# Implementation of Efficient Hybrid Encryption Based on Elliptic Curve

Ywel Nandi Aung, Khin Ei Ei Chan
*Computer University, (Sittway)*
*ywelnandiaung2010@gmail.com, khineieichan@gmail.com*

## Abstract

*This paper implements an efficient hybrid encryption that combines symmetric key encryption, one time pad (OTP) and asymmetric key encryption, Elliptic Curve Cryptography (ECC). Elliptic Curve Key Establishment Protocol (ECKEP) is used to generate session key. Elliptic Curve Encryption Scheme (ECES) is used to encrypt and decrypt session key. One time pad algorithm has the key distribution problem, but it can operate at the high speed. Elliptic Curve Cryptography is used to encrypt OTP key for key security and to solve key distribution problem. This cryptographic primitive simultaneously performs the functions of both entity authentication and data encryption. This cryptographic primitive provides confidentiality, unforgeability, and non-repudiation for the delivered data simultaneously. It is intended for security intensive applications.*

**Keywords:** ECC, ECES, ECKEP, OTP

## 1. Introduction

Today, encryption-based security services are critical for modern communications. Communication channel, certain security measures, e.g., confidentiality, authenticity, and un-traceability need to be provided. Modern communication techniques, using computers connected through networks, make all data even more vulnerable for various threats. The rapid growth of electronic communication means that issues in information security are of increasing practical importance. Messages exchanged over worldwide publicly accessible computer networks must be kept confidential and protected against manipulation. Modern cryptography provides solutions to all these problems. Essentially, there are two main types of modern crypto systems: symmetric and asymmetric encryption. A public key cryptosystem, unlike a traditional symmetric cryptosystem where the two parties in the communication process have exactly the same key, is an asymmetric cryptosystem where the encryption key is different from the decryption key. The encryption key should be made public so that anyone can use it to send an encrypted message. However, the decryption key should be kept private so that only the intended recipient can decrypt the secret message. The big problem with secret key cryptography is how two parties will share keys. Somehow, in advance of the communication, the secret keys need to be shared. With public key cryptography, this problem doesn't exist. Instead, one party looks up the other's public key and performs encryption. Only the receiver, using its private key, can decrypt the message. Symmetric cryptosystems use the same key for both encryption and decryption and thus require a prior secret key exchange in order to communicate securely in an open communication channel [2].

An authorized receiver should be able to decipher the cryptogram to recover the original plaintext message. An unauthorized receiver, however, must be unable to decrypt the cipher text. Public-key cryptosystems have one main advantage over secret-key cryptosystems: the absence of a key distribution problem. With conventional secret-key cryptography, a single key is used for both enciphering and deciphering. For a sender and receiver to communicate using a secret-key cryptosystem, both must possess the secret key. This leads to the problem of finding a secure way to communicate the secret-key to those who need to use it [9]. In this paper, an efficient hybrid cryptosystem is proposed. A public-key algorithm is used to encrypt a randomly generated encryption key, and the random key is used to encrypt the actual message using a symmetric algorithm. Hybrid cryptosystem uses public key encryption techniques to encrypt a key that is used to encrypt the original message using symmetric key encryption techniques.

Hybrid cryptosystems are very popular in IT related systems. Wireless networks, wired networks and mobile networks also use these systems for security. Hybrid cryptographic systems include developing digital signature systems, computerized voting systems, coin tossing protocols, remote user authentication protocols, protection against creating false messages, etc. Security issues are an important topic in e-commerce. There are many sensitive

financial data and asset data in e-commerce databases, such as transaction records, commercial transactions, user account, and market scheme and so on.

## 2. Related Works

ECC is already used today is the Berlin-Boon information network, which transfers highly confidential data between German government organizations. ECC is also part of the cryptography on the new German biometric passport introduced in 2005, and the new German electronic identity card, which will be used from 2010. Austria has also massively launched ECC: the so-called "e-card", banks and health care system. ECC is also used in a number of devices such as navigation systems, electricity and gas meters, and electronic scales [3].

One Time Pad cryptographic technique becomes popular due to its strong security. Soviet spies in the USA used one-time pads to communicate with their controllers, usually located inside Russian embassies and consulates. Not a single message was cracked by the FBI or NSA. And none of those messages ever will be cracked. The one-time pad system is still being used today by intelligence agencies like Britain's MI.6, Germany's BND, France's DGSE, Russia's MBRF, and China's Cheng Pao K'o. One-time pads are also being used by resistance groups like Northern Ireland's IRA, France's Action Direct, Uruguay's Tupamaros, Algeria's GIA, Lebanon's Hezbollah, Peru's Shining Path, and Argentina's Monteneros [5].

## 3. Elliptic Curve Cryptography (ECC)

Elliptic curves are not ellipses. ECC is an encryption system that uses the properties of elliptic curves to provide the same functionality of other public-key cryptosystems such as encryption, key agreements, and digital signatures. It is a public key cryptography. It has three basic algorithms, namely, ECES, elliptic curve signature schemes (ECSSs) and ECKEP. ECSSs have two algorithms, namely, elliptic curve signature scheme (ECSS), elliptic curve digital signature algorithm (ECDSA) [6]. In this paper, ECES and ECKEP algorithms are used.

Elliptic curve cryptography can operate in two finite fields, the prime field and the binary field. In this paper, the prime field is used. The equation of the elliptic curve on a prime field $F_p$ is $y^2 \bmod p = x^3 + ax + b \bmod p$ where $4a^3 + 27b^2 \bmod p \neq 0$. Each value of the 'a' and 'b' gives a different elliptic curve. All points (x, y) which satisfy the above equation and a point at infinity lies on the elliptic curve.

To use elliptic curve algorithms, required domain parameters or constants must be defined. The domain parameters for elliptic curve over prime field $F_p$ are **p, a, b, G, n** and **h.** p is the prime number defined for finite field $F_p$, a and b are the parameters defining the curve $y^2 \bmod p = x^3 + ax + b \bmod p$. G is the base point $(x_G, y_G)$, a point on the elliptic curve chosen for cryptographic operations. n is the order of the base point. h is the cofactor where h = #E(Fp) is the number of points on an elliptic curve. Each user requires two keys, private and public key. Private key is a random integer and public key is a point. The public key is obtained by multiplying the private key with the base point G. All operation performed in ECC use addition of point, doubling of point, multiplication of point methods and finite field arithmetic methods [7] [10].

### 3.1. ECES Algorithm

Encryption Process: Each entity, sender, performs the following steps:

1. Look up receiver's public key: Q.
2. Represent the message M as a pair of field elements (m1, m2).
3. Select a random integer k in the range [1, n - 1].
4. Compute the point (x1, y1):= kP.
5. Compute the point (x2, y2):= kQ.
6. Combine the field elements m1, m2 and x2 in a predetermined manner to obtain two field elements c1 and c2.
7. Transmit the data c: = (x1, y1, c1, c2) to receiver.

Decryption Process: Receiver decrypts cipher text, c = (x1, y1, c1, c2) received from sender. Receiver performs the following steps:

1. Compute the point (x2, y2):= d(x1, y1), using its private key d.
2. Recover the message m1 and m2 from c1, c2 and x2 [10].

In this paper, this algorithm is used to encrypt and decrypt session key for strong security.

### 3.3. ECKEP Algorithm

This section describes a protocol whereby two parties A and B establish a shared secret key K called the session key. The session key may subsequently used to achieve some cryptographic goal, such as privacy or authentication.

System Setup: It is assumed that A and B are using the same elliptic curve parameters $F_q$, E, P and n. A has private key a and public key QA = aP = (xA, yA). B has private key b and public key QB = bP = (xB, yB).

1. Entity A does the following:
   - Select a random integer kA, $1 \leq kA \leq n - 1$.
   - Compute the point RA: = kAP.

- Compute the point (x1, y1): = kAQB.
- Compute the integer sA: = kA + axAx1 mod n.
- A sends RA to B.

2. Entity B does the following:
   - Select a random integer kB, $1 \leq kB \leq n - 1$.
   - Compute the point RB: = kBP.
   - Compute the point (x2, y2): = kBQA.
   - Compute the integer sB: = kB + bxBx2 mod n.
   - B sends RB to A.
3. A does the following:
   - Compute (x2, y2): = aRB.
   - Compute the session key K: = sA(RB + xBx2QB).
4. B does the following:
   - Compute (x1, y1): = bRA.
   - Compute the session key K: = sB(RA + xAx1QA) [10].

The session key for both users must be same.

## 4. One Time Pad

The message is represented as a binary string (a sequence of 0's and 1's) using a coding mechanism such as ASCII coding. The key is a truly random sequence of 0's and 1's of the same length as the message. The encryption is done by adding the key to the message modulo 2, bit by bit. This process is often called exclusive or, and is denoted by XOR. The symbol $\oplus$ is used.

One-time pad is a very simple yet completely unbreakable symmetric cipher. The key for a one-time pad cipher is a string of random bits, usually generated by a cryptographically strong pseudo-random number generator. With a one-time pad, there are as many bits in the key as in the plaintext [5].

In this paper, one time pad is used for data encryption and session key is used as key for one time pad.

## 5. Pseudo Random Number Generator

A pseudorandom number generator (PRNG), also known as a deterministic random bit generator (DRBG), is an algorithm for generating a sequence of numbers that approximates the properties of random numbers. Common classes of these algorithms are linear congruential generators, Lagged Fibonacci generators, linear feedback shift registers, feedback with carry shift registers, and generalized feedback shift registers. Recent instances of pseudorandom algorithms include Blum Blum Shub, Fortuna, and the Mersenne twister.

The security of most cryptographic algorithms and protocols using PRNGs is based on the assumption that it is infeasible to distinguish use of a suitable PRNG from use of a truly random sequence. The simplest examples of this dependency are stream ciphers, which (most often) work by exclusive or-ing the plaintext of a message with the output of a PRNG, producing cipher text [8].

In this paper, a linear feedback shift register is used to produce random sequence. The input to the PRNG is session key. The outputs of the PRNG are use as key for one time pad.

## 6. Procedure of Hybrid Cryptosystem

First, every user must define required system setup and parameters. Each user must have a public key and private key. For each user who wants to encrypt data must do the following steps.

1. Obtains receiver's public key.
2. Inputs are message (data), its public key, private key and receiver's public key.
3. To calculate the session key, ECKEP algorithm is used.
4. Data is encrypted with one time pad by using session key. Cipher text is obtained.
5. Session key is encrypted with ECES by using receiver's public key. Cipher key is obtained.
6. Both cipher text and cipher key send to receiver.

To decrypt, each user must do the following steps.

1. Obtains sender's public key.
2. Inputs are its private key, public key and sender's public key.
3. Calculate the session key.
4. Decrypt cipher key with ECKEP algorithm by using its private key. Sender's session key will be obtained.
5. Compare two session keys. If same, sender is valid. If not, invalid sender.
6. Decrypt cipher text with one time pad technique by using session key. Original data will be obtained.

## 7. Sequence of Operation

Each entity must do the following steps for encryption and decryption. Parameters of the system must be predefined. For encryption, user inputs are message, user's public key, user's private key and receiver's public key. Cipher text and cipher key will obtain after encryption process. Both them send to another user. Figure 1 shows encryption process of the system.

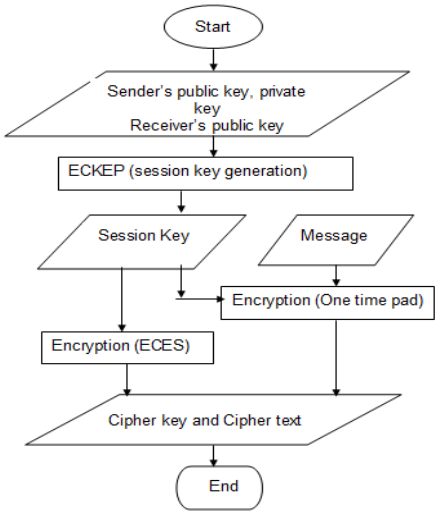


**Figure 1. System Flow Diagram for Encryption**

Figure 2 shows the decryption process of the system. User inputs are user's private, user's public key and another user's (who encrypts this message) public key. Calculate the user's session key and recover another user's session key from the cipher key, and then, compare these two keys. If these two keys are same, then the sender is valid and if not, it is an invalid sender. So the message should not be accepted.

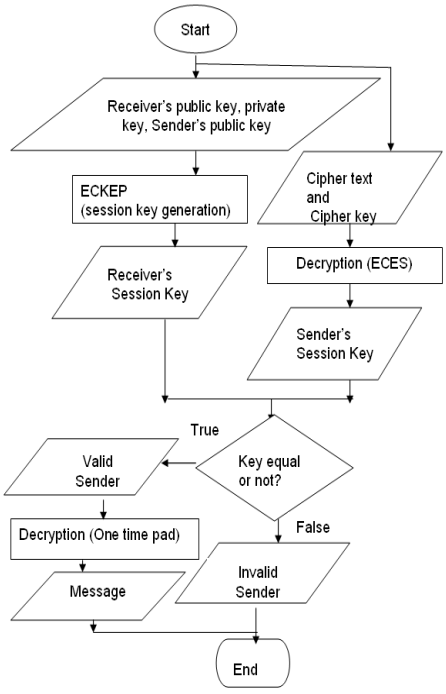


**Figure 2. System Flow Diagram for Decryption**

## 8. Conclusion

Using hybrid encryption technology can give full play to the respective advantages of two kinds of encryption algorithm and provides more reliable and efficient security for computerized systems. This system can provide strong security in data encryption. The hybrid encryption technology used in this paper can also be used to enhance the security of other network databases. This system can save time, memory and power requirements because it uses smaller key size than other cryptographic systems. Although key size is small, security is high. Using session key, it can give strong security and authentication. It is more suitable for small devices with limited memory and power, for example, mobile phone systems.

This system is implemented by C#2008 programming language. According to the encryption and decryption results, processing time is depends on hardware devices, e.g, processor speed and also depends on choosing system parameters. At 3.6 GHz processor, 50KB of data takes 1 min, 30KB takes 20 sec, 12KB takes 3sec etc and at 2.6 GHz processor, 50KB of data takes 2 min, 30KB takes 30 sec, 12KB takes 5 sec etc, for each time of encryption or decryption. These results obtain by choosing 2 digit system parameters. If we choose very large system parameters, the processing time is more longer than small parameters. This system can only encrypt text message. If the file size is larger than 50Kbytes, then the encryption speed will be slow. It is efficient for authentication.

## 9. References


[1] A.Knapp, Elliptic Curves Mathematical Notes 40, Princeton University, 1992.

[2] A.J. Menezes, P.C.ven Oorschot; S.A.Vanstone (1997). Handbook of Applied Cryptography.

[3] B.A. Forouzan, "Cryptography and Network Security", International Edition, 2008.

[4] J.Katz, Y.Lindell (2007), Introduction to Modem Cryptography.

[5] J.Lopez and R.Dahab. An Overview of Elliptic Curve Cryptography, May 2000.

[6] M.Brown, D.Hankerson, J.Lopez, A.Menezes, Software Implementation of the NIST Elliptic. Curves Over Prime Fields, 2001,Available at http://citeseer.ist.psu.edu/brown01software.html.

[7] Manuel Mogollon, CyberTech Publishing Cryptography and Security Mechanisms.

[8] R.A,Millin, "An Introduction to Cryptography",Chapman and Hall,2007.

[9] Schneier,Burce. "One Time Pads"http://www.schneier.com/crypto-gram 0210,html#7.

[10] V.Miller, "Uses of elliptic Curve in Cryptography", Advances in Cryptology-CRYPTO '85, Lecture Notes in Computer Science.