Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Diffie-Hellman key exchange on the Heisenberg group

Elahe Mehraban✉, T. Aaron Gulliver, Reza Ebrahimi Atani, Evren Hincal

ABSTRACT

This paper introduces Hadamard-type t-Fibonacci-Lehmer (HTFL) sequences, a new hybrid construction combining Lehmer and Fibonacci recurrences. We establish their fundamental properties, including simple periodicity, and extend the definition to finite groups, with a detailed study of the Heisenberg group. Building on these results, we propose two Diffie–Hellman-style key exchange protocols based on upper-triangular unipotent matrices parameterized by HTFL sequence terms. Our work thus connects sequence theory, group theory, and cryptography in a novel way. While the algebraic framework and periodicity analysis are rigorous, we present the cryptographic constructions primarily as a conceptual foundation. We also discuss potential security considerations and outline directions for strengthening these schemes under formal hardness assumptions. This study demonstrates that HTFL sequences provide a fertile ground for both combinatorial investigations and future cryptographic applications.

Keywords: period, Fibonacci sequence, Lehmer sequence, Diffie-Hellman key exchange

1. Introduction

Public key cryptography is built on algebraic structures that support hard computational problems, most notably the discrete logarithm problem in finite fields and elliptic curves. Diffie-Hellman key exchange is among the earliest and most widely used public key cryptographic techniques [4, 5, 9]. The classical Diffie Hellman key exchange protocol, derives its security from the presumed intractability of computing discrete logarithms in cyclic groups. Over the past two decades, there has been growing interest in exploring alternative algebraic and combinatorial settings for cryptography, including non-abelian groups

✉ Corresponding author.
E-mail address: e.mehraban.math@gmail.com (E. Mehraban).

Received 02 Apr 2024; Revised 11 Sep 2025; Accepted 02 Oct 2025; Published Online 17 Oct 2025.

DOI: 10.61091/jcmcc127-22

(such as braid groups, matrix groups, and Heisenberg groups) as well as number-theoretic sequences (such as Fibonacci, Lehmer, Pell, and Mersenne sequences). These directions are motivated both by the search for new hardness assumptions and by the potential to develop post-quantum secure primitives.

The Fibonacci and Lehmer sequences have been extensively investigated in number theory and have found applications in pseudorandom number generation and cryptography. Similarly, generalized Fibonacci-type sequences, including t-step recurrences, have been studied in algebraic structures and finite groups. However, the systematic combination of these sequences into hybrid constructions and their application in non-abelian groups for cryptographic purposes remains largely unexplored.

In this paper, we introduce Hadamard-type t-Fibonacci-Lehmer (HTFL) sequences, a new class of hybrid recurrences that generalize both Lehmer and t-step Fibonacci sequences. We prove that these sequences are simply periodic in the special case $M = \pm 1$, and extend the construction to finite groups. We then focus on the Heisenberg group, a well-known non-abelian nilpotent group with applications in mathematics and physics, and show how HTFL sequences can be realized in this setting.

Definition 1.1. [13] For integers L, M, and $LM \neq 0$, $L - 4M \neq 0$, the Lehmer sequence $\{U_n(L,M)\}_{n=0}^{\infty}$ is

$$U_n(L,M) = \begin{cases} 0, & \text{if } n = 0, \\ 1, & \text{if } n = 1, \\ LU_{n-1}(L,M) - MU_{n-2}(L,M), & \text{if } n \text{ odd}, \\ U_{n-1}(L,M) - MU_{n-2}(L,M), & \text{if } n \text{ even}. \end{cases}$$

Many studies have been conducted on the Lehmer sequence [2, 14, 24]. In [6], Lehmer sequences on finite groups were introduced and their period was studied. Three RSA algorithms were given in [17] based on the Lehmer sequences and Lehmer orbits on groups.

The $t-$Fibonacci sequence $\{F_n(t)\}_{n=0}^{\infty}$ is defined as

$$F_n(t) = F_{n-1}(t) + F_{n-2}(t) + \cdots + F_{n-t}(t), \quad n \geq t,$$

with initial conditions $F_0(t) = F_1(t) = \cdots = F_{n-t-2}(t) = 0$ and $F_{n-t-1}(t) = 1$ [10]. In [3], the Fibonacci length of certain centro-polyhedral groups was determined. The Fibonacci length of the 2-generator $p-$groups of nilpotency class 2 was given in [12].

In [19], a new generalization of the Fibonacci sequence was presented that gives the copper ratio. The generalized bronze Fibonacci sequences and their hyperbolic quaternions were obtained in [20] and the relationships between the roots of the characteristic equation of these sequences were given.

From [18] we have the following. For $m, s, v \in Z$, the elements of the Heisenberg group $H_{(m,s,v)}$ can be expressed in matrix form as

$$\begin{bmatrix} 1 & m & v + ms \\ 0 & 1 & s \\ 0 & 0 & 1 \end{bmatrix}.$$

Lemma 1.2. *Every element of $H_{(m,s,v)}$ can be written uniquely in the form $a^i b^j c^k$, where $1 \leq i \leq m, 1 \leq j \leq s$ and $1 \leq k \leq v$.*

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

Definition 1.3. [1] The Hadamard-type product of polynomials f and g is $f * g = \sum_{i=0}^{\infty}(a_i * b_i)x^i$ where

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

and $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$.

The classical Diffie-Hellman key exchange relies on exponentiation in cyclic groups and A universal algebraic generalization of the Diffie-Hellman scheme was presented in [23]. Although numerous generalizations to alternative algebraic settings have been explored [7, 23]. In particular, Partala introduced the *Algebraically Generalized Diffie–Hellman* (AGDH) framework [23], which abstracts key exchange to any algebraic structure admitting suitable endomorphisms, and formalized security through the *Homomorphic Image Problemma* (HIP) and its decision and computational variants. AGDH highlights that the essential ingredient of Diffie–Hellman protocols is the existence of commuting actions that enable both parties to derive a common secret from partially shared information.

In [16], two algorithms were given for Diffie-Hellman key exchange based on the generalized Pell $p-$numbers and Mersenne numbers. Here, the HTFL sequences are used for Diffie-Hellman key exchange on the Heisenberg group.

While our mathematical results are rigorous, we present the cryptographic application primarily as a conceptual framework. A preliminary security discussion is given, and we outline directions for strengthening the protocols under formal hardness assumptions. Our contributions can be summarized as follows:

- Definition and analysis of HTFL sequences: A hybrid of Lehmer and t-Fibonacci sequences with proven periodicity properties.
- Extension to finite groups: Formalization of HTFL sequences in group settings, with emphasis on the Heisenberg group.
- Cryptographic application: Two prototype Diffie-Hellman protocols using HTFL sequences in matrix form, together with initial security considerations.

Our work may be viewed as a concrete instantiation of this general paradigm. Specifically, we introduce *Hadamard-type t-Fibonacci–Lehmer (HTFL) sequences* and embed them into upper-triangular unipotent matrix groups, focusing on the Heisenberg model. In this setting, the commuting structure arises from matrix exponentiation with HTFL-parameterized elements. From this perspective, our protocols realize an instance of AGDH in a non-abelian group context, with hardness assumptions naturally corresponding to HIP in the HTFL–Heisenberg framework. Thus, while our scheme is specialized and sequence-driven, it aligns with the broader direction of algebraic generalizations of Diffie-Hellman and contributes a novel family of candidate constructions for study within this landscape.

The remainder of this paper is organized as follows: In Section 2, the Hadamard-type $t-$Fibonacci-Lehmer sequences are introduced and it is shown that they are simply periodic. The Hadamard-type $t-$Fibonacci-Lehmer sequences on a finite group are defined in Section 3 and they are studied on the Heisenberg group. In Section 4, the Hadamard-type $t-$Fibonacci-Lehmer sequences are used for Diffie-Hellman key exchange. Finally, Section 5 gives some concluding remarks.

2. Hadamard-type $t-$Fibonacci-Lehmer sequences

In this section, we define new sequences and then obtain results that will be used in the following sections. The characteristic polynomials of the Lehmer and $t-$Fibonacci sequences are

$$\begin{cases} x^2 - Lx + M, & \text{if } n \text{ odd}, \\ x^2 - x + M, & \text{if } n \text{ even}, \end{cases}$$

and $x^t - x^{t-1} - \cdots - x - 1$, respectively. From Definition 1.3 we have the following sequences.

Table 1. $UF_n(L,1)$ for $-10 \leq L \leq -1$ and $0 \leq n \leq 10$

n	0	1	2	3	4	5	6	7	8	9	10
$L=-1$	0	1	0	2	3	2	7	8	17	16	41
$L=-2$	0	1	0	2	3	7	6	23	24	76	75
$L=-3$	0	1	0	3	4	13	12	55	56	233	232
$L=-4$	0	1	0	4	5	21	20	109	110	565	2939
$L=-5$	0	1	0	5	6	31	30	191	197	1177	1176
$L=-6$	0	1	0	6	7	43	42	307	308	2192	2191
$L=-7$	0	1	0	7	8	57	56	463	464	3761	3760
$L=-8$	0	1	0	8	9	73	72	665	666	6058	6057
$L=-9$	0	1	0	9	10	91	90	919	920	9281	9280
$L=-10$	0	1	0	10	11	111	110	1231	1232	13652	13651

Definition 2.1. For integers L, M, t, and $LM \neq 0$, $L - 4M \neq 0$, the Hadamard-type $t-$Fibonacci-Lehmer sequence, $\{UF_n^t(L,M)\}_{n=0}^{\infty}$ is

$$UF_n^t(L,M) = \begin{cases} UF_{n-1}^t(L,M) + UF_{n-2}^t(L,M) + \cdots + UF_{n-t+2}^t(L,M) & \\ \quad - LUF_{n-t+1}^t(L,M) + MUF_{n-t}^t(L,M), & \text{if } n \text{ is odd}, \\ & \\ UF_{n-1}^t(L,M) + UF_{n-2}^t(L,M) + \cdots + UF_{n-t+2}^t(L,M) & \\ \quad - UF_{n-t+1}^t(L,M) + MUF_{n-t}^t(L,M), & \text{if } n \text{ is even}. \end{cases}$$

where $UF_0^t(L,M) = 0$, $UF_1^t(L,M) = 1$, $UF_2^t(L,M) = 0$, and $UF_3^t(L,M) = \cdots = UF_{t-1}^t(L,M) = 1$.

For example, if $M = 1$ and $t = 3$, we have

$$UF^3_n(L,1) = \begin{cases} UF^3_{n-1}(L,1) - LUF^3_{n-2}(L,1) + MUF^3_{n-3}(L,1), & \text{if } n \text{ odd,} \\ UF^3_{n-1}(L,1) - UF^3_{n-2}(L,M) + UF^3_{n-3}(L,1), & \text{if } n \text{ even.} \end{cases}$$

Table 1 gives $UF^3_n(L,1)$ for $-10 \le L \le -1$ and $0 \le n \le 10$.

Theorem 2.2. *For $t \ge 3$ and $M = \pm 1$, the sequence $\{UF^t_n(L,M)\}$ is simply periodic.*

Proof. Let $X_t = \{(x_1, x_2, \cdots, x_t) \mid x_i \in \mathbb{N} \text{ and } 1 \le x_t \le \alpha\}$ so then $\mid X_t \mid = \alpha^t$. Since there are only a finite number of possible pairs of α^t, the sequence must repeat. We then have that $\{UF^t_n(L,M)\}$ is periodic. Otherwise, assume that $M = \pm 1$. Then for $i \ge 0$, there exist $i \ge j$ such that

$$\begin{aligned} UF^{t,\alpha}_{i+t}(L,M) &\equiv UF^{t,\alpha}_{j+t}(L,M), UF^{t,\alpha}_{i+t-1}(L,M) \\ &\equiv UF^{t,\alpha}_{j+t-1}(L,M), \cdots, UF^{t,\alpha}_{i}(L,M) \equiv UF^{t,\alpha}_{j}(L,M). \end{aligned}$$

From the definition of the HTFL sequences we have

$$\begin{aligned} UF^{t,\alpha}_{i+t-j}(L,M) &\equiv UF^{t,\alpha}_{t}(L,M), UF^{t,\alpha}_{i+t-1-j}(L,M) \\ &\equiv UF^{t,\alpha}_{t-1}(L,M), \cdots, UF^{t,\alpha}_{i-j}(L,M) \equiv UF^{t,\alpha}_{0}(L,M). \end{aligned}$$

Thus, the HTFL sequences are simply periodic. □

Let $FK^t_\alpha(L,M)$ denote the minimal period of the HTFL sequences modulo α.

Example 2.3. (i) We have $\{UF^{3,5}_n(-3,1)\} = \{0,1,0,3,4,3,2,\cdots,0,1,0,3,\cdots\}$. Thus, $UF^3_0(-3,1) \equiv UF^3_{40}(-3,1), UF^3_1(-3,1) \equiv UF^3_{41}(-3,1), UF^3_2(-3,1) \equiv UF^3_{42}(-3,1)$, and so $FK^3_5(-3,1) = 40$.

(ii) We have $\{UF^{3,7}_n(-4,1)\} = \{0,1,0,4,5,0,6,4\cdots,0,1,0,4,\cdots\}$ and $UF^3_0(-4,1) \equiv UF^3_{12}(-4,1), UF^3_1(-4,1) \equiv UF^3_{13}(-4,1), UF^3_2(-4,1) \equiv UF^3_{14}(-4,1)$. Therefore, $FK^3_7(-4,1) = 12$.

Lemma 2.4. *For $t \ge 3, M = \pm 1, n \ge 2$, and i, j, we have*

(i) $UF^t_{FK^t_n(L,M)+i}(L,M) = UF^t_i(L,M) \pmod{n}$,

(ii) $UF^t_{j \times FK^t_n(L,M)+i}(L,M) = UF^t_i(L,M) \pmod{n}$.

Proof. (i) The result follows from the definition of the minimal period of the HTFL sequences modulo n.

(ii) We have

$$UF^t_{jFK^t_n(L,M)+i}(L,M) = UF^t_{FK^t_n(L,M)+(j-1)FK^t_n(L,M)+i}(L,M) = \cdots = UF^t_i(L,M).$$

□

Corollary 2.5. *For $t \geq 3, M = \pm 1$, and v an integer, if*

$$\begin{cases} UF_v^t(L,M) \equiv 0 \pmod{\alpha}, \\ UF_{v+1}^t(L,M) \equiv 1 \pmod{\alpha}, \\ UF_{v+2}^t(L,M) \equiv 0 \pmod{\alpha}, \\ UF_{v+3}^t(L,M) \equiv 1 \pmod{\alpha}, \\ \vdots \\ UF_{v+t-1}^t(L,M) \equiv 1 \pmod{\alpha}, \end{cases}$$

then $FK_\alpha^t(L,M)|v$.

Proof. Let $v = s \times FK_\alpha^t(L,M) + i$ where $0 \leq i < FK_\alpha^t(L,M)$. Since $FK_\alpha^t(L,M)$ is the smallest integer such that the assumption holds, the result follows from Lemma 2.4. □

3. The Hadamard-type $t-$Fibonacci-Lehmer sequences (HTFL) in finite groups

In this section, we define the HTFL sequences in finite groups and prove that they are simply periodic. We also study these sequences on the group $H_{(k,s,m)}$. The Hadamard-type $t-$Fibonacci-Lehmer sequences in a finite group are defined as follows.

Definition 3.1. For $t \geq 3$ and integers L, M, and $LM \neq 0$, $L - 4M \neq 0$, a Hadamard-type $t-$Fibonacci-Lehmer sequence on a finite group is a sequence of group elements $x_0, x_1, \cdots, x_n, \cdots$, given an initial (seed) set $X = \{a_1, a_2, \cdots, a_j\}$ where $j \geq 3$, is

$$x_{i+1} = \begin{cases} a_j, & \text{if } i+1 \leq j, \\ (x_{i-t+1}) \cdots x_{i-2}(x_{i-1})^{-L}(x_i)^M, & \text{if } i \text{ even}, \\ (x_{i-t+1}) \cdots x_{i-2}(x_{i-1})^{-1}x_i^M, & \text{if } i \text{ odd}. \end{cases} \tag{1}$$

The elements of the Hadamard-type $t-$Fibonacci-Lehmer sequences in a finite group are denoted by $UF_t^{L,M}(G)$ and the corresponding period is $PF_t^{L,M}(G)$.

Theorem 3.2. *The Hadamard-type $t-$Fibonacci-Lehmer sequences in a finite group are simply periodic if $M = \pm 1$, and periodic otherwise.*

Proof. Let G be a $j-$generator group and $(a_0, a_1, \cdots, a_{j-1})$ be a generating $j-$tuple for G. If $\mid G \mid = m$, then there are m^j distinct $j-$tuples of elements of G which implies that this subsequence repeats, i.e. the sequence is periodic. For simply periodic, there exist r and s in $\mathbb{N}$ with $s > r$ such that $x_s = x_r, x_{s+1} = x_{r+1}, \cdots, x_{s+t} = x_{r+t}$. From Definition 3.1, $x_{s-r} = x_0, x_{s-r+1} = x_1, \cdots, x_{s-r+t-1} = x_{t-1}$, so $UF_t^{L,M}(G)$ is simply periodic. □

For $M = 1$, we study the Hadamard-type $3-$Fibonacci-Lehmer sequences on the finite group $H_{(m,s,v)}$ with respect to $X = \{a, b, c\}$ and obtain that $FK_s^t(L, 1)$ divides

$PF_3^{L,1}(H_{(m,s,v)})$ when $L < 0$. Let $UF_n(L) := UF_n^3(L,1)$ and consider the following sequences

$$T_0(L) = 1, \;\; T_1(L) = 0, \;\; T_2(L) = 0,$$
$$T_{n+1}(L) = \begin{cases} T_{n-2}(L) + LT_{n-1}(L) + T_n(L), & \text{if } n \text{ even,} \\ T_{n-2}(L) - T_{n-1}(L) + T_n(L), & \text{if } n \text{ odd,} \end{cases}$$

and

$$w_0(L) = w_1(L) = 0, \;\; w_2(L) = 1,$$
$$w_{n+1}(L) = \begin{cases} \begin{array}{l} w_{n-2}(L) - w_{n-1}(L) + w_n(L) - (T_n(L) \\ \quad -T_{n-1}(L))(UF_{n-2}(L) - UF_{n-1}(L)), \end{array} & \text{if } n \text{ odd,} \\ \begin{array}{l} w_{n-2}(L) + Lw_{n-1}(L) + w_n(L) - (T_{n-1}(L)UF_{n-2}(L) \\ \quad +T_{n-1}(L)(UF_{n-2}(L) + UF_{n-1}(L)) \\ \quad + \cdots + T_{n-1}(L)(UF_{n-2}(L) + (L-1)UF_{n-1}(L)) \\ \quad +T_n(L)(UF_{n-2}(L) + LUF_{n-1}(L))), \end{array} & \text{if } n \text{ even.} \end{cases}$$

Lemma 3.3. *For $L < 0$ and $M = 1$, every element of the Hadamard-type $3-$Fibonacci-Lehmer sequences $UF_3^{L,1}(H_{(m,s,v)})$ can be written in the form $x_n = a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)}, n \geq 3$.*

Proof. For $n = 3$ and $n = 4$, we have $x_3 = x_0x_1x_2 = ab^Lc$ and $x_4 = x_1x_2x_3 = bc^{-1}(ab^Lc) = ab^{L+1}c^{-1}$. Then by induction on n, if n is even we have

$$\begin{aligned} x_{n+1} &= x_{n-2}x_{n-1}^L x_n \\ &= a^{T_{n-2}(L)} b^{UF_{n-2}(L)} c^{w_{n-2}(L)} \big(a^{T_{n-1}(L)} b^{UF_{n-1}(L)} c^{w_{n-1}(L)}\big)^L a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)} \\ &= a^{T_{n-2}(L)+T_{n-1}(L)} b^{UF_{n-2}(L)+UF_{n-1}(L)} c^{w_{n-2}(L)+w_{n-1}(L)-T_{n-1}(L)UF_{n-2}(L)} \\ &\quad \big(a^{T_{n-1}(L)} b^{UF_{n-1}(L)} c^{w_{n-1}(L)}\big)^{L-1} a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)} \\ &= \cdots \\ &= a^{T_{n-2}(L)+LT_{n-1}(L)} b^{UF_{n-2}(L)+LUF_{n-1}(L)} \\ &\quad c^{w_{n-2}(L)+Lw_{n-1}(L)-(T_{n-1}(L)UF_{n-2}(L)+T_{n-1}(L)(UF_{n-2}(L)+UF_{n-1}(L))+\cdots+T_{n-1}(L)} \\ &\quad c^{(UF_{n-2}(L)+(L-1)UF_{n-1}(L)))} a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)} \\ &= a^{T_{n-2}(L)+LT_{n-1}(L)+T_n(L)} b^{UF_{n-2}(L)+LUF_{n-1}(L)+UF_n(L)} \\ &\quad c^{w_{n-2}(L)+Lw_{n-1}(L)+w_n(L)-(T_{n-1}(L)UF_{n-2}(L)+T_{n-1}(L)(UF_{n-2}(L)+UF_{n-1}(L))+\cdots+T_{n-1}(L)} \\ &\quad c^{(UF_{n-2}(L)+(L-1)UF_{n-1}(L))+T_n(L)(UF_{n-2}(L)+LUF_{n-1}(L)))} \\ &= a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)}, \end{aligned}$$

and if n is odd

$$\begin{aligned} x_{n+1} &= x_{n-2}x_{n-1}^{-1}x_n = \\ &= a^{T_{n-2}(L)} b^{UF_{n-2}(L)} c^{w_{n-2}(L)} \big(a^{T_{n-1}(L)} b^{UF_{n-1}(L)} c^{w_{n-1}(L)}\big)^{-1} a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)} \\ &= a^{T_{n-2}(L)-T_{n-1}(L)} b^{UF_{n-2}(L)-UF_{n-1}(L)} \end{aligned}$$

$$\begin{aligned}
&\quad c^{w_{n-2}(L)-w_{n-1}(L)+(UF_{n-2}(L)-UF_{n-1}(L))T_{n-1}(L)}a^{T_n(L)}b^{UF_n(L)}c^{w_n(L)}\\
&= a^{T_{n-2}(L)-T_{n-1}(L)+T_n(L)}b^{UF_{n-2}(L)-UF_{n-1}(L)+UF_n(L)}\\
&\quad c^{w_{n-2}(L)-w_{n-1}(L)+w_n(L)-(T_n(L)-T_{n-1}(L))(UF_{n-2}(L)-UF_{n-1}(L))}\\
&= a^{T_n(L)}b^{UF_n(L)}c^{w_n(L)}.
\end{aligned}$$

□

Lemma 3.4. *If $Pk_3^{L,1}(H_{(m,s,v)}) = i$, then v is the least integer such that*

$$\begin{cases}
T_{i-2}(L) \equiv 1 \pmod{m},\\
T_{i-1}(L) \equiv 0 \pmod{m},\\
T_i(L) \equiv 0 \pmod{m},\\
UF_i(L) \equiv 0 \pmod{s},\\
UF_{i+1}(L) \equiv 1 \pmod{s},\\
UF_{i+2}(L) \equiv 0 \pmod{s},\\
w_i(L) \equiv 0 \pmod{v},\\
W_{i+1}(L) \equiv 0 \pmod{v},\\
W_{i+2}(L) \equiv 1 \pmod{v},
\end{cases}$$

all hold. Moreover, $FK_s^3(L,1)$ divides $PK_3^{(L,1)}(H_{(m,s,v)})$.

Proof. By Lemma 3.3, we have $x_n = a^{T_n(L)}b^{UF_n(L)}c^{w_n(L)}$. Since $x_v = a$, $x_{v+1} = b$, and $x_{v+2} = c$, by Lemma 1.2 we have

$$\begin{cases}
T_{i-2}(L) \equiv 1 \pmod{m},\\
T_{i-1}(L) \equiv 0 \pmod{m},\\
T_i(L) \equiv 0 \pmod{m},\\
UF_i(L) \equiv 0 \pmod{s},\\
UF_{i+1}(L) \equiv 1 \pmod{s},\\
UF_{i+2}(L) \equiv 0 \pmod{s},\\
w_i(L) \equiv 0 \pmod{v},\\
W_{i+1}(L) \equiv 0 \pmod{v},\\
W_{i+2}(L) \equiv 1 \pmod{v}.
\end{cases}$$

Then from Corollary 2.5, $FK_s^3(L,1) \mid v$. □

4. Diffie-Hellman key exchange using the Hadamard-type $t-$Fibonacci-Lehmer sequences on $H_{(m,s,v)}$

In this section, the Hadamard-type $t-$Fibonacci-Lehmer sequences on $H_{(m,s,v)}$ are used for Diffie-Hellman key exchange. For $n \geq 1$ and $m, s, v \in \mathbb{Z}$, each element of the Heisenberg group, $H_{(m,s,v)}$, can be written as

$$x_n = a^m b^s c^v = \begin{bmatrix} 1 & m & v+ms \\ 0 & 1 & s \\ 0 & 0 & 1 \end{bmatrix}.$$

Then from Lemma 3.3 and setting $M = 1$, we have

$$\begin{aligned} x_n &= a^{T_n(L)} b^{UF_n(L)} c^{w_n(L)} \\ &= \begin{bmatrix} 1 & T_n(L) & w_n(L) + T_n(L)UF_n(L) \\ 0 & 1 & UF_n(L) \\ 0 & 0 & 1 \end{bmatrix} := H_n(L). \end{aligned} \tag{2}$$

Algorithm 1

Alice and Bob want to establish a secret key. They select $H_n(L)$ and p a prime number over an insecure channel. Alice chooses a random number $n_1 \geq 4$ and sends $H_n(L)^{n_1} \pmod p$ to Bob. Bob chooses a random number $n_2 \geq 4$ and sends $H_n(L)^{n_2} \pmod p$ to Alice. Alice and Bob both compute $H_n(L)^{n_1 n_2} \pmod p$ and use this as their private key. The algorithm steps are given below and illustrated in Figure 1.

Step 1. The prime number p and generator $H_n(L) \pmod p$ are public (assume all users have agreed on the general linear group over a finite field F_p and $H_n(L)$).

Step 2. Alice chooses a random number $n_1 \geq 4$ and sends $H_n(L)^{n_1} \pmod p$ to Bob.

Step 3. Bob chooses a random number $n_2 \geq 4$ and sends $H_n(L)^{n_2} \pmod p$ to Alice.

Step 4. Alice and Bob both compute $H_n(L)^{n_1 n_2} \pmod p$ and use this as the private key for future communications.

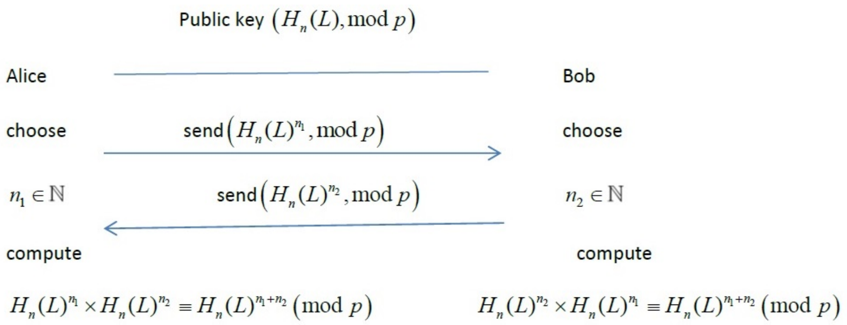
Public key $(H_n(L), \mathrm{mod}\ p)$
Alice
Bob
choose
send $(H_n(L)^{n_1}, \mathrm{mod}\ p)$
choose
$n_1 \in \mathbb{N}$
send $(H_n(L)^{n_2}, \mathrm{mod}\ p)$
$n_2 \in \mathbb{N}$
compute
compute
$H_n(L)^{n_1} \times H_n(L)^{n_2} \equiv H_n(L)^{n_1+n_2} \pmod p$
$H_n(L)^{n_2} \times H_n(L)^{n_1} \equiv H_n(L)^{n_1+n_2} \pmod p$

Fig. 1. Algorithm 1

Example 4.1. Let $(H_5(-1), 5)$ be the public key. Alice chooses $n_1 = 8$ and using (2) computes $H_5(-1) \pmod 5$

$$(H_5(-1))^8 = \begin{bmatrix} 1 & 16 & 192 \\ 0 & 1 & 24 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{bmatrix} \pmod 5,$$

and sends this to Bob. Bob chooses $n_2 = 4$ and obtains $H_{-1}(5) \pmod 5$

$$(H_5(-1))^4 = \begin{bmatrix} 1 & 8 & 48 \\ 0 & 1 & 12 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 3 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \pmod 5,$$

and sends this to Alice. Since $(H_5(-1))^4 \times (H_5(-1))^8 = (H_5(-1))^{12} = (H_5(-1))^8 \times (H_5(-1))^4$, Alice and Bob both compute

$$(H_5(-1))^4 \times (H_5(-1))^8 = \begin{bmatrix} 1 & 24 & 432 \\ 0 & 1 & 36 \\ 0 & 0 & 1 \end{bmatrix} \equiv \begin{bmatrix} 1 & 4 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \pmod 5.$$

This is used as the private key for future communications.

Now using $H_n(L)$, define the matrix Γ_i $i = 1, 2, 3, \cdots$, as

$$\Gamma_i(n, L) = \begin{bmatrix} H_n(L) & H_n(L) & H_n(L) & \cdots & H_n(L) & H_n(L) \\ 0 & I & 0 & \cdots & 0 & 0 \\ 0 & 0 & I & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & I & 0 \\ 0 & 0 & 0 & \cdots & 0 & I \end{bmatrix} \pmod p, \tag{3}$$

where 0 is a 3×3 matrix with entries 0 and I is the 3×3 identity matrix.

Algorithm 2

Algorithm 2 is similar to Algorithm 1, except $\Gamma_i(n, L)$ is used instead of the secret key $H_n(L)$. The algorithm steps are given below and illustrated in Figure 2.

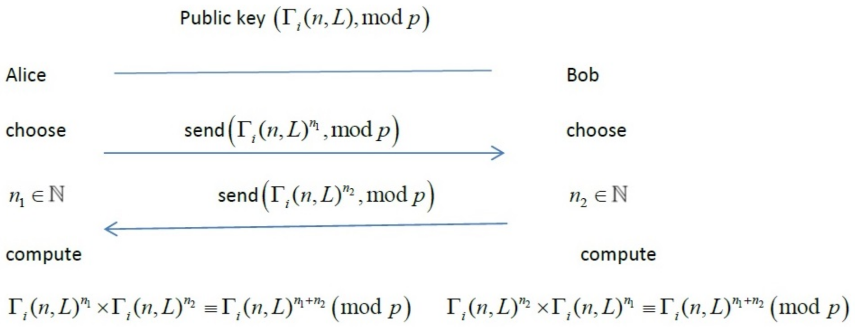
Public key $(\Gamma_i(n,L), \bmod p)$
Alice
Bob
choose
send$(\Gamma_i(n,L)^{n_1}, \bmod p)$
choose
$n_1 \in \mathbb{N}$
send$(\Gamma_i(n,L)^{n_2}, \bmod p)$
$n_2 \in \mathbb{N}$
compute
compute
$\Gamma_i(n,L)^{n_1} \times \Gamma_i(n,L)^{n_2} \equiv \Gamma_i(n,L)^{n_1+n_2} \pmod p$
$\Gamma_i(n,L)^{n_2} \times \Gamma_i(n,L)^{n_1} \equiv \Gamma_i(n,L)^{n_1+n_2} \pmod p$

Fig. 2. Algorithm 2

Example 4.2. Let $(\Gamma_2(3,2),5)$ be the public key

$$\Gamma_2(3,2)=\begin{bmatrix}1&1&3&1&1&3\\0&1&2&0&1&2\\0&0&1&0&0&1\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\pmod 5.$$

Alice chooses $n_1=5$ and using (3) computes $\Gamma_2(3,2)^5 \pmod 5$

$$(\Gamma_2(3,2))^5=\begin{bmatrix}1&5&35&5&15&85\\0&1&10&0&5&30\\0&0&1&0&0&5\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\equiv\begin{bmatrix}1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\pmod 5,$$

and sends this to Bob. Bob chooses $n_2=3$ and obtains $(\Gamma_2(3,2))^3 \pmod 5$

$$(\Gamma_2(3,2))^3=\begin{bmatrix}1&3&15&3&6&26\\0&1&6&0&3&12\\0&0&1&0&0&3\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\equiv\begin{bmatrix}1&3&0&3&1&1\\0&1&1&0&3&2\\0&0&1&0&0&3\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\pmod 5,$$

and sends this to Alice. Since $(\Gamma_2(3,2))^5\times(\Gamma_2(3,2))^3=(\Gamma_2(3,2))^8=(\Gamma_2(3,2))^3\times(\Gamma_2(3,2))^5$. Alice and Bob both compute

$$(\Gamma_2(3,2))^8=\begin{bmatrix}1&8&80&8&36&276\\0&1&16&0&8&72\\0&0&1&0&0&8\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\equiv\begin{bmatrix}1&3&0&3&1&1\\0&1&16&0&3&2\\0&0&1&0&0&3\\0&0&0&1&0&0\\0&0&0&0&1&0\\0&0&0&0&0&1\end{bmatrix}\pmod 5.$$

This is used as the private key for future communications.

4.1. Security analysis

In this section, we formalize the hardness assumptions underlying the proposed key exchange protocols, place them in a standard security model, and discuss complexity considerations and potential attacks.

4.1.1. Hardness assumptions. Let p be a relatively large prime and let $H_n(L)$ denote the 3×3 upper-triangular unipotent matrix defined earlier with entries parameterized by HTFL sequence terms.

- *HTFL Discrete Logarithm Problem (HTFL-DLP).* Given $(H_n(L), H_n(L)^a \bmod p)$ for a secret exponent a, recover a.
- *HTFL Computational Diffie-Hellman Problem (HTFL-CDH).* Given $(H_n(L)^a, H_n(L)^b)$, compute $H_n(L)^{ab}$.
- *HTFL Decisional Diffie–Hellman Problem (HTFL-DDH).* Given $(H_n(L)^a, H_n(L)^b, H_n(L)^c)$, decide whether $c = ab$.

The security of our protocols reduces to the hardness of HTFL-CDH in the Heisenberg group representation over $\mathbb{F}_p$.

4.1.2. Security model. We analyze the scheme in the *passive adversary model*, where the adversary observes all protocol messages but cannot alter them.

• *Correctness.* Both parties compute the same shared secret because matrix exponentiation is associative:

$$(H_n(L)^a)^b = (H_n(L)^b)^a = H_n(L)^{ab}.$$

• *Security.* An adversary observing only $H_n(L)^a \bmod p$ and $H_n(L)^b \bmod p$ cannot derive $H_n(L)^{ab}$ unless it can solve HTFL-CDH. Therefore, protocol secrecy reduces to the intractability of this problem.

As with classical Diffie-Hellman, the scheme without authentication is vulnerable to man-in-the-middle attacks. Strengthening against active adversaries would require integrating authentication mechanisms, which we leave for future work.

4.1.3. Complexity considerations.

- *Computation.* The dominant cost is matrix multiplication in $GL_3(\mathbb{F}_p)$. Exponentiation by square-and-multiply requires $O(\log a)$ matrix multiplications. For Algorithm 2, the matrices are $3i \times 3i$, yielding higher computational overhead but a larger key space.
- *Efficiency.* Compared to classical finite-field Diffie-Hellman, matrix exponentiation introduces extra cost, but the algebraic structure may yield new hardness assumptions distinct from traditional discrete log settings.

4.1.4. Resistance to known attacks.

- *Brute-force.* One of the most important attacks is a brute force attack. Because matrices are used to create keys in these algorithms, these matrices must be invertible. It is possible to check only the order of the general linear group $GL_m(F_p)$ which can be made very large by choosing p a relatively large prime number and m large. $GL_m(F_p)$, q a prime number, consists of all invertible matrices of order $m \times m$ over F_p [8]. This group has order

$$\mid GL_m(F_p) \mid= (p^m - p^{m-1})(p^m - p^{m-2}) \cdots (p^m - 1).$$

For Algorithm 1, consider $H_n(L)$. Since $H_n(L)$ is a 3×3 matrix

$$\mid GL_3(F_p) \mid= (p^3 - p^2)(p^3 - p^1)(p^3 - 1), \tag{4}$$

matrices are possible. For Algorithm 2, we have Γ_i which is a $3i \times 3i$ matrix, so

$$\mid GL_{3i}(F_p) \mid = (p^{3i} - p^{3i-1})(p^{3i} - p^{3i-2}) \cdots (p^{3i} - 1), \tag{5}$$

matrices are possible. Therefore for sufficiently large p, the attack is intractable. Exponent space can be made exponentially large by choosing p and exponents of sufficient size.

- *Linear algebra attacks.* Previous proposals of matrix-based Diffie–Hellman protocols have been shown vulnerable to linear algebraic attacks. Our construction differs by embedding HTFL sequences into the Heisenberg group, yielding a different algebraic structure. While this does not guarantee security, it motivates our hardness assumptions and highlights the importance of rigorous subgroup order analysis. While the matrices lie in $GL_m(\mathbb{F}_p)$, the embedding in HTFL sequences complicates reduction to standard discrete log.

The current analysis establishes correctness and passive security under the HTFL-CDH assumption. We therefore view the presented protocols as *conceptual prototypes* linking HTFL sequences and cryptographic constructions, laying groundwork for future rigorous analysis.

5. Conclusion

New sequences called the HTFL sequences were obtained using the Fibonacci and Lehmer sequences. The period of these sequences was investigated and it was proven that they are simply periodic. The HTFL sequences on a finite group were given and studied on the Heisenberg group. Finally, Diffie-Hellman key exchange using the HTFL sequences on the Heisenberg group was presented and the security was examined. This is an interesting and useful application of group theory in cryptography. As future work, other sequences such as Mersenne, Pell, and Lucas sequences [11, 15, 21, 22]) can be considered to develop new Diffie-Hellman key exchange and other algorithms.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] Y. Aküzüm and Ö. Deveci. The Hadamard-type k-step Fibonacci sequences in groups. *Communication in Algebra*, 48(7):2844–2856, 2020. https://doi.org/10.1080/00927872.2020.1723609.

[2] M. A. Bennett, V. Patel, and S. Siksek. Shifted powers in Lucas–Lehmer sequences. *Research in Number Theory*, 5(1):15, 2019. https://doi.org/10.1007/s40993-019-0153-2.

[3] C. M. Campbell and P. P. Campbell. The Fibonacci length of certain centro-polyhedral groups. *Journal of Applied Mathematics and Computing*, 19(1–2):231–240, 2005. https://doi.org/10.1007/BF02935801.

[4] L. Chen and Y. Chen. The n-Diffie–Hellman problem and multiple-key encryption. *International Journal of Information Security*, 11(5):305–320, 2012. https://doi.org/10.1007/s10207-012-0171-8.

[5] H. Chien. Provably secure authenticated Diffie–Hellman key exchange for resource-limited smart card. *Journal of Shanghai Jiaotong University (Science)*, 19(4):436–439, 2014. https://doi.org/10.1007/s12204-014-1521-7.

[6] Ö. Deveci and E. Karaduman. Lehmer sequences in finite groups. *Ukrainian Mathematical Journal*, 68(2):193–202, 2016. https://doi.org/10.1007/s11253-016-1218-1.

[7] A. Escala, G. Herold, E. Kiltz, C. Ràfols, and J. Villar. An algebraic framework for Diffie–Hellman assumptions. In R. Canetti and J. A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8043 of *Lecture Notes in Computer Science*, Berlin, Heidelberg. Springer, 2013. https://doi.org/10.1007/978-3-642-40084-1_8.

[8] P. A. Grillet. *Abstract Algebra*, volume 242 of *Graduate Texts in Mathematics*. Springer, Berlin, Germany, 2nd edition, 2007.

[9] L. Harn and C. Lin. Efficient group Diffie–Hellman key agreement protocols. *Computers & Electrical Engineering*, 40(6):1972–1980, 2014. https://doi.org/10.1016/j.compeleceng.2013.12.018.

[10] M. Hashemi and E. Mehraban. On the 3-nacci sequences of finitely generated groups. *Menemui Matematik (Discovering Mathematics)*, 37(1):20–27, 2015.

[11] M. Hashemi and E. Mehraban. The generalized order k-Pell sequences in some special groups of nilpotency class 2. *Communications in Algebra*, 50(4):1768–1784, 2021. https://doi.org/10.1080/00927872.2021.1988959.

[12] M. Hashemi and E. Mehraban. Fibonacci length and the generalized order k-pell sequences of the 2-generator p-groups of nilpotency class 2. *Journal of Algebra and Its Applications*, 22(3):2350061, 2023. https://doi.org/10.1142/S0219498823500615.

[13] D. H. Lehmer. An extended theory of Lucas' functions. *Ann. Math.*, 31(3):419–448, 1930. https://doi.org/10.2307/1968235.

[14] H. Liu and C. Yang. On a problem of d. h. Lehmer and pseudorandom binary sequences. *Boletim da Sociedade Brasileira de Matemática*, 39(3):387–399, 2008. https://doi.org/10.1007/s00574-008-0012-6.

[15] E. Mehraban, Ö. Deveci, and E. Hincal. The generalized order $(k;t)$-Mersenne sequences in groups. *Notes on Number Theory and Discrete Mathematics*, 30(2):271–282, 2024. https://doi.org/10.7546/nntdm.2024.30.2.271-282.

[16] E. Mehraban, T. A. 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 Mathematics*, 9(5):13537–13552, 2024. https://doi.org/10.3934/math.2024660.

[17] E. Mehraban, T. A. Gulliver, and E. Hincal. An RSA cryptosystem on Lehmer sequences in some classes of groups. *Advances in Mathematics of Communications*, 19(4):1026–1040, 2025. https://doi.org/10.3934/amc.2024039.

[18] D. V. Osipov. The discrete Heisenberg group and its automorphism group. *Mathematical Notes*, 98(1–2):185–188, 2015. https://doi.org/10.1134/S0001434615070160.

[19] E. Özkan and H. Akkuş. Copper ratio obtained by generalizing the Fibonacci sequence. *AIP Advances*, 14(7):075207, 2024. https://doi.org/10.1063/5.0207147.

[20] E. Özkan, H. Akkuş, and A. Özkan. Properties of generalized bronze Fibonacci sequences and their hyperbolic quaternions. *Axioms*, 14(1):14, 2025. https://doi.org/10.3390/axioms14010014.

[21] E. Özkan, B. Şen, H. Akkuş, and M. Uysal. A study on the k-Mersenne and k-Mersenne–Lucas sequences. *Universal Journal of Mathematics and Applications*, 8(1):1–7, 2025. https://doi.org/10.32323/ujma.1566270.

[22] E. Özkan and M. Uysal. d-Gaussian Fibonacci, d-Gaussian Lucas polynomials and their matrix representations. *Ukrainian Mathematical Journal*, 75(4):562–585, 2023. https://doi.org/10.37863/umzh.v75i4.6988.

[23] J. Partala. Algebraic generalization of Diffie–Hellman key exchange. *Journal of Mathematical Cryptology*, 12(1):1–21, 2018. https://doi.org/10.1515/jmc-2017-0015.

[24] M. Skałba. Note on Lehmer–pierce sequences with the same prime divisors. *Bulletin of the Australian Mathematical Society*, 97(1):11–14, 2018. https://doi.org/10.1017/S0004972717000843.

Elahe Mehraban
Mathematics Research Center, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey
Department of Mathematics, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey

T. Aaron Gulliver
Department of Electrical and Computer Engineering, University of Victoria
Victoria, BC, V8W 2Y2, Canada

Reza Ebrahimi Atani
Department of Computer Engineering, University of Guilan, Rasht, Iran

Evren Hincal
Mathematics Research Center, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey
Department of Mathematics, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey
Research Center of Applied Mathematics, Khazar University, Baku, Azerbaijan