdots + C^1_{n-1}(k,t)) - C^1_{n+t-2}(k,t) \\ \vdots & \vdots \\ C^1_{n+1}(k,t) & (C^1_{n-t+1}(k,t) + C^1_{n-t}(k,t) + \cdots + C^1_{n-1}(k,t)) - C^1_n(k,t) \\ C^1_n(k,t) & (C^1_{n-t}(k,t) + C^1_{n-t-1}(k,t) + \cdots + C^1_{n-2}(k,t)) - C^1_{n-1}(k,t) \end{bmatrix}$$
$$\begin{bmatrix} C^1_{n+t-1}(k,t) + C^1_{n+t-2}(k,t) + \cdots + C^1_{n+1}(k,t) & \cdots & C^1_{n+t-1}(k,t) + C^1_{n+t-2}(k,t) & C^1_{n+t-1}(k,t) \\ C^1_{n+t-2}(k,t) + C^1_{n+t-3}(k,t) + \cdots + C^1_n(k,t) & \cdots & C^1_{n+t-2}(k,t) + C^1_{n+t-3}(k,t) & C^1_{n+t-2}(k,t) \\ \vdots & \ddots & \vdots & \vdots \\ C^1_n(k,t) + C^1_{n-1}(k,t) + \cdots + C^1_{n-t+2}(k,t) & \cdots & C^1_n(k,t) + C^1_{n-1}(k,t) & C^1_n(k,t) \\ C^1_{n-1}(k,t) + C^1_{n-2}(k,t) + \cdots + C^1_{n-t+1}(k,t) & \cdots & C^1_{n-1}(k,t) + C^1_{n-2}(k,t) & C^1_{n-1}(k,t) \end{bmatrix} \quad (27)$$

Lemma 2.7. For $k \geq 2$ we have $det(v_t(1,k))^n = \begin{cases} -1, & \text{if } t \text{ and } n \text{ are odd,} \\ 1, & \text{otherwise.} \end{cases}$

Proof. By (2.8) we have

$$detv_t(1,k) = \begin{cases} -1, & \text{if } t \text{ is odd,} \\ 1, & \text{otherwise.} \end{cases} \quad (28)$$

and the result follows.

As with the first family, unimodularity ensures that $v_t(1,k)$ generates a cyclic subgroup of $\mathrm{GL}_{p+t}(\mathbb{F}_q)$, making it suitable for the MDLP. Using (2.6), we extend the recurrence to negative indices:

$$C^p_n(k,t) = C^p_{n+t+p}(k,t) - (2kC^p_{n+t+p-1}(k,t) - C^p_{n+t-1}(k,t) + \cdots + C^p_{n+1}(k,t)),\ n < 0, \quad (29)$$

which again enables computing negative matrix powers for signing.

Lemma 2.8. For $p = 1,\ t = 2, k \geq 2$ and $n \geq 3$ we have:

$$(v_2(1,k))^{-n} = \begin{bmatrix} C^1_{-n+2}(k,2) & C^1_{-n}(k,2) - C^1_{-n+1}(k,2) & C^1_{-n+1}(k,2) \\ C^1_{-n+1}(k,2) & C^1_{-n-1}(k,2) - C^1_{-n}(k,2) & C^1_{-n}(k,2) \\ C^1_{-n}(k,2) & C^1_{-n-2}(k,2) - C^1_{-n-1}(k,2) & C^1_{-n-1}(k,2) \end{bmatrix} \quad (30)$$

By induction on n, we have the following result:

Corollary 2.1. For $p = 1,\ k \geq 2$ and $t \geq$we obtain the negative power matrix:

$$(v_t(1,k))^{-n} =$$
$$\begin{bmatrix} C^1_{-n+t}(k,t) & (C^1_{-n+t-2}(k,t) + C^1_{-n+t-3}(k,t) + \cdots + C^1_{-n}(k,t)) - C^1_{-n+t-1}(k,t) \\ C^1_{-n+t-1}(k,t) & (C^1_{-n+t-3}(k,t) + C^1_{-n+t-4}(k,t) + \cdots + C^1_{-n-1}(k,t)) - C^1_{-n+t-2}(k,t) \\ \vdots & \vdots \\ C^1_{-n+1}(k,t) & (C^1_{-n-t+1}(k,t) + C^1_{-n-t}(k,t) + \cdots + C^1_{-n-1}(k,t)) - C^1_{-n}(k,t) \\ C^1_{-n}(k,t) & (C^1_{-n-t}(k,t) + C^1_{-n-t-1}(k,t) + \cdots + C^1_{-n-2}(k,t)) - C^1_{-n-1}(k,t) \end{bmatrix}$$
$$\begin{bmatrix} C^1_{-n+t-1}(k,t) + C^1_{-n+t-2}(k,t) + \cdots + C^1_{-n+1}(k,t) & \cdots & C^1_{-n+t-1}(k,t) + C^1_{-n+t-2}(k,t) & C^1_{-n+t-1}(k,t) \\ C^1_{-n+t-2}(k,t) + C^1_{-n+t-3}(k,t) + \cdots + C^1_{-n}(k,t) & \cdots & C^1_{-n+t-2}(k,t) + C^1_{-n+t-3}(k,t) & C^1_{-n+t-2}(k,t) \\ \vdots & \ddots & \vdots & \vdots \\ C^1_{-n}(k,t) + C^1_{-n-1}(k,t) + \cdots + C^1_{-n-t+2}(k,t) & \cdots & C^1_{-n}(k,t) + C^1_{-n-1}(k,t) & C^1_{-n}(k,t) \\ C^1_{-n-1}(k,t) + C^1_{-n-2}(k,t) + \cdots + C^1_{-n-t+1}(k,t) & \cdots & C^1_{-n-1}(k,t) + C^1_{-n-2}(k,t) & C^1_{-n-1}(k,t) \end{bmatrix}. \quad (31)$$

Remark on parameter selection. The results in this section demonstrate that increasing p or t expands the matrix dimension, thereby increasing the size of the general linear group and the difficulty of the MDLP. However, it also increases the computational cost of matrix exponentiation from $\mathcal{O}(n^3 \log x)$ to $\mathcal{O}((n)^3 \log x)$ where $n = p + 1$ or $n = p + t$. In practice, one

can choose p, t to achieve a desired security level (e.g., 128-bit) while balancing performance. For instance, setting $p = 5$ and $q \approx 2^{256}$ yields a matrix of dimension 6, offering a keyspace of approximately q^{36}, which is infeasible to enumerate.

3. New Digital Signature Schemes Using Generalized k-Chebyshev Sequences

The algebraic structures developed in section 2, specifically the cyclic subgroups generated by the companion matrices $\tau(p,k)$ and $v_t(1,k)$ naturally lend themselves to public-key cryptography. In analogy to the classical Discrete Logarithm Problem, the Matrix Discrete Logarithm Problem (MDLP) provides a hard one-way function suitable for digital signatures.

3.1. Motivation and Design Strategy

The design of a secure matrix-based signature scheme requires careful consideration of the algebraic structure: the signing equation must cryptographically bind the message to the nonce in a non-linear fashion to prevent algebraic manipulation. Our design philosophy centers on three core principles:

1. **Non-linear message binding**: The signature must depend on the message through a cryptographic hash function in a way that prevents an adversary from algebraically adjusting the exponent to forge a signature on a different message.
2. **Application of the full parameter space**: The parameters p and t that define our generalized sequences should be actively incorporated into the signing and verification processes, rather than serving merely as static structural choices. This creates a richer algebraic environment that complicates attacks.
3. **Algebraic consistency verification**: The determinant properties of our matrices (Lemmas 2.2 and 2.4) provide an additional algebraic invariant that can be exploited to detect signature tampering, adding a layer of security beyond the standard group equation.

To realize these principles, we adopt a **dual-challenge Fiat–Shamir construction** that extends the classical Schnorr paradigm in several novel directions. Unlike standard Schnorr signatures, which rely on a single nonce and a single challenge, our scheme employs *two independent nonces* $r_1 = \tau^{d_1}$ and $r_2 = \tau^{d_2}$, each bound to the message through separate hash challenges:

$$e_1 = H_1(m \parallel r_1 \parallel p), \qquad e_2 = H_2(m \parallel r_2 \parallel t). \tag{32}$$

The signing equation then becomes

$$s \equiv d_1 \cdot e_1 + d_2 \cdot e_2 + x \pmod{\ell}, \tag{33}$$

where x is the private key and $\ell = \mathrm{ord}(\tau)$ is the group order. This dual-exponent structure offers several significant advantages:

- **Enhanced security through independence**: Any adversary attempting to forge a signature must simultaneously solve two independent MDLP instances, as the relationship between r_1, r_2, and the private key x is obscured by two distinct nonces and hash challenges.
- **Parameter-dependent binding**: By including the parameters p and t in the hash inputs, we ensure that signatures are cryptographically bound to the specific sequence family and parameter choices, preventing cross-parameter attacks.
- **Determinant-based consistency check**: The signature includes $\delta = \det(r_1 \cdot r_2)$, which provides an algebraic invariant that must hold for any valid signature. This additional check exploits the determinant formulas derived in Section 2 and detects attempts to replace r_1 or r_2 with arbitrary matrices.
- **Resistance to algebraic manipulation**: The additive exponent attack, where an adversary adjusts the exponent by a linear offset, is rendered infeasible because any change to the message alters both e_1 and e_2 in a non-linear, unpredictable way through the cryptographic hash functions.

Importantly, the negative-power formulas derived in Lemmas 2.3 and 2.4, while not directly used in the signing equation of the current construction, provide algebraic flexibility for future extensions (e.g., blind signatures or multi-signatures where inverses are required). The dual-challenge structure also naturally accommodates both matrix families: the first family $\tau(p,k)$ provides a compact construction with dimension $p+1$, while the second family $v_t(1,k)$ offers a richer state space with dimension $p+t$, allowing a tunable trade-off between security and efficiency.

3.2. Preliminaries: Group Order and Exponent Space

Before presenting the algorithms, we must define the order of the cyclic subgroup generated by the matrix, as all exponents are reduced modulo this order.

Let $\tau = \tau(p,k)$ be the companion matrix from (2.2). Since $\det(\tau) = \pm 1$, τ is invertible modulo any prime q, and the set

$$\langle \tau \rangle_q = \{\tau^i \bmod q \mid i \geq 0\} \tag{34}$$

forms a cyclic subgroup of $\mathrm{GL}_{p+1}(\mathbb{F}_q)$. We denote its order by

$$\ell = \mathrm{ord}_q(\tau) = \min\{i > 0 \mid \tau^i \equiv I \pmod{q}\} \tag{35}$$

All exponents in the signature scheme are taken modulo ℓ. For the second family, we similarly define $\ell' = \mathrm{ord}_q(v_t(1,k))$. The security of our schemes relies on the hardness of the MDLP in these cyclic groups.

An important cryptographic property of our matrices is the determinant condition established in Lemmas 2.2 and 2.4:

$$\det(\tau^n) = \begin{cases} -1, & \text{if } p \text{ is even and } n \text{ is odd,} \\ 1, & \text{otherwise,} \end{cases} \tag{36}$$

and analogously for $v_t(1,k)$. We exploit this property in the verification step to detect signature forgery: a valid signature must satisfy not only the group equation but also the determinant-consistency condition, thereby providing an additional layer of security.

We now present the two signature schemes in detail, followed by numerical examples that illustrate their operation, and conclude with a comprehensive security analysis in Section 4.

3.3. Scheme I: Enhanced Digital Signature Using $\tau(p,k)$

We now present the first signature scheme based on the matrix $\tau(p,k)$. The scheme incorporates a dual-challenge mechanism and a determinant-based verification step, distinguishing it from standard Schnorr signatures. The signatures are shown in Figure 1.

Algorithm 1: Enhanced Digital Signature Using $\tau(p,k)$ with Dual-Challenge and Determinant Verification

Data: Prime q, matrix $\tau = \tau(p,k)$ with parameters p,k, its order ℓ, and two independent cryptographic hash functions $H_1, H_2 : \{0,1\}^* \to \mathbb{Z}_\ell$.
Input: Message $m \in \{0,1\}^*$.
Output: Signature $\sigma = (r_1, r_2, s, \delta)$, where $\delta = \det(r_1 \cdot r_2)$.

Key Generation:;
Choose private key $x \in \mathbb{Z}_\ell$ such that $\gcd(x,\ell) = 1$;
Compute public key $y \equiv \tau^x \pmod q$;
Store $\delta_y = \det(y)$ (public as well);
Signing (by Alice):;
Choose random nonces $d_1, d_2 \in \mathbb{Z}_\ell$ such that $d_1 \neq d_2$ and $\gcd(d_1 d_2, \ell) = 1$;
$r_1 \leftarrow \tau^{d_1} \bmod q$;
$r_2 \leftarrow \tau^{d_2} \bmod q$;
$e_1 \leftarrow H_1(m \,\|\, r_1 \,\|\, p)$;
$e_2 \leftarrow H_2(m \,\|\, r_2 \,\|\, p)$;
$s \leftarrow (d_1 \cdot e_1 + d_2 \cdot e_2 + x) \bmod \ell$;
$\delta \leftarrow \det(r_1 \cdot r_2) (\bmod q)$, Note that $\det(r_1 \cdot r_2)(\bmod q) = \det(r_1) \cdot \det(r_2)(\bmod q)$;
return $\sigma = (r_1, r_2, s, \delta)$;
Verification (by Bob):;
if $\det(r_1 \cdot r_2) \neq \delta$ then
  reject
end
;
$e_1 \leftarrow H_1(m \,\|\, r_1 \,\|\, p)$;
$e_2 \leftarrow H_2(m \,\|\, r_2 \,\|\, p)$;
if $\tau^s \equiv r_1^{e_1} \cdot r_2^{e_2} \cdot y \pmod q$ then
  accept
end
else
  reject
end

Figure 1. Enhanced digital signature algorithm using the generalized k-Chebyshev p-sequence companion matrix $\tau(p,k)$ with dual-challenge mechanism and determinant-based verification

3.3.1.Correctness

The verification holds by direct computation:

$$\tau^s = \tau^{d_1 e_1 + d_2 e_2 + x} = (\tau^{d_1})^{e_1} \cdot (\tau^{d_2})^{e_2} \cdot \tau^x = r_1^{e_1} \cdot r_2^{e_2} \cdot y \pmod q.$$

The determinant check $\det(r_1 \cdot r_2) = \delta$ ensures that the matrix product has not been tampered with; since $\det(\tau^{d_1+d_2}) = \det(\tau)^{d_1+d_2}$, the determinant is determined by the exponents and provides a consistency check.

3.3.2.Security Rationale

This scheme offers several novel security features:

1. Dual-challenge binding: The message is bound to both nonces r_1 and r_2 through the independent hashes e_1 and e_2. An adversary attempting to forge a signature on a different message m' would need to find s' satisfying

$$\tau^{s'} = r_1^{H_1(m' \| r_1 \| p)} \cdot r_2^{H_2(m' \| r_2 \| p)} \cdot y.$$

This requires solving two independent MDLP instances simultaneously, as the adversary does not know the relationship between r_1, r_2, and the private key x.

2. Determinant-based forgery detection: The inclusion of $\delta = \det(r_1 \cdot r_2)$ in the signature provides an algebraic consistency check. Any attempt to replace r_1 or r_2 with other matrices would require the adversary to maintain the determinant relationship, which is computationally infeasible without solving the MDLP.

3. Parameter-dependent hashing: Including p in the hash inputs ensures that the signature is bound to the specific sequence parameters, preventing cross-parameter attacks where an adversary might try to use a signature generated with one parameter set on another.
4. Resistance to additive exponent attacks: The additive forgery attack described in the introduction fails because s is a linear combination of two nonces multiplied by independent hash values. Any change to the message changes both e_1 and e_2 in a non-linear way, preventing simple exponent adjustments.

A formal security reduction to the MDLP is provided in Section 4.

3.4. Scheme II: Digital Signature Using $v_t(1,k)$

The same enhanced construction can be applied to the second family of matrices $v_t(1,k)$. Let $\ell' = \mathrm{ord}_q(v_t(1,k))$. The algorithm is analogous, with $v_t(1,k)$ replacing $\tau(p,k)$ and exponents taken modulo ℓ' which is shown in Figure 2.

Algorithm 2: Enhanced Digital Signature Using $v_t(1,k)$

Data: Prime q, matrix $v = v_t(1,k)$ with parameters t,k, its order ℓ', and hash functions $H_1, H_2 : \{0,1\}^* \to \mathbb{Z}_{\ell'}$.
Input: Message $m \in \{0,1\}^*$.
Output: Signature $\sigma = (r_1, r_2, s, \delta)$.

Key Generation:;
Choose $x \in \mathbb{Z}_{\ell'}$ with $\gcd(x, \ell') = 1$;
Compute $y \equiv v^x \pmod q$;
Signing:;
Choose random nonces $d_1, d_2 \in \mathbb{Z}_{\ell'}$ with $d_1 \neq d_2$ and $\gcd(d_1 d_2, \ell') = 1$;
$r_1 \leftarrow v^{d_1} \bmod q$;
$r_2 \leftarrow v^{d_2} \bmod q$;
$e_1 \leftarrow H_1(m \,\|\, r_1 \,\|\, p)$;
$e_2 \leftarrow H_2(m \,\|\, r_2 \,\|\, t)$;
$s \leftarrow (d_1 \cdot e_1 + d_2 \cdot e_2 + x) \bmod \ell'$;
$\delta \leftarrow \det(r_1 \cdot r_2 \bmod q)$, Note that $\det(r_1 \cdot r_2) (\bmod q) = \det(r_1) \cdot \det(r_2) (\bmod q)$;
return $\sigma = (r_1, r_2, s, \delta)$;
Verification:;
if $\det(r_1 \cdot r_2) \neq \delta$ then
  reject
end
;
$e_1 \leftarrow H_1(m \,\|\, r_1 \,\|\, p)$;
$e_2 \leftarrow H_2(m \,\|\, r_2 \,\|\, t)$;
if $v^s \equiv r_1^{e_1} \cdot r_2^{e_2} \cdot y \pmod q$ then
  accept
end
else
  reject
end

Figure 2. Enhanced digital signature algorithm using the (k,t)-Chebyshev p-sequence companion matrix $v_t(1,k)$

3.5. Parameter Selection and Efficiency

The enhanced scheme increases security by requiring an adversary to solve two independent MDLP instances. The recommended parameter sets for 128-bit security are shown in Table1.

Table 1. Recommended parameter sets for 128-bit security using both matrix families, showing dimension, field size, group order, and signature size

Family	Dimension	q (bits)	ℓ (bits)	Key size (bits)	Signature size (bits)
$\tau(5,2)$	6	256	≥ 256	≈ 9216	≈ 18432
$v_2(1,2)$	3	256	≥ 256	≈ 2304	≈ 4608

The signature size includes two matrices (r_1 and r_2), the scalar s, and the determinant δ. While larger than ECDSA, the enhanced scheme offers a stronger security guarantee due to the dual-challenge structure. Signing requires two matrix exponentiations ($O(2(n^3 \log \ell))$) and verification requires three ($O(3(n^3 \log \ell))$), where $n = p + 1$ or $n = p + t$. This is a reasonable trade-off for environments requiring post-quantum candidate security and tunable parameter spaces.

4. Security Analysis

In this section, we provide a comprehensive security analysis of the proposed digital signature schemes. We begin by formalizing the underlying hardness assumption, then define the adversarial model and security game, and finally present a reductionist proof of existential unforgeability under adaptive chosen-message attacks (EUF-CMA) in the random oracle model. We also analyze resistance to various classes of attacks, including brute-force, algebraic, and side-channel attacks.

4.1. Matrix Discrete Logarithm Problem (MDLP)

Let $\mathbb{F}_q$ be a finite field with q a large prime, and let $\tau \in \mathrm{GL}_n(\mathbb{F}_q)$ be an invertible matrix of order $\ell = \mathrm{ord}(\tau)$. The cyclic subgroup $\langle \tau \rangle = \{\tau^i \mid 0 \le i < \ell\}$ serves as the cryptographic group for our schemes.

Definition 1 (Matrix Discrete Logarithm Problem (MDLP)). *Given a matrix $\tau \in \mathrm{GL}_n(\mathbb{F}_q)$ and an element $y \in \langle \tau \rangle$, the Matrix Discrete Logarithm Problem is to find the unique exponent $x \in \mathbb{Z}_\ell$ such that $y \equiv \tau^x \pmod q$. We write $x = \log_\tau(y)$.*

Definition 2 (MDLP Assumption). *For any probabilistic polynomial-time (PPT) adversary $\mathcal{A}$, there exists a negligible function $\mathrm{negl}(\lambda)$ such that $\Pr[\mathcal{A}(q, \tau, \tau^x) = x \mid q \leftarrow \mathsf{Gen}(1^\lambda),\ \tau \leftarrow \mathrm{GL}_n(\mathbb{F}_q),\ x \leftarrow \mathbb{Z}_\ell] \le \mathrm{negl}(\lambda)$, where λ is the security parameter and the probability is taken over the random choices of Gen, τ, x, and the internal randomness of $\mathcal{A}$.*

This assumption generalizes the classical Discrete Logarithm Problem from multiplicative groups of finite fields to matrix groups. For our specific construction, τ is one of the companion matrices $\tau(p,k)$ or $\upsilon_t(1,k)$, and the group order ℓ is determined by the choice of q and the matrix parameters.

4.2. Adversarial Threat Model

We adopt the standard security framework for digital signatures, formalizing an adversary's capabilities and objectives in a rigorous game-based setting.

4.2.1.Adversarial Capabilities

We consider a probabilistic polynomial-time (PPT) adversary $\mathcal{A}$ that interacts with a challenger $\mathcal{C}$ in the EUF-CMA security game. The adversary possesses the following capabilities:

- **Full Knowledge of Public Parameters:** $\mathcal{A}$ knows all public cryptographic parameters, including:
  - The prime q and the finite field $\mathbb{F}_q$.
  - The matrix family $\tau(p,k)$ or $\upsilon_t(1,k)$ and the parameters p, k, t.
  - The group order ℓ (or ℓ').
  - The public key $y \equiv \tau^x \pmod q$.
  - The hash functions H_1, H_2 (modeled as random oracles).
- **Adaptive Signature Queries:** $\mathcal{A}$ may adaptively request valid signatures on any message m_i of its choice. The challenger responds with a valid signature $\sigma_i = (r_{1,i}, r_{2,i}, s_i)$ generated using the private key x.
- **Adaptive Hash Queries:** $\mathcal{A}$ may query the random oracles H_1 and H_2 on arbitrary inputs. The challenger responds with uniformly random values in $\mathbb{Z}_\ell$ (or $\mathbb{Z}_{\ell'}$).
- **Verification Oracle Access:** $\mathcal{A}$ may submit arbitrary signature candidates to a verification oracle, which returns whether the signature is valid.
- **Full Transcript Visibility:** $\mathcal{A}$ has access to the complete transcript of all interactions, including all signatures, hash queries and responses, and public parameters.
- **Malformed Input and Nonce Misuse:** $\mathcal{A}$ may attempt to exploit edge cases by submitting malformed messages or inducing nonce reuse. Our model assumes the signer uses a cryptographically secure random number generator.
- **Replay Attacks:** $\mathcal{A}$ may attempt to replay previously observed valid signatures on different messages or contexts.

4.2.2.Adversarial Objectives

The adversary's primary objective is to break existential unforgeability. Specifically, $\mathcal{A}$ aims to output a valid signature σ^* on a message m^* that was never queried to the signing oracle.

Secondary objectives include:

- **Key Recovery:** Recovering the private key x from $y = \tau^x$.
- **Selective Forgery:** Forging a signature on a predetermined message.
- **Universal Forgery:** Forging signatures on any message.
- **Hash Collisions:** Finding collisions in H_1 or H_2.

Our security proof demonstrates that none of these objectives can be achieved with non-negligible probability under the MDLP assumption.

4.2.3.Security Parameters and Key Generation

A security parameter parameterizes the security of our schemes λ:

1. The prime q is chosen such that $\log_2 q = \Theta(\lambda)$.
2. The group order ℓ has a largest prime factor ℓ_p with $\log_2 \ell_p \ge \lambda$.
3. The matrix dimension $n = p + 1$ or $n = p + t$ is such that $|\mathrm{GL}_n(\mathbb{F}_q)|$ is exponential in λ.

The key generation algorithm $\mathsf{Gen}(1^\lambda)$ proceeds as follows:

1. Select a prime q of the appropriate size.
2. Choose matrix parameters p, k (or p, t, k) according to the desired security level.

3. Construct the companion matrix τ (or υ).
4. Verify that $\ell = \mathrm{ord}(\tau)$ has a large prime factor $\ell_p \geq 2^{\lambda}$.
5. Choose $x \in_R \mathbb{Z}_{\ell_p}$ uniformly at random.
6. Compute $y \equiv \tau^x \pmod{q}$.
7. Output public key (q, τ, y, ℓ_p) and private key (x).

4.2.4.The EUF-CMA Security Game

The EUF-CMA security game is formally defined as follows:

Definition 3 (EUF-CMA Security Game). *The EUF-CMA game consists of the following phases:*

1. ***Setup Phase:*** *The challenger $\mathcal{C}$ runs* $\mathsf{Gen}(1^{\lambda})$ *to generate a key pair (x, y). The challenger gives the public key y to $\mathcal{A}$ and keeps x secret.*
2. ***Query Phase:*** *$\mathcal{A}$ may adaptively issue the following queries:*
   - ***Hash Query*** *$H_i(M)$: $\mathcal{C}$ maintains tables T_i. If M is in T_i, return the stored value. Otherwise, choose $e \in_R \mathbb{Z}_{\ell}$, store (M, e), and return e.*
   - ***Signature Query*** $\mathsf{Sign}(m)$*: $\mathcal{C}$ generates a valid signature σ on m using x and returns it.*
   - ***Verification Query*** $\mathsf{Verify}(m, \sigma)$*: $\mathcal{C}$ returns accept or reject.*
3. ***Forge Phase:*** *$\mathcal{A}$ outputs (m^*, σ^*).*
4. ***Win Condition:*** *$\mathcal{A}$ wins if σ^* is valid on m^* and m^* was never queried to* Sign.

Definition 4 (EUF-CMA Security). *A signature scheme is EUF-CMA secure if for every PPT adversary $\mathcal{A}$,* $\Pr[\mathcal{A}$ wins the EUF-CMA game$] \leq \mathrm{negl}(\lambda)$.

4.2.5.The Random Oracle Model

Our security proof operates in the random oracle model, where H_1, H_2 are modeled as truly random functions. In this model:

- Each distinct input returns a uniformly random value.
- The adversary cannot predict outputs without querying.
- The challenger can program the oracle by setting $H_i(M) = e$ for a chosen e.

The random oracle model is a standard heuristic in cryptography that enables efficient provable security proofs. In practice, the hash functions H_1 and H_2 can be instantiated using cryptographically secure hash functions such as SHA3, which are considered suitable for this model.

4.3. Formal Security Reduction

We now prove that the proposed signature scheme is EUF-CMA secure under the MDLP assumption in the random oracle model.

Theorem 1. *Let H_1, H_2 be modeled as random oracles. If the MDLP is hard in $\langle\tau\rangle$, then the dual-challenge signature scheme (*Scheme I, shown in Figure 1*) is EUF-CMA secure.*

Proof. We construct a PPT simulator $\mathcal{S}$ that, given an MDLP instance (q, τ, y) with $y = \tau^x$ for unknown x, uses a forger $\mathcal{A}$ that breaks EUF-CMA with non-negligible advantage ε to compute x.

Simulation Setup:

- $\mathcal{S}$ receives (q, τ, y) and sets the public key as y.
- $\mathcal{S}$ initializes tables T_1, T_2 for hash responses.

Simulating Hash Oracles: For $H_i(M)$, $\mathcal{S}$ returns the stored value if it exists; otherwise, chooses $e \in \mathbb{Z}_{\ell}$, stores (M, e), and returns e.

Simulating Signature Queries: When $\mathcal{A}$ requests a signature on m:

- Choose $s, e_1, e_2 \in \mathbb{Z}_{\ell}$.
- Choose $d_1, d_2 \in \mathbb{Z}_{\ell}$.
- Compute $r_1 \equiv \tau^{d_1} \pmod{q}$ and $r_2 \equiv \tau^{d_2} \pmod{q}$.
- Program the random oracles: $H_1(m \parallel r_1) = e_1$, $H_2(m \parallel r_2) = e_2$ (abort if already set).
- Return $\sigma = (r_1, r_2, s)$.

The simulated signature is valid since

$$r_1^{e_1} \cdot r_2^{e_2} \cdot y = \tau^{d_1 e_1 + d_2 e_2 + x} \tag{37}$$

and the distribution is identical to real signatures.

Extracting the Private Key: Suppose $\mathcal{A}$ outputs a valid forgery (m^*, r_1^*, r_2^*, s^*). Let $e_1^* = H_1(m^* \parallel r_1^*)$ and $e_2^* = H_2(m^* \parallel r_2^*)$. By validity,

$$\tau^{s^*} = (r_1^*)^{e_1^*} \cdot (r_2^*)^{e_2^*} \cdot y \tag{38}$$

By the forking lemma, rewinding $\mathcal{A}$ yields a second forgery (m^*, r_1^*, r_2^*, s') with different hash values e_1', e_2' but the same r_1^*, r_2^*, y. From the two forgeries:

$$\tau^{s^*-s'} = (r_1^*)^{e_1^*-e_1'} \cdot (r_2^*)^{e_2^*-e_2'} \tag{39}$$

Since $\mathcal{S}$ knows $r_1^* = \tau^{d_1^*}$ and $r_2^* = \tau^{d_2^*}$:

$$s^* - s' \equiv d_1^*(e_1^* - e_1') + d_2^*(e_2^* - e_2') \pmod{\ell}. \tag{40}$$

Repeating the forking argument on each hash challenge independently yields four forgeries, giving a system of linear equations that uniquely determines d_1^*, d_2^*. Then:

$$x \equiv s^* - d_1^* e_1^* - d_2^* e_2^* \pmod{\ell} \tag{41}$$

Probability Analysis: Let ε be the success probability of $\mathcal{A}$. By the forking lemma, the extraction probability is

$$\varepsilon' \geq \frac{\varepsilon}{q_H}\left(1 - \frac{1}{\ell}\right) - \frac{q_S}{\ell}. \tag{42}$$

Since ℓ is exponential in λ, this is non-negligible if ε is, contradicting the MDLP assumption. Therefore, no PPT adversary can break EUF-CMA with non-negligible probability. □

The proof for Scheme II follows identically with ℓ' replacing ℓ.

4.4. Resistance to Brute-Force Attacks

A brute-force attack attempts to guess the private key x by enumerating all possibilities. For our schemes:

For the $\tau(p, k)$ family:

$$|\langle\tau\rangle| = \ell \leq |\mathrm{GL}_{p+1}(\mathbb{F}_q)| = \prod_{i=0}^{p}(q^{p+1} - q^i) \tag{43}$$

For the $\upsilon_t(1, k)$ family:

$$|\langle\upsilon\rangle| = \ell' \leq |\mathrm{GL}_{p+t}(\mathbb{F}_q)| = \prod_{i=0}^{p+t-1}(q^{p+t} - q^i) \tag{44}$$

With recommended parameters $q \approx 2^{256}$ and $p = 5$ (dimension 6), the search space is approximately $q^{36} \approx 2^{9216}$, making exhaustive search infeasible. Pollard's rho algorithm requires $\ell \geq 2^{256}$ for 128-bit security—a condition satisfied by our parameter choices.

4.5. Resistance to Algebraic Attacks

4.5.1.Index-Calculus and Finite-Field Reductions

The primary algebraic vulnerability is a reduction of the MDLP to a classical finite-field DLP. This occurs when τ is conjugate to a companion matrix of an irreducible polynomial of degree n, in which case $\langle\tau\rangle \cong \mathbb{F}_{q^n}$.

To prevent this, we restrict parameter choices to ensure the minimal polynomial of τ is *not* irreducible of full degree. Specifically:

- The characteristic polynomial of $\tau(p, k)$ factors over $\mathbb{F}_q$ for suitable q, k.
- We select q such that the characteristic polynomial has a factor of degree at most $\lfloor(p + 1)/2\rfloor$.

For $\upsilon_t(1, k)$, analogous restrictions apply.

4.5.2.Pohlig-Hellman and Subgroup Attacks

The Pohlig-Hellman algorithm exploits the factorization of $\ell = \prod p_i^{e_i}$, computing discrete logs in $O(\sum e_i(\log\ell + \sqrt{p_i}))$ time. To resist this:

- We require ℓ to have a large prime factor $\ell_p \geq 2^{256}$.
- All exponents are reduced modulo ℓ_p, and y is verified to lie in the subgroup of order ℓ_p.

4.5.3.Linear Recurrence Attacks

The generalized k-Chebyshev sequences satisfy linear recurrences. An adversary might exploit linear relations among matrix entries across powers of τ. This is mitigated by:

- Random nonces d_1, d_2 for each signature.
- Hash-based binding of the message to nonces.
- The dual-challenge structure requiring two independent MDLP solutions.

4.6. Post-Quantum Security Considerations

Unlike classical DLP in finite fields, the MDLP in matrix groups is not known to be susceptible to Shor's algorithm in a direct manner. Shor's algorithm applies to abelian groups; while $\langle\tau\rangle$ is abelian, the full group $\mathrm{GL}_n(\mathbb{F}_q)$ is non-abelian for $n \geq 2$. The hidden subgroup problem in non-abelian groups is generally believed to be hard for quantum computers. However,

Battarbee et al. [2] have shown that certain instances admit subexponential quantum algorithms. The applicability of these algorithms to our construction requires further investigation, and the post-quantum security of matrix-based schemes remains an active area of research. Accordingly, the proposed schemes should be regarded as candidates for post-quantum security rather than established post-quantum-secure schemes

5. Conclusions

This paper introduced two novel generalizations of the classical *k-Chebyshev* sequences, the *k-Chebyshev p-sequences* and the *(k, t)-Chebyshev p-sequences* yielding companion matrices of dimensions $p+1$ and $p+t$. Applying these structures, we proposed a dual-challenge Schnorr-style digital signature scheme with parameter-dependent hashing that prevents algebraic forgeries. We proved EUF-CMA security under the MDLP assumption in the random oracle model and analyzed resistance to brute-force, index-calculus, Pohlig--Hellman, and linear recurrence attacks. For 128-bit security, we recommend $q \approx 2^{256}$ and $p=5$, yielding a keyspace of approximately2^{9216}. Limitations include larger signature sizes than ECDSA and candidate post-quantum status. Future work includes implementation and benchmarking, extension to blind and multi-signatures, and investigation of other sequence families. The results demonstrate that generalized sequence theory provides a powerful mathematical framework for designing efficient, provably secure public-key cryptography and digital signatures.

6. Statements & Declarations

6.1. Author Contributions

Conceptualization, R.E.A and E.M.; methodology, E.M.; software, R.E.A; validation, R.E.A. and E.M.; formal analysis, R.E.A.; investigation, R.E.A. and E.M.; writing—original draft preparation, E.M.; writing—review and editing, R.E.A.; visualization, R.E.A.; All authors have read and agreed to the published version of the manuscript.

6.2. Data Availability Statement

No new data were created or analyzed in this study. Data sharing is not applicable to this article.

6.3. Funding

This research received no external funding.

6.4. Acknowledgments

Not applicable.

6.5. Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this manuscript, the author(s) used Deepseek for language editing/grammar checking/improving readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take full responsibility for the content of the published article.

6.6. Ethics Approval

Not applicable.

6.7. Informed Consent

Not applicable.

6.8. Consent for Publication

Not applicable.

6.9. Conflicts of Interest

The author(s) declare no conflict of interest.

7. References

[1] M. Imran and G. Ivanyos, “Efficient quantum algorithms for some instances of the semidirect discrete logarithm problem,” Designs, Codes and Cryptography, vol. 92, no. 10, pp. 2825–2843, May 2024, doi:10.1007/s10623-024-01416-8.

[2] C. Battarbee, D. Kahrobaei, L. Perret, and S. F. Shahandashti, “A Subexponential Quantum Algorithm for the Semidirect Discrete Logarithm Problem,” Post-Quantum Cryptography, PQCrypto 2024. Lecture Notes in Computer Science, vol 14771, pp. 202–226, Springer, Cham, Switzerland, 2024, doi:10.1007/978-3-031-62743-9_7.

[3] D. Chaum, “Blind Signatures for Untraceable Payments,” Advances in Cryptology, pp. 199–203, Springer, Boston, United States, 1983, doi:10.1007/978-1-4757-0602-4_18.

[4] X. Hu, J. Wang, and Y. Yang, “Secure ID-Based Blind Signature Scheme without Random Oracle,” 2011 International Conference on Network Computing and Information Security, pp. 245–249, May 2011, doi:10.1109/ncis.2011.56.

[5] A. Rahman and K. Husain, “A Strong Blind Signature Using Cascade Blind Factors,” Int. J. Innov. Res. Comput. Sci. Technol. (IJIRCST, vol. 4, no. ue 1, pp. 7–9.

[6] E. Mehraban, T. A. Gulliver, R. E. Atani, and E. Hincal, “Blind Rsa Signatures from the T−Generalized Lehmer Sequences of Some Classes Of Groups,” Math. Found. Comput., vol. 11, pp. 1–17, 2026, doi: 10.3934/MFC.2025036.

[7] E. Mehraban, R. Ebrahimi Atani, T. A. Gulliver, and E. Hincal, "From Sequences to Cryptography: k-Division t-Fibonacci-Pell Matrices in ElGamal Cryptographic Schemes." To appear in the Contributions of Science and Technology for Engineering, Vol.4, No.1, 2027.

[8] E. Mehraban, T. Aaron Gulliver, R. Ebrahimi Atani, and E. Hincal, "Diffie-Hellman key exchange on the Heisenberg group[J," J. Comb. Math. Comb. Comput., vol. 127, pp. 301–315, doi: 10.61091/jcmcc127-22.

[9] E. Mehraban, R. Ebrahimi Atani, O. Deveci, and G. Golkarian, "Determinant-preserving blind signatures from Hadamard-type t-Jacobsthal–Leonardo sequences," Notes Number Theory Discret. Math., vol. 32, no. 1, pp. 96–111,, doi: 10.7546/nntdm.2026.32.1.96-111.

[10] M. Esmaeili, M. Moosavi, and T. A. Gulliver, "A new class of Fibonacci sequence based error correcting codes," Cryptogr. Commun., vol. 9, no. 3, pp. 379–396, 2017, doi:10.1007/s12095-015-0178-x.

[11] E. Mehraban and M. Hashemi, "Coding theory on the generalized balancing sequence," Notes Number Theory Discret. Math., vol. 29, no. 3, pp. 503–524, 2023, doi:10.7546/nntdm.2023.29.3.503-524.

[12] K. Prasad and H. Mahato, "Cryptography using generalized Fibonacci matrices with Affine-Hill cipher," J. Discret. Math. Sci. Cryptogr., vol. 25, no. 8, pp. 2341–2352, 2022, doi:10.1080/09720529.2020.1838744.

[13] E. Mehraban, T. Aaron Gulliver, S. M. Boulaaras, K. Hosseini, and E. Hincal, "New sequences from the generalized Pell p−numbers and mersenne numbers and their application in cryptography," AIMS Math., vol. 9, no. 5, pp. 13537–13552, 2024, doi:10.3934/math.2024660.

[14] J. Partala, "Algebraic generalization of Diffie-Hellman key exchange," J. Math. Cryptol., vol. 12, no. 1, pp. 1–21, 2018, doi:10.1515/jmc-2017-0015.

[15] M. K. Viswanath and M. R. Kumar, "A Public Key Cryptosystem Using Hiil's Cipher," J. Discret. Math. Sci. Cryptogr., vol. 18, no. 1–2, pp. 129–138, 2015, doi:10.1080/09720529.2014.962856.

[16] E. Mehraban, T. A. Gulliver, Ö. Deveci, and E. Hincal, "Affine-Hill cipher key generation using self-invertible matrices from k-division L-Lehmer-Pell sequences," J. Comb. Math. Comb. Comput., vol. 124, pp. 47–58, 2025, doi:10.61091/jcmcc124-03.

[17] L. Kocarev and Z. Tasev, "Public-key encryption based on Chebyshev maps," Proceedings of the 2003 International Symposium on Circuits and Systems, 2003. ISCAS '03., vol. 3, pp. III–28–III–31, doi:10.1109/iscas.2003.1204947.

[18] Z. Pucanović and M. Pešović, "Chebyshev polynomials and r-circulant matrices," Appl. Math. Comput., vol. 437, p. 127521, 2023, doi:10.1016/j.amc.2022.127521.

[19] A. R. Naseri, A. Abbasi, and R. E. Atani, "A new public key cryptography using Mq matrix," J. Math. Model., vol. 11, no. 4, pp. 681–693, 2023, doi: 10.22124/jmm.2023.23982.2142.

[20] O. Deveci and Y. Akuzum, "The Cyclic Groups and the Semigroups via MacWilliams and Chebyshev Matrices," J. Math. Res., vol. 6, no. 2, pp. 55–58, 2014, doi: 10.5539/jmr.v6n2p55.

[21] Ö. Deveci and E. Karaduman, "The cyclic groups via the Pascal matrices and the generalized Pascal matrices," Linear Algebra Appl., vol. 437, no. 10, pp. 2538–2545, 2012, doi: 10.1016/j.laa.2012.06.024.

[22] B. Kuloglu and E. Ozkan, "Matrix representation of (d, k) - Fibonacci polynomials," Bulletin of the Transilvania University of Brasov. Series III: Mathematics and Computer Science, pp. 185–200, Sep. 2024, doi:10.31926/but.mif.2024.4.66.2.11.

[23] M. Uysal and E. Özkan, "On Pell functions and Pell numbers," Research & Reviews: Discrete Mathematical Structures, vol. 10, no. 3, 2024.

[24] Deveci and E. Karaduman, "Lehmer sequences in finite groups," Ukr. Math. J., vol. 68, no. 2, pp. 193–202, 2016, doi: 10.1007/s11253-016-1218-1.

[25] E. Mehraban, T. A. Gulliver, E. Hinçal, and Y. Li, "New signature schemes from the Hadamard-type (k,t)-generalized Jacobsthal-Lehmer sequences on the 2-generator p-group of nilpotency class 2," Expert Syst. Appl., vol. 296, pt. A, 2026.

[26] M. Abchiche and H. Belbachir, "Generalized Chebyshev polynomials," Discussiones Mathematicae - General Algebra and Applications, vol. 38, no. 1, p. 79, 2018, doi: 10.7151/dmgaa.1278.

[27] J. Kishore and V. Verma, "Some identities involving Chebyshev polynomials, Fibonacci polynomials and their derivatives," Notes Number Theory Discret. Math., vol. 29, no. 2, pp. 204–215, 2023, doi: 10.7546/nntdm.2023.29.2.204-215.

[28] E. Ozkan and H. Akkus, "On K-Chebsyhev Sequence," WSEAS Trans. Math., vol. 22, pp. 503–507, 2023, doi: 10.37394/23206.2023.22.56.

[29] Z. Pucanović and M. Pešović, "Analyzing Chebyshev polynomial-based geometric circulant matrices," Electron. Res. Arch., vol. 32, no. 9, pp. 5478–5495, 2024, doi: 10.3934/era.2024254.