Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/13S119

Image Pixel Permutation Operation Based on Elliptic Curve Cryptography

Omar Reyad[1,2,*], *Hany S. Khalifa*[3] *and Radwan Kharabsheh*[4]

[1] Computer Science Department, Faculty of Science, Sohag University, Sohag, Egypt
[2] College of Computing & Information Technology, Shaqra University, Shaqra, Kingdom of Saudi Arabia
[3] Computer Science Department, Misr Higher Institute of Commerce and Computers, Egypt
[4] Department of Business Administration, Applied Science University, Bahrain

Received: 12 May 2019, Revised: 1 Jul 2019, Accepted: 10 Jul. 2019
Published online: 1 Aug. 2019

Abstract: In this paper, elliptic curve (EC) based pseudo-random bit generator is used to control the group operation (GRP) method which has good inherent cryptographic properties. The new proposed method named EC-GRP operation combines the cryptographic properties of both elliptic curve cryptography (ECC) and the group bit permutation operation. When applied to image pixels, the proposed EC-GRP bit-level permutation method controlled by the EC pseudo-random bit generator, presented higher performance characteristics in terms of security analysis test benchmarking.

Keywords: Elliptic Curve Cryptography, Group Permutation, Pseudo-random Bit Generator, Image Encryption

1 Introduction

The security of transmitted digital information through an insecure channel becomes more and more important security issue in the present and forthcoming future. Since 1985, Elliptic Curve Cryptography (ECC), were invented by Neal Koblitz [1] and Victor Miller [2] has been widely studied in secure communications and technology. The idea of taking advantage of elliptic curve discrete logarithm problem (ECDLP) computational intractability to construct modern cryptosystems has been extensively investigated and attracts more and more attention. A significant number of advantages that can be gained from using elliptic curve smaller parameters include fast computations and smaller key sizes and certificates. These advantages are important requirements in such secure data transmission where processing power and storage space is needed. EC operations which used in the generation of pseudo-random bit sequences with strong cryptographic properties have been studied in the literature, such as [3–6]. These pseudo-random bit sequences which present random statistical properties are used for both confusion and diffusion operations in digital multimedia processing and secure information transmission. As a primary method to achieve diffusion, permutation operation is widely used in cryptographic algorithms. Bit-level permutations particularly, are the core of many encryption algorithms. The first bit-level permutations called group permutation (GRP) is detailed in [7, 8]. This permutation operation is in fact, permutation instructions developed to efficiently implement arbitrary n-bit permutation in any programmable processors, whether they are general purpose microprocessors or application-specific cryptography processors.

In the following, we propose to control the GRP operation with EC based pseudo-random bit generator and we will call the new method the ”EC-GRP” instruction operation. The proposed EC-GRP operation combines the cryptographic properties of both of the group operation and the EC points operation. It may be possible for the support of new operations to lead to new designs offering higher performance and reduced energy consumption which would be particularly important for constrained environments such as Internet of Things (IoT) platforms.

The security of digital image data from unauthorized access is an important area of research in multimedia transmission over network communication. The ability to support fast bit-level permutations and their ability to

* Corresponding author e-mail: ormak4@yahoo.com

support next-generation secure multimedia processing may also be viewed as a further challenge of the basic security primitives in communication networks.

Digital images are used to test the proposed EC-GRP approach. Indeed, it is well known that images are different from plaintexts in many aspects, such as high redundancy and correlation properties. The main stumbling block in designing effective image encryption algorithms is that it is rather difficult to diffuse such image data pixels as discussed in [9–12]. In most of the natural images, the value of any given pixel can be reasonably predicted from the values of its neighbours.

The rest of the paper is organized as follows. In Section 2, the preliminaries of group permutation and elliptic curves are discussed. In Section 3, we presented the new EC-GRP method and it's cryptographic properties. An illustrative example and it's security analysis are presented in Section 4 with a simple application of the proposed method for image pixel encryption. Conclusions are given in Section 5.

2 Preliminaries

In this section, we present the GRP permutation method and an overview of the elliptic curve over a finite field of characteristic 2 ($\mathbb{F}_{2^m}$) arithmetic point operations.

2.1 Definition of Group Permutation

The GRP operation method will be written as:

$$R_3 = GRP(R_1, R_2), \tag{1}$$

where R_1 is the source data or the original image pixels in this case, R_2 is the configuration control bits and R_3 is the resulted bits for the permuted bits. In this work, we propose to control this method by elliptic curve bit sequences. Then, in each iteration, the control bits R_2 is filled by an elliptic curve binary sequence of 8-bits. Thus, each EC based byte can be used to control the permutation of a byte from the image pixel which means bits of R_1 [7, 8].

The basic idea of the GRP instruction is to divide the bits in the source data R_1 into two groups (Left and Right) according to the control bits in R_2. For each bit in R_1, we check the corresponding bit in R_2. If the bit in R_2 is equal 0, we move this bit from R_1 into the first group at the left end. Otherwise, we put this bit into the second group at the right end. In the case that the GRP operation is used in a cryptographic algorithm, the inverse operation, UNGRP for ungroup, may be needed for the decryption process.

Table 1: Points of E over $\mathbb{F}_{2^5}$

$(0,1)$	$(1,\alpha^{12})$	$(1,\alpha^{23})$	(α,α^{1})
(α,α^{18})	(α^{2},α^{27})	(α^{2},α^{23})	(α^{4},α)
(α^{4},α^{30})	(α^{5},α^{29})	(α^{5},α^{20})	(α^{8},α^{11})
(α^{8},α^{6})	(α^{9},α^{29})	(α^{9},α^{17})	$(\alpha^{10},\alpha^{11})$
$(\alpha^{10},\alpha^{28})$	(α^{11},α^{4})	$(\alpha^{11},\alpha^{26})$	$(\alpha^{13},\alpha^{20})$
(α^{13},α^{4})	(α^{15},α^{8})	$(\alpha^{15},\alpha^{30})$	(α^{16},α)
$(\alpha^{16},\alpha^{25})$	(α^{18},α^{4})	$(\alpha^{18},\alpha^{24})$	$(\alpha^{20},\alpha^{11})$
$(\alpha^{20},\alpha^{27})$	$(\alpha^{21},\alpha^{27})$	$(\alpha^{21},\alpha^{17})$	$(\alpha^{22},\alpha^{23})$
(α^{22},α^{9})	$(\alpha^{23},\alpha^{19})$	$(\alpha^{23},\alpha^{29})$	(α^{26},α^{3})
$(\alpha^{26},\alpha^{15})$	(α^{27},α^{4})	$(\alpha^{27},\alpha^{16})$	(α^{29},α^{5})
$(\alpha^{29},\alpha^{20})$	(α^{30},α^{1})	$(\alpha^{30},\alpha^{17})$	

2.2 Elliptic Curves over $\mathbb{F}_{2^m}$

An elliptic curve E over $\mathbb{F}_{2^m}$ can be defined by an equation of the form

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

where $a, b \in \mathbb{F}_{2^m}$, and $b \neq 0$. 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 (2), together with a special point O called the point at infinity [13].

Example 1. Consider the elliptic curve $E : y^2 + xy = x^3 + \alpha^4 x^2 + 1$ defined over $\mathbb{F}_{2^5}$ as represented by the irreducible trinomial $f(x) = x^5 + x^2 + 1$. This curve has order 44. Note that we have $a = \alpha^4$ and $b = 1$ and that $b \neq 0$, so E is indeed an elliptic curve. The points in $\mathbb{F}_{2^5}$ are listed in Table 1.

2.3 Elliptic Curve Point Operation

In the arithmetic of elliptic curves, there is a chord-and-tangent rule for adding two points on an elliptic curve $E(\mathbb{F}_{2^m})$ to give a third elliptic curve point [14]. Together with this addition operation, the set of points $E(\mathbb{F}_{2^m})$ forms a group with O serving as its identity. 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 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

$$x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \left(\frac{y_1+y_2}{x_1+x_2}\right) + x_1 + x_2 + a \tag{3}$$

and

$$y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + x_3 + y_1. \tag{4}$$

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

$$x_3=x_1^2+(\frac{b}{x_1^2}) \text{ and } y_3=x_1^2+(x_1+\frac{y_1}{x_1})x_3+x_3\,. \quad (5)$$

Example 2. Consider the elliptic curve defined in Example 1.

1. Let $P=(\alpha^8,\alpha^{11})$ and $Q=(\alpha^2,\alpha^{23})$. Then $P+Q=(x_3,y_3)$ is computed as follows:

$$\begin{aligned} x_3 &= \left(\frac{\alpha^{11}+\alpha^{23}}{\alpha^8+\alpha^2}\right)^2+\frac{\alpha^{11}+\alpha^{23}}{\alpha^8+\alpha^2}+\alpha^8+\alpha^2+\alpha^4 \\ &= (\frac{\alpha^3}{\alpha^{29}})^2+\frac{\alpha^3}{\alpha^{29}}+\alpha^8+\alpha^2+\alpha^4=\alpha^8 \end{aligned}$$

and

$$\begin{aligned} y_3 &= \left(\frac{\alpha^{11}+\alpha^{23}}{\alpha^8+\alpha^2}\right)(\alpha^8+\alpha^8)+\alpha^8+\alpha^{11} \\ &= (\frac{\alpha^3}{\alpha^{29}})(0)+\alpha^6=\alpha^6. \end{aligned}$$

Hence, $P+Q=(\alpha^8,\alpha^6)$.

2. Let $P=(\alpha^8,\alpha^{11})$. Then $2P=P+P=(x_3,y_3)$ is computed as follows:

$$x_3=(\alpha^8)^2+\frac{1}{(\alpha^8)^2}=\alpha^{16}+\alpha^{15}=\alpha^2 \quad (6)$$

and

$$y_3=(\alpha^8)^2+(\alpha^8+\frac{\alpha^{11}}{\alpha^8})\alpha^2+\alpha^2=\alpha^{27}\,. \quad (7)$$

Hence, $2P=(\alpha^2,\alpha^{27})$.

2.4 The EC Random Bit Generator

After applying the EC based pseudo-random bit generator in [15], we get the resulted points $U_i(x,y)$ and the $x-$ and $y-$coordinates of these points are used according to the construction method given in equation 8. This construction method result in mapping scheme by applying the ith iteration function R_i. For example, R_i for this scheme is given by:

$$R_i=[R_{i-1}\oplus X_i], \quad ,i\geq 1 \quad (8)$$

where $R_0=IV$ (IV is an initialization vector) and X is the $x-$coordinate of the first point U_1. The output R_i is the pseudo-random bit sequence which will be used to control the proposed EC-GRP operation.

3 The Proposed Elliptic Curve Group Permutation

In this section we will propose the EC-GRP operation for bit-level permutation to perform the permutation of each original data item.

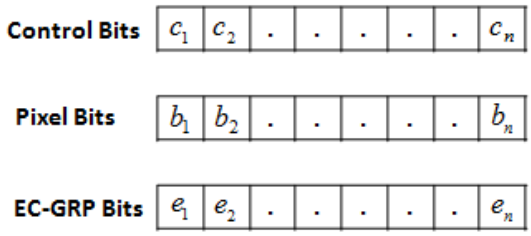

Fig. 1: EC-GRP operation

3.1 EC-GRP Permutation Operation

In this method, EC based pseudo-random bit generator is used to control group bit permutation GRP method which has good inherent cryptographic properties. The new method called EC-GRP operation combines the cryptographic properties of both elliptic curve cryptography and the group operation. Figure 1 shows the permutation of each image pixel bits $B=\{b_1,b_2,\cdots,b_n\}$ according to control bits $C=\{c_1,c_2,\cdots,c_n\}$. These control bits generated from the EC based pseudo-random bit generator described in section 2.4. The EC-GRP permutation operation resulted bits are $E=\{e_1,e_2,\cdots,e_n\}$. A pseudo code for the description of this method is given in Listing 1.

Listing 1: EC-GRP Operation Pseudo Code

```
function [E] = ECGRP(C, B)
index = 1;
  for i = 1:8
    if C(i) == 0
         E(index) = B(i);
         index = index + 1;
    end
  end
  for i = 1:8
    if C(i) == 1
        E(index) = B(i);
        index = index + 1;
    end
  end
end function
```

3.2 Cryptographic Properties of EC-GRP

The new EC-GRP permutation operation should have good cryptographic properties, and be resistant to common cryptanalytic attacks as well as not opening new weaknesses. Both of elliptic curves and permutation operations are based on difficult (hard) problems in number theory and have a rich mathematical structure. Thus, the EC-GRP should has at least the same level of

security and cryptographic properties that are resistant to differential attacks; a difference in any bit of the control bits should produce a large difference in the output (resulted) bits. The basic ideas of confusion and diffusion [16, 17] that are so prominent in block cipher designs also appear elsewhere during the permutation mechanism. Confusion might be viewed as a process by which small amounts of complex interaction are introduced locally, while diffusion can be viewed as the process by which this complexity is spread from being solely a local phenomenon. By alternating primitive functions that provide confusion and diffusion, the hope is that the final algorithm will exhibit globally complex, and cryptographically strong, behavior.

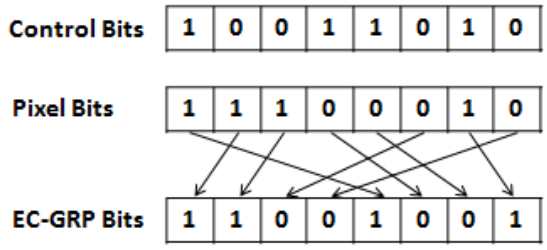

Fig. 2: EC-GRP permutation for encrypting Lena image pixel bits controlled by EC control bits

4 The Simulation Results

A given implementation of this EC-GRP mechanism need to include an approved elliptic curve. Once the designer decides upon the strength required by a given application, he can then choose to implement the single curve that most NIST SP 800-90A [18], appropriately meets this requirement. For a common level of optimization expended, the higher-strength curves will be slower and tend toward less efficient use of output blocks. To mitigate the latter, the designer should be aware that every distinct request for random bits requires the computational expense of at least one elliptic curve point multiplication.

4.1 Implementation 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 [19–22]. In this section, the EC-GRP permutation operation is used for encrypting a 256×256 grayscale Lena image pixels as shown in figure 2. Each pixel has a 8-bit value of between 0 and 255, so the control bits in turn divided into blocks of 8-bit each and the EC-GRP operation is applied. The resulted (EC-GRP) bits then grouped together to obtain the cipherimage and security analysis of the ciphered image is carried out.

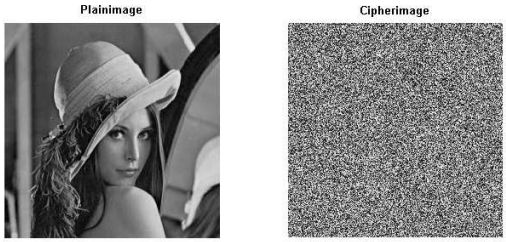

Fig. 3: Lena plainimage and the corresponding cipherimage with the EC-GRP operation

4.2 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:

$$H(m) = -\sum_{i=0}^{255} P(m_i) log_2 P(m_i) \qquad (9)$$

where $P(m_i)$ represents the probability of symbol m_i [27]. For the considered cipherimage shown in figure 3, the number of occurrence of each gray level is recorded and the probability of occurrence is computed. Table 2 indicates the various values of the entropy for the plain and encrypted image by the EC-GRP operation. It can be noted that the entropy of the encrypted image is very near to the theoretical value of 8 indicating that all the pixels in the encrypted image occur with almost equal probability. Therefore, the information leakage in the proposed EC-GRP operation is negligible, and it is secure against the entropy-based attack.

Table 2: Entropy and basic parameters for Lena image

Scheme	Entropy	PSNR	MSE	MAE
Proposed EC-GRP	7.9962	8.4781	9303.84	79.57
Ref [25]	7.9898	8.5838	9009.33	—-
Ref [26]	7.9968	11.30	4859.03	79.22

4.3 Peak Signal-to-noise Ratio (PSNR)

PSNR is defined by the ratio between the maximum possible value (power) of an image and the power of distorting noise that affects the quality of representation of that image [28]. PSNR is mainly used in image processing as a consistent image quality metric and the greater PSNR, the better the output image quality. The performance of the proposed EC-GRP method is evaluated on the basis of PSNR and measure values obtained are shown in Table 2. The results clearly explained that the EC-GRP permutation method is well suited for many kinds of image encryption operations.

4.4 Mean Square Error and Mean Absolute Error

The ciphered image should show a significant difference with it's corresponding plainimage. This difference can be measured with two main methods, Mean Square Error (MSE) and Mean Absolute Error (MAE) [27]. MSE and MAE values are computed by using the following equations:

$$MSE = \frac{1}{W*H}\sum_{j=1}^{H}\sum_{i=1}^{W}(P_{ij}-C_{ij})^2 \tag{10}$$

$$MAE = \frac{1}{W*H}\sum_{j=1}^{H}\sum_{i=1}^{W}|(P_{ij}-C_{ij})| \tag{11}$$

In the two above equations, parameters W and H are the width and height of the image. Also P_{ij} is the gray level of the pixel in the plainimage and $C_{i,j}$ is the gray level of the pixel in the encrypted image. MSE and MAE values of the encrypted image are reported in Table 2. As viewed from the table, MSE and MAE tests have yielded high values which can ensure the resistance of the proposed EC-GRP against differential attacks.

4.5 Correlation Analysis

It is known that two adjacent pixels in a plainimage are strongly correlated vertically, horizontally and diagonally. This is the property in connection with any ordinary image. The maximum value of correlation coefficient is 1 and the minimum value is 0. A robust encrypted image versus statistical attack should have a correlation coefficient value of ˜0 as discussed in [23]. Results of horizontal, vertical and diagonal directions are obtained as shown in Table 3 for Lena plainimage and the ciphered image by the EC-GRP method respectively. In the encrypted image, the adjacent pixel correlation will be less if the encryption process is capable of hiding the details of the plainimage. The obtained results expound that there is negligible correlation between the two adjacent pixels in the encrypted image, even when the two adjacent pixels in the plainimage are highly correlated as shown in figure 5.

4.6 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) [24]. We have tested the NPCR and UACI with the generated control bit sequences to assess the influence of changing a single pixel in the plainimage on the encrypted image. From the results, we have found that the average values of the percentage of pixels changed in encrypted image is greater than 99.58% for NPCR and 30.46% for UACI for the generated sequence. This implies that the EC-GRP method are very sensitive with respect to small changes in the plainimage.

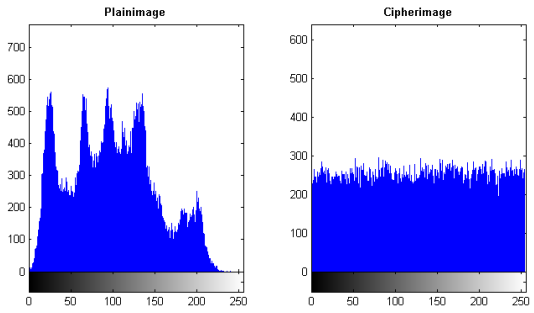

Fig. 4: Histogram of encrypted Lena image with the EC-GRP operation

4.7 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 histogram is plotted for Lena plain and encrypted image. The histogram of Lena plainimage contains large spikes as shown in figure 4 while the histogram of it's cipherimage is almost flat and uniform which indicates equal probability of occurrence of each pixel as shown in figure 4. It is significantly different from the respective histogram of the Lena plainimage and hence does not provide any clue to employ any statistical attack on the proposed image pixel permutation operation.

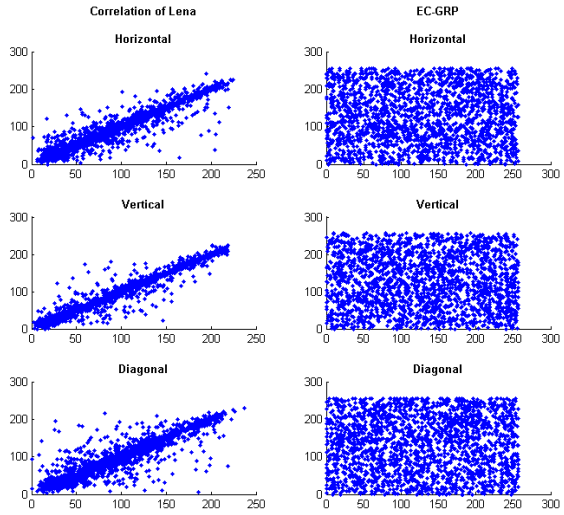

Fig. 5: Correlation of encrypted Lena image with the EC-GRP operation

Table 3: Correlation coefficients for Lena image

Scheme	Horizontal	Vertical	Diagonal
Lena	0.93915	0.96890	0.91686
Proposed EC-GRP	-0.00311	0.05420	0.00231
Ref [25]	-0.00041	-0.00025	-0.000027
Ref [26]	-0.0043	-0.0090	-0.0031

5 Conclusion

In this paper, we have presented a new EC-GRP permutation method controlled by an EC based pseudo-random bit generator. The general scheme for generating binary sequences from EC over a binary finite field ($\mathbb{F}_{2^m}$) is used. The pseudo-random bit sequences generated are used as a control bits for the group permutation operation to obtain scrambled bits. The EC-GRP operation is applied to image pixel encryption as an application example. Also the security analysis of the ciphered images are carried out presented higher performance characteristics in terms of security test benchmarking.

References

[1] N. Koblitz, Elliptic curve cryptosystems, Mathematics of Computation, 48, 203–209 (1987).
[2] V. Miller, Uses of elliptic curves in cryptography, Advances in Cryptology-CRYPTO'85, vol. 218, Springer Heidelberg, 417–426, (1986).
[3] 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, 38–48, (2014).
[4] B. S. Kaliski, One-way permutations on elliptic curves, Journal of Cryptology 3, 187–199 (1991). doi:10.1007/BF00196911
[5] 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, 285–294, (2006).
[6] 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, 34–45, (2015).
[7] R. B. Lee, Z. Shi and X. Yang, Efficient permutation instructions for fast software cryptography, IEEE Micro. 21(6), 56–69 (2001).
[8] Z. Shi and R. B. Lee, Bit permutation instructions for accelerating software cryptography, In Proceedings of the 11th International Conference on Application-Specific Systems, Architectures and Processors, 138–148 (2000).
[9] W. M. Abd-Elhafiez, O. Reyad, M. A. Mofaddel and M. Fathy, Image Encryption Algorithm Methodology Based on Multi-mapping Image Pixel, In: A. Hassanien, et al. (eds.): AMLTA 2019. AISC, vol. 921, Springer Cham, 645–655 (2020).
[10] O. Reyad, Text message encoding based on elliptic curve cryptography and a mapping methodology, Inf. Sci. Lett. 7(1), 7–11 (2018).
[11] 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. 12, 137–150 (2011).
[12] T. Zhang, A. A. Abd El-Latif, M. Amin and A. Zhagloul, Diffusion-substitution mechanism for color image encryption based on multiple chaotic systems, Advanced Materials Research 981, 327–330 (2014).
[13] 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, 19, 84–94 (2010), doi:10.1080/19393550903482759
[14] J. H. Silverman, The arithmetic of elliptic curves, Springer-Verlag, New York, (2009). doi:10.1007/978-0-387-09494-6
[15] O. Reyad and Z. Kotulski, Pseudo-Random Sequence Generation from Elliptic Curves over a Finite Field of Characteristic 2, In: Federated Conference on Computer Science and Inf. Sys., FedCSIS, ACSIS 8, IEEE, 991–998 (2016).
[16] C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28(4), 656–715 (1949).
[17] X. Yan, S. Wang, L. Li, A. A. Abd El-Latif, Z. Wei and X. Niu, A new assessment measure of shadow image quality based on error diffusion techniques, Journal of Information Hiding and Multimedia Signal Processing (JIHMSP) 4(2), 119–127 (2013).
[18] 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).
[19] O. Reyad, Z. Kotulski and W.M. AbdElhafiez, Image Encryption using Chaos-Driven Elliptic Curve Pseudo-Random Number Generators, J. Appl. Math. Inf. Sci. 10, 1283–1292 (2016).
[20] A. A. Abd El-Latif, L. Li and X. Niu, A New Image Encryption Scheme Based on Cyclic Elliptic Curve and Chaotic System, Multimedia Tools and Applications 70(3), 1559–1584 (2014).
[21] O. Reyad, M. Mofaddel, W. Abd-Elhafiez and M. Fathy, A novel image encryption scheme based on different block sizes for grayscale and color images, In: 12th international conference on computer engineering and systems (ICCES), IEEE, 455–461 (2017).
[22] A. Belazi, A. A. Abd EI-Latif, R. Rhouma, S. Belghith, Selective image encryption scheme based on DWT AES S-box and chaotic permutation, International Wireless Communications and Mobile computing Conference (IWCMC), 606–610 (2015).
[23] G. Zhang and Q. Liu, A novel image encryption method based on total shuffling scheme, J. Optics Communications 284, 2775–2780 (2011). doi:10.1016/j.optcom.2011.02.039
[24] 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), 31–38 (2011).
[25] S. Y. Wang, J. F. Zhao, X. F. Li and L. T. Zhang, Image Blocking Encryption Algorithm Based on Laser Chaos Synchronization, J. of Elect. and Comp. Eng. 2016, Hindawi P. C., 1–14 (2016).
[26] I. Younas and M. Khan, A New Efficient Digital Image Encryption Based on Inverse Left Almost Semi Group and Lorenz Chaotic System, Entropy 2018, 20(12), 913, 1–22 (2018).
[27] R. C. Gonzalez and R. E. Woods, Digital Image Processing (3rd Edition), Prentice-Hall, Inc., Upper Saddle River, NJ, (2006).
[28] M. Khfagy, Y. AbdelSatar, O. Reyad and N. Omran, An Integrated Smoothing Method for Fingerprint Recognition Enhancement, In: A. Hassanien, et al. (eds.) AISI 2016, AISC, vol. 533, Springer Cham, 407–416 (2016).

Omar Reyad is a Lecturer of Computer Science at the Faculty of Science, Sohag University, Egypt. He received his PhD degree from the Faculty of Electronics and Information Technology, Warsaw University of Technology, Poland. He received his MSc in Computer Science from Sohag University, Egypt. His main research interests are in Elliptic curve cryptography, Cryptographic protocols, Biometric security, Chaos-based cryptography and Post-Quantum Cryptography.

Hany Said Al-Sayed Khalifa received his Bachelor of Education Technology (Computer) at Faculty of Specific Education, Mansoura University, 1994 and Master degree with excellent grade in Education Technology (Computer) also. Dr. Hany received his PhD degree in computer applications from the University of Tanta in cooperation with Mubarak City for Scientific Research and Technological Applications. He is currently a Computer Science Instructor at the Department of Computer Science at the Misr Institute of Commerce and Computers, Egypt. His research interests include Artificial intelligence, Cloud computing, Mobile applications, Image processing and Cryptosystems.

Radwan Kharabsheh received his Bachelor of Science majoring in physics from Yarmouk University Jordan. He then finished an MBA and a PhD in international business from Charles Sturt University Australia where he worked as a full time lecturer. His research interests include international business, strategic management and knowledge management. He obtained numerous grants from Charles Sturt University, the Hashemite University and obtained a fellowship from the Australia-Malaysia Institute and is a fellow of the higher Education academy in the UK.