Computers, Materials & Continua
DOI:10.32604/cmc.2022.023685
Article

Tech Science Press

Text Encryption Using Pell Sequence and Elliptic Curves with Provable Security

Sumaira Azhar[1], Naveed Ahmed Azam[2,*] and Umar Hayat[1]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, 45320, Pakistan
[2]Department of Applied Mathematics and Physics, Graduate School of Informatics, Kyoto University, Kyoto, 606-8501, Japan
*Corresponding Author: Naveed Ahmed Azam. Email: azam@amp.i.kyoto-u.ac.jp
Received: 17 September 2021; Accepted: 11 November 2021

Abstract: The demand for data security schemes has increased with the significant advancement in the field of computation and communication networks. We propose a novel three-step text encryption scheme that has provable security against computation attacks such as key attack and statistical attack. The proposed scheme is based on the Pell sequence and elliptic curves, where at the first step the plain text is diffused to get a meaningless plain text by applying a cyclic shift on the symbol set. In the second step, we hide the elements of the diffused plain text from the attackers. For this purpose, we use the Pell sequence, a weight function, and a binary sequence to encode each element of the diffused plain text into real numbers. The encoded diffused plain text is then confused by generating permutations over elliptic curves in the third step. We show that the proposed scheme has provable security against key sensitivity attack and statistical attacks. Furthermore, the proposed scheme is secure against key spacing attack, ciphertext only attack, and known-plaintext attack. Compared to some of the existing text encryption schemes, the proposed scheme is highly secure against modern cryptanalysis.

Keywords: Text encryption; pell numbers; elliptic curves; key sensitivity; statistical cryptanalysis

1 Introduction

There is a high demand for data security schemes due to the recent advancement in the fields of computation and communication technologies. Cryptography and steganography are the two main branches of data security schemes. Cryptography is the study of data security schemes where secret data is transformed into an unreadable data [1]. Steganography is the study of data security schemes where secret data is embedded into host data so that the attackers cannot detect the existence of secret data [2].

Different data security schemes have been proposed based on different mathematical structures such as elliptic curves [3–9], algebraic structures [10–15], chaotic maps [16–21] and fuzzy set theory

[22,23]. Security and privacy of the text messages are major concerns of the users while communicating on popular messaging platforms such as WhatsApp and Signal. So, the security of the text messages gained great attention now a days. We briefly review some of the recent text encryption schemes. Abdullah et al. [23] proposed a cryptosystem based on fuzzy logic where triangular fuzzy numbers are used to represent plain text and ciphertext. Gupta et al. [24] proposed a data security algorithm based on logical and shifting operations. Pattanayak et al. [25] used linear congruences and extended Euclidean algorithm to design a text encryption scheme. By utilizing 8-bit code values of alphabets, Agrawal et al. [26] proposed an efficient algorithm for text encryption. Ghrare et al. [27] designed a hidden encrypted symmetric key algorithm by hiding the secret key inside the ciphertext. Linear recurrences such as generalized Fibonacci numbers, Pell numbers and Pell-Lucas numbers have many applications in the field of mathematics and computer science [28–30]. The schemes in [31–33] used linear recurrences for cryptography purpose. Luma et al. [31] explored a relationship between Fibonacci and Lucas sequence and used it for encryption and decryption purpose. Overmars et al. [32] proposed an efficient method to compute the golden ratio to avoid cryptographic breaches. Agarwal et al. [33] proposed a data encryption scheme based on Fibonacci numbers. Recently, DNA sequences are also used to generate secret keys for data security [34–36]. Clelland et al. [34] combined a DNA based technique and the microdot to send messages secretly. Abbasy et al. [36] employed useful features of DNA sequences for data hiding. Chaotic maps are used to develop new security schemes due to their high sensitivity to the initial condition [37–42]. Murillo-Escobar et al. [37] proposed a new text encryption scheme based on a logistic map. Similarly, elliptic curves (ECs) received great attention in the field of cryptography for image encryption [43–47], text encryption [48–53] and signcryption [54–56] due to comparable security against modern cryptanalysis with low key size. Sunneetha et al. [48] proposed a secure algorithm using elliptic curves and algebraic operations to transmit messages. Naji et al. [49] proposed a novel text encryption scheme by representing characters of the plain text with the affine points on an EC. Agrawal et al. [50] designed a text encryption method using ECC and Hill cipher with better security and complexity. Keerthi et al. [51] proposed a novel text encryption scheme where the hexadecimal form of the ASCII values of plain text are mapped to affine points of an ECs. Kumar et al. [52] used paired ASCII values corresponding to the plain text as an input for the elliptic curve. Singh and Singh developed an algorithm that can be used for encryption and decryption of any size of text message with given ASCII values. Ullah et al. [54] provided a critical review of hyper elliptic curves based signcryption algorithms. A hyper elliptic curve based signcryption scheme more suitable for emerging resource constraints environment is proposed by Ullah et al. [56].

Most of the text encryption schemes available in the literature such as the schemes presented in [23–27,33,34,36,37,48–51,53] are not secure against well know attacks including key spacing, key sensitivity, statistical attack, ciphertext only attack and known-plaintext attack. The aim of this paper is to propose a novel text encryption scheme that has high security against modern cryptanalysis including key spacing, key sensitivity, statistical attack, ciphertext only attack and known-plaintext attack as compared to the existing text encryption schemes [23–27,33,34,36,37,48–51,53]. The proposed scheme is based on the Pell sequence and elliptic curves and has three main steps, where we first diffuse the plain text. Then an encoding procedure is applied to the diffused plain text based on the Pell sequence in step 2. Finally, the encoded diffused plain text is confusedin step 3 based on ECs. The rest of the paper

is organized as follows. Section 2 contains some preliminaries. We discuss a novel text encryption scheme in Section 3. Security analysis and a detailed comparison of the proposed scheme with the existing text encryption schemes [23–27,33,34,36,37,48–51,53] is discussed in Section 4. A conclusion is drawn in Section 5.

2 Preliminaries

2.1 Pell Sequence

For initial values $P_0 = 0$ and $P_1 = 1$, the n-th term P_n of the Pell sequence is defined with the recurrence relation

$$P_n = 2P_{n-1} + P_{n-2}. \tag{1}$$

The first six terms of the Pell sequence are 0, 1, 2, 5, 12, and 29. By [30] it is known that for $i \to \infty$ it holds that $\frac{P_i}{P_{i-1}} \to 1 + \sqrt{2}$.

2.2 Elliptic Curves (EC)

For a finite prime field $\mathbb{F}_p$ with characteristic other than 2 and 3, prime p and two integers $a,\ b \in [0,\ p-1]$ such that $4a^3 + 27b^2 \neq 0 \pmod p$, the short Weiestrass form elliptic curve $E_{p,a,b}$ over the field $\mathbb{F}_p$ is the set

$$\{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p | (y^2 = x^3 + ax + b) (\text{mod } p)\} \cup \{\delta\}, \tag{2}$$

where δ is the identity element of the EC. We call the integers $p,\ a$ and b the parameters of the EC $E_{p,a,b}$.

By [57], when $a = 0$ and $p \equiv 2 \pmod 3$, the EC $E_{p,a,b}$ has exactly $p + 1$ points with no repetition in their y-coordinates. Azam et al. [4] defined three orderings on an EC $E_{p,a,b}$ that have good cryptographic properties. These orderings are natural ordering N, diffusion ordering D, and modulo diffusion ordering M such for any two points $(x,\ y)$ and $(x',\ y')$ on an EC $E_{p,0,b}$ it holds that

$$(x, y)\ \text{N}\ (x', y') \Leftrightarrow \text{“}x < x'\text{”} \text{ or “}x = x' \text{ and } y < y'\text{”}; \tag{3}$$

$$(x, y)\ \text{D}\ (x', y') \Leftrightarrow \text{“}x + y < x' + y'\text{”} \text{ or “}x + y = x' + y' \text{ and } x < x'\text{”}; \tag{4}$$

$$(x, y)\ \text{M}\ (x', y') \Leftrightarrow \text{“}x + y < x' + y' (\text{mod } p)\text{”} \text{ or “}x + y = x' + y' (\text{mod } p) \text{ and } x < x'\text{”}; \tag{5}$$

The key features of these orderings are: (i) they diffuse the y-coordinates of the ordered EC; and (ii) the ordered ECs generated by these orderings are highly uncorrelated. Furthermore, it can be observed from Fig. 1 that the three orderings are non-equivalent and are capable of generating randomness. Due to these properties, Azam et al. [4,5] showed that these orderings are cryptographically suitable for generating a large number of secure permutations over ECs.

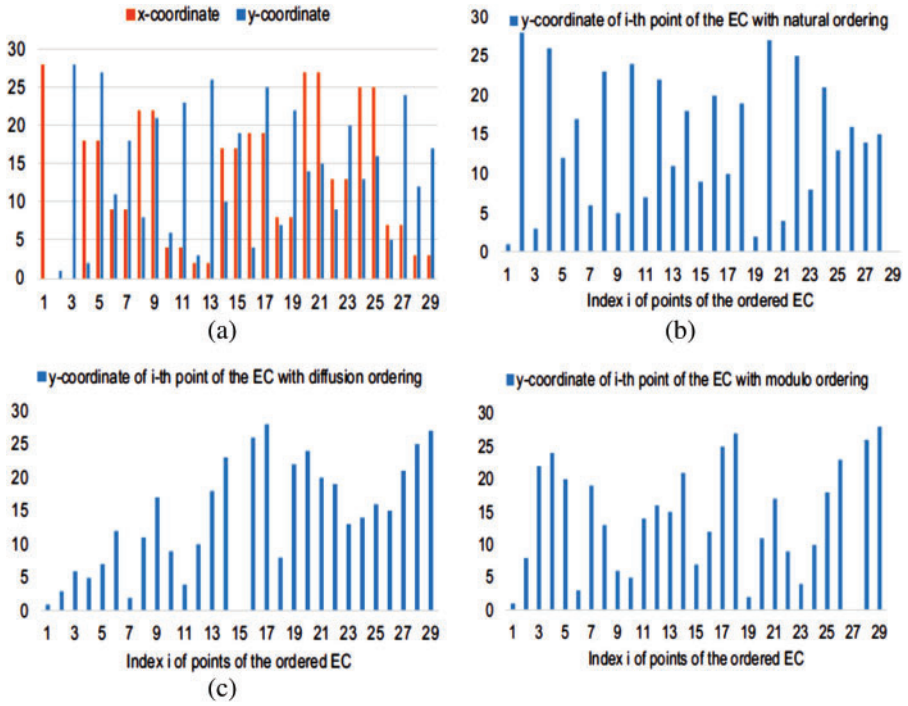

Figure 1: EC $E_{29,0,1}$ and the effect of the natural, diffusion and modulo ordering on the EC $E_{29,0,1}$: (a) Points of the EC $E_{29,0,1}$ are shown w.r.t. non-decreasing x-coordinate from left to right; (b) y-coordinates of the points of the ordered EC $E_{29,0,1}$ with natural ordering; (c) y-coordinates of the points of the ordered EC $E_{29,0,1}$ with diffusion ordering; (d) y-coordinates of the points of the ordered EC $E_{29,0,1}$ with modulo ordering

3 The Proposed Scheme

For an encryption scheme, it is essential to diffuse and confuse the plain text up to a certain level [2]. Therefore, our scheme consists of three main steps where we first diffuse the plain text followed by an encoding procedure and then create confusion in the encoded diffused plain text. The diffusion step is performed by permuting the symbol set of the plain text. We use a restricted Pell sequence, a weight function, and a binary sequence to encode each element and its position in the diffused plain text with real numbers. Due to the sensitivity of the ECs over its parameters, we generate permutations over ECs to create confusion in the encoded diffused plain text. We discuss these three steps in detail below.

Let S be a finite symbol set of size m, and for $i \in [0, m-1]$, let $S(i)$ denote the i-th element of S. Suppose that the sender wants to send the plain text $T = T(1) \cdots T(i) \cdots T(n)$ of length n which is a sequence over S where $T(i), i \in [1, n]$ denotes the i-th element of T and $T(i) \in S$. In this scheme, we encode plain text to real numbers in the interval $[-1, 1]$ with at most $\beta \geq 14$ digits after the decimal.

3.1 Encryption Procedure

Step 1. Diffuse plain text: We select an integer $k \in [0, m-1]$ and permute the entries of S by using the permutation $\psi_k : S \to S$ defined as

$$\psi_k(S(i)) = S((i+k)(\text{mod } m)), \tag{6}$$

i.e., ψ_k maps the i-th entry of S on its $(i+k) \pmod m$-th entry. Now generate a diffused plain text $T' = T'(1)\cdots T'(i)\cdots T'(n)$ by using the permutation ψ_k such that the i-th element $T'(i) = \psi_k(T(i)$, $i \in [1, n]$. The diffusion step is similar to the Caesar cipher [58].

Step 2. Encode diffused plain text: To encode the elements of the diffused plain text T', we generate a restricted Pell sequence, a weight function, and a binary sequence as follows.

Select two positive integers h and h' such that $h < h'$ and $h' - h + 1 \leq \beta$, and generate the restricted Pell sequence $Q_{h,h'} = q_1 \cdots q_i \cdots q_m$, if it exists, such that for each integer $i \in [1, m]$ the following hold:

- $q_i = \log(P_i/P_i - 1)$ and q_i has exactly $h' - h + 1$ digits from h-th digit to h'-th digit after the decimal, where P_i is the i-th entry of the Pell sequence, and
- all entries of $Q_{h,h'}$ are distinct, i.e., for any two distinct $i, j \in [1,\ m]$, it holds that $q_i \neq q_j$. We apply this condition so that each symbol in the diffused plain text can be encoded uniquely.

Observe that the entries of the restricted Pell sequence $Q_{h,h'}$ are in the closed interval $[0,\ 1]$ since $P_i/P_{i-1} \to 1 + (2)^{1/2}$ as $i \to \infty$ by [30]. We added the constraint $h' - h + 1 \leq \beta$ to generate a restricted Pell sequence to control the length of the ciphertext and increase the key size, since for a fixed integer τ, there exists different pairs h, h' such that $h' - h + 1 = \tau$, and hence different restricted Pell sequences.

Generate a *weight function* $w : \{1, 2, \cdots, n\} \to [-1,\ 1]$ which is an injection, i.e., for any two $i, j \in \{1, 2, \cdots, n\}$ such that $i \neq j$, it holds that $w(i) \neq w(j)$. The aim of this weight function is to uniquely encode the position of each element of T'.

Generate a *binary sequence* $\alpha = \alpha_1 \cdots \alpha_i \cdots \alpha_n$. Based on the i-th entry α_i of α, decide if we use weight $w(i)$ with q_j or $q_j - 1, j \in [1, n]$ during the encoding procedure.

Now, generate an encoded diffused plain text $(C, D) = (c_1, d_1)\cdots(c_i, d_i)\cdots(c_n, d_n)$ such that the i-th element $T'(i)$ of T' is encoded (c_i, d_i) as with

$$(c_i, d_i) = (q_{(j+k)(\text{mod } m)} + \alpha_i w(i),\ 1 - q_{(j+k)(\text{mod } m)} + (1-\alpha_i)w(i)), \tag{7}$$

where $T(i) = S(j)$, for some $j \in [1, m]$ and $T'(i) = \psi_k(S(j)) = S((j+k) \pmod m)$.

Step 3. Confuse encoded plain text: In this step, we create confusion in the encoded plain text (C, D). For this purpose, we generate two bijections $\sigma : C \to C$ and $\sigma' : D \to D$ by using ordered subsets of two ECs. These ordered subsets are such that each integer in $[1, n]$ appears exactly once as y-coordinates of the points. The existence of such subsets is ensured by considering the ECs with $a = 0$ and $p \equiv 2 \pmod 3$. Finally, the i-th entries of C and D are mapped on some entries of C and D whose indices are determined by the y-coordinates of the i-th points in the ordered sets. More precisely, select two primes $p,\ p' \geq n$ with $p \equiv 2 \pmod 3$ and $p' \equiv 2 \pmod 3$, two integers $b \in [1, p-1]$ and $b' \in [1, p'-1]$, and two orderings $\prec$ and $\prec'$. Compute the ordered subsets $\{(a_i, b_i) | b_i \in [1, n]$ and $(a_i, b_i) \in E_{p,0,b}\}$ and $\{(a'_i, b'_i) | b'_i \in [1, n]$ and $(a'_i, b'_i) \in E_{p',0,b'}\}$ ordered w.r.t. the orderings $\prec$ and $\prec'$, where for each $i \in [1, n-1]$ it holds that $(a_i, b_i) \prec (a_{i+1}, b_{i+1})$ and $(a'_i, b'_i) \prec' (a'_{i+1}, b'_{i+1})$, respectively. From these ordered subsets, get the sequences $H = b_1 b_2 \cdots b_n$ and $H' = b'_1 b'_2 \cdots b'_n$. Now, generate a confused encoded

plain text $(\sigma(C), \sigma'(D))(\sigma(c_1), \sigma'(d_1)) \cdots (\sigma(c_i), \sigma'(d_i)) \cdots (\sigma(c_n), \sigma'(d_n))$ by using the permutations $\sigma : C \to C$ and $\sigma' : D \to D$ such that $\sigma(c_i) = c_{b_i}$ and $\sigma'(d_i) = d_{b'_i}$.

3.2 Ciphertext

Transmit the confused sequence $\sigma(C)$ as a ciphertext of the plain text T.

3.3 Secret Keys

The integers h, h' and k, the weight function w and the encoded sequence $\sigma'(D)$ are the secret keys of our encryption scheme. The integers h, h' and k are used to get the representation of symbols in S, the weight function w is used to get the index of the symbols in the plain text, and the sequence $\sigma'(D)$ is used to get w.

Note that for a given β, the proposed scheme can encrypt a plain text over a symbol set S with size at most $|Q_{h=1,\, h'=\beta}|$, i.e., for the proposed scheme it holds that $m \leq |Q_{h=1,\, h'=\beta}|$. Furthermore, the proposed scheme can encrypt a plain text T of any arbitrary size, since it encodes each symbol of T individually.

3.4 Decryption Procedure

Assume that the channel between sender and receiver is noiseless, and therefore the receiver receives the ciphertext $G = \sigma(c_1)\sigma(c_2) \cdots \sigma(c_n)$. Let g be the l-th element of G. We find the position of g in the plain text by using the keys $\sigma'(D) = \sigma'(d_1)\sigma'(d_2) \cdots \sigma'(d_n)$ and weight function as follows. Compute a real $d \in \sigma'(D)$ such that

$$g + d = r + 1, \tag{8}$$

for some $r = w(i) \in [-1, 1]$ with $i \in [1, n]$. Observe that for each g such a real d always exists by Eq. (7). The integer i is the position of the element of the plain text corresponding to the element g of the ciphertext. By using the secret key h, compute the restricted Pell sequence $Q_{h,h'}$ and compute the inverse $\psi_k^{-1} : S \to S$ defined as

$$(S(i)) = S((i - k)(\text{mod } m)), \tag{9}$$

of the permutation by using the secret key k. To get the plain text $T(i)$ at the i-th position of the plain text T, find the real $q_t \in Q_{h,h'}$ such that $g = q_t$ *or* $d = 1 - q_t$ for some index t. Find the index t by using Tab. 1, and finally get the i-th plain text $T(i)$ as $T(i) = \psi_k^{-1}(S(t))$ corresponding to the l-th element g of G.

By repeating the above procedure for each $g \in G$, we get the plain text T. The proposed encryption and decryption scheme is illustrated in Fig. 2.

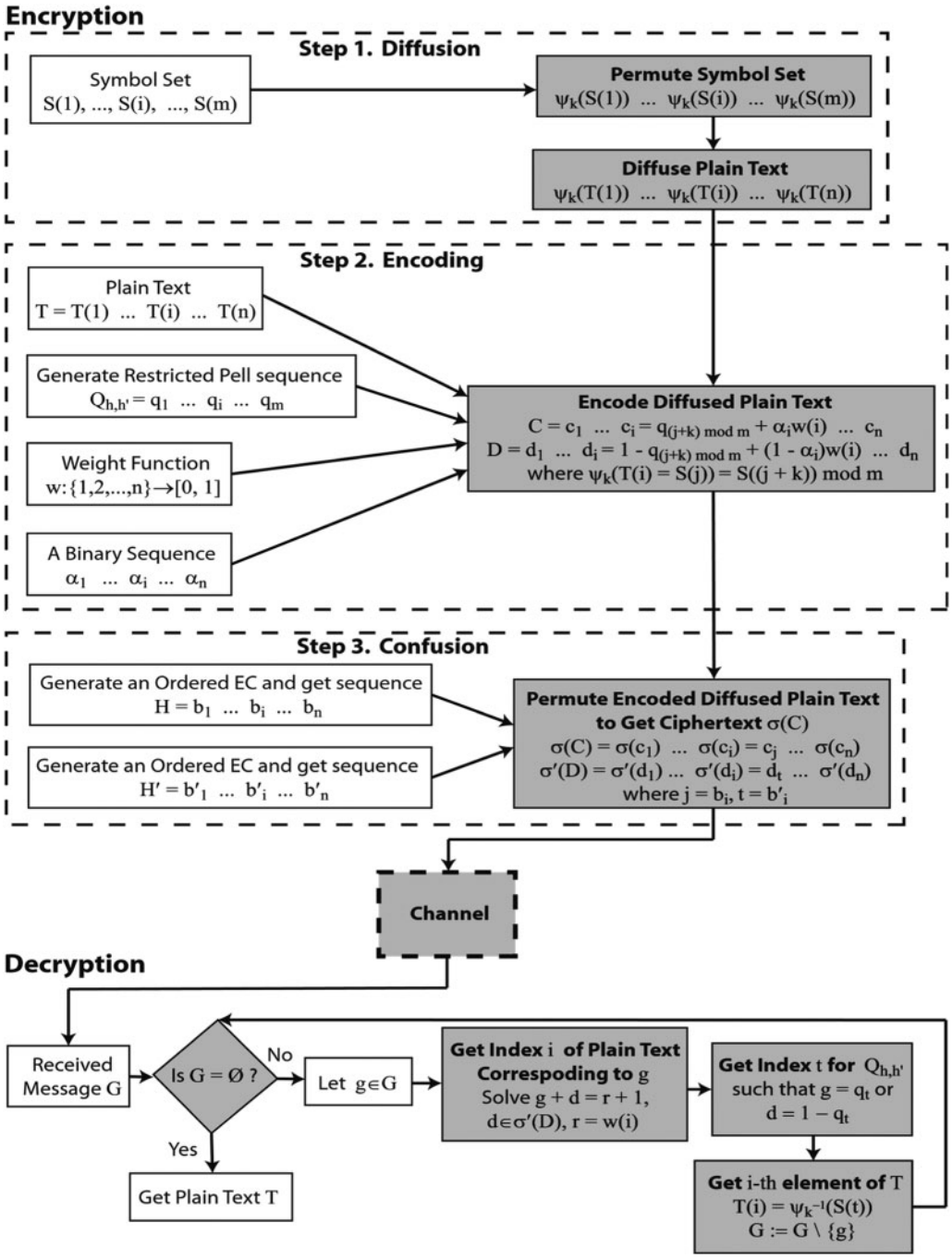

Figure 2: Flowchart of the proposed encryption and decryption scheme

We demonstrate our proposed encryption and decryption procedures in detail in Example 1.

3.5 Example 1

3.5.1 Encryption

Let the ordered symbol set S be the set of the capital English alphabet including blank-space and full-stop. This set is listed in the fourth column of Tab. 1. Let $\beta = 14$, and for $h = 18$ and $h' = 22$, the entries q_i of the restricted Pell sequence $Q_{h,h'}$ are listed in the second column of Tab. 1, while the third column of Tab. 1 contains $1 - q_i$. Select integer $k = 6$ to generate a permutation $\psi_{k=6}$ on the symbol set S. The entries of $\psi_{k=6}$ are listed in the fifth column of Tab. 1.

Table 1: Entries $S(i)$, $\psi_{k=6}(S(i))$, and q_i of an ordered symbol set S, the permuted symbol set $\psi_{k=6}(S)$, and the restricted pell sequence $Q_h = 18$, $h' = 22$, respectively

Index i	q_i	$1 - q_i$	$S(i)$	$\psi_{k=6}(S(i))$
1	0.52137	0.47863	A	W
2	0.95725	0.04275	B	X
3	0.29362	0.70638	C	Y
4	0.96103	0.03896	D	Z
5	0.33794	0.66206	E	Space
6	0.77007	0.22993	F	.
7	0.30634	0.69366	G	A
8	0.06816	0.93184	H	B
9	0.48980	0.51020	I	C
10	0.73249	0.26751	J	D
11	0.68854	0.31146	K	E
12	0.91754	0.08246	L	F
13	0.81868	0.18132	M	G
14	0.83642	0.16358	N	H
15	0.81864	0.18136	O	I
16	0.79073	0.20927	P	J
17	0.39322	0.60678	Q	K
18	0.38890	0.61110	R	L
19	0.92887	0.07113	S	M
20	0.69338	0.30662	T	N
21	0.56639	0.43361	U	O
22	0.56379	0.43621	V	P
23	0.70637	0.29363	W	Q
24	0.85348	0.14652	X	R
25	0.82824	0.17176	Y	S
26	0.83257	0.16743	Z	T
27	0.83183	0.16817	Space	U
28	0.83196	0.16804	.	V

Suppose the sender wants to send the plain text T = STAY SAFE with nine elements. For each integer $i \in [1, 9]$, the i-th element $T(i)$ of the plain text T, the i-th element $T'(i)$ of the diffused plain text, weight value $w(i)$, binary value α_i and i-th element (c_i, d_i) of the encoded plain text are listed in Tab. 2.

Table 2: Entries $T(i)$, $T'(i)$, $w(i)$, α_i and (c_i, d_i) of a plain text T, diffused plain text T', weight function w, binary sequence α_i, and encoded diffused plain text (C, D), respectively

Index i	$T(i)$	$T'(i)$	$w(i)$	α_i	Encoded diffused plain text(C, D)	
					c_i	d_i
1	S	Y	−0.007	1	0.28662	0.70638
2	T	Z	−0.321	0	0.96103	−0.28204
3	A	G	0.4	1	1.21868	0.18132
4	Y	C	−0.49751	0	0.48980	0.01269
5	Space	F	0.8812	1	1.79874	0.08246
6	S	Y	0.163	1	0.45662	0.70638
7	A	G	0.97350	1	1.79218	0.18132
8	F	L	0.65	0	0.38890	1.26110
9	E	K	0.2817	0	0.39322	0.88848

To permute the encoded diffused plain text, we generated the ordered ECs $E_{11,0,9}$ and $E_{11,0,4}$ using natural and diffusion orderings respectively. The sequences H and H' generated by these ordered ECs are listed in Tab. 3.

Table 3: Permutations due to the ordered ECs $E_{11,0,9}$ and $E_{11,0,4}$ with natural and diffusion ordering, respectively

Index i	1	2	3	4	5	6	7	8	9
Entries b_i of H due to $E_{11,0,9}$	3	8	1	5	6	9	2	4	7
Entries b_i' of H' due to $E_{11,0,4}$	2	1	4	3	7	9	8	5	6

The confused encoded plain text $\sigma(C)$ and $\sigma'(D)$ are listed in Tab. 4.

Table 4: Entries of $\sigma(c_i)$ and $\sigma'(d_i)$ of the confused plain text $\sigma(C)$ and $\sigma'(D)$, respectively

Index i	Ciphertext $\sigma(c_i)$	Key $\sigma(d_i)$
1	1.21868	−0.28204
2	0.38890	0.70638
3	0.28662	0.01269

(Continued)

Table 4: Continued

Index i	Ciphertext $\sigma(c_i)$	Key $\sigma(d_i)$
4	1.79874	0.18132
5	0.45662	0.18132
6	0.39322	0.88848
7	0.96103	1.26110
8	0.48980	0.08246
9	1.79218	0.70638

3.5.2 Decryption

We demonstrate the decryption procedure for the 5-th element $g = \sigma(c_5) = 0.45662$ of the ciphertext G. Note that $g + d = r + 1$ holds for $d = \sigma(d_2) = 0.70638$, $r = w(i) = 0.163$ with $i = 6$. This implies that g is the $(i = 6)-$th element of the plain text. The real q_t for which it holds that $g = 1 - q_t$ has index $t = 3$ in the third column $Q_{h=18,h'=22}$ of Tab. 1. We get the $(i = 6)$-th element $T(6) = \psi_k^{-1}(S(3)) = \psi_k^{-1}(Y) = S$ of the plain text T from the fourth column of Tab. 1.

4 Security Analysis and Comparison

To analyze the security of the proposed scheme, we apply some well-known security tests including key spacing analysis, key sensitivity analysis, histogram test, information entropy analysis, ciphertext only attack and known-plaintext attack. We briefly explain these tests and their results for the proposed scheme in Sections 4.1–4.5. Furthermore, we give a detailed comparison of the security of the proposed scheme and some of the existing text encryption schemes in Section 4.6.

4.1 Key Spacing Analysis

Brute-force attack is commonly used by cryptanalysts to decrypt ciphertext. Key spacing analysis is used to analyze the security of an encryption scheme against brute-force attack. For an encryption scheme, key spacing is defined to be the number of distinct secret keys that it can generate. An encryption scheme is secure if its key spacing is at least 2^{100} by [59]. The proposed scheme has five secret keys, three integers k, h, and h', a weight function w and the sequence $\sigma'(D)$, where the key $\sigma'(D)$ depends on m, h, h', k, and w, by Eq. (7). There are m choices for k and $(10^{\beta})^n$ choices for w, when the plain text is encoded to real numbers with at most $\beta \geq 14$ digits after the decimal and n is the size of the plain text. This implies that the key spacing of the proposed scheme is at least $m(10^{\beta})^n > 2^{100}$ for $n \geq 4$, $m \geq 1$ and $\beta \geq 14$. This implies that the proposed scheme satisfies key spacing analysis. In particular, when computation accuracy is 10^{-14}, $m = 5$, $\beta = 14$ and $n \geq 4$, then there are 88 choices for selecting a pair of integers h and h' such that $h' - h + 1 \leq \beta$ and there exists a restricted Pell sequence. This implies that the key spacing of the proposed scheme in this case is at least $5 \cdot 88 \cdot (10^{14})^4 > 2^{194}$.

4.2 Key Sensitivity Analysis

An encryption scheme is secure if it can generate a significantly different ciphertext for the same plaintext when the secret keys are slightly changed. In the next lemma, we show that for any plain text our scheme can generate a different ciphertext when any of the secret keys k, h, h', and w is changed.

Lemma 1. Let T be a plain text of size n over symbol set S of size m and $G = \sigma(c_1)\sigma(c_2)\ldots\sigma(c_n)$ be a ciphertext of T that is obtained by the proposed scheme using the secret keys k, h, h' and weight function w.

(i) The ciphertext G' generated by the proposed scheme by using $k' \neq k,\ k' \in [0, m-1],\ h, h'$, and w is not equal to G.
(ii) The ciphertext G' generated by the proposed scheme by using $k,\ t \neq h$ *or* $t' \neq h'$ that satisfies conditions of step 2, and w is not equal to G.
(iii) If $\alpha_i = 1,\ i \in [1, n]$, the ciphertext G' generated by the proposed scheme by using $k,\ h, h'$, and w' such that $w'(i) \neq w(i)$, for all $i \in [1, n]$, is not equal to G.

Proof. Let $G' = \sigma(c'_1)\sigma(c'_2)\ldots,\sigma(c'_n)$

(i) The integer $k' \neq k$ used at step 1 of the proposed scheme is to shift the elements of the symbol set S. Then for all $j \in [1, n]$ it holds that $S((j + k')(\text{mod } m)) \neq S((j + k)(\text{mod } m))$. This implies that $q_{(j+k')(\text{mod } m)} + \alpha_i w(i) \neq q_{(j+k)(\text{mod } m)} + \alpha_i w(i)$ for each $i \in [1, n]$ in Eq. (7), where $T(i) = S(j)$. This implies that $c'_i \neq c_i$ for each $i \in [1, n]$, and hence $G' \neq G$.
(ii) For any integer $t \neq h$ or $t'' \neq h'$ that satisfies conditions of Step 2, the restricted Pell sequence $Q'_{t,t''} = q'_1 q_2{}' \cdots q'_n \neq Q_{h,h'} = q_1 q_2 \cdots q_n$, since the length of the elements of $Q'_{t,t''}$ is different from the length of the elements of $Q_{h,h'}$. This implies that $q'_{(j+k)(\text{mod } m)} + \alpha_i w(i) \neq q_{(j+k)(\text{mod } m)} + \alpha_i w(i)$ for each $i \in [1, n]$. This implies that $c'_i \neq c_i$, and hence $\sigma(c'_i) \neq \sigma(c_i)$, $i \in [1, n]$, from which it follows that $G' \neq G$.
(iii) Since $w'(i) \neq w(i)$ and $\alpha_i = 1$ therefore $q_{(j+k)(\text{mod } m)} + \alpha_i w(i) \neq q_{(j+k)(\text{mod } m)} + \alpha_i w'(i)$ for each $i \in [1, n]$ in Eq. (7), where $T(i) = S(j)$. This implies that $c'_i \neq c_i$, and hence $G' \neq G$.

By Lemma 1, our scheme is highly sensitive to the secret keys k, h, h', and w. We demonstrate Lemma 1 with an example by generating ciphertexts for the plain text $T =$ STAY SAFE by slightly changing one key and fixing all other keys. The ciphertext for $k = 6, h = 18, h' = 22$, and weight function w listed in Tab. 2, ordered MEC $E_{11,0,4}$ with diffusion ordering is listed in the first column of Tab. 5. The ciphertext generated by only changing the integer k to 7 following Lemma 1(i) is listed in the third column of Tab. 5. The ciphertext generated by only changing integer h' to 23 following Lemma 1(ii) listed in the second column of Tab. 5. The ciphertext generated by only changing weight function to $w'(i) = w(i) + 10^{-4}$ following Lemma 1(iii) is listed in the fourth column of Tab. 5. The ciphertext generated by only changing EC $E_{11,0,5}$ parameter b to 5 with diffusion ordering is listed in the fifth column of Tab. 5. From Tab. 5 it is evident that the ciphertext generated by slight changes in the secret keys are totally different. Hence, the proposed scheme satisfies the key sensitivity analysis.

Table 5: Different ciphertexts generated by the proposed scheme for a fixed plain text

Original ciphertext	Effect of h	Effect of k	Effect of w	Ordered EC
0.96103	0.961034	0.34106	0.64013	0.48980
0.28662	0.286624	0.95404	0.28672	1.79218
0.48980	0.489799	0.73249	−0.00761	0.28662
1.21868	1.218677	1.23643	1.21878	1.21868
1.79218	1.792177	1.80992	1.79318	1.79874
0.39322	0.393223	0.38890	0.67502	0.45662

(Continued)

Table 5: Continued

Original ciphertext	Effect of h	Effect of k	Effect of w	Ordered EC
0.38890	0.388903	0.92887	1.03900	0.96103
1.79874	1.798742	1.69988	1.79884	0.38890
0.45662	0.456624	1.12404	0.45672	0.39322

4.3 Statistical Analysis

An encryption scheme is highly secure against statistical attacks if it can generate a highly random ciphertext. Histogram analysis and entropy analysis are the two commonly used tests to analyze the security of a scheme against statistical attacks. A scheme is secure against statistical attacks if it can generate ciphertexts with uniform histogram and optimal entropy.

Let X be a data set over a symbol set Ω and for $\omega \in \Omega, f(\omega)$ denotes the frequency of w in X. The entropy $H(X)$ of X is defined to be

$$H(X) = -\sum\nolimits_{\omega\in\Omega}(f(\omega)/|X|)\log_2(f(\omega)/|X|) \tag{10}$$

In the following result, we show that for each plain text, our scheme can generate a ciphertext with a uniform histogram and optimal entropy.

Lemma 2. For any plaint text, there exists at least one weight function w such that the frequency of each element in the ciphertext generated by the proposed scheme is 1.

Proof. Let T be a plain text of size n over a symbol set S and $T(i),\ i \in [1,n]$ be the i-th element of T. Our proof will complete if we show that there exists at least one weight function w such that for any two distinct $i, i' \in [1,n]$ it holds that the $c_i \neq c'_i$, where c_i and c'_i are generated by Eq. (7). Let $g_i = q_{(j+k) \pmod m}$ for $i \in [1,n]$, where $T(i) = S(j)$, for some $j \in [1,m]$ and $\psi_k(S(j)) = S((j+k)(\text{mod } m))$. Let $g_{i'}$ be an ordering of $g_1, g_2, \ldots, g_n$ such that $g_{i'} \geq g_{i'+1}$ for $i' \in [1,n]$. Let w be a mapping such that $w(i'+1)$ is a real in the open interval $(-1, w(i'))$ and $c_{i'+1} = g_{i'+1} + w(i'+1)$ for $i' \in [1,n]$. Note that w is an injection since $w(i') > w(i'+1)$ for each $i' \in [1, n-1]$. Furthermore, for each $i' \in [1,n]$ it holds that $g_{i'} + w(i') > g_{i'+1} + w(i'+1)$, since $g_{i'} \geq g_{i'+1}$ and $w(i') > w(i'+1)$ for each $i' \in [1,n]$. This implies that $c_{i'} > c_{i'+1}$ for each $i' \in [1,n]$, and hence $c_1{}'c_2{}' \ldots c_n{}'$ is a strictly decreasing sequence. This implies that $\sigma(c_i) \neq \sigma(c_j)$ for each distinct $i, j \in [1,n]$ from which the proof follows.

By Lemma 2, it follows that for each plain text, the proposed scheme can generate a ciphertext with uniform histogram and optimal entropy by using the weight function w constructed in Lemma 2 and $\alpha_i = 1$ for each i. Hence the proposed scheme has provable security against statistical attacks. We demonstrate the claim in Lemma 2 in Tab. 6 by generating a ciphertext for the plain text $T =$ STAY SAFE with secret keys $k = 6, h = 18, h' = 22$, ordered ECs $E_{11,0,4}$ with diffusion ordering and weight function w listed in Tab. 6.

Table 6: A ciphertext generated by the proposed scheme with uniform histogram and optimal entropy

Index i	Weight $w(i)$	Ciphertext $\sigma(\boldsymbol{c}_i)$
1	−0.49751	−0.20389
2	−0.321	0.64003
3	−0.007	0.81168
4	0.163	0.65280
5	0.2817	1.19924
6	0.4	−0.10038
7	0.65	1.46868
8	0.8812	1.27010
9	0.97350	0.67492

4.4 Ciphertext Only Attack

In ciphertext only attack, the cryptanalyst has access to some ciphertexts and try to get secret keys and hence the plain text. The cryptanalyst cannot reveal the plain text without the secret keys of the proposed scheme. Furthermore, there are at least 2^{100} keys for a fixed plain text of size at least 4, as discussed in Section 4.1, and therefore the brute-force attack requires lots of time to decrypt the ciphertext without keys. Hence by [53] the proposed scheme is secure against ciphertext only attack.

4.5 Known-plaintext Attack

In this attack, the attacker knows a pair of plain text and ciphertext and tries to generate secret keys. In our scheme, the attacker tries to generate h, h', k, w and $\sigma(D')$. The plain text consists of symbols in S and the ciphertext consists of real numbers with at most β digits after the decimal in our scheme, and therefore there is no relationship between the plain text and the keys h, h', k and w. Recall that $w(i) \in [-1, 1]$, and therefore it is not necessary that $h' - h + 1$ is at most the minimum number of digits after the decimal in the ciphertext. Thus, the attacker needs to try all possibilities for h, h' such that $h' - h + 1 \leq \beta$ and there exists a restricted Pell sequence of the size $|S|$, and k to know the representation of symbols in S, the weight function w to know the index of the symbols in the plain text, and $\sigma(D')$ which depends on the latter keys. Furthermore, for a given plain text the proposed scheme can generate a completely different ciphertext when keys are changed, as discussed in Section 4.3. Hence the proposed scheme is highly secure against known-plaintext attack by [53].

4.6 Security Comparison

The proposed scheme has five secret keys, the three integers h, h' *and* k, the weight function w, and the encoded sequence $\sigma'(D)$. The secret key depends on $\sigma'(D)$ the choice of h, h', k, w and the plain text. The main purpose of $\sigma'(D)$ is to get the weight value $w(i)$, and hence the index i when $\alpha_i = 0$. However, if $\alpha_i = 1$ for all i, then the weight $w(i)$ are in the ciphertext by Eq. (7), and therefore the key $\sigma'(D)$ is not necessary to get the weight function. More precisely, when $\alpha_i = 1$ for all i, we solve Eq. (8) for $d = 1 - q_i$, where $q_i \in Q_{h,h'}$ to get w. This implies that in the case of $\alpha_i = 1$ for all i, k, h, h' and w are sufficient keys to decrypt a ciphertext. Note that these keys are independent of the plain text. Furthermore, the proposed scheme also satisfies the key spacing analysis, key sensitivity analysis,

statistical analysis, ciphertext only attack and known-plaintext attack for the case of $\alpha_i = 1$ for all i as discussed in Sections 4.1–4.5.

We compared the security strength of the proposed scheme when $\alpha_i = 1$ for all i, the case where all secret keys are independent of the plain text, and the schemes in [23–27,33,34,36,37,48–51,53] against key spacing attack, key sensitivity attack, statistical attack, ciphertext only attack and known-plaintext attack in Tab. 7. We write "No" (resp. "NA") in the second, fifth and sixth columns of Tab. 7 if the corresponding scheme is not secure (resp. the analysis of the scheme against key spacing attack, ciphertext only attack and known-plaintext attack is not available.) Similarly, we write "No" in the third and fourth columns of Tab. 7 if the corresponding scheme does not have provable security against key sensitivity attack and statistical attack. From Tab. 7 observe that the security of the schemes in [23–27,33,34,36,37,48–51,53] is suspected against key spacing attack, key sensitivity attack, statistical attack, ciphertext only attack and known-plaintext attack. Therefore from Sections 4.1–4.5, the proposed scheme is more secure against listed attacks as compared to the schemes [23–27,33,34,36,37,48–51,53].

Table 7: Security comparison of the proposed scheme with the existing schemes

Method	High key spacing	Provable key sensitivity	Provable security against statistical attack	Secure against ciphertext only attack	Secure against known-plaintext attack
Ref. [23–27,33,36,37]	NA	No	No	NA	NA
Ref. [34]	NA	No	No	**Yes**	**Yes**
Ref. [48]	NA	No	No	NA	NA
Ref. [49]	**Yes**	No	No	**Yes**	**Yes**
Ref. [50,51]	NA	No	No	NA	NA
Ref. [53]	**Yes**	No	No	**Yes**	**Yes**
Proposed scheme	**Yes**	**Yes**	**Yes**	**Yes**	**Yes**

Note: The security of the scheme in [34] is suspected against key spacing attack and does not have provable security against key sensitivity attack and statistical attack. On the other hand, the proposed scheme has high key spacing and has provable security against key sensitivity and statistical attacks. This implies that the proposed scheme is more secure than the scheme in [34].

The schemes in [49] and [53] do not have provable security against key sensitivity attack and statistical attack. By Sections 4.2 and 4.3, the proposed scheme has high security against key sensitivity and statistical attacks as compared to the security of the schemes in [49] and [53].

5 Conclusion

We proposed a secure text encryption scheme. The scheme has three main steps, where we first diffuse the plain text by permuting the symbol set to convert the plain text into a meaningless message. In the second step, the diffused plain text is encoded with real numbers based on the Pell sequence, a weight function, and a binary sequence to hide the diffused plain text. In the third step, the scheme creates confusion in the encoded diffused plain text by generating permutations over ECs. We analyzed the security of the proposed scheme against several modern attacks including key spacing attack, key sensitivity attack, statistical attacks, ciphertext only attack and known-plaintext attack. From the

analysis it is clear that the proposed scheme has high resistance against modern attacks. Furthermore, we compared the security strength of the proposed scheme with the existing text encryption schemes in [23–27,33,34,36,37,48–51,53]. It is evident from the comparison that the proposed scheme is more secure as compared to the existing scheme against modern cryptanalysis.

By this scheme, we gave an application of the Pell sequence and ordered ECs in cryptography. In this scheme, we used binary sequence and weight function, which can be generated by any available method.

An interesting future direction would be to generate binary sequence and weight function by using ordered EC and propose an encryption scheme that can provide provable confidentiality and integrity.

Funding Statement: This research is funded through JSPS KAKENHI Grant Number 18J23484, QAU-URF 2015 and HEC project NRPU-7433.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] C. G. Kessler, *An Overview of Cryptography*, 2010. [Online]. Available: http://www.garykessler.net/library/crypto.html.
[2] C. E. Shannon, "Communication theory of secrecy systems," *The Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.
[3] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, 2019.
[4] N. A. Azam, U. Hayat and I. Ullah, "Efficient construction of a substitution box based on a Mordell elliptic curve over a finite field," *Frontiers of Information Technology and Electronic Engineering*, vol. 20, no. 10, pp. 1378–1389, 2019.
[5] N. A. Azam, U. Hayat and I. Ullah, "An injective S-box design scheme over an ordered isomorphic elliptic curve and its characterization," *Security and Communication Networks*, vol. 2018, Article ID 3421725, 9 pages, 2018.
[6] U. Hayat, N. A. Azam and M. Asif, "A method of generating 8 x 8 substitution boxes based on elliptic curves," *Wireless Personal Communications*, vol. 101, no. 1, pp. 439–451, 2018.
[7] A. A. Khan, V. Kumar and M. Ahmad, "An elliptic curve cryptography based mutual authentication scheme for smart grid communications using biometric approach," *Journal of King Saud University-Computer and Information Sciences*, 2019. https://doi.org/10.1016/j.jksuci.2019.04.013.
[8] V. Kumar, M. Ahmad, A. Kumari, S. Kumari and M. K. Khan, "SEBAP: A secure and efficient biometric-assisted authentication protocol using ECC for vehicular cloud computing," *International Journal of Communication Systems*, vol. 34, no. 2, pp. 4103, 2019.
[9] Z. E. Dawahdeh, S. N. Yaakob and R. R. B. Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349355, 2018.
[10] A. Razaq, H. Alolaiyan, M. Ahmad, M. A. Yousaf, U. Shuaib *et al.,* "A novel method for generation of strong substitution-boxes based on coset graphs and symmetric groups," in *IEEE Access*, vol. 8, pp. 75473–75490, 2020.
[11] M. A. Yousaf, H. Alolaiyan, M. Ahmad, M. Dilbar and A. Razaq, "Comparison of pre and post-action of a finite abelian group over certain nonlinear schemes," *IEEE Access*, vol. 8, pp. 39781–39792, 2020.
[12] M. Khan and N. A. Azam, "Right translated AES gray S-boxes," *Security and Communication Networks*, vol. 8, no. 9, pp. 1627–1635, 2015.

[13] M. Khan and N. A. Azam, "S-boxes based on affine mapping and orbit of power function," *3D Research*, vol. 6, no. 2, pp. 12, 2015.
[14] Ö. Koruoğlu and R. Sahin, "Generalized fibonacci sequences related to the extended hecke groups and an application to the extended modular group," *Turkish Journal of Mathematics*, vol. 34, no. 3, pp. 325–332, 2010.
[15] S. Ullah, L. Zhang, M. W. Sardar and M. T. Hussain, "T-Access policy: Attribute-based encryption scheme for social network based data trading," *China Communications*, vol. 18, no. 8, pp. 183–198, 2021.
[16] Z. Hua, S. Yi and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134–144, 2018.
[17] O. Vilardy, M. Juan, J. Barba, M. Torres and O. Cesar, "Image encryption and decryption systems using the jigsaw transform and the iterative finite field cosine transform," *Photonics*, vol. 6, no. 4, pp. 121, 2019.
[18] D. Lambić, A. Janković and M. Ahmad, "Security analysis of the efficient chaos pseudo-random number generator applied to video encryption," *Journal of Electronic Testing*, vol. 36, no. 4, pp. 709–715, 2018.
[19] H. A. Ahmed, M. F. Zolkipli and M. Ahmad, "A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map," *Neural Computing and Applications*, vol. 31, no. 11, pp. 7201–7210, 2019.
[20] M. Ahmad, S. Khurana, S. Singh and H. D. AlSharari, "A simple secure hash function scheme using multiple chaotic maps," *3D Research*, vol. 8, no. 28, pp. 13, 2017.
[21] M. Ahmad, M. N. Doja and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.
[22] N. A. Azam, "A novel fuzzy encryption technique based on multiple right translated AES Gray S-boxes and phase embedding," *Security and Communication Networks*, vol. 2017, Article ID 5790189, 9 pages, 2017.
[23] K. Abdullah, S. A. Bakar, N. H. Kamis and H. Aliamis, "RSA cryptosystem with fuzzy set theory for encryption and decryption," in *AIP Conference Proceedings*, vol. 1905, no. 1, pp. 030001, 2017.
[24] V. Gupta, G. Singh and R. Gupta, "Advance cryptography algorithm for improving data security," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 2, no. 1, pp. 1–6, 2012.
[25] S. Pattanayak and D. Dey, "Text encryption and decryption with extended Euclidean algorithm and combining the features of linear congruence generator," *International Journal of Development Research*, vol. 6, no. 7, pp. 8753–8756, 2016.
[26] E. Agrawal and P. R. Pal, "A secure and fast approach for encryption and decryption of message communication," *International Journal of Engineering Science*, vol. 7, no. 5, pp. 11481, 2017.
[27] S. E. Ghrare, H. A. Barghi and N. R. Madi, "New text encryption method based on hidden encrypted symmetric key," in *Int. Conf., Advanced Computer Information Technologies*, Ceske Budejovice, Czech Republic, 2018.
[28] Q. Mushtaq and U. Hayat, "Horadam generalized Fibonacci numbers and the modular group," *Indian Journal of Pure and Applied Mathematics*, vol. 38, no. 5, pp. 345, 2007.
[29] Q. Mushtaq and U. Hayat, "Pell numbers, Pell-Lucas numbers and modular group," *Algebra Colloquium*, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, and Suzhou University, vol. 14, no. 1, pp. 97–102, 2007.
[30] T. Koshy, *Pell and Pell-Lucas Numbers with Applications*, New York: Springer, 2014.
[31] A. Luma and B. Raufi, "Relationship between fibonacci and lucas sequences and their application in symmetric cryptosystems," in *Proc. of the 4th Int. Conf. on Circuits, Systems and Signals, World Scientific and Engineering Academy and Society (WSEAS)*, Corfu Island, Greece, pp. 146–150, 2010.
[32] A. Overmars and S. Venkatraman, "An efficient golden ratio method for secure cryptographic applications," *Mathematical and Computational Applications*, vol. 23, no. 4, pp. 58, 2018.
[33] P. Agarwal, N. Agarwal and R. Saxena, "Data encryption through fibonacci sequence and unicode characters," *MIT International Journal of Computer Science and Information Technology*, vol. 5, no. 2, pp. 79–82, 2015.

[34] T. Clelland, V. Risca and C. Bancroft, "Hiding messages in DNA microdots," *Nature*, vol. 399, no. 6736, pp. 533–534, 1999.
[35] M. Borda and O. Tornea, "DNA secret writing techniques," in *2010 8th Int. Conf. on Communications IEEE*, Bucharest, Romania, pp. 451–456, 2010.
[36] M. R. Abbasy, A. A. Manaf and M. A. Shahidan, "Data hiding method based on DNA basic characteristics," in *Int. Conf. on Digital Enterprise and Information Systems*, Springer, Berlin, Heidelberg, pp. 53–62, 2011.
[37] M. A. Murillo-Escobar, F. Abundiz-Prez, C. Cruz-Hernndez and R. M. Lpez-Gutirrez, "A novel symmetric text encryption algorithm based on logistic map," in *Proc. of the Int. Conf. on Communications, Signal Processing and Computers*, Honolulu, Hawaii, USA, vol. 4953, 2014.
[38] H. Perez-Meana, E. Hernandez-Diaz and V. Silva-Garcia, "Encryption of RGB images by means of a novel cryptosystem using elliptic curves and chaos," *IEEE Latin America Transactions*, vol. 18, no. 8, pp. 1407–1415, 2020.
[39] I. Hussain, N. A. Azam and T. Shah, "Stego optical encryption based on chaotic S-box transformation," *Optics and Laser Technology*, vol. 61, pp. 50–56, 2014.
[40] M. Ahmad and M. S. Alam, "A new algorithm of encryption and decryption of images using chaotic mapping," *International Journal on Computer Science and Engineering*, vol. 2, no. 1, pp. 46–50, 2009.
[41] X. Zhang, Y. Mao and Z. Zhao, "An efficient chaotic image encryption based on alternate circular S-boxes," *Nonlinear Dynamics*, vol. 78, no. 1, pp. 359–369, 2014.
[42] M. Ahmad, M. N. Doja and M. M. S. Beg, "Security analysis and enhancements of an image cryptosystem based on hyperchaotic system," *Journal of King Saud University-Computer and Information Sciences*, vol. 33, no. 1, pp. 77–85, 2021.
[43] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013.
[44] R. I. Abdelfatah, "Secure image transmission using chaotic-enhanced elliptic curve cryptography," *IEEE Access*, vol. 8, pp. 3875–3890, 2019.
[45] I. Ullah, U. Hayat and M. D. Bustamante, "Image encryption using elliptic curves and Rossby/drift wave triads," *Entropy*, vol. 22, no. 4, pp. 454, 2020.
[46] S. Toughi, M. H. Fathi and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Processing*, vol. 141, pp. 217–227, 2017.
[47] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 472–481, 2015.
[48] C. H. Suneetha, T. Surendra and C. H. Neelima, "Implementation of double fold text encryption based on elliptic curve cryptography (ECC) with digital signature," *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 8, no. 5, pp. 3840–3846, 2020.
[49] M. A. Naji, D. A. Hammood, H. A. Atee, R. S. Jebur, H. A. Rahim *et al.,* "Cryptanalysis cipher text using new modeling: text encryption using elliptic curve cryptography," in *AIP Conf. Proc.*, Putrajaya, Malaysia, vol. 2203, no. 1, pp. 020003, 2020.
[50] K. Agrawal and A. Gera, "Elliptic curve cryptography with hill cipher generation for secure text cryptosystem," *International Journal of Computer Applications*, vol. 106, no. 1, pp. 18–24, 2014.
[51] K. Keerthi and B. Surendiran, "Elliptic curve cryptography for secured text encryption," in *Int. Conf. on Circuit, Power and Computing Technologies (ICCPCT)*, Kollam, India, IEEE, pp. 1–5, 2017.
[52] A. Kumar, S. S. Tyagi, M. Rana, N. Aggarwal and P. Bhadana, "A comparative study of public key cryptosystem based on ECC and RSA," *International Journal on Computer Science and Engineering*, vol. 3, no. 5, pp. 1904–1909, 2011.
[53] L. D. Singh and K. M. Singh, "Implementation of text encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 73–82, 2015.
[54] S. Ullah, X. Li and L. Zhang, "A review of signcryption schemes based on hyper elliptic curve," in *3rd Int. Conf. on Big Data Computing and Communications (BIGCOM)*, Chengdu, China, pp. 51–58, 2017.

[55] S. Ullah, X. Y. Li and Z. Lan, "A novel trusted third party based signcryption scheme," *Multimedia Tools and Applications*, vol. 79, pp. 22749–22769, 2020.
[56] S. Ullah and N. Din, "Blind signcryption scheme based on hyper elliptic curves cryptosystem," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 917–932, 2021.
[57] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, New York: CRC Press, 2008. [Online]. Available: https://https://doi.org/10.1201/9781420071474.
[58] Keith M. Martin, *Everyday Cryptography: Fundamental Principles and Applications*, Oxford University Press, 2012.
[59] S. M. Seyedzadeh, B. Norouzi, M. R. Mosavi and S. Mirzakuchaki, "A novel color image encryption algorithm based on spatial permutation and quantum chaotic map," *Nonlinear Dynamics*, vol. 81, no. 1–2, pp. 511–529, 2015.