Optik 168 (2018) 370–375

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

Cryptanalysis of multimedia encryption using elliptic curve cryptography

Khoirom Motilal Singh*, Laiphrakpam Dolendro Singh, Themrichon Tuithung

Department of Computer Science and Engineering, National Institute of Technology, Nagaland 797103, India

ARTICLE INFO

Article history:
Received 9 March 2018
Accepted 11 April 2018

Keywords:
Multimedia encryption
Elliptic curve cryptography
Elliptic curve discrete logarithmic problem
Cryptanalysis

ABSTRACT

The encryption scheme proposed by Tawalbeh et al. [1] is based on elliptic curve cryptography (ECC). ECC depends on the difficulty to solve the elliptic curve discrete logarithmic problem. However we found that the order of Tawalbeh et al. elliptic curve is not large enough to protect from attacks like Baby Step, Giant Step attack or Pollard's Rho attack. Simulation of the encryption scheme using the elliptic curve parameters proposed by Tawalbeh et al. is carried out. Cryptanalysis has been successfully carried out to extract the private key from the public key and the encrypted image is deciphered revealing the plain image.

1. Introduction

With the rapid growth in Internet and modern information communication technology, multimedia data are easily stored and shared between communication parties. Many researchers have come up with several cryptographic schemes in order to avoid unauthorized access to sensitive multimedia data. Classical encryption scheme such as Rivest–Shamir–Adleman (RSA), Data Encryption Standard (DES) are not effective for large and highly correlated data. Chaotic system, being the most commonly used techniques for encrypting data, many researchers have utilized its properties. The properties include sensitivity to initial conditions and ergodicity to define various encryption schemes. Despite of its benefits in applying to an encryption scheme, there are certain issues that need to address such as small key size and weak security. Many chaos-based encryption schemes [2–6] have already been cryptanalysed by various authors [7–11] respectively. ECC is a strong public key encryption scheme which can provide high security for a given key size compared to other encryption schemes whose difficulty depends on integer factorization or discrete logarithmic problem [12,13]. Detail explanation about ECC, mathematical proofs and applications are given in [14,15]. Various authors have used ECC base encryption scheme for securing multimedia data [16–19]. Hong et al. [20] cryptanalyse the encryption scheme proposed by Ahmed et al. [21] based on hybrid chaotic system and cyclic elliptic curve using known-plaintext attack. In this paper, cryptanalysis of the encryption scheme proposed by Tawalbeh et al. [1] is carried out, revealing the private key from the public key. Using the retrieved private key, the cipher image generated using Tawalbeh et al. encryption scheme is deciphered recovering the plain image transmitted by the sender.

The rest of the paper is organized as: Tawalbeh et al. encryption scheme is explained in Section 2. Section 3 explains the concept of attacks applied on ECC (Naive attack, Baby Step, Giant Step attack and Pollard's Rho attack). The simulation of the cryptanalysis performed on Tawalbeh et al. chosen elliptic curve is shown in Section 4. Conclusion is given in Section 5.

* Corresponding author.
E-mail address: khmotilal@gmail.com (M.S. Khoirom).

https://doi.org/10.1016/j.ijleo.2018.04.068
0030-4026/

2. Tawalbeh et al. multimedia encryption scheme using elliptic curve cryptography

Tawalbeh et al. presented two algorithms for performing encryption of multimedia data based on elliptic curve cryptography using the elliptic curve $E_{53330939}(2, 7) : y^2 = x^3 + 2x + 7 \bmod 53330939$.

2.1. Joint compression and encryption

The source image is divided into 8×8 pixel blocks and Discrete Cosine Transform (DCT) is applied followed by quantization. Out of each 8×8 pixel blocks, only the DC component is processed for encryption using ECC. Each DC component is encoded onto elliptic curve using Koblitz embedding technique where the elliptic curve is given by:

$$E_{53330939}(2, 7) : y^2 = x^3 + 2x + 7 \bmod 53330939 \tag{1}$$

After encoding the DC component into elliptic curve point, ECC is applied to generate the ciphertext K_m.

$$K_m = \{iG, (T_m + iR_B)\} \tag{2}$$

where$G$generator point.$i$random integer in the range of $(1, \eta)$.ηcyclic order of finite elliptic curve for a given Generator G.$T_m$encoded plain message m using Koblitz embedding technique.$R_B$public key of receiver.Each cipher text consists of two points iG and points addition of $T_m + iR_B$. As each point consist of x and y coordinate, the ciphertext consists of four values. These four values are stored in the higher frequency coefficient lower right corner of each block. The DCT coefficients along with the encrypted data constitute the cipher image. The cipher image is transmitted to the receiver.

2.2. Compression-independent encryption

Given a greyscale image, the image is divided along each bit plane b_i, where i ranges from (1 to 8). Bitplane 8 constitute the most significant bits (MSB) and bitplane 1 constitutes the least significant bits (LSB). The higher bits contain most of the significant visual information. To achieve perceptual encryption, only the higher bits are selected for encryption. From a bitplane, 8 bits are grouped to form segments. Each segment is encoded as a point in an elliptic curve $E_{53330939}(2, 7)$ and encrypted to generate four cipher values represented by 32 bits. The cipher values are stored in the LSB bitplane. Each encrypted segment is linked to 4 cipher values each of 32 bits. The 4 cipher values are grouped to form a block of 128 bits. An 8 bits segment can have values ranging from 0 to 255. So, 256 blocks can store all the segments. Block number is stored in place of the original segment.

3. Attacks on elliptic curve discrete logarithmic problem

The strength of ECC relies on the difficulty to solve the elliptic curve discrete logarithmic problem (ECDLP). Given a point R and G such that $R = iG$ where, iG is point multiplication of i and G. It is exponentially difficult to find i given R and G. Here, three attacks associated with ECDLP are explained.

3.1. Naive attack

In naive approach, the adversary tries all the possible values of i until $iG == R$. This approach is practically impossible if the order η of the elliptic curve for a given generator G is very large. There are recommended curves given by organizations like National Institute of Standard and Technology (NIST) [22], Brainpool [23], etc. Using one of the recommended elliptic curve parameters will prevent the naive attack.

3.2. Baby Step, Giant Step

Baby Step, Giant Step (BSGS) was developed by Shank [24]. BSGS requires around $\sqrt{\eta}$ steps and $\sqrt{\eta}$ storage to solve an ECDLP, where η is the cyclic order of an elliptic curve over a finite field. BSGS is performed as follows:

1. Select an integer $i \geq \sqrt{\eta}$ and compute iG.
2. Compute and store a list of jG where, $0 \leq j < i$.
3. Calculate the points $R - kiG$ where, $k = 0, 1, 2, \ldots, i - 1$. For different k values, more then one match may be found from the list of jG.
4. If $jG == R - kiG$, then $l \equiv j + ki \bmod \eta$.
5. If multiple l values are obtained denoted as l_i, counter check l_iG with R_B. If $l_iG == R_B$, then the secret key is l_i.

3.3. Pollard's Rho attack

Pollard's Rho method is a probabilistic approach and it was developed by Pollard [25]. The procedure for Pollard's Rho attack is as follows:

1. Randomly choose α_0 and β_0 and compute $R_0 = \alpha_0 G + \beta_0 R$.
2. Define some σ number of $M_i = \alpha_i G + \beta_i R$ where, α_i and β_i are random integers less than η.
3. Compute $R_{j+1} = f(R_j)$ till a match between R_{j+1} and any precomputed R_j is found. Keep recording how R_j is expressed in term of G and R.
   $f(R_j) = R_j + M_i$
   i in M_i is chosen such that $i = x$-coordinate of R_j mod σ
4. If $R_j = u_j G + v_j R$ and $R_{j+1} = R_j + M_i$, then $R_{j+1} = (u_j + \alpha_i)G + (v_j + \beta_i)R$, so $(u_{j+1}, v_{j+1}) = (u_j, v_j) + (\alpha_i, \beta_i)$. When, $R_{j0} = R_{i0}$ we have,

$$u_{j0}G + v_{j0}R = u_{i0}G + v_{i0}R \quad (3)$$

Hence,

$$(u_{i0} - u_{j0})G = (v_{j0} - v_{i0})R \quad (4)$$

If GCD $(v_{j0} - v_{i0}, \eta) = d$,

$$k \equiv (v_{j0} - v_{i0})^{-1}(u_{i0} - u_{j0}) \bmod \eta/d \quad (5)$$

The above process requires storing of all previous computed R_j. Another approach is to compute pairs (R_i, R_{2i}). This method does not require storing all the pre computed R_j except for the pairs. If $R_i == R_{2i}$, use the coefficient of G and R in R_i and R_{2i} to compute the value of k as given in (5).

4. Simulation

Simulation for cryptnalysis of Tawalbeh et al. multimedia encryption scheme is shown in this section. The simulation was performed on a core i7 processor with 8 GB RAM using Mathematica. The elliptic curve parameters given in Tawalbeh et al. encryption scheme are:

$a = 2$
$b = 7$
$p = 53330939$
$G = (503152, 736)$

Various algorithms are available to find the order of a finite elliptic curve for a given generator G. Hasse's theorem [14] gave an upper and lower bound for the order η of an elliptic curve E_p.

$$p + 1 - 2\sqrt{p} \le \eta \le p + 1 + 2\sqrt{p} \quad (6)$$

On computation, the order of the elliptic curve $E_{53330939}(2, 7)$ was found to be $\eta = 53339460$. The order of the Tawalbeh et al. elliptic curve $E_{53330939}(2, 7)$ is not big enough to provide security. We randomly chose some secret integer $\eta A \in (1, \eta - 1)$ and computed $R_B = \eta AG$. Using R_B and the elliptic curve parameters given by Tawalbeh et al., ηA is solved using naive, BSGS and Pollard's Rho attack. As η is not large enough, applying naive approach can solve the private key ηB in R_B requiring around 138 min.

4.1. Implementing BSGS attack on Tawalbeh et al. elliptic curve parameter

Using the Tawalbeh et al. elliptic curve parameters given in Table 1. We implement BSGS attack to solve ηB from R_B. Following the procedure given in Section 3.2.

Table 1
Elliptic curve parameters.

Parameter	Value
a	2
b	7
p	53330939
G	(503152, 736)
η	53339460
R_B	(31866363, 21842041)

Table 2
Elliptic curve parameters.

Parameter	Value
a	2
b	7
p	53330939
G	(503152, 736)
η	53339460
R_B	(10442931, 9599293)

1. $i = \text{Round}[\sqrt{\eta}] + 1 = 7304$.
2. A list of jG is computed and stored where j ranges from 1 to i.
3. $R_B - kiG$ is computed for k ranging from 1 to $i-1$. $R_B - kiG == jG$ holds true at multiple instances of $\{(k=2404, j=6280), (k=4839, j=860), (k=7273, j=2744)\}$.
4. Using the values from Step 3, the possible ηB values are $\{17565096, 35344916, 53124736\}$ where $\eta B = j + k \times i$.
5. lG is computed with the values obtained in Step 4 and cross checked with the value of R_B. The correct ηB value is obtained as 53124736.

The whole process just took 13.09 s to successfully find the secret value ηB using BSGS attack.

4.2. Implementing Pollard's Rho attack on Tawalbeh et al. elliptic curve parameter

In this section, Pollard's Rho attack is implemented on Tawalbeh et al. elliptic curve parameter, solving ηB from R_B. The parameters are shown in Table 2.

Following the procedure given in Section 3.3.

1. $R_0 = 5G + 20R_B$.
2. For $i = 9$, M_i are set as:
   $M_0 = 69G + 226R_B$
   $M_1 = 396G + 965R_B$
   $M_2 = 2383G + 8006R_B$
   $M_3 = 40710G + 60693R_B$
   $M_4 = 135045G + 458013R_B$
   $M_5 = 779111G + 835994R_B$
   $M_6 = 923726G + 3526012R_B$
   $M_7 = 24491991G + 31418134R_B$
   $M_8 = 37827445G + 47379639R_B$
3. Keeping tract of the coefficient of G and R_B during the random walk, a match was found at:
   $29011122658G + 37917280635R_B = 60461180758G + 78801061911R_B$
   $-31450058100G = 40883781276R_B$
   $d = \text{GCD}(40883781276, 53339460) = 12$
   $\eta/d = 4444955$
   Using Eq. (5), k is computed as: $k \equiv \frac{-31450058100}{40883781276} \bmod 4444955$
   $k = 2337625$.
4. Compute kG and compared with R_B. $kG = (10442931, 9599293) = R_B$.
5. Hence, k = secret key $\eta B = 2337625$.

The whole process took just 0.91 s to find the correct key.

Using naive attack, it is possible to determine the private key for the Tawalbeh et al. elliptic curve parameter, but the time taken is very large compared to BSGS or Pollard's Rho method. So, BSGS or Pollard's Rho attack is used to obtain the private key of the receiver and easily decrypt the cipher data encrypted using Tawalbeh et al. elliptic curve parameter. Security of an encryption scheme depends on the key/keys used. The algorithm will be known to all. Once the original key is obtained, any data encrypted using Tawalbeh et al. encryption scheme can be easily deciphered.

4.3. Cryptanalysis of Tawalbeh et al. encryption scheme

In this section, we generate a cipher image using Tawalbeh et al. join compression and encryption scheme with Tawalbeh et al. elliptic curve parameters. Sample plain images are shown in Fig. 1a–c. Cipher images are shown in Fig. 1d–f. Deciphered images are shown in Figs. 1g–i. The encrypted cipher images contain some concentrated white pixels in each 8×8 which depicts the outline of the original images. This became one of the disadvantages for the scheme. The private keys are derived

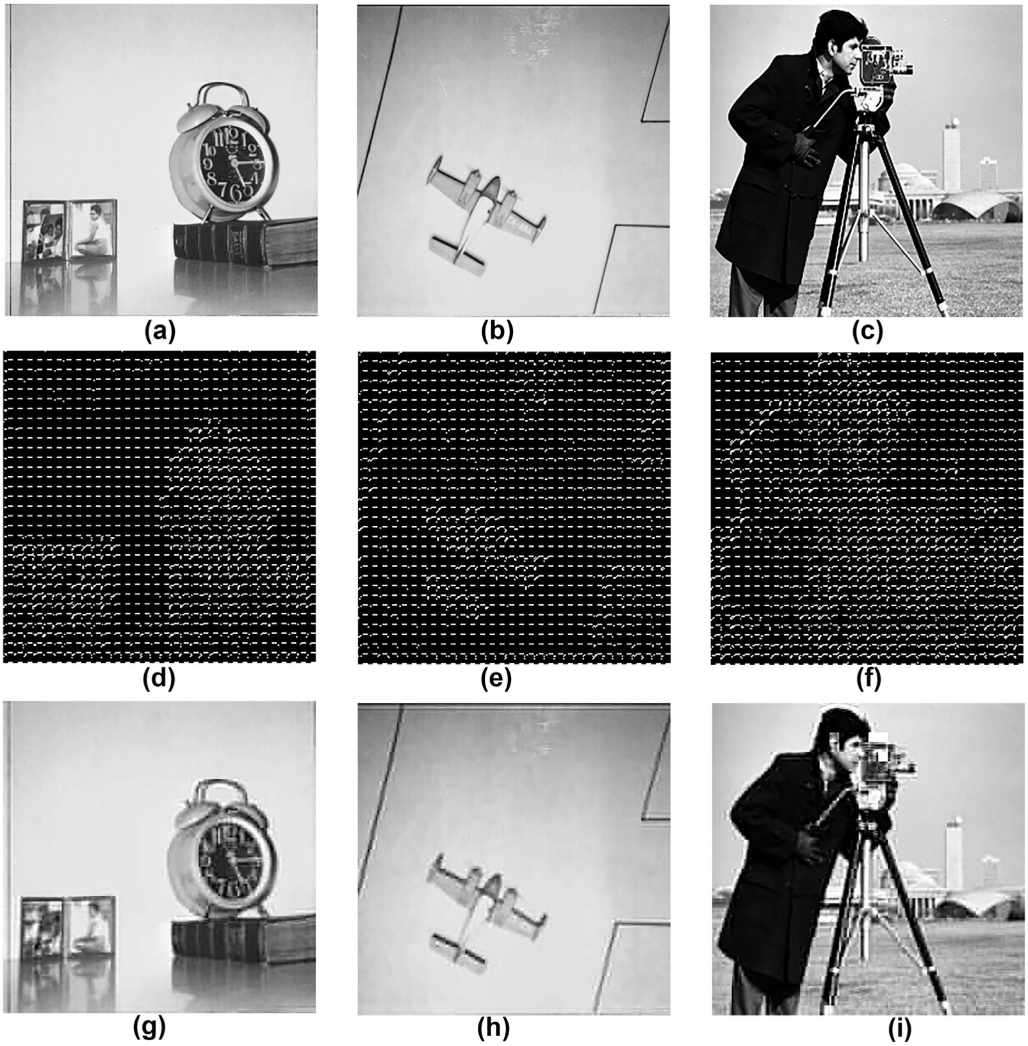

Fig. 1. Images showing simulation for cryptanalysis of Tawalbeh et al. encryption scheme. (a–c) Plain images: clock, airplane and cameraman respectively. (d–f) Encrypted images using public key as (43328336, 28765282), (11459588, 44637139) and (52116656, 32595475) respectively. (g–i) Decrypted images after cryptanalysis of private key (50780860, 45705293 and 1329512) from the corresponding public key.

by solving elliptic curve discrete logarithmic problem using BSGS and Pollard's Rho attack. As some of the AC component of the DCT coefficient are quantised to 0 before encryption, the deciphered image is degraded.

5. Conclusion

The encryption scheme presented by Tawalbeh et al. depends on ECDLP but the parameters chosen for performing the encryption operation has got a small order size η, not large enough to provide efficient security. The BSGS approach took around 13 s and Pollard's Rho attack around 1 s to solve the private key from a given public key. Simulation results of the cryptanalysis of Tawalbeh et al. encryption scheme is presented in this paper. If recommended elliptic curve parameter supplied by organizations like NIST or Brainpool are used then the attack using naive approach, BSGS or Pollard's Rho would be practically infeasible.

References

[1] L. Tawalbeh, M. Moad, A. Walid, Use of elliptic curve cryptography for multimedia encryption, IET Inf. Secur. 7 (2012) 67–74.
[2] Z. Congxu, A novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 29–37.
[3] W. Xingyuan, T. Lin, Q. Xue, A novel colour image encryption algorithm based on chaos, Signal Process. 92 (4) (2012) 1101–1108.
[4] E. Ziba, B. Atieh, An improvement over an image encryption method based on total shuffling, Opt. Commun. 286 (2013) 51–55.
[5] S. Chun-Yan, Q. Yu-Long, Z. Xing-Zhou, An image encryption scheme based on new spatio temporal chaos, Optik 124 (2013) 3329–3334.

[6] K.M. Mrinal, K. Madhumita, K.S. Sandesh, K.B. Vivek, Symmetric key image encryption using chaotic Rossler system, Secur. Commun. Netw. 7 (2014) 2145–2152.
[7] O. Fatih, B.O. Ahmet, Y. Srma, Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, Opt. Commun. 285 (2012) 4946–4948.
[8] T. Guangyou, L. Xiaofeng, X. Tao, Cryptanalysis of a color image encryption algorithm based on chaos, Optik 124 (2013) 5411–5415.
[9] A. Akhavan, A. Samsudin, A. Akhshani, Cryptanalysis of "An improvement over an image encryption method based on total shuffling", Opt. Commun. 350 (2015) 77–82.
[10] B. Rabei, H. Houcemeddine, A.A.E. Ahmed, R. Rhouma, B. Safya, Breaking an image encryption scheme based on a spatiotemporal chaotic system, Signal Process. Image Commun. 39 (2015) 151–158.
[11] L. Dolendro, Kh. Manglem, Cryptanalysis of symmetric key image encryption using chaotic Rossler system, Optik 135 (2017) 200–209.
[12] N. Koblitz, Elliptic curve cryptosystems, Math. Comput. 48 (177) (1987) 203–209.
[13] V. Miller, Use of elliptic curves in cryptography, Advances in Cryptology-CRYPTO'85, 218 (1986) 417–426.
[14] L.C. Washington, Elliptic Curves Number Theory and Cryptography, 2nd ed., CRC Press Taylor & Francis Group, Florida, New York and United Kingdom, 2008.
[15] D. Hankerson, A. Menezes, S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, New York, 2004.
[16] L. Li, A.A.L. Ahmed, N. Xiamu, Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images, Signal Process. 92 (2012) 1069–1078.
[17] K. Manish, I. Akhlad, K. Pranjal, A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography, Signal Process. 125 (2016) 187–202.
[18] S. Behnia, A. Akhavan, A. Akhshani, A. Samsudin, Image encryption based on the Jacobian elliptic maps, J. Syst. Softw. 86 (2013) 2419–2438.
[19] A.A.L. Ahmed, L. Li, X. Niu, A new image encryption scheme based on cyclic elliptic curve and chaotic system, Multimed. Tools Appl. 70 (3) (2014) 1559–1584.
[20] L. Hong, L. Yanbing, Cryptanalysis an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Opt. Laser Technol. 56 (2014) 15–19.
[21] A.A.L. Ahmed, N. Xiamu, A hybrid chaotic system and cyclic elliptic curve for image encryption, Int. J. Electron. Commun. (AE) 67 (2013) 136–143.
[22] NIST elliptic curve, csrc.nist.gov/groups/ST/toolkit/documents/dss/NISTReCur.pdf accessed 19 May 2015.
[23] Elliptic curve parameter, http://www.ecc-brainpool.org/download/Domain-parameters.pdf, accessed 19 May 2015.
[24] D. Shanks, Class number, a theory of factorization, and genera, in: Proc. Sympos. Pure Math., vol. XX, Number Theory Institute, State Univ. New York, Stony Brook, NY, 1969, pp. 415–440.
[25] J.M. Pollard, Monte Carlo methods for index computation (mod p), Math. Comput. 32 (143) (1978) 918–924.