J. COMBIN. MATH. COMBIN. COMPUT. 130 (2026) 187–205

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

Combinatorial Press

Massey-Omura encryption with the generalized (k,t)-Jacobsthal p-numbers in finite groups

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

ABSTRACT

This work introduces two algebraic variants of the Massey-Omura cryptosystem based on newly defined generalized (k,t)-Jacobsthal p-numbers and their extensions to finite groups. We first generalize the classical Jacobsthal recurrence and establish structural properties including periodicity, invertibility conditions, and recurrence behavior modulo finite integers. These results are then extended to group-theoretic settings, where we construct the corresponding (k,t)-Jacobsthal sequences in specific finite groups and derive their sequence periods. Leveraging these algebraic foundations, we propose two Massey-Omura-type encryption schemes in which private exponents are selected from the generalized Jacobsthal sequences. We formally prove the correctness of both constructions and analyze the implications of periodicity on exponent invertibility and protocol feasibility. The proposed schemes do not introduce new hardness assumptions beyond those inherent in the underlying platform group. Instead, they provide a mathematically structured alternative to classical exponent selection in three-pass protocols. The results highlight a new connection between recurrence-defined sequences and multiplicative exponentiation in finite groups, offering an algebraically motivated direction for exploring generalized exponent families in symmetric and non-abelian cryptosystems.

Keywords: Jacobsthal sequence, Massey-Omura cryptosystem, Period, Special groups

2020 Mathematics Subject Classification: 11K31, 11C20, 68R01, 68P30, 94A60.

* Corresponding author.

Received 06 Oct 2025; Revised 29 Dec 2025; Accepted 10 Jan 2026; Published Online 30 Mar 2026.

DOI: 10.61091/jcmcc130-13

1. Introduction

Cryptography plays a central role in securing modern communication systems, enabling confidentiality, authenticity, and integrity in the presence of adversaries with increasing computational capabilities. Many cryptographic constructions, both classical and modern, draw deeply on algebraic structures, including number-theoretic sequences, finite fields, and groups. Recurrence-defined sequences such as the Fibonacci, Pell, and Jacobsthal numbers have been used in pseudorandom number generation, key-scheduling mechanisms, algebraic code constructions, and various symmetric and asymmetric schemes. Their predictable recurrence relations and well-defined behavior modulo integers or within finite groups make them attractive for both theoretical study and potential cryptographic applications.

The Jacobsthal sequence $\{J_n\}$ is defined as

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

with initial conditions $J_0 = 0$ and $J_1 = 1$ [17]. In 2008, the Jacobsthal Lucas E-matrix and R-matrix were given which are similar to the Fibonacci Q-matrix [18]. In [3], Gaussian Jacobsthal sequences were introduced and the corresponding generating functions were given. Generalized Jacobsthal sequences were introduced in [10] and the $k-$Jacobstal sequences in [27]. In [1], the Jacobsthal-Padovan p-sequences in finite groups were presented, and the orbits of these groups were given.

The Jacobsthal numbers have been generalized in several ways [6, 7]. One of these generalizations is as follows. For $n \geq 0$ and $k \geq 2$, the generalized Jacobsthal sequence $J(k, n)$ is defined as

$$J(k, n) = (k-1)J(k, n-1) + kJ(k, n-2) \text{ for } n \geq 2,$$

with initial conditions $J(k, 0) = 0$ and $J(k, 1) = 1$ [5]. For example, if $k = 2$, we have

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

and thus $\{J(2, n)\}_0^\infty = \{0, 1, 1, 3, 5, \cdots\}$.

Algebra, in particular group algebra, plays an important role in modern encryption. The properties of groups and rings have been used to create public and private keys [4, 13, 20, 21, 24, 23]. In 1986, the Massey-Omura cryptosystem was introduced [19]. It has become one of the most well-known private key cryptosystems [2, 11, 28]. In [26], a Massey-Omura cryptosystem was developed in $GF(2^m)$. The Massey-Omura algorithm was used for a three-pass protocol in [25]. In [12], Massey-Omura encryption was considered using symmetric groups.

In this paper, we define the generalized (k, t)-Jacobsthal p-numbers, analyze their modular periodic behavior, and then extend the construction to selected finite groups. The resulting algebraic framework is used to build two Massey–Omura-type protocols in which the private exponents are chosen from recurrence-defined families rather than from unrestricted residue classes. Our aim is not to claim a stronger cryptosystem than the

classical Massey–Omura scheme, but to study how structured exponent families interact with correctness, invertibility, and effective keyspace in finite-group settings.

The remainder of this paper is organized as follows. Section 2 introduces the generalized Jacobsthal recurrence and studies its modular behavior. Section 3 defines the corresponding sequences in finite groups and specializes them to G_m and $H_{(t,l,m)}$. Section 4 presents two Massey–Omura-type constructions based on these sequences, and Section 5 discusses their scope, limitations, and keyspace implications. Finally, Section 6 summarizes the main conclusions and possible extensions.

2. The generalized (k,t)-jacobsthal p-numbers

In this section, we introduce the generalized (k,t)-Jacobsthal p-numbers and study their modular recurrence properties. We first record the defining recurrence and then examine the periodic behavior that arises after reduction modulo a positive integer. These results will be used later in the group-theoretic and cryptographic constructions.

Definition 2.1. For integers $k \geq 1$, $p \geq 1$ and $t \geq 2$, the generalized (k,t)-Jacobsthal $p-$numbers denoted $\{J_n^p(k,t)\}$ are defined as

$$J_n^p(k,t) = kJ_{n-1}^p(k,t) + 2J_{n-p-1}^p(k,t) + J_{n-p-2}^p(k,t) + \cdots + J_{n-p-t}^p(k,t), \ n \geq t+p+1, \tag{1}$$

where $J_0^p(k,t) = J_1^p(k,t) = \cdots = J_{t+p-1}^p(k,t) = 0$ and $J_{t+p}^p(k,t) = 1$.

Note that Definition 2.1 can be rewritten as

$$J_n^p(k,t) = kJ_{n-1}^p(k,t) + 2J_{n-p-1}^p(k,t) + \sum_{r=2}^{t} J_{n-p-r}^p(k,t), \ n \geq t+p+1. \tag{2}$$

For example, if $p = 1$ and $k = 3$, from Definition 2.1 we have

$$J_n^1(3,t) = 3J_{n-1}^1(3,t) + 2J_{n-2}^1(3,t) + \cdots + J_{n-1-t}^1(3,t), \ n \geq t+1. \tag{3}$$

Table 1 gives $J_n^1(3,t)$, for $0 \leq n \leq 10$ and $2 \leq t \leq 8$.
The generalized (k,t)-Jacobsthal p-numbers modulo m are

$$\{J_i^{p,m}(k,t)\} = \{J_0^{p,m}(k,t), J_1^{p,m}(k,t), \cdots, J_n^{p,m}(k,t), \cdots\},$$

where $i \geq 0$ and $J_i^{p,m}(k,t) \equiv J_i^p(k,t) \pmod{m}$.

Theorem 2.2. *For $t \geq 2$, the generalized (k,t)-Jacobsthal p-numbers $\{J_n^{p,m}(k,t)\}$ are eventually periodic modulo m.*

Proof. Consider the state vector

$$S_n := (J_n^{p,m}(k,t), J_{n+1}^{p,m}(k,t), \cdots, J_{n+t+p-1}^{p,m}(k,t)) \in \mathbb{Z}_m^{t+p}.$$

Because the recurrence in Definition 2.1 depends only on the previous $t+p$ terms, the state vector S_n uniquely determines the next value $J^{p,m}_{n+t+p}(k,t)$ and hence the next state vector

$$S_{n+1} := (J^{p,m}_{n+1}(k,t), J^{p,m}_{n+2}(k,t), \cdots, J^{p,m}_{n+t+p}(k,t)).$$

Thus the sequence of states evolves under a deterministic map

$$S_{n+1} = F(S_n),$$

for some function $F : \mathbb{Z}_m^{t+p} \longrightarrow \mathbb{Z}_m^{t+p}$. Since each coordinate of S_n lies in $\mathbb{Z}_m$, there are only m^{t+p} possible state vectors. Therefore the infinite sequence $S_0, S_1, S_2, \ldots$ must contain a repeated state, say $S_i = S_j$ with $0 \leq i < j$. By determinism, this implies $S_{i+r} = S_{j+r}$ for every $r \geq 0$. Hence the state sequence is periodic from index i onward, and the original scalar sequence $\{J^{p,m}_n(k,t)\}$ is eventually periodic modulo m. □

Table 1. $J^1_n(3,t)$ for $0 \leq n \leq 10$ and $2 \leq t \leq 8$

n	$J^1_n(3,2)$	$J^1_n(3,3)$	$hJ^1_n(3,4)$	$J^1_n(3,5)$	$J^1_n(3,6)$	$J^1_n(3,7)$	$J^1_n(3,8)$
0	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0
3	1	0	0	0	0	0	0
4	3	1	0	0	0	0	0
5	11	3	1	0	0	0	0
6	40	11	3	1	0	0	0
7	145	40	11	3	1	0	0
8	526	146	40	11	3	1	0
9	1903	532	146	40	11	3	1
10	6921	1939	533	146	40	11	3

Whenever the initial state reappears, we write $hJ^p_m(k,t)$ for the least positive return length. The values listed below were computed from the first return of the initial state and serve as a small-parameter validation of the modular behavior discussed above.

Table 2 gives $hJ^1_m(k,2)$ for $2 \leq m \leq 10$ and $2 \leq k \leq 7$. The data show that the observed return lengths vary substantially with both m and k and need not behave monotonically. This variability is important later, because it indicates that the effective exponent space induced by the recurrence may differ considerably across parameter choices even for small moduli.

Table 2. $hJ_m^1(k,2)$ for $2 \le m \le 10$ and $2 \le k \le 7$

m	$hJ_m^1(2,2)$	$hJ_m^1(3,2)$	$hJ_m^1(4,2)$	$hJ_m^1(5,2)$	$hJ_m^1(6,2)$	$hJ_m^1(7,2)$
2	3	7	3	7	3	7
3	13	8	4	13	8	4
4	6	14	6	14	6	14
5	8	5	31	20	31	8
6	39	56	12	51	24	28
7	57	42	48	8	21	16
8	12	32	12	28	12	28
9	39	24	12	39	24	12
10	24	35	93	140	93	56

Lemma 2.3. *Assume that $hJ_m^p(k,t)$ is the least positive return length of the initial state modulo m. Then for integers s, n and $m \ge 2$, we have*

(i) $J^p_{hJ_m^p(k,t)+n}(k,t) \equiv J_n^p(k,t) \pmod m$,

(ii) $J^p_{s\times(hJ_m^p(k,t))+n}(k,t) \equiv J_n^p(k,t) \pmod m$.

Proof. Part (i) follows directly from the definition of $hJ_m^p(k,t)$. For Part (ii), we have

$$\begin{aligned} J^p_{s\times(hJ_m^p(k,t))+n}(k,t) \equiv & J_{(hJ_m^p(k,t))+(s-1)\times(hJ_m^p(k,t))+n}(k,t) \\ \equiv & J^p_{(s-1)(hJ_m^p(k,t))+n}(k,t) \\ \equiv & \vdots \\ \equiv & J_n^p(k,t) \pmod m, \end{aligned}$$

which gives the result. □

Lemma 2.4. *Assume that $hJ_m^p(k,t)$ exists. Let n be an integer and $m \ge 2$ be a positive number. If*

$$\begin{cases} J_n^p(k,t) \equiv 0 & \pmod m, \\ J^p_{n+1}(k,t) \equiv 0 & \pmod m, \\ \vdots & \\ J^p_{n+t+p-2}(k,t) \equiv 0 & \pmod m, \\ J^p_{n+t+p-1}(k,t) \equiv 0 & \pmod m, \\ J^p_{n+t+p}(k,t) \equiv 1 & \pmod m, \end{cases}$$

then $hJ_m^p(k,t) \mid n$.

Proof. There exists $0 \le i \le hJ_m^p(k,t)$ such that $n = t \times (hJ_m^p(k,t)) + i$. Then for all $0 \le j \le t+p$, $J^p_{n+j}(k,t) \equiv J^p_{i+j}(k,t) \pmod m$, we have

$$\begin{cases} J_i^p(k,t) \equiv 0 & (\text{mod } m), \\ J_{i+1}^p(k,t) \equiv 0 & (\text{mod } m), \\ \vdots & \\ J_{i+t+p-2}^p(k,t) \equiv 0 & (\text{mod } m), \\ J_{i+t+p-1}^p(k,t) \equiv 0 & (\text{mod } m), \\ J_{i+t+p}^p(k,t) \equiv 1 & (\text{mod } m). \end{cases}$$

Thus, i is a period of the generalized (k,t)-Jacobsthal p-numbers modulo m so $hJ_m^p(k,t) \mid i$. Since $0 \leq i < hJ_m^p(k,t)$, we have that $i = 0$, and the result follows. □

3. The generalized (k,t)-Jacobsthal p-numbers in a finite group

We now define the generalized (k,t)-Jacobsthal p-numbers in a finite group and examine the periodic behavior induced by the finite-state recurrence. We then specialize the construction to G_m and $H_{(t,l,m)}$, where explicit normal forms make it possible to write the sequence terms in closed algebraic form.

Definition 3.1. For integers $k \geq 1$, $p \geq 1$ and $t \geq 2$, the generalized (k,t)-Jacobsthal p-numbers in a finite group is a sequence of group elements $x_0, x_1, \cdots, x_n, \cdots$ for which, given finite group generators $X = \{a_0, a_1, \cdots, a_j\}$, the elements are $x_0 = a_0,\ x_1 = a_1,\ \cdots,\ x_j = a_j$ and

$$x_n = \begin{cases} x_0 x_1 \cdots x_{n-3} x_{n-2}^2 x_{n-1}^k, & \text{for } j < n < t+p, \\ x_{n-p-t} \cdots x_{n-p-2} x_{n-p-1}^2 x_{n-1}^k, & \text{for } n \geq p+t. \end{cases} \tag{4}$$

The (k,t)-Jacobsthal p-numbers in a group are denoted by $Q_p^{k,t}(G,X)$ and the corresponding sequence period is denoted by $JQ_p^{k,t}(G,X)$.

Theorem 3.2. *The generalized (k,t)-Jacobsthal p-numbers in a finite group are eventually periodic. If the initial generator tuple reappears, the resulting sequence is purely periodic.*

Proof. Let G be a finite group with $|G| = m$. The recurrence in Definition 3.1 is determined by the current $(t+p)$-tuple of consecutive group elements. Since there are only m^{t+p} such tuples, the infinite sequence generated by $Q_p^{k,t}(G,X)$ must contain a repeated state. Once a state repeats, the determinism of the recurrence implies that all subsequent states repeat as well. Hence the sequence is eventually periodic. If one of the repeated states is the initial generator tuple $(x_0, x_1, \ldots, x_{t+p-1})$, then the sequence is purely periodic from the beginning. □

For $m \in \mathbb{N}$, consider the finitely presented group G_m given by

$$G_m =< a, b | a^m = b^m = 1, [a,b]^a = [a,b], [a,b]^b = [a,b] >, m \geq 2.$$

Lemma 3.3. [9] *Every element of G_m may be uniquely presented by $a^r b^s [a,b]^t$ where $0 \leq r, s, t \leq m-1$, and $\mid G_m \mid = m^3$.*

For $p = 1$ and $t = 2$, we define the sequences $U_n(2)$ and $w_n(2)$ as follows

$$\begin{aligned}
U_0(2) =& 1,\\
U_1(2) =& 0,\\
U_2(2) =& 2,\\
U_n(2) =& U_{n-3}(2) + 2U_{n-2}(2) + 2U_{n-1}(2), \quad n \geq 3.\\
w_0(2) =& w_1(2) = w_2(2) = 0,\\
w_n(2) =& w_{n-3}(2) + 2w_{n-2}(2) + 2w_{n-1}(2) - (U_{n-2}(2)J^1_{n-1}(2,2) + (J^1_{n-1}(2,2)\\
&+ J^1_n(2,2))U_{n-2}(2) + (J^1_{n-1}(2,2) + 2J^1_n(2,2))U_{n-1}(2)\\
&+ (J^1_{n-1}(2,2) + 2J^1_n(2,2) + J^1_{n+1}(2,2))U_{n-1}(2)), \ n \geq 3.
\end{aligned}$$

Lemma 3.4. *Every element of $Q_1^{2,2}(G_m, X)$ can be expressed as $x_n = a^{U_n(2)} b^{J^1_{n+2}(2,2)} [a,b]^{w_n(2)}$, $n \geq 3$.*

Proof. For $n = 2$ and $n = 3$, we have $x_2 = x_0^2 x_1^2 = a^2 b^2$ and $x_3 = x_0 x_1^2 x_2^2 = a^5 b^6 [a,b]^{-12}$, respectively. Then by induction on n, we have

$$\begin{aligned}
x_n &= x_{n-3}(x_{n-2})^2 (x_{n-1})^2\\
&= a^{U_{n-3}(2)} b^{J^1_{n-1}(2,2)} [a,b]^{w_{n-3}(2)} (a^{U_{n-2}(2)} b^{J^1_n(2,2)[a,b]^{w_{n-2}(2)}})^2 (a^{U_{n-1}(2)} b^{J^1_{n+1}(2,2)[a,b]^{w_{n-1}(2)}})^2\\
&= a^{U_{n-3}(2)+U_{n-2}(2)} b^{J^1_{n-1}(2,2)+J^1_n(2,2)} [a,b]^{w_{n-3}(2)+w_{n-2}(2)-U_{n-2}(2)J^1_{n-1}(2,2)} a^{U_{n-2}(2)} b^{J^1_n(2,2)[a,b]^{w_{n-2}(2)}}\\
&\quad (a^{U_{n-1}(2)} b^{J^1_{n+1}(2,2)[a,b]^{w_{n-1}(2)}})^2\\
&= \cdots\\
&= a^{U_{n-3}(2)+2U_{n-2}(2)+2U_{n-1}(2)} b^{J^1_{n+2}(2,2)}\\
&\quad [a,b]^{w_{n-3}(2)+2w_{n-2}(2)+2w_{n-1}(2)-(U_{n-2}(2)J^1_{n-1}(2,2)+(J^1_{n-1}(2,2)+J^1_n(2,2))U_{n-2}(2)+(J^1_{n-1}(2,2)+2J^1_n(2,2))U_{n-1}(2)}\\
&\quad [a,b]^{-(J^1_{n-1}(2,2)+2J^1_n(2,2)+J^1_{n+1}(2,2))U_{n-1}(2)+\cdots+(J^1_{n-1}(2,2)+2J^1_n(2,2)+(2-1)J^1_{n+1}(2,2))U_{n-1}(2))}\\
&= a^{U_n(2)} b^{J^1_{n+2}(2,2)} [a,b]^{w_n(2)},
\end{aligned}$$

and the assertion holds. □

For $p = 1$ and $t = 2$, we define the sequences $U_n(k)$ and $w_n(k)$ as follows

$$\begin{aligned}
U_0(k) =& 1,\\
U_1(k) =& 0,\\
U_2(k) =& 2,\\
U_n(k) =& U_{n-3}(k) + 2U_{n-2}(k) + kU_{n-1}(k), \quad n \geq 3.\\
w_0(k) =& w_1(k) = w_2(k) = 0,\\
w_n(k) =& w_{n-3}(k) + 2w_{n-2}(k) + kw_{n-1}(k) - (U_{n-2}(k)J^1_{n-1}(k,2) + (J^1_{n-1}(k,2)\\
&+ J^1_n(k,2))U_{n-2}(k) + (J^1_{n-1}(k,2) + 2J^1_n(k,2))U_{n-1}(k) + (J^1_{n-1}(k,2) + 2J^1_n(k,2)
\end{aligned}$$

$$+ J^1_{n+1}(k,2))U_{n-1}(k) + \cdots + (J^1_{n-1}(k,2) + 2J^1_n(k,2)$$
$$+ (k-1)J^1_{n+1}(k,2))U_{n-1}(k)),\ n \geq 3.$$

Lemma 3.5. *Every element of $Q_1^{k,2}(G_m, X)$ can be expressed as*

$$x_n = a^{U_n(k)} b^{J^1_{n+2}(k,2)} [a,b]^{w_n(k)}, \qquad n \geq 3.$$

Proof. For $n = 2$, we have $x_2 = x_0^2 x_1^k = a^2 b^k$. Then by induction on n, we have

$$\begin{aligned}
x_n &= x_{n-3}(x_{n-2})^2 (x_{n-1})^k \\
&= a^{U_{n-3}(k)} b^{J^1_{n-1}(k,2)} [a,b]^{w_{n-3}(k)} (a^{U_{n-2}(k)} b^{J^1_n(k,2)[a,b]^{w_{n-2}(k)}})^2 (a^{U_{n-1}(k)} b^{J^1_{n+1}(k,2)[a,b]^{w_{n-1}(k)}})^k \\
&= a^{U_{n-3}(k)+U_{n-2}(k)} b^{J^1_{n-1}(k,2)+J^1_n(k,2)} [a,b]^{w_{n-3}(k)+w_{n-2}(k)-U_{n-2}(k)J^1_{n-1}(k,2)} a^{U_{n-2}(k)} \\
&\quad b^{J^1_n(k,2)[a,b]^{w_{n-2}(k)}} (a^{U_{n-1}(k)} b^{J^1_{n+1}(k,2)[a,b]^{w_{n-1}(k)}})^k \\
&= \cdots \\
&= a^{U_{n-3}(k)+2U_{n-2}(k)+kU_{n-1}(k)} b^{J^1_{n+2}(k,2)} \\
&\quad [a,b]^{w_{n-3}(k)+2w_{n-2}(k)+kw_{n-1}(k)-(U_{n-2}(k)J^1_{n-1}(k,2)+(J^1_{n-1}(k,2)+J^1_n(k,2))U_{n-2}(k)} \\
&\quad [a,b]^{+(J^1_{n-1}(k,2)+2J^1_n(k,2))U_{n-1}(k)+(J^1_{n-1}(k,2)+2J^1_n(k,2)+J^1_{n+1}(k,2))U_{n-1}(k)} \\
&\quad [a,b]^{+\cdots+(J^1_{n-1}(k,2)+2J^1_n(k,2)+(k-1)J^1_{n+1}(k,2))U_{n-1}(k))} \\
&= a^{U_n(k)} b^{J^1_{n+2}(k,2)} [a,b]^{w_n(k)},
\end{aligned}$$

and the assertion holds. □

Lemma 3.6. *If $JQ_1^{k,2}(G_m, X) = s$, then s is the least integer such that*

$$\begin{cases}
U_n(k) \equiv 1 & (\text{mod } m), \\
U_{n+1}(k) \equiv 0 & (\text{mod } m), \\
U_{n+2}(k) \equiv 2 & (\text{mod } m), \\
J^1_{n+2}(k,2) \equiv 0 & (\text{mod } m), \\
J^1_{n+3}(k,2) \equiv 1 & (\text{mod } m), \\
J^1_{n+4}(k,2) \equiv k & (\text{mod } m), \\
w_n(k) \equiv 0 & (\text{mod } m), \\
w_{n+1}(k) \equiv 0 & (\text{mod } m), \\
w_{n+2}(k) \equiv 0 & (\text{mod } m),
\end{cases}$$

hold. Further, $hJ^1_m(k,2) \mid JQ_1^{k,2}(G_m, X)$.

Proof. By Lemma 3.3, we obtain that $x_n = a^{U_n(k)} b^{J^1_{n+2}(k,2)} [a,b]^{w_n(k)}$. Since $x_s = a$,

$x_{s+1} = b$ and $x_{s+2} = a^2b^k$, by the defining initial conditions we have

$$\begin{cases} U_s(k) \equiv 1 & (\text{mod } m), \\ U_{s+1}(k) \equiv 0 & (\text{mod } m), \\ U_{s+2}(k) \equiv 2 & (\text{mod } m), \\ J^1_{s+2}(k,2) \equiv 0 & (\text{mod } m), \\ J^1_{s+3}(k,2) \equiv 1 & (\text{mod } m), \\ J^1_{s+4}(k,2) \equiv k & (\text{mod } m), \\ w_s(k) \equiv 0 & (\text{mod } m), \\ w_{s+1}(k) \equiv 0 & (\text{mod } m), \\ w_{s+2}(k) \equiv 0 & (\text{mod } m). \end{cases}$$

Then Lemma 2.4 gives that $hJ^1_m(k,2) \mid JQ^{k,2}_1(G_m, X)$. □

For $t, l, m \in \mathbb{N}$, consider the Heisenberg group $H_{(t,l,m)}$ given by

$$H_{(t,l,m)} =< a, b, c | a^t = b^l = c^m = 1, [a,b] = c, [a,c] = [b,c] = 1 > .$$

Lemma 3.7. [22] *Element $H_{(t,l,m)}$ of the Heisenberg group can be written uniquely in the form $a^ib^jc^k$ where $0 \le i \le t-1, 0 \le j \le l-1$ and $0 \le k \le m-1$.*

For $p = 1$ and $t = 2$, define the sequences $T_n(2)$ and $g_n(2)$ as follows

$$\begin{aligned} T_0(2) =& 0, \\ T_1(2) =& 1, \\ T_2(2) =& 0, \\ T_n(2) =& T_{n-3}(2) + 2T_{n-2}(2) + 2T_{n-1}(2), \quad n \ge 3. \\ g_0(2) =& g_1(2) = 0, g_2(2) = 1, \\ g_n(2) =& g_{n-3}(2) + 2g_{n-2}(2) + 2g_{n-1}(2) - (T_{n-3}(2)J^1_{n-4}(2,2) + (T_{n-3}(2) + T_{n-2}(2))J^1_{n-4}(2,2) \\ & + (T_{n-3}(2) + 2T_{n-2}(2))J^1_{n-3}(2,2) + (T_{n-3}(2) + 2T_{n-2}(2) \\ & + T_{n-1}(2))J^1_{n-3}(2,2)), n \ge 3. \end{aligned}$$

Lemma 3.8. *Every element of $Q^{2,2}_1(H_{(t,l,m)}, X)$ can be expressed as $x_n = a^{J^1_{n-2}(2,2)}b^{T_n(2)}c^{g_n(2)}$, $n \ge 3$.*

Proof. For $n = 3$ and $n = 4$, we have $x_3 = x_0x_1^2x_2^2 = ab^2c^2$ and $x_4 = x_1x_2^2x_3^2 = a^6b^{14}c^{-19}$, respectively. Then by induction on n, we have

$$\begin{aligned} x_n &= x_{n-3}(x_{n-2})^2(x_{n-1})^2 \\ &= a^{J^1_{n-5}(2,2)}b^{T_{n-3}(2)}c^{g_{n-3}(2)}(a^{J^1_{n-4}(2,2)}b^{T_{n-2}(2)}c^{g_{n-2}(2)})^2(a^{J^1_{n-3}(2,2)}b^{T_{n-1}(2)}c^{g_{n-1}(2)})^2 \\ &= a^{J^1_{n-5}(2,2)+J^1_{n-4}(2,2)}b^{T_{n-3}(2)+T_{n-2}(2)}c^{g_{n-3}(2)+g_{n-2}(2)-(T_{n-3}(2)J^1_{n-4}(2,2))}a^{J^1_{n-4}(2,2)} \\ &\quad b^{T_{n-2}(2)}c^{g_{n-2}(2)}(a^{J^1_{n-4}(2,2)}b^{T_{n-1}(2)}c^{g_{n-1}(2)})^2 \\ &= a^{J^1_{n-5}(2,2)+2J^1_{n-4}(2,2)}b^{T_{n-3}(2)+2T_{n-2}(2)} \end{aligned}$$

$$
\begin{aligned}
&c^{g_{n-3}(2)+2g_{n-2}(2)-(T_{n-3}(2)J^1_{n-4}(2,2)+(T_{n-3}(2)+T_{n-2}(2))J^1_{n-4}(2,2))}\\
&(a^{J^1_{n-3}}(2,2)b^{T_{n-1}(2)}c^{g_{n-1}(2)})^2\\
&= \cdots\\
&= a^{J^1_{n-2}(2,2)}b^{T_n(2)}c^{g_{n-3}(2)+2g_{n-2}(2)+2g_{n-1}(2)}c^{-(T_{n-3}(2)J^1_{n-4}(2,2)+(T_{n-3}(2)}\\
&\quad \times c^{T_{n-2}(2))J^1_{n-4}(2,2)+(T_{n-3}(2)+2T_{n-2}(2))J^1_{n-3}(2,2)+(T_{n-3}(2)+2T_{n-2}(2)+T_{n-1}(2))J^1_{n-3}(2,2))}\\
&= a^{J^1_{n-2}(2,2)}b^{T_n(2)}c^{g_n(2)},
\end{aligned}
$$

and the assertion holds. □

For $p = 1$ and $t = 2$, we define the sequences $T_n(2)$ and $g_n(2)$ as follows

$$
\begin{aligned}
T_0(k) =&0,\\
T_1(k) =&1,\\
T_2(k) =&0,\\
T_n(k) =&T_{n-3}(k) + 2T_{n-2}(k) + kT_{n-1}(k), \quad n \geq 3.\\
g_0(k) =&g_1(k) = 0,\\
g_2(k) =&1,\\
g_n(k) =&g_{n-3}(k) + 2g_{n-2}(k) + kg_{n-1}(k) - (T_{n-3}(k)J^1_{n-4}(k,2) + (T_{n-3}(k)\\
&+ T_{n-2}(k))J^1_{n-4}(k,2) + (T_{n-3}(k) + 2T_{n-2}(k))J^1_{n-3}(k,2)\\
&+ (T_{n-3}(k) + 2T_{n-2}(k) + T_{n-1}(k))J^1_{n-3}(k,2) + (T_{n-3}(k) + 2T_{n-2}(k)\\
&+ 2T_{n-1}(k))J^1_{n-3}(k,2) + \cdots + (T_{n-3}(k) + 2T_{n-2}(k)\\
&+ (k-1)T_{n-1}(k))J^1_{n-3}(k,2)), \quad n \geq 3.
\end{aligned}
$$

The proof of the following lemma is similar to that for Lemma 3.6 and so is omitted.

Lemma 3.9. *Every element of* $Q_1^{k,2}(H_{(t,l,m)}, X)$ *can be expressed as* $x_n = a^{J^1_{n-2}(k,2)}b^{T_n(k)}c^{g_n(k)}$, $n \geq 3$.

Lemma 3.10. *If* $JQ_1^{k,2}(H_{(t,l,m)}, X) = i$, *then* i *is the least integer such that*

$$
\begin{cases}
J^1_{n-2}(k,2) \equiv 1 \pmod{t},\\
J^1_{n-1}(k,2) \equiv 0 \pmod{t},\\
J^1_n(k,2) \equiv 0 \pmod{t},\\
T_n(k) \equiv 0 \pmod{l},\\
T_{n+1}(k) \equiv 1 \pmod{l},\\
T_{n+2}(k) \equiv 0 \pmod{l},\\
g_n(k) \equiv 0 \pmod{m},\\
g_{n+1}(k) \equiv 0 \pmod{m},\\
g_{n+2}(k) \equiv 1 \pmod{m},
\end{cases}
$$

holds. Moreover, $hJ^1_t(k,2) \mid JQ_1^{k,2}(H_{(t,l,m)}, X)$.

Proof. By Lemma 3.7, we obtain that $x_n = a^{J^1_{n-2}(k,2)} b^{T_n(k)} c^{g_n(k)}$. Since $x_i = a$, $x_{i+1} = b$ and $x_{i+2} = c$, the explicit representation above yields

$$\begin{cases} J^1_{i-2}(k,2) \equiv 1 \pmod{t}, \\ J^1_{i-1}(k,2) \equiv 0 \pmod{t}, \\ J^1_i(k,2) \equiv 0 \pmod{t}, \\ T_i(k) \equiv 0 \pmod{l}, \\ T_{i+1}(k) \equiv 1 \pmod{l}, \\ T_{i+2}(k) \equiv 0 \pmod{l}, \\ g_i(k) \equiv 0 \pmod{m}, \\ g_{i+1}(k) \equiv 0 \pmod{m}, \\ g_{i+2}(k) \equiv 1 \pmod{m}. \end{cases}$$

Then from the return condition encoded in the displayed congruences,

$$hJ^1_t(k,2) \mid JQ^{k,2}_1(H_{(t,l,m)}, X).$$

□

4. Massey-Omura encryption with the generalized (k,t)-Jacobsthal p-numbers

In this section, we present two Massey–Omura-type encryption algorithms based on generalized Jacobsthal exponent families. The emphasis here is on algebraic correctness rather than on claiming a security advantage over the classical protocol.

Algorithm 1

1: Alice and Bob agree on a public key $(m, J^1_n(k,2))$.
2: Alice chooses $a, b \in J^1_n(k,2)$ such that $ab \equiv 1 \pmod{m}$.
3: Bob chooses $c, d \in J^1_n(k,2)$ such that $cd \equiv 1 \pmod{m}$.
4: Alice sends a message $Y \in Q^{k,2}_1(G_m, X)$ to Bob by computing $Y^a \pmod{m}$.
5: Using c, Bob obtains $Y^{ac} \pmod{m}$ and sends it to Alice.
6: Alice uses b and sends the ciphertext $Z = Y^{acb} \pmod{m}$ to Bob.
7: Bob decrypts Z and obtains the message Y.

Alice and Bob first agree on public parameters $(m, J^1_n(k,2))$. They then choose exponents a, b, c, d from the Jacobsthal-derived set so that $ab \equiv 1 \pmod{m}$ and $cd \equiv 1 \pmod{m}$. In other words, the admissible exponents are restricted to sequence values that satisfy the invertibility condition required by the three-pass protocol. In Algorithm 1, the message space is $Q^{k,2}_1(G_m, X)$. Alice sends a message $Y \in Q^{k,2}_1(G_m, X)$ to Bob by computing $Y^a \pmod{m}$, Bob returns $Y^{ac} \pmod{m}$, and Alice then uses b to obtain $Z = Y^{acb} \equiv Y^c \pmod{m}$. Bob finally decrypts with d and recovers Y because $cd \equiv 1 \pmod{m}$. All computations are performed in the relevant group using the normal

form with exponents reduced modulo m. The algorithm steps are given in Algorithm 1 and illustrated in Figure 1.

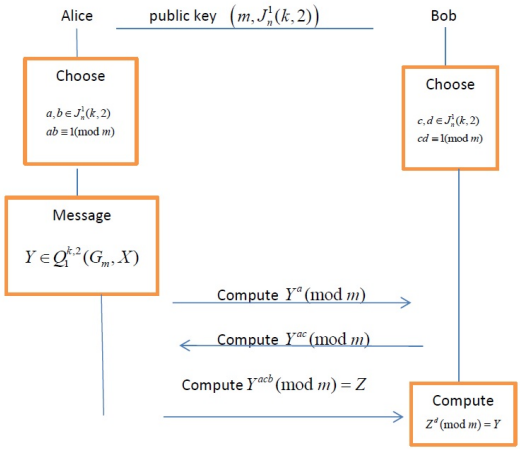

Fig. 1. A flowchart of Algorithm 1

Lemma 4.1. *The original message Y is obtained by Bob after decrypting the ciphertext Z.*

Proof. We show that $Z^d = Y$. We have that

$$Z = (Y^{ac})^b \equiv Y^{acb} \pmod m.$$

Using $ab \equiv 1 \pmod m$, we obtain $Z = Y^c \pmod m$, and Bob decrypts using d. Since $Y \in Q_1^{k,2}(G_m, X)$, Lemma 3.3 and the fact that $cd \equiv 1 \pmod m$ give

$$Z^d = Y^{cd} \equiv Y \pmod m.$$

□

Consider the following example.

Example 4.2. Let $p = 1, t = 2$ and $k = 2$.

1. Alice and Bob agree on a public key $(7, J_n^1(2,2))$.
2. Alice chooses $a := J_4^1(2,2) = 2$ and $b := J_{14}^1(2,2) = 70032$ such that $ab \equiv 1 \pmod 7$.
3. Bob chooses $c := J_6^1(2,2) = 3$ and $d := J_{10}^1(2,2) = 1090$ such that $cd \equiv 1 \pmod 7$.
4. Alice sends the message $Y = a^5b^6[a,b]^2 \in Q_1^{2,2}(G_m, X)$ to Bob by computing $(a^5b^6[a,b]^2)^2 = (a^5b^6[a,b]^2)(a^5b^6[a,b]^2) = a^{10}b^{12}[a,b]^{-26} \equiv a^3b^5[a,b]^2 \pmod 7$.
5. Using c, Bob obtains $(a^3b^5[a,b]^2)^3 = a^2b^1[a,b]^3 \pmod 7$ and sends it to Alice.
6. Using b, Alice sends the ciphertext $Z = (a^2b^1[a,b]^3)^{70032} = ab^4 \pmod 7$ to Bob.
7. Bob decrypts Z as $Z^{1090} = (ab^4)^{1090} := a^5b^6[a,b]^2 \pmod 7$ and obtains the message Y.

Consider the Heisenberg group $H_{(t,l,m)}$ and suppose that $t = l = m$. Algorithm 2 is similar to Algorithm 1 but $Q_1^{k,2}(H_{(t,m,l)}, X)$ is used for the message.

Algorithm 2

1: Alice and Bob agree on a public key $(m, J_n^1(k,2))$.
2: Alice chooses $a, b \in J_n^1(k,2)$ such that $ab \equiv 1 \pmod{m}$.
3: Bob chooses $c, d \in J_n^1(k,2)$ such that $cd \equiv 1 \pmod{m}$.
4: Alice sends a message $Y \in Q_1^{k,2}(H_{(t,m,l)}, X)$ to Bob by computing $Y^a \pmod{m}$.
5: Using c, Bob obtains $Y^{ac} \pmod{m}$ and sends it to Alice.
6: Alice uses b and sends the ciphertext $Z = Y^{acb} \pmod{m}$ to Bob.
7: Bob decrypts Z and obtains the message Y.

The algorithm steps are illustrated in Figure 2. In this algorithm, the message Y is obtained by Bob after decrypting the ciphertext Z. Since the verification is analogous to that of Lemma 4.1, we record the argument below only for completeness.

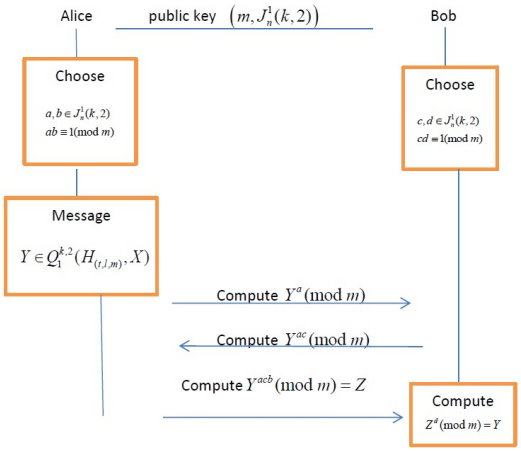

Fig. 2. A flowchart of Algorithm 2

Lemma 4.3. *The original message Y is obtained by Bob after decrypting the ciphertext Z.*

Proof. We show that $Z^d = Y$. We have that

$$Z = (Y^{ac})^b \equiv Y^{acb} \pmod{m}.$$

Using $ab \equiv 1 \pmod{m}$, we obtain $Z = Y^c \pmod{m}$, and Bob decrypts using d. Since $Y \in Q_1^{k,2}(H_{(t,m,l)}, X)$, Lemma 3.7 and the fact that $cd \equiv 1 \pmod{m}$ give

$$Z^d = Y^{cd} \equiv Y \pmod{m}.$$

□

Consider the following example.

Example 4.4. Let $p = 1, t = 2$ and $k = 2$.

1. Alice and Bob agree on a public key $(5, J_n^1(2,2))$.
2. Alice chooses $a := J_6^1(2,2) = 17$ and $b := J_7^1(2,2) = 48$ such that $ab \equiv 1 \pmod 5$.
3. Bob chooses $c := J_{14}^1(2,2) = 70032$ and $d := J_{15}^1(2,2) = 198273$ such that $cd \equiv 1 \pmod 5$.
4. Alice sends a message $Y = ab^2c^2 \in Q_1^{2,2}(H_{(t,m,l)}, X)$ to Bob by computing $(ab^2c^2)^{17} \equiv a^2b^4c^2 \pmod 5$.
5. Using c, Bob obtains $(a^2b^4c^2)^{70032} \equiv a^4b^3c \pmod 5$ and sends it to Alice.
6. Using b, Alice sends the ciphertext $Z = (a^4b^3c)^{48} \equiv a^2b^4c^2 \pmod 5$ to Bob.
7. Bob decrypts Z as $Z^{198273} = (a^2b^4c^2)^{198273} \equiv ab^2c^2 \pmod 5$ and obtains the message Y.

5. Security considerations and limitations

This section discusses the security-related aspects of the proposed constructions. We emphasize that the primary contribution of this work is *algebraic and structural*, rather than the establishment of a cryptosystem with modern, provable security guarantees. Accordingly, the discussion is framed to clarify correctness, assumptions, and limitations, and to position the proposed schemes as mathematically motivated variants of the classical Massey-Omura protocol.

5.1. Comparison with classical Massey-Omura

The proposed constructions should be understood as algebraic variants of the classical Massey-Omura protocol, rather than as replacements or improvements in a security-theoretic sense. While the use of structured exponent sequences introduces novel mathematical behavior, no claim is made that the resulting schemes provide stronger security guarantees than the original Massey–Omura protocol. Any comparisons are limited to algebraic structure and correctness properties, and not to resistance against cryptanalytic attacks. We now consider attacks on the proposed Massey-Omura encryption with the generalized (k,t)-Jacobsthal p-numbers and compare it with the original Massey-Omura encryption. The original Massey–Omura encryption is implemented in $\mathbb{Z}_p^*$, so Alice chooses private exponents e_A, d_A such that $e_A d_A \equiv 1 \pmod{p-1}$ and Bob chooses private exponents e_B, d_B such that $e_B d_B \equiv 1 \pmod{p-1}$. Thus the admissible exponents are units modulo $p-1$, and their number is $\varphi(p-1)$. In the proposed construction, Alice selects a and b from values of $J_n^p(k,t)$ satisfying $ab \equiv 1 \pmod m$, while Bob selects c and d satisfying $cd \equiv 1 \pmod m$. The crucial difference is therefore not the logical structure of the three-pass protocol, but the restriction of the exponent set to a recurrence-defined family that must still satisfy the same invertibility requirement.

5.2. Threat model and scope

The security considerations of the proposed constructions are analyzed within the same conceptual framework as the classical Massey–Omura three-pass protocol. In this setting, the communication channel is assumed to be observable, and an adversary may obtain all transmitted group elements exchanged between legitimate parties. The purpose of this work is not to introduce a new adversarial model or to redefine security notions, but rather to study the algebraic behavior and correctness of Massey-Omura-type protocols when private exponents are selected from structured recurrence-based sequences. Accordingly, the analysis focuses on algebraic feasibility, invertibility conditions, and the preservation of the protocol's functional properties under such constraints.

5.3. Underlying hardness assumptions

As in the classical Massey-Omura protocol, the security intuition underlying the proposed schemes relies on the assumed hardness of the discrete logarithm problem (DLP) in the chosen platform group. Specifically, given a group element g and an exponentiated element g^x, it is assumed to be computationally infeasible for a passive adversary to recover x without additional information. The present work does not introduce new computational hardness assumptions beyond this classical setting. However, it is important to note that the constructions employ finite groups with specific algebraic structure, including nilpotent and class-2 groups. From a security perspective, both approaches rely on exponentiation in finite groups and do not introduce fundamentally different hardness assumptions. The structured nature of the Jacobsthal-based exponent selection primarily affects the algebraic form and distribution of admissible keys rather than the underlying attack model. No claim is made that the structured key selection provides increased resistance to cryptanalytic attacks compared to the classical setting. Instead, the contribution of the proposed schemes lies in demonstrating that Massey-Omura encryption can be realized using recurrence-defined exponent sequences in finite groups while preserving functional correctness and algebraic feasibility. The resulting constructions thus extend the classical protocol framework in an algebraic direction without altering its foundational security assumptions.

5.4. Periodicity and keyspace considerations, complexity estimates and attack costs

Although the defining sequences are infinite over the integers, all cryptographic operations take place in finite groups or modulo finite integers. As a result, the induced exponent sequences are periodic on a finite state space, and the effective cryptographic keyspace is finite. The infinitude of the underlying integer sequence therefore does not imply an infinite cryptographic keyspace. Instead, the security-relevant parameters are determined by the order or exponent of the underlying group, the period of the recurrence modulo the relevant modulus, and the subset of sequence values satisfying the required invertibility conditions. The variability already visible in Table 2 provides a small computational illustration of this point. We now analyze the computational hardness of recovering private exponents or plaintexts from the publicly transmitted values in the proposed

Massey–Omura-type protocols. As in the classical three-pass protocol, a passive adversary observes the values Y^a, Y^{ac}, and Y^{acb}, all lying in G, where G is either G_m or $H(t, \ell, m)$. The security of the scheme therefore depends on the difficulty of recovering exponents from group exponentiation and on the effective size of the exponent space induced by the generalized (k, t)-Jacobsthal p-numbers.

5.4.1. Cost of recovering exponents in the underlying group. Let $g \in G$ be a group generator and suppose an adversary attempts to recover the exponent a from g^a. In general, nilpotent groups of class 2, the discrete logarithm problem (DLP) does not have known polynomial-time solutions, and the best generic attacks (e.g., adaptations of Pollard's rho or baby-step/giant-step) run in time $O(\sqrt{|G|})$. Thus, if exponents were chosen uniformly, recovering a or c would require $O(\sqrt{m})$ group operations. Since the proposed scheme preserves the same exponentiation structure as the classical Massey-Omura protocol, it inherits this attack complexity provided that the exponent space is sufficiently large.

5.4.2. Effective keyspace induced by Jacobsthal periodicity. In the present construction, private exponents are not arbitrary residues modulo m, but are selected from the generalized (k, t)-Jacobsthal p-sequence reduced modulo m. Because this sequence is ultimately periodic with period $hJ_m^p(k, t)$, the total number of admissible exponents is at most $\mathcal{K} = hJ_m^p(k, t)$. Therefore, an adversary needs to search only this set, and the cost of a brute-force exponent-recovery attack reduces to $O\left(\sqrt{hJ_m^p(k, t)}\right)$. If $hJ_m^p(k, t) \ll m$, then the effective exponent entropy is significantly reduced, and the protocol becomes easier to attack than the classical Massey-Omura scheme.

The recurrence defining the generalized Jacobsthal numbers has order $t + p$, and its reduction modulo m is periodic. Although an upper bound on the maximum possible period is m^{t+p}, the *actual* period may be much smaller for certain moduli, particularly those with small prime factors or special algebraic properties. If $hJ_m^p(k, t)$ is small, then

- the entropy of private exponents decreases to $\log_2(hJ_m^p(k, t))$;
- brute-force exponent enumeration may be feasible;
- the protocol's security degrades below that of the classical three-pass scheme.

Thus, periodicity plays a central role in the practical security of the proposed method.

5.4.3. Practical implications for parameter selection. To maintain security comparable to the classical Massey-Omura protocol, the parameters (k, t, p, m) must be chosen so that the Jacobsthal period $hJ_m^p(k, t)$ is large. In particular

- the modulus m should avoid values known to induce short recurrence periods;
- the recurrence order $t + p$ should be sufficiently large to support long periods;
- the actual period $hJ_m^p(k, t)$ should be estimated or empirically validated for any proposed parameter set.

The computational cost of attacking the proposed schemes is dominated by exponent recovery. However, because exponents are drawn from periodic Jacobsthal sequences, the effective keyspace is $hJ_m^p(k, t)$, not m. Consequently, attack costs scale as $O(\sqrt{hJ_m^p(k, t)})$, emphasizing the importance of ensuring that the Jacobsthal period is sufficiently large.

6. Conclusions

In this work, we introduced the generalized (k, t)-Jacobsthal p-numbers and analyzed their structural properties in both integer and finite-group settings. We established modular periodicity results, derived recurrence relations for the induced group sequences, and extended the construction to the specific finite groups G_m and $H(t, \ell, m)$. These algebraic foundations enabled the formulation of two Massey–Omura-type encryption mechanisms in which private exponents are drawn from recurrence-defined sequences rather than from unrestricted residue classes. We proved the correctness of the proposed schemes and clarified how periodicity controls both the feasibility of invertible exponent selection and the size of the effective keyspace. The contribution of the paper is therefore algebraic: it shows that structured exponent families arising from generalized Jacobsthal recurrences can be incorporated into three-pass protocols without changing the underlying security assumptions. At the same time, the analysis in Section 5 makes clear that the resulting constructions should be viewed as mathematically motivated variants of the classical Massey–Omura scheme, not as universally stronger replacements. Similar ideas may also be explored with other recurrence families, including Fibonacci- and Pell-type sequences on finite groups [8, 14, 15, 16], which may further illuminate the mathematical and practical implications of recurrence-based exponent selection in cryptographic protocols.

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. On the jacobsthal–padovan p-sequences in groups. *Topological Algebra and Its Applications*, 5:63–66, 2017. https://doi.org/10.1515/taa-2017-0010.

[2] N. F. H. Al Saffar, I. R. Al-Saiq, and R. R. M. Abo Alsabeh. Asymmetric image encryption scheme based on massey–omura scheme. *International Journal of Electrical and Computer Engineering*, 12(1):1040–1047, 2022. https://doi.org/10.11591/ijece.v12i1.pp1040-1047.

[3] M. Asci and E. Gurel. Gaussian jacobsthal and gaussian jacobsthal–lucas polynomials. *Notes on Number Theory and Discrete Mathematics*, 19(1):25–36, 2013.

[4] R. E. Atani, S. E. Atani, and S. Mirzakuchaki. Public key cryptography using semigroup actions and semirings. *Journal of Discrete Mathematical Sciences and Cryptography*, 11(4):437–445, 2008. https://doi.org/10.1080/09720529.2008.10698195.

[5] D. Bród and A. Michalski. On generalized jacobsthal and jacobsthal–lucas numbers. *Annales Mathematicae Silesianae*, 36(32):115–128, 2022. https://doi.org/10.2478/amsil-2022-0011.

[6] D. Bród and A. Szynal-Liana. On $J(r, n)$-jacobsthal quaternions. *Pure and Applied Mathematics Quarterly*, 14(3–4):579–590, 2018. https://doi.org/10.4310/PAMQ.2018.v14.n3.a7.

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

[8] Ö. Deveci. The k-nacci sequences and the generalized order-k pell sequences in the semi-direct product of finite cyclic groups. *Chiang Mai Journal of Science*, 40(1):89–98, 2013.

[9] H. Doosti and M. Hashemi. Fibonacci lengths involving the wall number $k(n)$. *Journal of Applied Mathematics and Computation*, 20(1–2):171–180, 2006. https://doi.org/10.1007/BF02831931.

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

[11] A. P. Fournaris and O. Koufopavlou. Optimized $GF(2^k)$ onb type i multiplier architecture based on the massey–omura multiplication pattern. In *Journal of Physics: Conference Series*, volume 10, pages 381–384, 2005. https://doi.org/10.1088/1742-6596/10/1/093.

[12] S. Haley. *Non-commutative Massey–Omura Encryption with Symmetric Groups*. Honors Thesis, University of Mary Washington, Fredericksburg, VA, USA, 2018.

[13] D. Hankerson, S. Vanstone, and A. Menezes. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York, NY, USA, 2004.

[14] M. Hashemi and E. Mehraban. On the generalized order 2-pell sequence of some classes of groups. *Communications in Algebra*, 46(9):4104–4119, 2018. https://doi.org/10.1080/00927872.2018.1435793.

[15] 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, 2022. https://doi.org/10.1080/00927872.2021.1988959.

[16] 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.

[17] A. F. Horadam. Jacobsthal and pell curves. *The Fibonacci Quarterly*, 26(1):79–83, 1988. https://doi.org/10.1080/00150517.1988.12429664.

[18] F. Koken and D. Bozkurt. On the jacobsthal–lucas numbers by matrix method. *International Journal of Contemporary Mathematical Sciences*, 3(13):605–614, 2008.

[19] J. L. Massey and J. K. Omura. Method and apparatus for maintaining the privacy of digital messages conveyed by public transmission. (US 4,567,600). 1986.

[20] 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. *Mathematical Foundations of Computing*, 11:103–119, 2025. https://doi.org/10.3934/mfc.2025036.

[21] E. Mehraban, T. A. Gulliver, R. E. Atani, and E. Hincal. Diffie–hellman key exchange on the heisenberg group. *Journal of Combinatorial Mathematics and Combinatorial Computing*, 127:301–315, 2023. https://doi.org/10.61091/jcmcc127-22.

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

[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. G. Prasad, P. P. Chari, and K. P. Satyam. Affine hill cipher key generation matrix of order 3 by using reflects in an arbitrary line $y = ax + b$. *International Journal of Science Technology and Management*, 5(8):268–272, 2016.

[25] D. Rachmawati, M. A. Budiman, and M. A. Rikzan. Analysis of file security with three-pass protocol scheme using massey–omura algorithm in android. *Journal of Physics: Conference Series*, 1235:012175, 2019. https://doi.org/10.1088/1742-6596/1235/1/012075.

[26] A. Reyhani-Masoleh and M. A. Hasan. A new construction of massey–omura parallel multiplier over $GF(2^m)$. *IEEE Transactions on Computers*, 51(5):511–520, 2002. https://doi.org/10.1109/TC.2002.1004590.

[27] Ş. Uygun and H. Eldogan. Properties of k-jacobsthal and k-jacobsthal lucas sequences. *General Mathematics Notes*, 36(1):34–47, 2016.

[28] R. Winton. Enhancing the massey–omura cryptosystem. *Journal of Mathematical Sciences and Mathematics Education*, 2(1):21–29, 2007.

Elahe Mehraban
Mathematics Research Center, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey
E-mail e.mehraban.math@gmail.com

Reza Ebrahimi Atani
Department of Computer Engineering, University of Guilan, Rasht, Iran
E-mail rebrahimi@guilan.ac.ir,

T. Aaron Gulliver
Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, V8W 2Y2, Canada
E-mail agullive@uvic.ca

Evren Hincal
Mathematics Research Center, Near East University TRNC, Mersin 10, 99138 Nicosia, Turkey
Department of Mathematical Sciences, Saveetha School of Engineering, SIMATS, Chennai - 602105, Tamilnadu, India
Research Center of Applied Mathematics, Khazar University, Baku, Azerbaijan
E-mail evren.hincal@neu.edu.tr