Proceedings of the Federated Conference on Computer Science and Information Systems pp. 991–998
DOI: 10.15439/2016F94
ACSIS, Vol. 8. ISSN 2300-5963

Pseudo-random Sequence Generation from Elliptic Curves over a Finite Field of Characteristic 2

Omar Reyad
Warsaw University of Technology
Warsaw, Poland
Email: ormak4@yahoo.com

Zbigniew Kotulski
Warsaw University of Technology
Warsaw, Poland
Email: zkotulsk@tele.pw.edu.pl

***Abstract*—In this paper, the randomness of binary sequences generated from elliptic curves over a finite field of characteristic 2 is studied. A scheme of construction based on the Chaos-Driven Elliptic Curve Pseudo-random Number Generator (C-D ECPRNG) is proposed. The generators based of this scheme are verified by using tests from the NIST Statistical Test Suite to analyze their statistical properties. An elliptic curve used in the numerical example is defined over $\mathbb{F}_{2^8}$. The investigations which made for the generated series of two output sequences of the lengths of 2^{10} and 2^{20} bits shown that 14 generators working according to our general scheme exhibit good randomness properties. Next, the binary sequences generated by these 14 schemes were used for encrypting a 256×256 grayscale Lena image as an application example and the security analysis of the ciphered images was carried out.**

I. Introduction

IN 1985, Neil Koblitz [1] and Victor Miller [2] independently proposed one of the most important public-key cryptosystems named the elliptic curve cryptosystem, whose security rests on the discrete logarithm problem over points on an elliptic curve (EC) [3]. Elliptic curve public-key cryptosystems over finite fields ($\mathbb{F}_{2^m}$ or $\mathbb{F}_p$) have become widely used in applications such as smart cards which provide limited space for implementation of modular computations. Recently, the operations (Add, Double, Multiply) of points on elliptic curves over $\mathbb{F}_{2^m}$ or $\mathbb{F}_p$ have a well-developed technology in both hardware and software implementations.

Elliptic curves applications in, both, cryptography and communications are currently the subject of extensive investigation, as means for increasing security in transmission and reception of data over an insecure communication channel. The advantage is that elliptic curves over finite fields ($\mathbb{F}_{2^m}$ and $\mathbb{F}_p$) provide an inexhaustible supply of finite abelian groups. It is found that different elliptic curves defined over the same field have a different structure as finite fields of the same order are isomorphic to each other. With the increase in available computation power, it is found for a given key size that an EC public-key cryptosystem has higher security compared to RSA cryptosystem [4]. EC operations which used in the generation of pseudo-random sequences with strong cryptographic properties have been studied in the literature, such as [5], [6], [7].

In this paper, new constructions for the generation of pseudo-random sequences based on the properties of random numbers and elliptic curves over a finite field of characteristic 2 ($\mathbb{F}_{2^m}$) are proposed. These constructions are based on the C-D ECPRNG which takes benefits from a chaotic generator to reinforce the quality of an Elliptic Curve Pseudo-random Number Generator (ECPRNG). The addition of chaos will define a family of ECPRNGs that are chaotic while being fast, statistically perfect and cryptographically secure as discussed in [8], [9]. The randomness properties of the new constructions are also tested and found to pass tests in the NIST randomness test suite [26]. Such sequences can be used for generating random numbers in the EC digital signature algorithm and a session key in their encryption phases.

The paper is organized as follows. In Section II, the preliminaries of EC are discussed. An overview of various EC based pseudo-random sequence generators are given in Section III. In Section IV, we present several construction methods of binary sequences obtained from the C-D ECPRNG. An illustrative example is presented in Section V. In Section VI, randomness properties of the proposed sequences are discussed. A simple application of the proposed sequences for image encryption is executed in Section VII while conclusions are given in Section VIII.

II. Preliminaries

The definition of elliptic curves over a finite field of characteristic 2 and their arithmetic are given here to provide the general background for our exposition.

A. Elliptic Curve over a Binary Finite Field

The field $\mathbb{F}_{2^m}$ called a *characteristic-two* finite field or a *binary* finite field, can be viewed as a vector space of dimension m over the field $\mathbb{F}_2$ which consists of the two elements $\{0,1\}$. A non-supersingular elliptic curve E over the binary field $\mathbb{F}_{2^m}$ is defined by an equation of the form

$$y^2 + xy = x^3 + ax^2 + b \tag{1}$$

where the parameters $a, b \in \mathbb{F}_{2^m}$ with $b \neq 0$. The set $E(\mathbb{F}_{2^m})$ consists of all points $(x,y), x \in \mathbb{F}_{2^m}, y \in \mathbb{F}_{2^m}$, which satisfy the defining equation (1), together with a special point O called the point at infinity. These set of points form an abelian group with respect to the addition rules given in the following section.

978-83-60810-90-3/$25.00

B. Arithmetic of Elliptic Curve Group over $E(\mathbb{F}_{2^m})$

As mentioned in the previous section, when $b \neq 0$, the set of all points on the elliptic curve E along with a point at infinity constitute an abelian group under addition operation with O serving as its identity element [10]. It is to be noted here that this addition operation $(+)$ is not the "conventional addition" operation as it is based on the arithmetic of elliptic curves [11].

The algebraic formula for the sum of two points and the double of a point are the following:

1) $P+O=O+P$ for all $P \in E(\mathbb{F}_{2^m})$.
2) If $P=(x,y) \in E(\mathbb{F}_{2^m})$, then $(x,y)+(x,x+y)=O$, note that the point $(x,x+y)$ is denoted by $-P$, and it is called the negative of P; observe that $-P$ is indeed a point on the curve E.
3) Point addition: Let $P=(x_1,y_1) \in E(\mathbb{F}_{2^m})$ and $Q=(x_2,y_2) \in E(\mathbb{F}_{2^m})$, where $P \neq \pm Q$. Then $P+Q=(x_3,y_3)$ where
$$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \left(\frac{y_1+y_2}{x_1+x_2}\right) + x_1 + x_2 + a \tag{2}$$
and
$$y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1+x_3) + x_3 + y_1. \tag{3}$$
4) Point doubling: Let $P=(x_1,y_1) \in E(\mathbb{F}_{2^m})$, where $P \neq -P$. Then $2P=(x_3,y_3)$ where
$$x_3 = x_1^2 + \left(\frac{b}{x_1^2}\right) \ . \tag{4}$$
and
$$y_3 = x_1^2 + (x_1 + \frac{y_1}{x_1})x_3 + x_3 \ . \tag{5}$$

III. Literature Review

A pseudo-random number generator (PRNG) is a deterministic algorithm which takes a random binary sequence of length k and outputs a binary sequence of length $n \gg k$ which "appears" to be random [12]. The input to the PRNG is called the seed, while the output is called a pseudo-random sequence. Different EC-based PRNG schemes suggested in literature use different ways to proceed from seed value for ith iteration to that for $(i+1)$th iteration and different predicates the output sequences, while the used one-way function is the EC point addition operation. Various suggestions for PRNG which based on ECs and their brief analysis are presented below.

A. The EC Power Generator

The Power Generator on EC (EC-PG) is introduced in [13], [14]. The definition of EC-PG for a given point $G(x,y) \in E(\mathbb{F}_p)$ of high order ℓ and an initial secret key $e \geq 2$ provided that the greatest common divisor (gcd) of $(gcd(e,\ell)=1)$ is generated by:

$$U_i = [e]U_{i-1} = [e^i]G \quad , i = 1,2,\ldots, \tag{6}$$

where $U_0(x,y) \in E(\mathbb{F}_p)$ is the "initial value". The output point sequence is the truncated x-coordinate of the resulted points $U_i(x,y)$.

B. The EC Linear Congruential Generator

The Linear Congruential Generator on EC (EC-LCG) has been suggested in [15] and then studied in a number of papers such as [16], [17], [18]. For a given point $G(x,y) \in E(\mathbb{F}_p)$ of high order ℓ, the EC-LCG is defined as the following sequence:

$$U_i = G + U_{i-1} = [i]G + U_0 \quad , i = 1,2,\ldots, \tag{7}$$

where $U_0(x,y) \in E(\mathbb{F}_p)$ is the "initial value". The output point sequence is generated as the resulted points $U_i(x,y)$ and passes through the complete cyclic subgroup of the point $G(x,y)$.

C. The Pseudo-random Bit Sequence Generator-B

The Pseudo-random Bit Sequence Generator (PBSG-B) which presented in [19] is a modification of the EC-LCG such that the periodicity is independent of the order of point $G(x,y)$ and the output sequence does not have any symmetric properties which makes the cryptanalysis easier. For security, the authors of [19] assume that both point $G(x,y)$ and the seed value of the Linear Feedback Shift Register (LFSR) are kept secret.

D. The Chaos-Driven Elliptic Curve Pseudo-random Number Generator

The Chaos-Driven Elliptic Curve Pseudo-random Number Generator (C-D ECPRNG) which presented in [20] for the finite field $\mathbb{F}_p$ is considered to be the EC-LCG driven by a chaotic map. Such a modification improves randomness of the sequence generated and increases it's periodicity. The C-D ECPRNG for a given seed point $G(x,y) \in E(\mathbb{F}_{2^m})$ as the secret key, is defined as the following sequences generated by additive EC-points operation:

$$\begin{aligned} U_i &= [i(1+b_i)]G + U_0 \\ &= \begin{cases} [i]G + U_0 & if \quad b_i = 0 \\ [2i]G + U_0 & if \quad b_i = 1 \end{cases} \quad , i = 1,2,\ldots \end{aligned} \tag{8}$$

where $U_0(x,y) \in E(\mathbb{F}_{2^m})$ is the "initial value" and b_i is the random bits generated by a chaotic map Φ

$$b_i = \begin{cases} 0 & if \quad \Phi^i(s) \in S_0 \\ 1 & if \quad \Phi^i(s) \in S_1 \end{cases} \quad , i = 1,2,\ldots \tag{9}$$

where the state space $S=[0,1]$ is the interval and $S_0=[0,0.5]$, $S_1=(0.5,1]$ are two subsets of the interval equal to 0.5. (For more details see [21]).

E. The EC Based Random Number Generator

The random number generator proposed in [22] has reduced latency and increased periodicity with a single point multiplication operation in each iteration. The output point sequence is $U_i=[k_i]G$ and $k_i=(i-1)+x_{i-1}$ where x_{i-1} is the x-coordinate of the point $U_{i-1}(x,y)$. The random number generator has good statistical properties and high periodicity.

F. The Dual-EC Generator

The Dual-EC generator has appeared in NIST recommendations [23]. It makes use of two points $G(x,y)$ and $Q(x,y)$ on a non-super singular elliptic curve $E(\mathbb{F}_p)$ for generation of random numbers. One point for generating the iterating key k as $k_i = x([k_{i-1}]G)$ and the other point for generating the output bit sequence as $t_i = x([k_i]Q)$ where t is the truncation function. The Dual-EC generator mechanism represents an EC scalar multiplication operation, followed by the extraction of the $x-$coordinate for the resulting points followed by truncation to produce the output sequence. We mention here that this recommendation is now withdrawn.

G. The Pseudo-random Bit Sequence Generator-A

A modification of the Dual-EC generator with increased periodicity named Pseudo-random Bit Sequence Generator-A (PBSG-A) is published in [19]. In PBSG-A, the iteration key k is modified as $k_{i+1} = [k_i]G + [i]C$ where $C = x([e]G)$ and "e" is the seed value. In addition to two point multiplication operations the modified algorithm requires a finite field multiplication of iteration number "i" and the value "C" to be carried out in each iteration. This increases both the hardware complexity and the time complexity of the system.

IV. Proposed constructions for EC Binary Sequences

In this section, we propose 22 different schemes resulted from different construction methods based on the C-D ECPRNG discussed in Section III-D.

The points resulted $U_i(x,y)$ with $x-$ and $y-$coordinates of each point are used to obtain the binary sequences. We will shortcut the word sequence to (Seq) throughout this paper and mention that an Initialization Vector (IV) is a fixed initialization vector that should be specified with the scheme. The exclusive or (XOR) logical operation with the symbol $\oplus$ is used here and one can show that it can be replaced by any operation that is an *easy-to-invert* permutation of one of its inputs when the second input is fixed.

After applying the C-D ECPRNG, we get the resulted points $U_i(x,y)$ and the $x-$ and $y-$coordinates of these points are used according to the construction methods listed in table I. These construction methods result in 22 different schemes by applying the ith iteration function R_i. For example, R_i for the first scheme is given by:

$$R_i = [R_{i-1} \oplus X_i], \quad , i \geq 1 \tag{10}$$

where $R_0 = IV$ and X is the $x-$coordinate of the first point U_1. The output R_i is the pseudo-random bit sequence. We will use the notion of a permutation operation (appear in table I as *Perm*) of the results from XOR operation for mapping the bit elements then considering them into the output sequence R for the next iteration process in some schemes. In other schemes, the substitution-box operation ($S-box$) which considers the heart of some ciphers because they are highly nonlinear is also used. $S-box$ takes the results from XOR operation and transforms them into the corresponding output then considering them into the output sequence R. $S-box$ is a basic component of symmetric key algorithms which performs substitution. In our calculations we used the Advanced Encryption Standard (AES) block cipher $S-box$ which discussed in [24].

V. Implementation Example

For experimental results we consider the EC defined over $\mathbb{F}_{2^8}$ given by:

$$E : y^2 + xy = x^3 + \alpha x^2 + 1 \tag{11}$$

where the parameters $a = \alpha, b = 1 \in \mathbb{F}_{2^8}$ with $b \neq 0$ and the EC is based on the irreducible polynomial $x^8 + x^4 + x^3 + x^2 + 1$ over $\mathbb{F}_2$. The total number of EC points is found to be 288 including O (point at infinity) and the element α is a generator of $\mathbb{F}_{2^8}$. The EC point $G = (\alpha^{186}, \alpha^{225})$ is chosen as the base point, which has the order $\ell = 288$ and the initial point is $U_0 = (\alpha^{34}, \alpha^{99})$. Also, $\{G, [2]G, \ldots, [288]G\}$ generates all the elements of EC over $\mathbb{F}_{2^8}$, hence the given elliptic curve group is cyclic. In the case of C-D ECPRNG, we use the Logistic map [25] as our chaotic map to generate the random bits b_i defined in (9).

VI. Randomness Properties

The purpose of this section is to check experimentally the randomness properties of the sequences generated in Section IV. The whole sequences generated by Section IV should have good statistical properties, we also decided to check the statistical properties and test the randomness using six basic statistical tests from [26], [27]. These tests are:

1) **Frequency (Monobit) Test**, it verifies if the number of "1" bits in the sequence lies within specified limits.
2) **8-bit Poker test**, it verifies whether bytes of each possible value appear approximate the same number of times.
3) **Runs Test**, it checks whether the number of runs (the test is carried out for runs of zeros and runs of ones) of length 1, 2, 3, 4 and 5 as well as the number of runs which are longer than 5, each lies within specified limits.
4) **Discrete Fourier Transform (Spectral) Test**, it detects the periodic features in the tested sequence that would indicate a deviation from the assumption of randomness.
5) **Linear Complexity Test**, it determines whether or not the sequence is complex enough to be considered random. Random sequences are characterized by longer LFSRs. An LFSR that is too short implies non-randomness.
6) **Cumulative Sums (Cusums) Test**, it determines whether the cumulative sum of the partial sequences occurring in the tested sequence is too large or too small relative to the expected behavior of that cumulative sum for random sequences. The test has two modes, which are either forward through the sequence or backward through the sequence, named in the Tables *Cusums (forward)* and *Cusums (reverse)*, respectively.

All the generated sequences from $Seq-1$ to $Seq-22$ is tested using the six basic tests discussed above. The test

TABLE I
THE 22 PROPOSED SEQUENCE SCHEMES

No.	scheme expression	No.	scheme expression
1	$[R_{i-1} \oplus X_i]$	12	$[R_{i-1} \oplus Y_i]$
2	$Perm[R_{i-1} \oplus X_i]$	13	$Perm[R_{i-1} \oplus Y_i]$
3	$S-box[R_{i-1} \oplus X_i]$	14	$S-box[R_{i-1} \oplus Y_i]$
4	$X_i \oplus Perm[R_{i-1} \oplus X_i]$	15	$Y_i \oplus Perm[R_{i-1} \oplus Y_i]$
5	$Y_i \oplus Perm[R_{i-1} \oplus X_i]$	16	$X_i \oplus Perm[R_{i-1} \oplus Y_i]$
6	$R_i \oplus Perm[R_{i-1} \oplus X_i]$	17	$R_i \oplus Perm[R_{i-1} \oplus Y_i]$
7	$[R_i \oplus Y_i] \oplus Perm[R_{i-1} \oplus X_i]$	18	$[R_i \oplus X_i] \oplus Perm[R_{i-1} \oplus Y_i]$
8	$X_i \oplus S-box[R_{i-1} \oplus X_i]$	19	$Y_i \oplus S-box[R_{i-1} \oplus Y_i]$
9	$Y_i \oplus S-box[R_{i-1} \oplus X_i]$	20	$X_i \oplus S-box[R_{i-1} \oplus Y_i]$
10	$R_i \oplus S-box[R_{i-1} \oplus X_i]$	21	$R_i \oplus S-box[R_{i-1} \oplus Y_i]$
11	$[R_i \oplus Y_i] \oplus S-box[R_{i-1} \oplus X_i]$	22	$[R_i \oplus X_i] \oplus S-box[R_{i-1} \oplus Y_i]$

TABLE II
TEST RESULTS FOR SEQ-1 AND SEQ-5

	Seq-1		Seq-5	
Test name	2^{10}	2^{20}	2^{10}	2^{20}
Monobit	0.5737	0.6157	0.4917	0.2597
Poker	0.2122	0.2220	0.2872	0.2869
Runs	0.1204	0.8510	0.1735	0.8507
DFT	0.2561	0.6139	0.6264	0.8313
L. Comp.	0.9196	0.2846	0.9196	0.4670
Cusums (F)	0.3999	0.7256	0.8035	0.3911
Cusums (R)	0.8831	0.9280	0.3999	0.1933

TABLE III
TEST RESULTS FOR SEQ-12 AND SEQ-16

	Seq-12		Seq-16	
Test name	2^{10}	2^{20}	2^{10}	2^{20}
Monobit	0.1691	0.8177	0.4917	0.1351
Poker	0.2771	0.0548	0.0849	0.7276
Runs	0.1028	0.9765	0.1071	0.9068
DFT	0.4905	0.3124	0.5980	0.4599
L. Comp.	0.9196	0.6583	0.1246	0.2629
Cusums (F)	0.0488	0.5020	0.8579	0.2025
Cusums (R)	0.2219	0.3369	0.3011	0.1273

results are shown that 14 schemes of the proposed 22 schemes exhibits good randomness properties. The other 8 schemes are found to have non-random properties especially with long binary sequences (2^{20} bits) and fail to pass most of the six tests. We presented in Tables II and III the test results for four schemes as examples to discuss. In Table II are presented results for the sequence $Seq-1$ and $Seq-5$. As it is noted, the generator works correctly for short and long binary sequences (2^{10} and 2^{20}bits). In Table III, results for the sequence $Seq-12$ and $Seq-16$ are presented. Also it is clear that the C-D ECPRNG enables generating correctly short and long sequences and the generator passes all the presented tests. For the rest of the paper, we will consider only the 14 schemes (namely $Seq-1$, $Seq-2$, $Seq-3$, $Seq-5$, $Seq-8$, $Seq-9$, $Seq-11$,$Seq-12$, $Seq-13$, $Seq-14$, $Seq-16$, $Seq-19$, $Seq-20$, $Seq-22$) that had good randomness properties.

VII. IMAGE ENCRYPTION APPLICATION EXAMPLE

Image encryption is a potential application where stream cipher is highly preferred over block cipher due to the bulky nature of the data and high correlation between the adjacent pixels. The pseudo-random sequence used for image encryption must have good randomness properties and high periodicity so that the encrypted image is secure. Recently, several attempts for using ECs in image encryption has been proposed in literature such as [28],[29],[30]. In this section, the pseudo-random sequences generated by the considered 14 schemes are used for encrypting a 256×256 grayscale Lena image in which each pixel has a 8-bit value of between 0 and 255 and the security analysis of the ciphered images are carried out.

A. Entropy Analysis

Entropy is defined to express the degree of uncertainties in the system. It is well known that the entropy $H(m)$ of a message source m can be calculated as:

$$H(m) = -\sum_{i=0}^{255} P(m_i) log_2 P(m_i) \tag{12}$$

where $P(m_i)$ represents the probability of symbol m_i. For all the considered cipherimages shown in Figs. 3(a – n), the number of occurrence of each gray level is recorded and the probability of occurrence is computed. Table IV indicates the various values of the entropies for the plain and encrypted images by the considered 14 schemes. It can be noted that the entropy of the encrypted images are very near to the theoretical value of 8 indicating that all the pixels in the encrypted images occur with almost equal probability. Therefore, the information leakage in the considered cipher schemes is negligible, and it is secure against the entropy-based attack. Also it is comparable

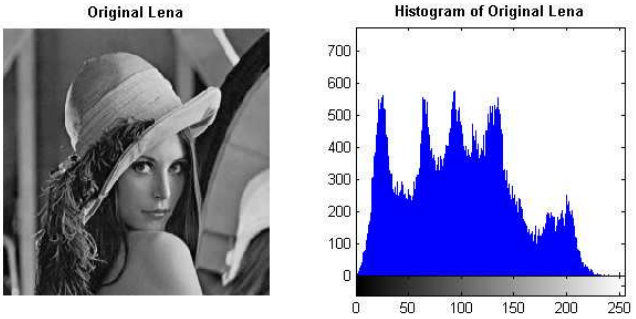

Fig. 1. Lena image and it's Histogram

to the entropy values presented by references [30], [31] and [32].

TABLE IV
ENTROPY AND CORRELATION COEFFICIENTS FOR LENA IMAGE

Scheme	Entropy	Horizontal	Vertical	Diagonal
Lena	7.5807	0.93915	0.96890	0.91686
Seq-1	7.9973	-0.00201	0.04720	0.00132
Seq-2	7.9971	-0.00431	0.00513	-0.00443
Seq-3	7.9975	0.00061	-0.00319	-0.00572
Seq-5	7.9970	0.00390	0.00879	-0.00030
Seq-8	7.9972	0.00591	-0.03651	0.00481
Seq-9	7.9977	-0.00007	-0.00345	0.00378
Seq-11	7.9972	0.00638	-0.01068	-0.00391
Seq-12	7.9973	-0.00071	0.03101	0.00501
Seq-13	7.9972	0.00220	-0.01799	-0.00583
Seq-14	7.9973	-0.00331	-0.00323	0.00588
Seq-16	7.9968	0.00690	0.01358	0.00325
Seq-19	7.9972	-0.00287	-0.04253	-0.00174
Seq-20	7.9973	-0.00076	-0.00670	0.00003
Seq-22	7.9967	0.00026	0.00259	-0.00645
Ref.[30]	7.9964	-0.00079	-0.0013	-0.0046
Ref.[31]	7.9885	0.0132	0.0017	0.0034
Ref.[32]	7.9968	0.0025	0.0037	0.0011

B. Correlation Analysis

It is known that two adjacent pixels in a plainimage are strongly correlated vertically, horizontally and diagonally. This is the property of any ordinary image. The maximum value of correlation coefficient is 1 and the minimum is 0. A robust encrypted image to statistical attack should have a correlation coefficient value of ˜0 as discussed in [33]. Results of horizontal, vertical and diagonal directions are obtained as shown in Table IV for Lena plainimage and the ciphered images by the considered 14 schemes respectively. These results demonstrate that there is negligible correlation between the two adjacent pixels in the encrypted images, even when the two adjacent pixels in the plainimage are highly correlated.

C. Sensitivity Analysis

In order to avoid the known-plaintext attack, the changes in the cipherimage should be significant even with a small change in the plainimage. If one small change in the plainimage can cause a significant change in the cipherimage, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. To quantify this requirement, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [34]. We have tested the NPCR and UACI with the considered 14 sequence schemes to assess the influence of changing a single pixel in the plainimages on the encrypted images. From the results, we have found that the average values of the percentage of pixels changed in encrypted image is greater than 99.60% for NPCR and 30.50% for UACI for all the 14 generated sequences. This implies that the considered 14 schemes are very sensitive with respect to small changes in the plainimage.

D. Histogram Analysis

To prevent the leakage of information to an adversary, it is important to ensure that cipherimage does not have any statistical resemblance to the plainimage. A good image encryption scheme should always generate a cipherimage of the uniform histogram for any plainimage. In this work, the histograms are plotted for Lena plain and encrypted images. The histogram of Lena plainimage contains large spikes as shown in Fig. 1 while the histograms of it's cipherimages are almost flat and uniform which indicates equal probability of occurrence of each pixel as shown in Figs. 2(a – n). They are significantly different from the respective histogram of the Lena plainimage and hence does not provide any clue to employ any statistical attack on the considered 14 image encryption schemes.

VIII. CONCLUSION

In this paper, we have presented several construction methods based on a common general scheme for generating binary sequences from EC over a binary finite field ($\mathbb{F}_{2^m}$). The proposed scheme is based on the C-D ECPRNG with simple arithmetic transformations (XOR and permutation or $S-box$) to produce long size binary sequences with good randomness properties. The generated sequences are tested using tests from the NIST randomness test suite to analyze their statistical properties. It is found that 14 schemes of the 22 proposed specific schemes have passed the selected six complementary tests and the sequences generated by these 14 schemes work correctly

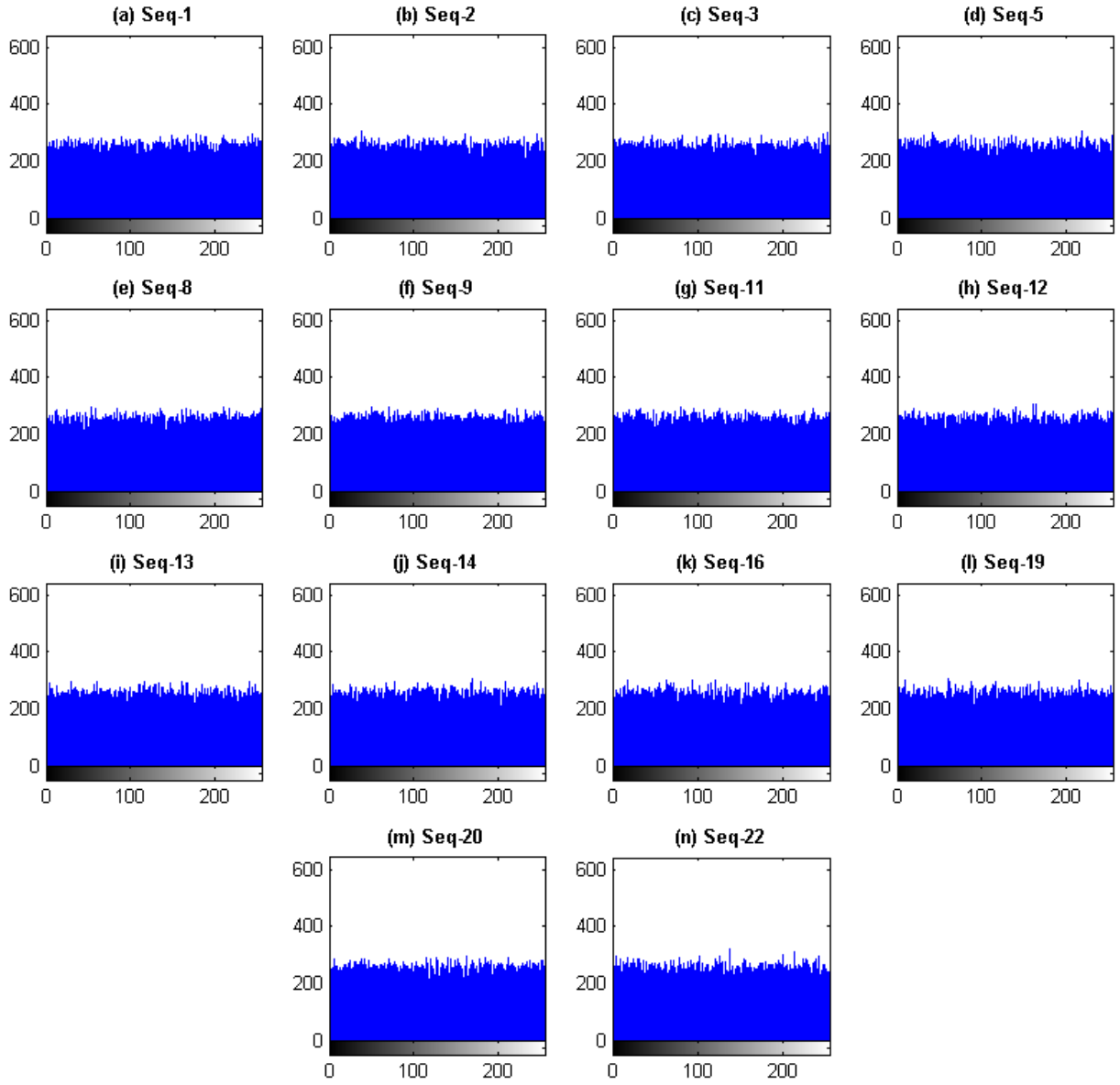

Fig. 2. Histogram of encrypted Lena image with the considered 14 sequences

with short (2^{10} bits) and long (2^{20} bits) size sequences. The pseudo-random sequences generated by these 14 schemes are applied to image encryption as an application example and the security analysis of the ciphered images are carried out. It is found also that the sequences generated using the C-D ECPRNG had high periodicity so that the encrypted images are secure. In addition, it has large key space, which is by far very safe for image encryption applications, and outperforms the competitive image encryption algorithms in terms of efficiency comparing to other encryption schemes.

ACKNOWLEDGMENT

This work has been supported financially by the Ministry of Higher Education of Egypt. Calculations in this paper were performed at the Interdisciplinary Center for Mathematical and Computational Modeling (ICM) of the University of Warsaw part of the grant calculation No. G63-2.

REFERENCES

[1] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of Computation,* vol. 48, 1987, pp. 203–209.

[2] V. Miller, "Uses of elliptic curves in cryptography," *Advances in Cryptology-CRYPTO'85,* vol. 218, Springer, Heidelberg, 1986, pp. 417–426, doi:10.1007/3-540-39799-X_31

[3] A. Menezes, *Elliptic Curve Public Key Cryptosystems,* Kluwer Academic, Dordrecht 1993, doi:10.1007/978-1-4615-3198-2

[4] N. Gura, A. Patel, A. Wander, H. Eberle and S.C. Shantz, "Comparing elliptic curve cryptography and RSA on 8-bit CPUs," *Cryptographic Hardware and Embedded Systems (CHES),* vol. 3156, Springer, Heidelberg, 2004, doi:10.1007/978-3-540-28632-5_9

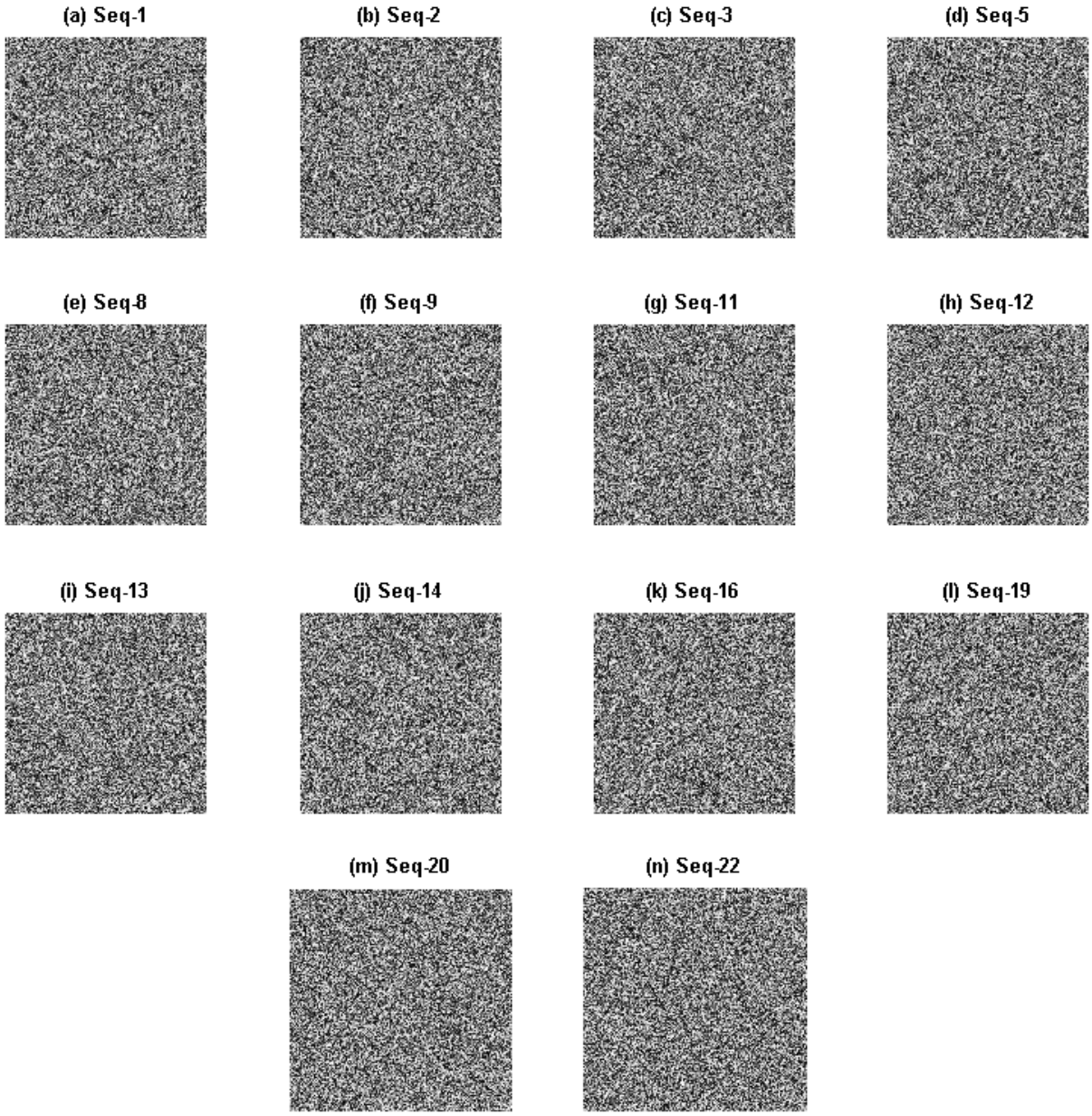

Fig. 3. Encrypted Lena image with the considered 14 sequences

[5] B. S. Kaliski, "One-way permutations on elliptic curves," *Journal of Cryptology 3,* 1991, pp. 187–199, doi:10.1007/BF00196911

[6] Z. Chen, S. Li and G. Xiao, "Construction of pseudo-random binary sequences from elliptic curves by using discrete logarithm," *In: G. Gong, et al. (eds.): SETA 2006. LNCS,* vol. 4086, Springer, Heidelberg, 2006, pp. 285–294, doi:10.1007/11863854_24

[7] S. V. Sathyanarayana, M. A. Kumar and K. N. H. Bhat, "Random binary and non-binary sequences derived from random sequence of points on cyclic elliptic curve over finite field $GF(2^m)$ and their properties," *Information Security J.: A Global Perspective,* vol. 19, 2010, pp. 84–94, doi:10.1080/19393550903482759

[8] J. M. Bahi and C. Guyeux, *Discrete Dynamical Systems and Chaotic Machines: Theory and Applications,* CRC Press, Numerical Analysis and Scientific Computing, London 2013.

[9] R. L. Tataru, "Image hashing secured with chaotic sequences," *Proceedings of the 2014 Federated Conference on Computer Science and Information Systems (FedCSIS),* IEEE, 2014, pp. 735–740, doi:10.15439/2014F250

[10] D. Johnson, A. Menezes and S. Vanstone, "The Elliptic Curve Digital Signature Algorithm," *International Journal of Information Security,* vol. 1, 2001, pp. 36–63, doi:10.1007/s102070100002

[11] J. H. Silverman, *The arithmetic of elliptic curves,* Springer-Verlag, New York 2009, doi:10.1007/978-0-387-09494-6

[12] D. Szalkowski and P. Stpiczynski, "Template Library for Multi-GPU Pseudorandom Number Recursion-based Generators," *Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS),* IEEE, 2013, pp. 515–519.

[13] T. Lange and I. E. Shparlinski, "Certain exponential sums and random walks on elliptic curves," *Canad. J. Math.,* vol. 57, 2005, pp. 338–350, doi:10.4153/CJM-2005-015-8

[14] E. El Mahassni and I. E. Shparlinski, "On the distribution of the elliptic curve power generator," *Proc. 8th Conf. on Finite Fields and Appl.,*

Contemp. Math., vol. 461, Amer. Math. Soc., Providence, RI, 2008, pp. 111–119.
[15] S. Hallgren, "Linear congruential generators over elliptic curves," *Preprint CS94-143*, Dept. of Comp. Sci., Cornegie Mellon Univ., 1994.
[16] G. Gong, T.A. Berson and D.R. Stinson, "Elliptic curve pseudorandom sequence generators," *Selected areas in cryptography,* vol. 1758, Springer, Berlin, 2000, doi:10.1007/3-540-46513-8_3
[17] O. Reyad and Z. Kotulski, "On Pseudo-random Number Generators Using Elliptic Curves and Chaotic Systems," *J. Appl. Math. Inf. Sci.,* vol. 9, 2015, pp. 31-38, doi:10.12785/amis/090105
[18] P. Beelen and J. Doumen, "Pseudorandom sequences from elliptic curves," *Finite Fields with Applications to Coding Theory,* Cryptography and Related Areas, Springer, Berlin, 2002, doi:10.1007/978-3-642-59435-9_3
[19] P. P. Deepthi and P. S. Sathidevi, "New stream ciphers based on elliptic curve point multiplication," *Computer Communications,* vol. 32, 2009, pp. 25–33, doi:10.1016/j.comcom.2008.09.002
[20] O. Reyad and Z. Kotulski, "Statistical Analysis of the Chaos-Driven Elliptic Curve Pseudo-random Number Generators," *In: Z. Kotulski, et al. (eds.) CSS 2014. CCIS,* vol. 448, Springer, Heidelberg, 2014, pp. 38–48, doi:10.1007/978-3-662-44893-9_4
[21] J. Szczepanski and Z. Kotulski, "Pseudorandom number generators based on chaotic dynamical systems," Open Systems & Information Dynamics, vol. 8, 2001, pp. 137–146, doi:10.1023/A:1011950531970
[22] L. P. Lee and K. W. Wong, "A random number generator based elliptic curve operations," *Computers & Mathematics with Appl.,* vol. 47, 2004, pp. 217–226, doi:10.1016/S0898-1221(04)90018-1
[23] E. B. Barker and J. M. Kelsey, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)," *US Department of Commerce, Technology Administration, National Institute of Standards and Technology,* Computer Security Division, Information Technology Laboratory, 2007.
[24] J. A. Buchmann, *Introduction to Cryptography,* Undergraduate Texts in Mathematics, Springer-Verlag New York, 2004, doi:10.1007/978-1-4419-9003-7
[25] S. C. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical Review E* vol. 51, 1995,pp. 3670–3678, doi:10.1103/PhysRevE.51.3670
[26] A. Rukhin, J. Soto, J. Nechvatal, et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication 800-22 with revisions,* May 2001.
[27] T. Rachwalik, J. Szmidt, R. Wicik and J. Zablocki, "Generation of Nonlinear Feedback Shift Registers with special-purpose hardware," IEEE Transl. Military Communications and Information Systems Conference (MCC), pp. 1–4, October 2012.
[28] S. Maria and K. Muneeswaran, "Key generation based on elliptic curve over finite prime field, " *Int. J. Elect. Sec. and Digital Forensics,* vol. 4, 2012, pp. 65–81, doi:10.1504/IJESDF.2012.045391
[29] O. Reyad and Z. Kotulski, "Image Encryption Using Koblitz's Encoding and New Mapping Method Based on Elliptic Curve Random Number Generator," *In: A. Dzich, et al. (eds.): MCSS 2015. CCIS,* vol. 566, Springer, Heidelberg, 2015, pp. 34–45, doi:10.1007/978-3-319-26404-2_3
[30] S. V. Sathyanarayana, M. Aswatha Kumar and K. N. Hari Bhat, "Symmetric key image encryption scheme with key sequences derived from random sequence of cyclic elliptic curve points," *Int. J. Netw. Secur.,* vol. 12, 2011, pp. 137–150.
[31] A. Soleymani, M. J. Nordin, Z. M. Ali and L. Golafshan, "A Binary Grouping Approach for Image Encryption Based on Elliptic Curves over Prime Group Field," IEEE Transl. 11th Malaysia International Conference on Communications (MICC), pp. 373–378, November 2013, doi:10.1109/MICC.2013.6805857
[32] J. Payingat and P. P. Deepthi, "Pseudorandom Bit Sequence Generator for Stream Cipher Based on Elliptic Curves," *Mathematical Problems in Engineering,* Hindawi Pub. Cor., vol. 2015, 2015, pp. 1–16, doi:10.1155/2015/257904
[33] G. Zhang and Q. Liu, "A novel image encryption method based on total shuffling scheme," *J. Optics Communications,* vol. 284, 2011, pp. 2775–2780, doi:10.1016/j.optcom.2011.02.039
[34] Y. Wu, J. P. Noonan and S. Agaian, "NPCR and UACI Randomness Tests for Image Encryption," IEEE Transl. J. of Selected Areas in Telecommunications (JSAT), pp. 31–38, April 2011.