Pairing Based Elliptic Curve Cryptosystem for Message Authentication

T.Punitha\textsuperscript{1}
\textsuperscript{1}Sethu Institute of technology, Computer Science & Engineering, tpunitha.cse@gmail.com

M.Sindhu\textsuperscript{2}
\textsuperscript{2}Sethu Institute of Technology, Computer Science & Engineering, Sindhuces18@gmail.com

Abstract— Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. Recently the bilinear pairing such as Weil Pairing or Tate Pairing on elliptic curves and hyper elliptic curves has been found various applications in cryptography. Several identity-based cryptosystems using bilinear pairings of elliptic curves or hyper elliptic curves were presented. Blind signature and ring signature are very useful to provide the user’s anonymity and the signer’s privacy. The proposed method focuses an ID-based ring signature scheme which is based on the pairings with elliptic curve cryptography. The proposed method is used to reduce the number of computation of the pairing for the verification of the id based signature and also decoding of the id based public key cryptosystems with authentication by factor of 2.

Index Terms— Asymmetric Cryptography, Bilinear pairing, Elliptic Curve, Elliptic Curve CryptoSystem(ECC), Secure ID based signature.

1 INTRODUCTION

ECC is a public key encryption technique based on the theory of elliptic curves [1]. It can be used to create faster, smaller and more efficient cryptographic keys. And also it generates keys through the properties of the elliptic curve equation rather than the traditional method of generation, as the product of very large prime numbers [2]. This technology can be used in conjunction with most of the public key encryption methods such as RSA and Diffie-Hellman. ECC can yield a level of security with a 224-bit keys compared with other systems that require a 2,048-bit keys. ECC provides features such as security and computational efficiency [3]. The security of ECC depends on the difficulty of solving the elliptic curve logarithm problem.

Cryptography was used to assure only secrecy. Wax seals, signatures, and other physical mechanisms were typically used to assure integrity of the media and authenticity of the sender. With the advent of electronic funds transfer, the applications of cryptography for integrity began to surpass its use for secrecy [4]. The problem with proving properties of protocols under other schemes is that the mathematics is extremely complex for the RSA, and there is no sound mathematical basis for the DES [5].

Public key cryptosystems are constructed by relying on the hardness of mathematical problem. RSA based on Integer Factorization Problem and DH based on the Discrete Logarithm Problem [6]. The main problem of conventional Public key Cryptosystems is that the Key size has to be sufficiently large in order to meet the high level security requirement, resulting in lower speed and consumption of more bandwidth [7].

The basic concept of cryptography is very simple. In a typical cryptographic exchange, information that is meant to be hidden for whatever reason is encrypted, or ciphered into a difficult-to-interpret form. This is called conversion, encryption because it involves the change of clear text, or understandable data, into cipher text, or difficult-to-interpret data. The encryption process is one-half of the entire cryptographic exchange [8].

At the other end of the process is decryption, or the conversion of cipher text into clear text. Decryption is not always a part of encryption, however – some algorithms are called “hashes” as they only apply encryption (that is, from clear to cipher text) and have no means of deciphering the information. However, most cryptographic algorithms can theoretically be cracked, but require extraordinary amounts of computational power to do so.

A safety message authentication scheme networks using an ID-based signature and verification mechanism. An ID-based technique offers a certificate-less public key verification, while a proxy signature provides flexibilities in message authentication and trust management [1]. Message authentication, to ensure the receiving message is true and coming from the claimed source, the traditional PKI security schemes are not suitable for VANET [9]. Aiding of roadside unit (RSU) make message authentication in VANET easily, but it is still embedded some problems: how to authenticate the message transmitted from different RSU range, and to process the vehicle's message hand-off among the different RSU communication range. A comprehensive message authentication
scheme which enables the message authentication in intra and inter RSU range, and the hand-off within the different RSUs. The proposed scheme makes the balance in the overhead of computations and communication, and the security against the attacking. The results of efficiency analysis and comparison with the related works show the proposed scheme is a superior message authentication method in VANET [10].

The most important research challenge is the authentication of VANET messages with less communication as well as storage overhead. So, Elliptic Curve Cryptography has chosen.

2 PROPOSED METHODOLOGY

The overall concept is explained through the flow diagram as shown in the figure 1.

![Fig. 1. Flow diagram of the proposed Methodology](image)

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers [13]. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications.

A. Elliptic Curve

An Elliptic Curve can be described as the set of solutions of an equation of the form \( Y^2 = x^3 + ax + b \) over some field[4]. The importance of elliptic curves is its rich structure.

B. Elliptic Curve Cryptosystem

The system based on the elliptic curve is called Elliptic curve cryptosystem. To form a cryptosystem, generally a set of three algorithms is required:

1. Key-generation: An algorithm for generating an encryption/decryption key.
2. Encryption: An algorithm for encrypting plain texts.

In traditional symmetric or private-key cryptography, the generated key is used for both encryption and decryption, with the consequence that anybody that possesses the key is able to en- and decrypt messages. To ensure confidentiality, the key has to be kept secret between communication partners [17].

C. Elliptic Curve Parameters

The most important thing defines all the elements in the elliptic curve before used by all the parties. That is called as the domain parameters of the scheme. Let \( p \) be the field in the prime case and the pair \( (m, f) \) in the binary case. The elliptic curve is defined by the constants \( a \) and \( b \) use in elliptic curve equation. And the order of \( G \), be the smallest non-negative number \( n \) such that \( nG=\infty \), it is prime. Since is the size of a subgroup of \( E(F_p) \) follows from Lagrange's theorem that the number \( H=|E(F_p)| \) is an integer. In cryptographic applications \( h \), called the cofactor, must be small \((H \leq)\) and, preferably \( h=1 \). The prime case the domain parameters are \((p, a, b, N, g, h) \) and in the binary case they are \((M, P, a, b, n, G, h) \) [11].

Several classes of curves are weak and should be avoided: Curves over \( F_{2^m} \) non-prime \( m \) are vulnerable to Weil descent attacks. Curves such that \( n \) divides \( p^n+1 \) where \( p \) is the characteristic of the field – \( q \) for a prime field, or 2 for a binary field] for sufficiently small \( B \) are vulnerable to Menezes-Okamoto-Vanstone (MOV) attack which applies usual Discrete Logarithm Problem (DLP) on a small degree extension field of \( F_q \) to solve ECDLP [12]. Curves such that \( E(F_q) \) are vulnerable to the attack that maps the points on the curve to the additive group of \( F_q \).

D. Key Sizes

ECC achieves the security level with smaller keys. Key length is most important feature in Elliptic Curve Cryptography. For example, for 80-bit security one needs a curve over \( F_2^{160} \), where \( Q=2^{160} \). This can be contrasted with finite-field cryptography (e.g., DSA) which requires 3072-bit public keys and 160-bit private keys, and integer factorization cryptography (e.g., RSA) which requires a 1024-bit value of \( n \), where the private key should be just as large.

E. Asymmetric Data Encryption

Group manager distributes and efficiently allocates the public keys and authenticate by using the ECC authentication mechanism. The Group owner's file has been applied security. The confidentiality of this transformation is data in theory secure; we will simply give the safety via the cryptography formula named as ECC [15]. Since client files are stored in the server, they have lesser security options. For crypto process we use the ECC algorithm for the encryption and decryption process.

F. Asymmetric Data Decryption

Using the ECC algorithm file is converted as crypto files. In order to get view the original content of the files, the encrypted files should be decrypted. Each and every encrypted file should be decrypted. Using Respective Private keys, files are decrypted using the ECC Key Generator Decryption process is done by ECC Algorithm, Since ECC has 166 key lengths it executes faster and...
more secured algorithm than RSA [16]. Our methodology gives the results using ECC based algorithm, such as public key encryption for sending the keys to co-distributors and secret key encryption for further distribution of key.

G. Pairing

Pairing-based cryptography is used to pair two cryptographic groups to a third group to construct cryptographic systems [17]. If the same group is used for the first two groups, the pairing is called symmetric and is a mapping from two elements of one group to an element from a second group [3]. In this way, pairings can be used to reduce a hard problem in one group to a different, usually an easier problem in another group.

3 RESULTS AND DISCUSSION

The NetBeans IDE is a reusable framework that is used to simplify the Java desktop applications developments. NetBeans visual libraries are used. The additional SDK is required.

Installation of modules can be performed dynamically. It also includes the features such as memory management, user setting management, storage management.

The result shown in figure 2 and 3 describes message creation and its corresponding Key pair generated by using Elliptic Curve Cryptosystem.

Fig 2: Message Creation

Fig 3 : ECC Key Pair Generation

Fig 4: ECC Encryption

Fig 5: ECC Decryption

Fig.4. Shown the encrypted message of the given message. Fig.5. Shown the decrypted message of the given encrypted format of the message and finally we got an original message. From the result, Message authentication be achieved by Elliptic Curve Cryptosystem.

4 CONCLUSION

The developed method has to provide an efficient method for a class of ID based cryptosystem using Elliptic Curve Cryptography (ECC). The proposed method focuses an ID-based ring signature scheme which is based on the pairings with elliptic curve cryptography. Also, we analyze their security and efficiency. The pairing on elliptic curves is applied for secure id based cryptography. The proposed method is used to reduce the number of computations of the pairing for the verification of the id based signature and also decoding of the id based public key cryptosystems with authentication by factor of 2.

Elliptic Curve Cryptography (ECC) will be applied in the Vehicular Ad hoc Network (VANET). Hash function is going to use to verify the messages exchanged with the VANET environment. This will be helpful to achieve message authentication.
ACKNOWLEDGMENT

I would like to express my special thanks of gratitude to my college management. In addition, I would also like to thank my parents who helped me a lot in finalizing this project within the limited time frame.

REFERENCES


