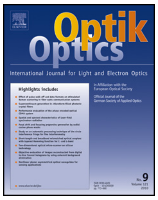
Contents lists available at ScienceDirect

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/© 2018 Elsevier GmbH. All rights reserved.

## 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:

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

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 $(1, \eta)$.$\eta$cyclic 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 $\eta$ 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 $\eta$ 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: