

Implementation of Blom's key scheme using the (q,m) -Lucas-Pell sequences

Elahe Mehraban *

Mathematics Research Center

Near East University

Turkish Republic of Northern Cyprus

Mersin 10

99138 Nicosia

Turkey

and

Department of Mathematics

Near East University

Turkish Republic of Northern Cyprus

Mersin 10

99138 Nicosia

Turkey

and

Faculty of Art and Science

University of Kyrenia

Turkish Republic of Northern Cyprus

Mersin 10

99320 Kyrenia

Turkey

T. Aaron Gulliver [†]

Department of Electrical and Computer Engineering

University of Victoria

Victoria

BC, V8W 2Y2

Canada

* E-mail: e.mehraban.math@gmail.com (Corresponding Author)

[†] E-mail: agullive@ece.uvic.ca

Evren Hinçal [§]

*Mathematics Research Center
Near East University
Turkish Republic of Northern Cyprus
Mersin 10
99138 Nicosia
Turkey*

and

*Department of Mathematics
Near East University
Turkish Republic of Northern Cyprus
Mersin 10
99138 Nicosia
Turkey*

and

*Faculty of Art and Science
University of Kyrenia
Turkish Republic of Northern Cyprus
Mersin 10
99320 Kyrenia
Turkey*

Abstract

In this paper, we define new sequences using Lucas and Pell sequences. Then the (q, m) -Lucas-Pell sequence matrix is introduced and some interesting structural results are obtained. These sequences are used to implement Blom's key scheme and the security is examined. This is the first use of such sequences to obtain cryptographic keys.

Subject Classification (2010): Primary: 11K31, 11C20, 68P25 Secondary: 68R01, 68P30, 15A15.

Keywords: Lucas sequence, Pell sequence, Blom's key scheme, symmetric key, security.

1. Introduction

The Pell sequence $\{P_n\}_0^\infty$ is

$$P_n = 2P_{n-1} + P_{n-2}, n \geq 2,$$

with initial terms $P_0 = 0$ and $P_1 = 1$. It is important in mathematics and other fields, and so has been the subject of significant research [5, 7, 8]. The generalized

[§] E-mail: evren.hincal@neu.edu.tr

order 2-Pell sequences of some classes of groups were studied in [6]. In [2], the quaternion-Pell sequence was defined and some interesting results were obtained. The quaternion-type cyclic-Pell sequences in finite groups were given in [18].

The Lucas sequence $\{L_n\}_0^\infty$ is

$$L_n = L_{n-1} + L_{n-2}, n \geq 2,$$

with initial terms $L_0 = 2$ and $L_1 = 1$. The following generalization of the Lucas sequence was introduced in [18].

Definition 1.1: 1The m -extension of the Lucas q -numbers, $\{L_{q,m}(n)\}_0^\infty$, is given by

$$L_{q,m}(n) = mL_{q,m}(n-1) + L_{q,m}(n-q-1),$$

with initial terms

$$L_{q,m}(1) = a_1, L_{q,m}(2) = a_2, \dots, L_{q,m}(q+1) = a_{q+1},$$

where $q \geq 0$ is an integer, $m > 0$, $n > q+1$, and $a_1, a_2, a_3, \dots, a_{q+1}$ are arbitrary real or complex numbers.

Example 1.1: 2

(i) If $m = 1$ and $q = 3$, then

$$L_{3,1}(n) = L_{3,1}(n-1) + L_{3,1}(n-4),$$

with initial terms

$$L_{3,1}(1) = L_{3,1}(2) = L_{3,1}(3) = 0, L_{3,1}(4) = 1,$$

$$\text{so } \{L_{3,1}(n)\}_0^\infty = \{0, 0, 0, 1, 1, 1, 2, 3, 4, \dots\}.$$

(ii) If $m = 1$ and $q = 5$, then

$$L_{5,1}(n) = L_{5,1}(n-1) + L_{5,1}(n-6),$$

with initial terms

$$L_{5,1}(1) = L_{5,1}(2) = \dots = L_{5,1}(5) = 0, L_{5,1}(6) = 1,$$

$$\text{so } \{L_{5,1}(n)\}_0^\infty = \{0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 2, 3, \dots\}.$$

Define the sequence $\{x_n\}_0^\infty$ as

$$x_n = x_{n-1} + x_{n-2} + \dots + x_{n-t}, n \geq t,$$

so that

$$x_n - x_{n-1} - x_{n-2} - \dots - x_{n-t} = 0.$$

For a solution r^n we have

$$r^n - r^{n-1} - \dots - r^{n-t} = 0,$$

which gives the characteristic polynomial

$$r^t - r^{t-1} - \dots - 1 = 0.$$

The Pell sequence and m -extension of the Lucas q -numbers have characteristic polynomials $x^2 - 2x - 1$ and $x^{q+1} - mx^q - 1$, respectively.

New generalizations of the Fibonacci and Lucas p –numbers were introduced in [17] and Binet formulas were derived. In [3], representations of the real numbers were derived using k –Lucas series.

Blom's scheme is a symmetric threshold key exchange cryptography protocol [12] and is given below.

1. There is a trusted party (Trent) and a group of users.
2. A secret symmetric matrix $D_{k \times k}$ over the finite field $\mathbb{F}_p$, p a prime number, is randomly chosen by Trent.
3. For new users (Alice and Bob), that want to join the group, Trent chooses k –element vectors $I_{Alice}, I_{Bob} \in \mathbb{F}_p^k$ as their public identifiers. He then computes $g_{Alice} = DI_{Alice} \pmod{p}$ and $g_{Bob} = DI_{Bob} \pmod{p}$ as their private keys. These private keys are used to obtain shared keys with other group members.
4. To communicate with each other, Alice and Bob do the following. Alice uses I_{Bob} and her private key g_{Alice} to obtain the shared key $K_{Alice \setminus Bob} = g_{Alice}^T I_{Bob}$ where T denotes matrix transpose. Bob uses I_{Alice} and his private key g_{Bob} and gets the same result

$$\begin{aligned} K_{Alice \setminus Bob} &= K_{Alice \setminus Bob}^T = (g_{Alice}^T I_{Bob})^T = (I_{Alice}^T D^T I_{Bob})^T \\ &= I_{Bob}^T D I_{Alice} = g_{Bob}^T I_{Alice} = K_{Bob \setminus Alice}. \end{aligned}$$

The security of the Multiple-Key Blom's (MKB) key agreement scheme was studied in [16]. In [1], preliminary Blom's key distribution was presented. This requires a function of three variables and key construction is not symmetric. Elliptic Curve Cryptography (ECC) was used in [15] to improve the security of Blom's original scheme. These results motivate this work which introduces new sequences from the Pell sequence and m –extension of the Lucas q –numbers. They are employed to implement Blom's scheme. The next section presents the new sequences and some associated results are given. These sequences are used in Section 3 to implement Blom's key scheme and the security is examined.

2. The (q, m) –Lucas-Pell sequences

This section gives some new sequences and some associated results.

Definition 2.1: For integers $q \geq 3$ and $m \geq 1$, the (q, m) – Lucas-Pell sequences $\{LP_n(q, m)\}_0^\infty$ are given by

$$\begin{aligned} LP_{n+q+3}(q, m) &= (2 + m)LP_{n+q+2}(q, m) - (-1 + 2m)LP_{n+q+1}(q, m) \\ &\quad - mLP_{n+q}(q, m) + LP_{n+2}(q, m) - 2LP_{n+1}(q, m) \\ &\quad - LP_n(q, m), n \geq q + 3, \end{aligned}$$

where $LP_0(q, m) = LP_1(q, m) = \dots = LP_{q+1}(q, m) = 0$ and $LP_{q+2}(q, m) = 1$.

Example 2.1:

(i) For $q = 3$ and $m = 1$ we have

$$LP_{n+6}(3,1) = 3LP_{n+5}(3,1) - LP_{n+4}(3,1) - LP_{n+3}(3,1) + LP_{n+2}(3,1) \\ - 2LP_{n+1}(3,1) - LP_n(3,1), n \geq 6.$$

Therefore, the sequence is

$$\{LP_n(3,1)\}_0^\infty = \{0,0,0,0,1,3,8,20,50,123,300,728,1763, \dots\}.$$

(ii) For $q = 3$ and $m = 2$ we have

$$LP_{n+6}(3,2) = 4LP_{n+5}(3,1) - 3LP_{n+4}(3,2) - 2LP_{n+3}(3,2) + LP_{n+2}(3,2) \\ - 2LP_{n+1}(3,2) - LP_n(3,2), n \geq 6,$$

so the sequence is

$$\{LP_n(3,2)\}_0^\infty = \{0,0,0,0,1,4,13,38,106,286,754,1954,4999, \dots\}.$$

(iii) For $q = 4$ and $m = 1$ we have

$$LP_{n+7}(4,1) = 3LP_{n+6}(4,1) - LP_{n+5}(4,1) - 1LP_{n+4}(4,1) + LP_{n+2}(4,1) \\ - 2LP_{n+1}(4,1) - LP_n(4,1), n \geq 7.$$

Thus, the sequence is

$$\{LP_n(4,1)\}_0^\infty = \{0,0,0,0,0,1,3,8,20,49,120,292,708,1713,4140,10001, \dots\}.$$

Lemma 2.1: The generating function of the (q, m) –Lucas-Pell sequences is

$$g_{LP_n(q,m)} = \frac{x^{q+2}}{1-(2+m)x+(-1+2m)x^2+mx^3-x^{q+1}+2x^{q+2}+x^{q+3}}. \quad (2.1)$$

Proof: We have

$$\begin{aligned} g_{LP_n(q,m)} &= \sum_{n=1}^\infty LP_n(q,m)x^n \\ &= LP_1(q,m)x + LP_2(q,m)x^2 + \dots + LP_{q+2}(q,m)x^{q+2} + \sum_{n=q+3}^\infty LP_n(q,m)x^n \\ &= x^{q+2} + \sum_{n=q+3}^\infty (2+m)LP_{n+q+2}(q,m) - (-1+2m)LP_{n+q+1}(q,m) - \\ &\quad mLP_{n+q}(q,m) + LP_{n+2}(q,m) - 2LP_{n+1}(q,m) - LP_n(q,m)x^n \\ &= x^{q+2} + \sum_{n=q+3}^\infty (2+m)LP_{n+q+2}(q,m)x^n - \sum_{n=q+3}^\infty (-1+2m) \\ &\quad LP_{n+q+1}(q,m)x^n - \sum_{n=q+3}^\infty mLP_{n+q}(q,m)x^n + \sum_{n=q+3}^\infty LP_{n+2}(q,m)x^n - \\ &\quad \sum_{n=q+3}^\infty 2LP_{n+1}(q,m)x^n - \sum_{n=q+3}^\infty LP_n(q,m)x^n \\ &= x^{q+2} + (2+m)x \sum_{n=1}^\infty LP_n(q,m)x^n - (-1+2m)x^2 \sum_{n=1}^\infty LP_n(q,m)x^n - \\ &\quad mx^3 \sum_{n=1}^\infty LP_n(q,m)x^n + x^{q+1} \sum_{n=1}^\infty LP_n(q,m)x^n - 2x^{q+2} \sum_{n=1}^\infty \\ &\quad LP_n(q,m)x^n - x^{q+3} \sum_{n=1}^\infty LP_n(q,m)x^n, \end{aligned}$$

so

$$g_{LP_n(q,m)} = \frac{x^{q+2}}{1-(2+m)x+(-1+2m)x^2+mx^3-x^{q+1}+2x^{q+2}+x^{q+3}}.$$

Lemma 2.2: The generating function of the (q, m) –Lucas-Pell sequences has the following exponential representation

$$g_{LP_n(q,m)} = x^{q+2} \exp \sum_{i=1}^{\infty} \frac{x^i}{i} ((2+m) - (-1+2m)x - mx^2 + x^q - 2x^{q+1} - x^{q+2})^i,$$

where $q \geq 3$.

Proof: From (2.1) we have

$$\begin{aligned} \ln \frac{g_{LP_n(q,m)}}{x^{q+3}} &= -\ln(1 - (2+m)x + (-1+2m)x^2 + mx^3 - x^{q+1} + 2x^{q+2} + x^{q+3}). \\ &= -\ln(1 - (2+m)x + (-1+2m)x^2 + mx^3 - x^{q+1} + 2x^{q+2} + x^{q+3}) \\ &= -[-x((2+m) - (-1+2m)x - mx^2 + x^q - 2x^{q+1} - x^{q+2}) \\ &\quad - \frac{1}{2}x^2((2+m) - (-1+2m)x - mx^2 + x^q - 2x^{q+1} - x^{q+2})^2 - \dots \\ &\quad - \frac{1}{n}x^n((2+m) - (-1+2m)x - mx^2 + x^q - 2x^{q+1} - x^{q+2})^n - \dots]. \end{aligned}$$

Let $q \geq 3$ and $m \geq 1$. From the recurrence relation (2.1) we have

$$\begin{bmatrix} LP_{n+q+3}(q,m) \\ LP_{n+q+2}(q,m) \\ LP_{n+q+1}(q,m) \\ \vdots \\ LP_{n+2}(q,m) \\ LP_{n+1}(q,m) \end{bmatrix} = \begin{bmatrix} 2+m & 1-2m & -m & 0 & \cdots & 0 & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} LP_{n+q+2}(q,m) \\ LP_{n+q+1}(q,m) \\ LP_{n+q}(q,m) \\ \vdots \\ LP_{n+1}(q,m) \\ LP_n(q,m) \end{bmatrix},$$

which has companion matrix

$$M_q(m) = \begin{bmatrix} 2+m & 1-2m & -m & 0 & \cdots & 0 & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}_{(q+3) \times (q+3)}.$$

$M_q(m)$ is called the (q, m) –Lucas-Pell sequence matrix.

Lemma 2.3: For $q = 3, m = 1$, and $n \geq 6$ we have

$$\begin{aligned} (M_3(1))^n &= \\ \begin{bmatrix} LP_{n+5}(3,1) & -(LP_{n+4}(3,1) + LP_{n+3}(3,1) - L_{n+1}(3,1)) & -(LP_{n+4}(3,1) - L_{n+2}(3,1)) \\ LP_{n+4}(3,1) & -(LP_{n+3}(3,1) + LP_{n+2}(3,1) - L_n(3,1)) & -(LP_{n+3}(3,1) - L_{n+1}(3,1)) \\ LP_{n+3}(3,1) & -(LP_{n+2}(3,1) + LP_{n+1}(3,1) - L_{n-1}(3,1)) & -(LP_{n+2}(3,1) - L_n(3,1)) \\ LP_{n+2}(3,1) & -(LP_{n+1}(3,1) + LP_n(3,1) - L_{n-2}(3,1)) & -(LP_{n+1}(3,1) - L_{n-1}(3,1)) \\ LP_{n+1}(3,1) & -(LP_n(3,1) + LP_{n-1}(3,1) - L_{n-3}(3,1)) & -(LP_n(3,1) - L_{n-2}(3,1)) \\ LP_n(3,1) & -(LP_{n-1}(3,1) + LP_{n-2}(3,1) - L_{n-4}(3,1)) & -(LP_{n-1}(3,1) - L_{n-3}(3,1)) \end{bmatrix} \end{aligned}$$

$$\begin{bmatrix} L_{n+3}(3,1) & -(2LP_{n+4}(3,1) + LP_{n+3}(3,1)) & -LP_{n+4}(3,1) \\ L_{n+2}(3,1) & -(2LP_{n+3}(3,1) + LP_{n+2}(3,1)) & -LP_{n+3}(3,1) \\ L_{n+1}(3,1) & -(2LP_{n+2}(3,1) + LP_{n+1}(3,1)) & -LP_{n+2}(3,1) \\ L_n(3,1) & -(2LP_{n+1}(3,1) + LP_n(3,1)) & -LP_{n+1}(3,1) \\ L_{n-1}(3,1) & -(2LP_n(3,1) + LP_{n-1}(3,1)) & -LP_n(3,1) \\ L_{n-2}(3,1) & -(2LP_{n-1}(3,1) + LP_{n-2}(3,1)) & -LP_{n-1}(3,1) \end{bmatrix}.$$

Proof: The proof is by induction on n . The result is true for $n = 6$ which gives

$$\begin{aligned} (M_3(1))^n &= \begin{bmatrix} 300 & -172 & -121 & 3 & -296 & -123 \\ 123 & -69 & -49 & 2 & -120 & 50 \\ 50 & -27 & -19 & 1 & -48 & -20 \\ 20 & -10 & -7 & 1 & -19 & -8 \\ 8 & -4 & -2 & 1 & -7 & -3 \\ 3 & -1 & -1 & 1 & -2 & -1 \end{bmatrix} \\ &= \begin{bmatrix} LP_{11}(3,1) & -(LP_{10}(3,1) + LP_9(3,1) - L_7(3,1)) & -(LP_{10}(3,1) - L_8(3,1)) \\ LP_{10}(3,1) & -(LP_9(3,1) + LP_8(3,1) - L_6(3,1)) & -(LP_9(3,1) - L_7(3,1)) \\ LP_9(3,1) & -(LP_8(3,1) + LP_7(3,1) - L_5(3,1)) & -(LP_8(3,1) - L_6(3,1)) \\ LP_8(3,1) & -(LP_7(3,1) + LP_6(3,1) - L_4(3,1)) & -(LP_7(3,1) - L_5(3,1)) \\ LP_7(3,1) & -(LP_6(3,1) + LP_5(3,1) - L_3(3,1)) & -(LP_6(3,1) - L_4(3,1)) \\ LP_6(3,1) & -(LP_5(3,1) + LP_4(3,1) - L_2(3,1)) & -(LP_5(3,1) - L_3(3,1)) \end{bmatrix} \\ &\quad \begin{bmatrix} L_9(3,1) & -(2LP_{10}(3,1) + LP_9(3,1)) & -LP_{10}(3,1) \\ L_8(3,1) & -(2LP_9(3,1) + LP_8(3,1)) & -LP_9(3,1) \\ L_7(3,1) & -(2LP_8(3,1) + LP_7(3,1)) & -LP_8(3,1) \\ L_6(3,1) & -(2LP_7(3,1) + LP_6(3,1)) & -LP_7(3,1) \\ L_5(3,1) & -(2LP_6(3,1) + LP_5(3,1)) & -LP_6(3,1) \\ L_4(3,1) & -(2LP_5(3,1) + LP_4(3,1)) & -LP_5(3,1) \end{bmatrix}. \end{aligned}$$

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

$$\begin{aligned} (M_3(1))^{s+1} &= \begin{bmatrix} LP_{s+5}(3,1) & -(LP_{s+4}(3,1) + LP_{s+3}(3,1) - L_{s+1}(3,1)) & -(LP_{s+4}(3,1) - L_{s+2}(3,1)) \\ LP_{s+4}(3,1) & -(LP_{s+3}(3,1) + LP_{s+2}(3,1) - L_s(3,1)) & -(LP_{s+3}(3,1) - L_{s+1}(3,1)) \\ LP_{s+3}(3,1) & -(LP_{s+2}(3,1) + LP_{s+1}(3,1) - L_{s-1}(3,1)) & -(LP_{s+2}(3,1) - L_s(3,1)) \\ LP_{s+2}(3,1) & -(LP_{s+1}(3,1) + LP_s(3,1) - L_{s-2}(3,1)) & -(LP_{s+1}(3,1) - L_{s-1}(3,1)) \\ LP_{s+1}(3,1) & -(LP_s(3,1) + LP_{s-1}(3,1) - L_{s-3}(3,1)) & -(LP_s(3,1) - L_{s-2}(3,1)) \\ LP_s(3,1) & -(LP_{s-1}(3,1) + LP_{s-2}(3,1) - L_{s-4}(3,1)) & -(LP_{s-1}(3,1) - L_{s-3}(3,1)) \end{bmatrix} \\ &\quad \begin{bmatrix} L_{s+3}(3,1) & -(2LP_{s+4}(3,1) + LP_{s+3}(3,1)) & -LP_{s+4}(3,1) \\ L_{s+2}(3,1) & -(2LP_{s+3}(3,1) + LP_{s+2}(3,1)) & -LP_{s+3}(3,1) \\ L_{s+1}(3,1) & -(2LP_{s+2}(3,1) + LP_{s+1}(3,1)) & -LP_{s+2}(3,1) \\ L_s(3,1) & -(2LP_{s+1}(3,1) + LP_s(3,1)) & -LP_{s+1}(3,1) \\ L_{s-1}(3,1) & -(2LP_s(3,1) + LP_{s-1}(3,1)) & -LP_s(3,1) \\ L_{s-2}(3,1) & -(2LP_{s-1}(3,1) + LP_{s-2}(3,1)) & -LP_{s-1}(3,1) \end{bmatrix} \end{aligned}$$

$$\begin{bmatrix} 3 & -1 & -1 & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}
= \begin{bmatrix} LP_{s+6}(3,1) & -(LP_{s+5}(3,1) + LP_{s+4}(3,1) - L_{s+2}(3,1)) & -(LP_{s+5}(3,1) - L_{s+3}(3,1)) \\ LP_{s+5}(3,1) & -(LP_{s+4}(3,1) + LP_{s+3}(3,1) - L_{s+1}(3,1)) & -(LP_{s+4}(3,1) - L_{s+2}(3,1)) \\ LP_{s+4}(3,1) & -(LP_{s+3}(3,1) + LP_{s+2}(3,1) - L_s(3,1)) & -(LP_{s+3}(3,1) - L_{s+1}(3,1)) \\ LP_{s+3}(3,1) & -(LP_{s+2}(3,1) + LP_{s+1}(3,1) - L_{s-1}(3,1)) & -(LP_{s+2}(3,1) - L_s(3,1)) \\ LP_{s+2}(3,1) & -(LP_{s+1}(3,1) + LP_s(3,1) - L_{s-2}(3,1)) & -(LP_{s+1}(3,1) - L_{s-1}(3,1)) \\ LP_{s+1}(3,1) & -(LP_s(3,1) + LP_{s-1}(3,1) - L_{s-3}(3,1)) & -(LP_s(3,1) - L_{s-2}(3,1)) \end{bmatrix}$$

$$\begin{bmatrix} L_{s+4}(3,1) & -(2LP_{s+5}(3,1) + LP_{s+4}(3,1)) & -LP_{s+5}(3,1) \\ L_{s+3}(3,1) & -(2LP_{s+4}(3,1) + LP_{s+3}(3,1)) & -LP_{s+4}(3,1) \\ L_{s+2}(3,1) & -(2LP_{s+3}(3,1) + LP_{s+2}(3,1)) & -LP_{s+3}(3,1) \\ L_{s+1}(3,1) & -(2LP_{s+2}(3,1) + LP_{s+1}(3,1)) & -LP_{s+2}(3,1) \\ L_s(3,1) & -(2LP_{s+1}(3,1) + LP_s(3,1)) & -LP_{s+1}(3,1) \\ L_{s-1}(3,1) & -(2LP_s(3,1) + LP_{s-1}(3,1)) & -LP_s(3,1) \end{bmatrix},$$

which gives the result.

In general, for $q = 3$ and $m \geq 2$, by induction on n the n th power of the (q, m) -Lucas-Pell sequence matrix is

$$(M_3(m))^n = \begin{bmatrix} LP_{n+5}(3, m) & -((2m-1)LP_{n+4}(3, m) + mLP_{n+3}(3, m) - L_{n+1}(3, m)) & -(mLP_{n+4}(3, m) - L_{n+2}(3, m)) \\ LP_{n+4}(3, m) & -((2m-1)LP_{n+3}(3, m) + mLP_{n+2}(3, m) - L_n(3, m)) & -(mLP_{n+3}(3, m) - L_{n+1}(3, m)) \\ LP_{n+3}(3, m) & -((2m-1)LP_{n+2}(3, m) + mLP_{n+1}(3, m) - L_{n-1}(3, m)) & -(mLP_{n+2}(3, m) - L_n(3, m)) \\ LP_{n+2}(3, m) & -((2m-1)LP_{n+1}(3, m) + mLP_n(3, m) - L_{n-2}(3, m)) & -(mLP_{n+1}(3, m) - L_{n-1}(3, m)) \\ LP_{n+1}(3, m) & -((2m-1)LP_n(3, m) + mLP_{n-1}(3, m) - L_{n-3}(3, m)) & -(mLP_n(3, m) - L_{n-2}(3, m)) \\ LP_n(3, m) & -((2m-1)LP_{n-1}(3, m) + mLP_{n-2}(3, m) - L_{n-4}(3, m)) & -(mLP_{n-1}(3, m) - L_{n-3}(3, m)) \end{bmatrix}$$

$$\begin{bmatrix} L_{n+3}(3, m) & -(2LP_{n+4}(3, m) + LP_{n+3}(3, m)) & -LP_{n+4}(3, m) \\ L_{n+2}(3, m) & -(2LP_{n+3}(3, m) + LP_{n+2}(3, m)) & -LP_{n+3}(3, m) \\ L_{n+1}(3, m) & -(2LP_{n+2}(3, m) + LP_{n+1}(3, m)) & -LP_{n+2}(3, m) \\ L_n(3, m) & -(2LP_{n+1}(3, m) + LP_n(3, m)) & -LP_{n+1}(3, m) \\ L_{n-1}(3, m) & -(2LP_n(3, m) + LP_{n-1}(3, m)) & -LP_n(3, m) \\ L_{n-2}(3, m) & -(2LP_{n-1}(3, m) + LP_{n-2}(3, m)) & -LP_{n-1}(3, m) \end{bmatrix}.$$

For $q = 3$ and $m \geq 1$, $\det(M_3(m))^n = 1$.

Theorem 2.1: For $m \geq 1, n \geq 6$, and $t \geq 1$ we have

- (i) $(M_3(m))^n(M_3(m))^t = ((M_3(m)))^{n+t}$, and
- (ii) $(M_3(m))^n(M_3(m))^t = (M_3(m))^t(M_3(m))^n$.

Proof: The proof of Part (i) is by induction on t . For $t = 1$ we have

$$\begin{aligned}
(M_3(m))^n M_3(m) = & \begin{bmatrix} LP_{n+5}(3, m) & -((2m-1)LP_{n+4}(3, m) + mLP_{n+3}(3, m) - L_{n+1}(3, m)) & -(mLP_{n+4}(3, m) - L_{n+2}(3, m)) \\ LP_{n+4}(3, m) & -((2m-1)LP_{n+3}(3, m) + mLP_{n+2}(3, m) - L_n(3, m)) & -(mLP_{n+3}(3, m) - L_{n+1}(3, m)) \\ LP_{n+3}(3, m) & -((2m-1)LP_{n+2}(3, m) + mLP_{n+1}(3, m) - L_{n-1}(3, m)) & -(mLP_{n+2}(3, m) - L_n(3, m)) \\ LP_{n+2}(3, m) & -((2m-1)LP_{n+1}(3, m) + mLP_n(3, m) - L_{n-2}(3, m)) & -(mLP_{n+1}(3, m) - L_{n-1}(3, m)) \\ LP_{n+1}(3, m) & -((2m-1)LP_n(3, m) + mLP_{n-1}(3, m) - L_{n-3}(3, m)) & -(mLP_n(3, m) - L_{n-2}(3, m)) \\ LP_n(3, m) & -((2m-1)LP_{n-1}(3, m) + mLP_{n-2}(3, m) - L_{n-4}(3, m)) & -(mLP_{n-1}(3, m) - L_{n-3}(3, m)) \end{bmatrix} \\
& \begin{bmatrix} L_{n+3}(3, m) & -(2LP_{n+4}(3, m) + LP_{n+3}(3, m)) & -LP_{n+4}(3, m) \\ L_{n+2}(3, m) & -(2LP_{n+3}(3, m) + LP_{n+2}(3, m)) & -LP_{n+3}(3, m) \\ L_{n+1}(3, m) & -(2LP_{n+2}(3, m) + LP_{n+1}(3, m)) & -LP_{n+2}(3, m) \\ L_n(3, m) & -(2LP_{n+1}(3, m) + LP_n(3, m)) & -LP_{n+1}(3, m) \\ L_{n-1}(3, m) & -(2LP_n(3, m) + LP_{n-1}(3, m)) & -LP_n(3, m) \\ L_{n-2}(3, m) & -(2LP_{n-1}(3, m) + LP_{n-2}(3, m)) & -LP_{n-1}(3, m) \end{bmatrix} \\
& \begin{bmatrix} 2+m & 1-2m & -m & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} = ((M_3(m)))^{n+1}.
\end{aligned}$$

Now suppose the result is true for $t = s$. Then for $t = s + 1$

$$\begin{aligned}
(M_3(m))^n (M_3(m))^{s+1} &= (M_3(m))^{n+s} (M_3(m))^1 = \\
& \begin{bmatrix} LP_{n+s+5}(3, m) & -((2m-1)LP_{n+s+4}(3, m) + mLP_{n+s+3}(3, m) - L_{n+s+1}(3, m)) \\ LP_{n+s+4}(3, m) & -((2m-1)LP_{n+s+3}(3, m) + mLP_{n+s+2}(3, m) - L_{n+s}(3, m)) \\ LP_{n+s+3}(3, m) & -((2m-1)LP_{n+s+2}(3, m) + mLP_{n+s+1}(3, m) - L_{n+s-1}(3, m)) \\ LP_{n+s+2}(3, m) & -((2m-1)LP_{n+s+1}(3, m) + mLP_{n+s}(3, m) - L_{n+s-2}(3, m)) \\ LP_{n+s+1}(3, m) & -((2m-1)LP_{n+s}(3, m) + mLP_{n+s-1}(3, m) - L_{n+s-3}(3, m)) \\ LP_{n+s}(3, m) & -((2m-1)LP_{n+s-1}(3, m) + mLP_{n+s-2}(3, m) - L_{n+s-4}(3, m)) \end{bmatrix} \\
& \begin{bmatrix} -(mLP_{n+s+4}(3, m) - L_{n+s+2}(3, m)) & L_{n+s+3}(3, m) & -(2LP_{n+s+4}(3, m) + LP_{n+s+3}(3, m)) \\ -(mLP_{n+s+3}(3, m) - L_{n+s+1}(3, m)) & L_{n+s+2}(3, m) & -(2LP_{n+s+3}(3, m) + LP_{n+s+2}(3, m)) \\ -(mLP_{n+s+2}(3, m) - L_{n+s}(3, m)) & L_{n+s+1}(3, m) & -(2LP_{n+s+2}(3, m) + LP_{n+s+1}(3, m)) \\ -(mLP_{n+s+1}(3, m) + LP_{n+s}(3, m)) & LP_{n+s}(3, m) & -(2LP_{n+s+1}(3, m) + LP_{n+s}(3, m)) \\ -(mLP_{n+s}(3, m) - L_{n+s-2}(3, m)) & L_{n+s-1}(3, m) & -(2LP_{n+s}(3, m) + LP_{n+s-1}(3, m)) \\ -(mLP_{n+s-1}(3, m) - L_{n+s-3}(3, m)) & L_{n+s-2}(3, m) & -(2LP_{n+s-1}(3, m) + LP_{n+s-2}(3, m)) \end{bmatrix} \\
& \begin{bmatrix} -LP_{n+s+4}(3, m) \\ -LP_{n+s+3}(3, m) \\ -LP_{n+s+2}(3, m) \\ -LP_{n+s+1}(3, m) \\ -LP_{n+s}(3, m) \\ -LP_{n+s-1}(3, m) \end{bmatrix} \begin{bmatrix} 2+m & 1-2m & -m & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \\
& = ((M_3(m)))^{n+s+1},
\end{aligned}$$

and the proof is complete. For Part (ii), from Part (i) we have $(M_3(m))^n (M_3(m))^t = (M_3(m))^{n+t} = (M_3(m))^{t+n} = (M_3(m))^t (M_3(m))^n$.

In general, for $q \geq 4$ and $m = 1$, by induction on $n \geq q + 3$ the n th power of the (q, m) –Lucas-Pell sequence matrix is

$$(M_q(1))^n = \begin{bmatrix} LP_{n+q+2}(q, 1) & -(LP_{n+q+1}(q, 1) + LP_{n+q}(q, 1) - L_{2n-q-2}(q, 1)) & -(LP_{n+q+1}(q, 1) - L_{2n-q-1}(q, 1)) \\ LP_{n+q+1}(q, 1) & -(LP_{n+q}(q, 1) + LP_{n+q-1}(q, 1) - L_{2n-q-3}(q, 1)) & -(LP_{n+q}(q, 1) - L_{2n-q-2}(q, 1)) \\ \vdots & \vdots & \vdots \\ LP_{n+1}(q, 1) & -(LP_n(q, 1) + LP_{n-1}(q, 1) - L_{n-q}(q, 1)) & -(LP_n(q, 1) - L_{n-q+1}(q, 1)) \\ LP_n(q, 1) & -(LP_{n-1}(q, 1) + LP_{n-2}(q, 1) - L_{n-q-1}(q, 1)) & -(LP_{n-1}(q, 1) - L_{n-q}(q, 1)) \\ \\ L_{2n-q}(q, 1) & \cdots & L_{n+q-1}(q, 1) & L_{n+q}(q, 1) & -(2LP_{n+q+1}(q, 1) + LP_{n+q}(q, 1)) \\ L_{2n-q-1}(q, 1) & \cdots & L_{n+q-2}(q, 1) & L_{n+q-1}(q, 1) & -(2LP_{n+q}(q, 1) + LP_{n+q-1}(q, 1)) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ L_{n-q+2}(q, 1) & \cdots & L_{q+1}(q, 1) & L_{q+2}(q, 1) & -(2LP_n(q, 1) + LP_{n-1}(q, 1)) \\ L_{n-q+1}(q, 1) & \cdots & L_q(q, 1) & L_{q+1}(q, 1) & -(2LP_{n-1}(q, 1) + LP_{n-2}(q, 1)) \\ \\ -LP_{n+q+1}(q, 1) \\ -LP_{n+q}(q, 1) \\ \vdots \\ -LP_n(q, 1) \\ -LP_{n-1}(q, 1) \end{bmatrix}.$$

For $q \geq 4$ and $m = 1$, $\det(M_q(m))^n = (-1)^{n(q+1)}$.

Theorem 2.2: For $q \geq 4, t \geq 1$, and $n \geq q + 3$ we have

- (i) $(M_q(1))^n(M_q(1))^t = ((M_q(1)))^{n+t}$, and
- (ii) $(M_q(1))^n(M_q(1))^t = (M_q(1))^t(M_q(1))^n$.

Proof: The proof is similar to that for Theorem 2.1 and so is omitted.

3. Blom's Key Scheme Using the (q, m) –Lucas-Pell Sequences

In this section, the (q, m) –Lucas-Pell sequences are used to implement Blom's key scheme and the security is examined. The scheme has a trusted party (Trent) and a group of users. First, Trent chooses $(M_q(m))^i$ where $q \geq 3$ and $m \geq 1, i \in \mathbb{N}$ and p is a prime number. For new users who want to join the group (Alice and Bob), Trent chooses the public identifiers

$$U_{Alice} \equiv M_q(m)^{n_1} \pmod{p}, n_1 \geq q + 3,$$

and

$$U_{Bob} \equiv M_q(m)^{n_2} \pmod{p}, n_2 \geq q + 3.$$

He then calculates their private keys $g_{Alice} = M_q(m) \times M_q(m)^{n_1} \pmod{p}$ and $g_{Bob} = M_q(m) \times M_q(m)^{n_2} \pmod{p}$. These are used to compute shared keys with other group members. To communicate with each other, Alice and Bob do the following. Alice uses U_{Bob} and her private key g_{Alice} to obtain the shared key $K_{Alice \setminus Bob} \equiv U_{Bob} \times g_{Alice} \pmod{q}$. Bob uses U_{Alice} and his private key g_{Bob} and gets the same result. The algorithm steps are given below and illustrated in Fig. 1.

Algorithm 1

There is a trusted party (Trent) and a group of users.

1. Trent chooses $(M_q(m))^i$ where $q \geq 3$ and $m \geq 1, i \in \mathbb{N}$ and p is a prime number.
2. For new users (Alice and Bob), that want to join the group, Trent chooses the public identifiers

$$U_{Alice} \equiv M_q(m)^{n_1} \pmod{p}, n_1 \geq q + 3,$$

and

$$U_{Bob} \equiv M_q(m)^{n_2} \pmod{p}, n_2 \geq q + 3.$$

3. He then calculates their private keys

$$\begin{aligned} g_{Alice} &= M_q(m) \times M_q(m)^{n_1} \pmod{p} \text{ and } g_{Bob} \\ &= M_q(m) \times M_q(m)^{n_2} \pmod{p}. \end{aligned}$$

These are used to compute shared keys with other group members.

4. To communicate with each other, Alice and Bob do the following. Alice uses U_{Bob} and her private key g_{Alice} to obtain the shared key $K_{Alice \setminus Bob} \equiv U_{Bob} \times g_{Alice} \pmod{q}$. Bob uses U_{Alice} and his private key g_{Bob} and gets the same result. By Theorem 2.2, we have

$$\begin{aligned} K_{Alice \setminus Bob} &\equiv U_{Bob} \times g_{Alice} = M_q(m)^{n_2} \times (M_q(m))^i \times (M_q(m))^{n_1} \\ &= (M_q(m))^{n_2+n_1+i} \equiv K_{Bob \setminus Alice} \pmod{p}. \end{aligned}$$

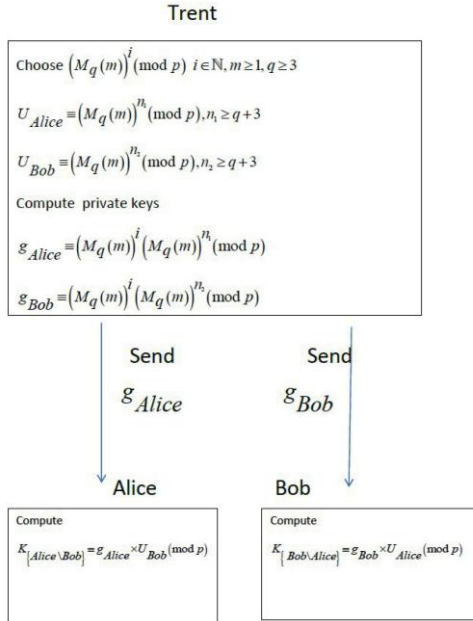


Figure 1
Algorithm 1

Example 3.1: Trent chooses $M_3(1) \pmod{5}$. He then chooses public identifiers for new users Alice and Bob $U_{Alice} \equiv M_3(1)^6 \pmod{5}$ and $U_{Bob} \equiv M_3(1)^7 \pmod{5}$

$$U_{Alice} = M_3(1)^6 = \begin{bmatrix} 300 & -172 & -121 & 3 & -296 & -123 \\ 123 & -69 & -49 & 2 & -120 & -50 \\ 50 & -27 & -19 & 1 & -48 & -20 \\ 20 & -10 & -7 & 1 & -19 & -8 \\ 8 & -4 & -2 & 1 & -7 & -3 \\ 3 & -1 & -1 & 1 & -2 & -1 \end{bmatrix} \equiv \begin{bmatrix} 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \\ 3 & 4 & 4 & 1 & 3 & 4 \end{bmatrix} \pmod{5},$$

and

$$U_{Bob} \equiv M_3(1)^7 = \begin{bmatrix} 728 & -421 & -297 & 4 & -723 & -300 \\ 300 & -172 & -121 & 3 & -296 & -123 \\ 123 & -69 & -49 & 2 & -120 & -50 \\ 50 & -27 & -19 & 1 & -48 & -20 \\ 20 & -10 & -7 & 1 & -19 & -8 \\ 8 & -4 & -2 & 1 & -7 & -3 \end{bmatrix} \equiv \begin{bmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} \pmod{5}.$$

Trent then computes their private keys

$$g_{Alice} = M_3(1) \times M_3(1)^6 = \begin{bmatrix} 3 & -1 & -1 & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \\ 3 & 4 & 4 & 1 & 3 & 4 \end{bmatrix} \equiv \begin{bmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} \pmod{5},$$

and

$$g_{Bob} = M_3(1) \times M_3(1)^7 = \begin{bmatrix} 3 & -1 & -1 & 1 & -2 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} \equiv \begin{bmatrix} 3 & 0 & 1 & 0 & 4 & 2 \\ 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 4 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 4 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \end{bmatrix} \pmod{5}.$$

To communicate with each other, Alice and Bob do the following. Alice uses U_{Bob} and her private key g_{Alice} to obtain

$$K_{Alice \setminus Bob} \equiv U_{Bob} \times g_{Alice} = M_3(1)^7 \times M_3(1)^7 =$$

$$\begin{bmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} \times \begin{bmatrix} 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \end{bmatrix} \equiv \begin{bmatrix} 3 & 4 & 3 & 1 & 2 & 2 \\ 3 & 4 & 2 & 1 & 3 & 3 \\ 2 & 2 & 4 & 4 & 4 & 2 \\ 3 & 3 & 0 & 4 & 1 & 0 \\ 0 & 3 & 3 & 0 & 4 & 1 \\ 4 & 3 & 2 & 2 & 1 & 2 \end{bmatrix} \pmod{5},$$

and similarly, Bob gets

$$K_{Bob \setminus Alice} \equiv U_{Alice} \times g_{Bob} = M_3(1)^6 \times M_3(1)^8 =$$

$$\begin{bmatrix} 0 & 3 & 4 & 3 & 1 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 1 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \\ 3 & 1 & 3 & 1 & 3 & 2 \\ 3 & 4 & 4 & 1 & 3 & 4 \end{bmatrix} \times \begin{bmatrix} 3 & 0 & 1 & 0 & 4 & 2 \\ 3 & 4 & 3 & 4 & 2 & 0 \\ 0 & 3 & 4 & 3 & 4 & 2 \\ 3 & 1 & 1 & 2 & 0 & 0 \\ 0 & 3 & 4 & 1 & 2 & 0 \\ 0 & 0 & 3 & 1 & 1 & 2 \end{bmatrix} \equiv \begin{bmatrix} 3 & 4 & 3 & 1 & 2 & 2 \\ 3 & 4 & 2 & 1 & 3 & 3 \\ 2 & 2 & 4 & 4 & 4 & 2 \\ 3 & 3 & 0 & 4 & 1 & 0 \\ 0 & 3 & 3 & 0 & 4 & 1 \\ 4 & 3 & 2 & 2 & 1 & 2 \end{bmatrix} \pmod{5}.$$

3.1 Security Analysis

Blom's scheme is a symmetric key exchange protocol in which a trusted third party creates a secret key and provides public identifiers. This allows new users to calculate shared keys for communication with other group members. This algorithm is symmetric and resistant to quantum attacks. Since the size of the keys in the proposed algorithm is much larger than the size in the original algorithm, it is more secure against these attacks. Consider the following attacks.

1. **Brute force attack:** In a brute force attack [14], all possible cases are tested. In the proposed algorithm, the keys are constructed using $(M_q(m))^n$. Since these matrices are invertible, we must check the order of the group $GL_{q+3}(\mathbb{F}_p)$. For p prime, this group is the set of all invertible matrices of size $m \times m$ over $\mathbb{F}_p$ [4], so it has order

$$|GL_m(\mathbb{F}_p)| = (p^m - p^{m-1})(p^m - p^{m-2}) \dots (p^m - 1).$$

Since $(M_q(m))^n$ is an invertible matrix of size $q + 3 \times q + 3$, we have

$$|GL_{q+3}(\mathbb{F}_p)| = (p^{q+3} - p^{q+2})(p^{q+3} - p^{q+1}) \dots (p^{q+3} - 1).$$

As p and q increase, $|GL_{q+3}(\mathbb{F}_p)| \rightarrow \infty$. Therefore, the key space is large and greater than that of the original algorithm.

2. **Side channel attack:** In a side channel attack, the cryptographic system is broken using information that is accidentally leaked or maliciously obtained. In the proposed algorithm, the key is a very large matrix and m is a very large prime number. Thus, this attack would be very time consuming and unlikely to provide complete information, so it is not feasible.
3. **Timing attack:** In a timing attack, information about the cryptographic system is obtained by analyzing the algorithm execution time. Because the

keys in the proposed algorithm are in the form of a matrix and multiplication is employed, accessing the system and obtaining the required information will be very time-consuming and prone to errors, so this is not a useful attack.

4. **Chosen ciphertext attack:** A chosen ciphertext attack is where the attacker gathers information by obtaining decryptions of ciphertext. As with the other attacks, this will be very time consuming and significant data is required, thus it is infeasible.
5. **Fault attack:** In this approach, the attacker intentionally introduces faults or errors into the cryptographic system to exploit vulnerabilities and extract information. Considering that the keys are very large, the calculations will likely be done on very powerful computer systems. Thus, accessing and damaging these systems is not viable.

The computational complexity of the proposed algorithm is higher than Blom's original scheme because matrices are used rather than vectors, but the keys are larger. This increases the difficulty of attacks, so there is a tradeoff between complexity and security.

4. Conclusion

New sequences were introduced using the Lucas and Pell sequences. The (q, m) –Lucas-Pell sequence matrices were constructed and some interesting structural results were obtained. These were used in Blom's key scheme and the security was studied. Since the matrices are commutative and invertible, they are suitable for key generation and the security is high due to their very large size. Other sequences such as Mersenne, balanced, and Fibonacci sequences and their generalizations [9, 10, 11, 13] can be used to create algorithms for Blom's key scheme.

5. Conflicts of Interest

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

References

- [1] S. V. Belim and S. Yu. Belim, "Modification of preliminary Blom's key distribution scheme taking into account simplex channels," *Autom. Control Comput. Sci.*, vol. 52, no. 8, pp. 1134–1137 (2018).
- [2] Ö. Deveci and A. G. Shannon, "The quaternion-Pell sequence," *Commun. Algebra*, vol. 46, no. 12, pp. 5403–5409 (2018).
- [3] Y. Doğru, "New presentations of real numbers with Lucas numbers," *J. BAUN Inst. Sci. Technol.*, vol. 25, no. 1, pp. 31–36 (2023).

- [4] P. A. Grillet, *Abstract Algebra*, 2nd ed., Graduate Texts in Mathematics, vol. 242. Berlin, Germany: Springer (2007).
- [5] S. Halici and S. Oz, "On Gaussian Pell polynomials and their some properties," *Palest. J. Math.*, vol. 7, no. 1, pp. 251–256 (2018).
- [6] M. Hashemi and E. Mehraban, "On the generalized order 2-Pell sequence of some classes of groups," *Commun. Algebra*, vol. 46, no. 9, pp. 4104–4119 (2018).
- [7] M. Hashemi and E. Mehraban, "The generalized order k -Pell sequences in some special groups of nilpotency class 2," *Commun. Algebra*, vol. 50, no. 4, pp. 1768–1784 (2022).
- [8] E. Kiliç, "The generalized Pell (p, i) -numbers and their Binet formulas, combinatorial representations, sums," *Chaos Solitons Fractals*, vol. 40, no. 4, pp. 2047–2063 (2009).
- [9] E. Mehraban and M. Hashemi, "Fibonacci length and the generalized order k -Pell sequences of the 2-generator p -groups of nilpotency class 2," *J. Algebra Appl.*, vol. 22, no. 3, Article ID 2350061 (2023).
- [10] E. Mehraban and M. Hashemi, "Coding theory on the generalized balancing sequence," *Notes Number Theory Discrete Math.*, vol. 29, no. 3, pp. 503–524 (2023).
- [11] E. Mehraban, Ö. Deveci, and E. Hincal, "The generalized order (k, t) -Mersenne sequences in groups," *Notes Number Theory Discrete Math.*, vol. 30, no. 2, pp. 271–282 (2024).
- [12] R. Blom, "Non-public key distribution," in *Advances in Cryptology: Proceedings of Crypto 82*, D. Chaum, R. L. Rivest, and A. T. Sherman, Eds. Boston, MA, USA: Springer, pp. 231–236 (198).
- [13] Y. Soykan, "On generalized p -Mersenne numbers," *Earthline J. Math. Sci.*, vol. 8, pp. 83–120 (2022).
- [14] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7th ed. Harlow, UK: Pearson (2017).
- [15] M. N. Udin, F. A. M. Amin, A. A. Malek, N. A. Zulkifili, N. A. Ghazali, and S. A. M. Ridzuwan, "Implementation of Blom's key predistrib-

- tion scheme by using elliptic curve cryptography," *Malays. J. Comput.*, vol. 6, no. 2, pp. 812–822 (2021).
- [16] M. L. Yang, A. A. Anbuky, and W. Liu, "Security of the multiple-key Blom's key agreement scheme for sensor networks," in *ICT Systems Security and Privacy Protection: SEC 2014*, N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. Abou El Kalam, and T. Sans, Eds., IFIP Adv. Inf. Commun. Technol., vol. 428, Berlin, Germany: Springer, pp. 66–79 (2014).
- [17] Y. Yazlik, C. Köme, and V. Madhusudanan, "A new generalization of Fibonacci and Lucas p-numbers," *J. Comput. Anal. Appl.*, vol. 25, no. 4, pp. 657–669 (2018).
- [18] N. Yılmaz, E. K. Çetinalp, Ö. Deveci, and E. S. Oztas, "The quaternion-type cyclic-Pell sequences in finite groups," *Bull. Int. Math. Virtual Inst.*, vol. 13, no. 1, pp. 169–178 (2023).

Received April, 2025