ANALYSIS OF ELLIPTIC KEY ALGORITHMS

S. Nithya, Dr. E. George Dharma Prakash Raj

Abstract— **The secure communications includes key exchange and signatures which is required for public key like RSA, DSA and Elliptic Curve Cryptography (ECC). Elliptic Curve Cryptography is a branch of cryptography that can be used for encrypting data, generating digital signatures or exchanging keying material during the initial phases of a secure communication. In wireless devices the dependency has been increased for security purpose on to do secure Web browsing, secure email and virtual private networking to corporate networks, Integrated Encryption Scheme (IES). In this paper, the elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is a hybrid scheme that uses a public key system to transport a session key for the use of symmetric cipher. It generates a random number for public key generation and enhances security for public key generation by converting the public key into a cipher text. Hence, on compromising the public key will lead to identify the encrypted data.**

I. Introduction

Cryptography

Cryptography is a cornerstone of the modern electronic security technologies used today to protect valuable information resources on intranets, extranets, and the internet. Cryptography is the science of providing security for information.

The objective of cryptography-based security is to protect information resources by making unauthorized acquisition of the information or tampering with the information more costly than the potential value that might be gained. Because the value of information usually decreases over time, good cryptography-based security protects information until its value is significantly less than the cost of illicit attempts to obtain or tamper with the information. Good cryptography, when properly implemented and used, makes attempts to violate security cost-prohibitive. Another objective of all information security systems, including cryptography-based security systems, is to protect information resources at less cost than the value of the information that is being protected. A cryptography-based security system must provide information security at acceptable costs. Determining acceptable costs involves weighing the cost of the security versus the benefits of the security.

Encryption

A process of the original message into an unreadable from is known as Encryption. A process of converting Plain Text into Cipher Text is called as Encryption. Cryptography uses the encryption technique to send the confidential information over a channel. The process of encryption requires two things- an encryption algorithm and a key. An encryption algorithm means the technique that has been used in encryption. Encryption takes place at the sender side. Encryption Algorithm is used to make content unreadable by all but the intended receivers. Encrypt (plaintext, key) = ciphertext. Decrypt (cipher text, key) = plaintext.

Decryption

A reverse process of encryption is called as Decryption. It is a process of converting Cipher Text into Plain Text. Cryptography uses the decryption technique at the receiver side to obtain the original message from non readable message (Cipher Text). The process of decryption requires two things- a Decryption algorithm and a key. A Decryption algorithm means the technique that has been used in Decryption. Generally the encryption and decryption algorithm are same.

Security Functions of Cryptography

Cryptography is most often associated with the confidentiality of information that it provides. However, cryptography can offer the following four basic functions:

Confidentiality: Assurance that only authorized users can read or use confidential information. For example, unauthorized users might be able to intercept information, but the information is transmitted and stored as cipher text and is useless without a decoding key that is known only to authorize users.

Authentication: Verification of the identity of the entities that communicate over the network. For example, online entities can choose to trust communications with other online entities based on the other entities ownership of valid digital authentication credentials.

Integrity: Verification that the original contents of information has not been altered or corrupted. Without integrity, someone might alter information or information might become corrupted, and the alteration could be undetected. For example, an intruder might covertly alter a file, but change the unique digital thumbprint for the file, causing other users to detect the tampering by comparing the changed digital thumbprint to the digital thumbprint for the original contents.

Non-repudiation: Assurance that a party in a communication cannot falsely deny that a part of the actual communication occurred. Without non-repudiation, someone can communicate and then later either falsely deny the communications entirely or claim that it occurred at a different time. For example, without non-repudiation, an originator of information might falsely deny being the originator of that information. Likewise, without non-repudiation, the recipient of a communication might falsely deny having received the communication.

TYPES OF CRYPTOGRAPHIC ALGORITHMS

There are several ways of classifying cryptographic algorithms. In this paper, they will be categorized based on the number of keys that are employed for encryption and decryption.

The three types of algorithms are:

1) Secret Key (Symmetric) Cryptography (SKC): Uses a single key for both encryption and decryption.

2) Public Key (Asymmetric) Cryptography (PKC): Uses one key for encryption and another for decryption.

3) Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.

II. RELATED WORK

Elliptic Curve Cryptography (ECC) is a public key cryptography. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication. Some public key algorithm may require a set of predefined constants to be known by all the devices taking part in the communication. ‘Domain parameters’ in ECC is an example of such constants. Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but it is much slower than the private key cryptography.

“Elliptic Curve Cryptography in securing networks by mobile authentication”, Manoj Prabhakar, International Journal on Cryptography and Information Security, September 2013. [1]

It proposes an enhanced authentication model, which is suitable for low-power mobile devices. It uses an Extended Password Key Exchange Protocols and elliptic-curve-cryptosystem based trust delegation mechanism to generate a delegation pass code for mobile station authentication, and it can effectively defend all known attacks to mobile networks including the denial-of-service attack. Moreover, the mobile station only needs to receive one message and send one message to authenticate itself to a visitor’s location register, and the model only requires a single elliptic-curve scalar point multiplication on a mobile device. Therefore, this model enjoys both computation efficiency and communication efficiency as compared to known mobile authentication models.

“Prospective utilization of Elliptic Curve Cryptography for security enhancement”, Sonali Nimbhorkar and Dr. L. G. Malik, International Journal of Application or Innovation in Engineering and Management, January 2013. [2]

Elliptic curve cryptography (ECC) is the most efficient public key encryption scheme based on elliptic curve concepts that can be used to create faster, smaller, and efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the conventional method of key generation. This scheme can be used with public key encryption methods, such as RSA, and Diffie-Hellman key exchange Digital Signature. This paper presents potential use of elliptic curve cryptography for communication network.

“Effective implementations of GF (p) Elliptic Curve Cryptography computations using parallelism”, N. Sivasankari and M. Kannan, International Journal of Emerging Technology and Advanced Engineering, November 2013. [3]

It aims at analyzing the impact of parallelism available in two common Elliptic Curve Cryptography (ECC) projective forms on speed and cost factors. The time consuming multiplication is implemented with m-ary algorithm. Using scalable multipliers for various key sizes. To implement large bit-length multiplications we used a novel partitioning and pipeline folding scheme to fit at least 256-bit modular multiplications on a single Xilinx FPGA. Comparisons to several other schemes are presented. That is by analyzing the impact of using the *m*-ary algorithm as an alternative to the binary algorithm to implement ECC multiplication operations in projective form. The *m*-ary algorithm over the binary algorithm and speed-up factors can be doubled.

“Achieving authentication and integrity using Elliptic Curve Cryptography architecture”, Ms. Manali Dubal and Ms. Aaradhana Deshmukh, International Journal of Computer Applications, May 2013. [4]

Communication security is one of the areas where research is highly required. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system. This research is all about securing the messages or data that is being communicated among two parties. The recent branch of Network security is

Cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public-key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards. The key establishment protocol is Elliptic Curve MQV, with implicit certificates and symmetric key cryptographic techniques. The research focuses on achieving secrecy using ECIES algorithm for encryption, and authentication using Hashing technique. The hashed plaintext is again encrypted with RSA. At the receiver end, the hashed text is decrypted first. The hash value of the plaintext decrypted is compared with the latter hash. If they are found equal, the integrity can also be assured. The parameters to considered choosing Elliptic Curves are presented in NIST document of recommended elliptic curves.

"Comprehensive security system for mobile network using Elliptic Curve Cryptography over GF (p)", Lokesh Giripunje and Sonali Nimbhorkar, International Journal of Advanced Research in Computer Science and Software Engineering, May 2013. [5]

Mobile devices have many differences in their capabilities, computational powers and security requirements. Mobile devices can be used as the enabling technology for accessing Internet based services, as well as for personal communication needs in networking environments. Mobile services are spread throughout the wireless network and are one of the crucial components needed for various applications and services. However, the security of mobile communication has topped the list of concerns for mobile phone users. Confidentiality, Authentication, Integrity and Non-repudiation are required security services for mobile communication. Currently available network security mechanisms are inadequate; hence there is a greater demand to provide a more flexible, reconfigurable, and scalable security mechanism. This project provides effective security solution using Public key cryptography. The implementation of this project is divided into two parts first, design of API for ECC (Elliptic Curve Cryptography) which generates shared secret key required for secure communication and secondly, a web service is created which distributes this key to validate mobile user.

"An Efficient SDRP with Elliptic Curve Integrated Encryption Scheme", Ruchika Markan and Gurvinder Kaur, International Journal of Advanced Research in Computer Science and Software Engineering, November 2013. [6]

Wireless reprogramming in a wireless sensor network (WSN) is the process of propagating a new code image or relevant commands to sensor nodes. As a WSN is usually deployed in hostile environments, so for security reasons every code update must be authenticated to prevent an adversary from installing malicious code in the network. The reprogramming protocols based on the distributed reprogramming approach allow multiple authorized network users to simultaneously and directly reprogram sensor nodes without involving the base station. SDRP is the first distributed reprogramming protocol. In this research Elliptic Curve Integrated Encryption Scheme is used for providing strong security to sensor network. Only authorized users will be allowed to update the system reprogramming and with according to privileges carried by user, system upgrade options will be provided. User privilege and identity will be checked with signature of the message. For managing privacy preservation between owner and other user's different session keys for owner and users are introduced so that both can have different views of network and can also preserve their privacy from each other.

"Literature survey on Elliptic Curve Encryption Techniques", Ruchika Markan and Gurvinder Kaur, International Journal of Advanced Research in Computer Science and Software Engineering, September 2013. [7]

It is preventing unauthorized access to corporate information systems is essential for many organizations. Communication security is one of the major areas of interest. The data used in communication is very sensitive and needs to be protected and made abstract from intruders of system. The recent branch of network security is cryptography using Elliptic Curve Architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public key based mechanisms that provide encryption, digital signatures and key exchange algorithms. The best known encryption scheme is the Elliptic Curve Integrated Encryption Scheme (ECIES) which is included in IEEE and also in SECG SEC 1 standards.

"Survey: Elliptic Curve Cryptography using scalar multiplication algorithms", Kaalidoss Rajamani and Dr. A. Arul L. S, International Journal of Innovative Research in Advanced Engineering, March 2014. [8]

Stopping unauthorized access to corporate information systems is crucial for many organizations. In which communication security is playing one of the key areas of interest to protect the sensitive/valuable data. The data used in communication is very sensitive or valuable and needs to be protected and made abstract from intruders of system or over the network. The recent way to provide precious security mechanism of network security is cryptography using Elliptic Curve architectures which is based on the arithmetic of elliptic curves and discrete logarithmic problems. ECC schemes are public key based mechanisms that provide cipher text (encryption), digital signatures and key exchange algorithms. The most crucial operation in the cryptosystem is the scalar multiplication operation. In this paper, has studies various scalar multiplication algorithms with respect to the efficiency, weight and features etc and also gives an idea about algorithms and the areas where is the need to researchers can proceed further in the computation of cryptosystem

"An efficient implementation for key management technique using smart card and ECIES cryptography", Neha Gupta, Harsh kumar Singh, Anurag Jain, International Journal of Control Theory and Computer Modeling, November 2013. [9]

An Elliptic curve cryptosystem are become popular because of the reduced number of keys bits required in comparison to other cryptosystem. In existing work ECC technique are used to describe the encryption data to provide a security over a network. ECC satisfy the smart cards requirements in term of memory, processing and cost. In existing work ECC cryptographic algorithm works with a smart card technique. Many existing approaches work with smart card with various techniques and produce a better efficient result. In this paper, defines a smart card technique using a ECIES cryptographic algorithm. So the technique key management using smart card and ECIES. ECC basically based on a discrete logarithm over appoint on an elliptic curve. The ECIES is standard elliptic curve that is totally based on encryption algorithm.

"Review on secure and distributed reprogramming protocol", Ruchika Markan and Gurvinder Kaur, International Journal of Engineering and Computer Science, August 2013. [10]

Wireless reprogramming is very important in sensor networks. Reprogramming is defined as the process of loading a new code image or relevant commands to sensor nodes. For security reasons every code update must be authenticated to prevent an attacker from installing malicious scripts in the network. A number of protocols have been defined for reprogramming the wireless sensor networks. SDRP is the first distributed reprogramming protocol in which multiple authorized network users can simultaneously and directly reprogram sensor nodes without involving the base station. The protocol uses identity-based cryptography to secure the reprogramming and to reduce the communication and storage requirements of each node. Preserving data privacy is a challenging problem in wireless sensor networks. On comparison, Elliptic Curve Integrated Encryption Scheme (ECIES) provides great solution for security and authorization in the sensor network.

III. PROPOSED WORK

Elliptic Curve Integrated Encryption System (ECIES)

Integrated Encryption Scheme (IES) is a hybrid encryption scheme which provides semantic security against an adversary who is allowed to use chosen-plaintext and chosen-ciphertext attacks. The security of the scheme is based on the Diffie–Hellman problem. The elliptic curve integrated encryption system (ECIES) is the standard elliptic curve based on encryption algorithm. It is called integrated, since it is a hybrid scheme that uses a public key system to transport a session key for use by a symmetric cipher. ECIES is a public-key encryption algorithm.

ECIES is an integrated encryption scheme based on elliptic curves that includes public key operations, encryption algorithms, authentication codes and hash computations. More precisely, ECIES is the generic term used to identify a set of slightly different encryption schemes. The encryption scheme DHIES (Diffie Hellman Integrated Encryption Scheme) which represents the kernel of ECIES. The Random number for the public key generation seems to be unsecure. Since, we can easily identify the key for the encrypted data.

It provides a security for the random number generation in order to secure the key values. The key generation is process is quite normal for one or two elliptical curves. Since there occur a mathematical complexity in key generation if it goes for more than three or four elliptical curves used for encryption. The key size is small when compared to existing recent algorithm. The Key generation is faster because of the key size is small.

To send an encrypted message to Bob using ECIES Alice needs the following information:

- ➢ cryptographic suite to be used:
  - KDF
  - MAC
  - symmetric encryption scheme E
- ➢ EC domain parameters(p,a,b,G,n,h) for a curve over prime field or (m,f(x),a,b,G,n,h) for a curve over binary field;
- ➢ Bob's public key: K_B(Bob generates it as follows: $K_B = K_BG$, where K_B is the private key he chooses at random: $K_B€ [1, n-1]$
- ➢ Optional shared information: S_1 and S_2.

To encrypt a message m Alice does the following:

1. Generates a random number r € [1,n-1] and calculates $R = rG$;
2. Derives a shared secret: $S = P_x$, where $P = (P_x, P_y) = rK_B$ (and $P \neq 0$)
3. Uses KDF to derive a symmetric encryption and a MAC keys: $K_E \| K_M = KDF(S\|S_1)$;
4. Encrypts the message: $c = E (K_E; m)$;
5. Computes the tag of encrypted message and S_2: $d = MAC (K_M; c\|S_2)$; outputs $R\|c\|d$.

To decrypt the ciphertext $R\|c\|d$ Bob does the following:

1. Derives the shared secret: $S = P_x$, where $P = (P_x, P_y) = K_BR$ (it is the same as the one Alice derived because $P = K_BR = K_BrG = rK_BG =rK_B$), or outputs *failed* if $P = 0$;
2. Derives keys the same way as Alice did: $K_E\|K_M = KDF (S\|S_1)$;

3. Uses MAC to check the tag and outputs *failed* if d ≠ MAC (K_M ; c||S2);

4. Uses symmetric encryption scheme to decrypt the message m = E $_{-1}$(K_E; c)

IV. IMPLEMENTATION WORK

ECIES is an integrated encryption scheme which uses the following functions:

• Key Agreement (KA): Function used for the generation of a shared secret by two parties.

• Key Derivation Function (KDF): Mechanism that produces a set of keys from keying material and some optional parameters.

• Encryption (ENC): Symmetric encryption algorithm.

• Message Authentication Code (MAC): Data used in order to authenticate messages.

• Hash (HASH): Digest function, used within the KDF and the MAC functions.

To describe the steps has to be taken in order to encrypt a clear message, follow in tradition way and assume that Alice wants to send a message to Bob. In that scenario, Alice's ephemeral private and public keys will be represented as u and U, respectively. Similarly, we will refer to Bob's private and public keys as v and V, respectively. Where random number r is generates between (1, n-1). With the random number value G the generated point in the Elliptical curve is collected and the R is calculated R=r*G is generated. The random number R is key value for the Encrypt File or data. Hence R is not having privacy in the system. Since system is compromised by an attacker, he/she can easily obtain the original data. In order to provide system privacy the random number R is encrypted. So that the encrypted data can be protected from the unauthorized user even though the system is compromised.

To encrypt a message m Alice does the following:

1. Generates a random number r € [1,n-1] and calculates R = rG;

2. The random value R is encrypted which will be in cipher text.

3. Derives a shared secret: S = P_x, where P = (P_x, P_y) = rK_B (and P ≠ 0)

4. Uses KDF to derive a symmetric encryption and a MAC keys: K_E || K_M = KDF(S||S_1);

5. Encrypts the message: c = E(K_E; m);

6. Computes the tag of encrypted message and $S_{2:}$ d = MAC(K_M; c||S_2); outputs R||c||d.

To decrypt the cipher text R||c||d Bob does the following:

7. Derives the shared secret: S = P_x , where P = (P_x, P_y) = K_BR (it is the same as the one Alice derived because P =K_BR = K_BrG = rK_BG =rK_B), or outputs *failed* if P = 0;

8. Derives keys the same way as Alice did: K_E||K_M = KDF(S||S_1);

9. Uses MAC to check the tag and outputs *failed* if d ≠ MAC(K_M ; c||S2);

10. Uses symmetric encryption scheme to decrypt the message m = E $_{-1}$(K_E; c)

V. CONCLUSION AND FUTURE ENHANCEMENT

Elliptic Curve Integrated Encryption Scheme (ECIES) provides greater security and more efficient performance than the first generation public key techniques. ECIES provides various advantages on the random number. ECIES is the best known encryption scheme in the scope of ECC, which is one of the most interesting current cryptographic trends. Even though ECIES provides some valuable advantages over other cryptosystems as RSA, the number of slightly different versions of ECIES included in the standards may obstruct the adoption of ECIES.

Hence for the security purpose the random number (R) is encrypted. Due to this encryption process it extends time duration for the encrypted random number. Since, the time taken is in millisecond or nanosecond can be considered in future work.

REFERENCES

[1] Manoj Prabhakar, "Elliptic Curve Cryptography in securing networks by mobile authentication", International Journal on Cryptography and Information Security, ISSN 2013.3304, vol 3 no 3, September 2013.

[2] Sonali Nimbhorkar and Dr. L. G. Malik, "Prospective utilization of Elliptic Curve Cryptography for security enhancement", International Journal of Application or Innovative in Engineering and Management, ISSN 2319 – 4847, vol 2 issue 1, January 2013.

[3] N. Sivasankari and M. Kannan, "Effective implementations of GF (p) Elliptic Curve Cryptography computations using parallelism", International Journal of Emerging Technology and Advanced Engineering, ISSN 2250-2459, vol 3 issue 11, November 2013.

[4] Ms. Manali Dubal, Ms. Aaradhana Deshmukh, "Achieving authentication and integrity using Elliptic Curve Cryptography architecture", International Journal of Computer Applications, ISSN 0975 – 8887, vol 69 no 24, May 2013.

[5] Lokesh Giripunje and Sonali Nimbhorkar, "Comprehensive security system for mobile networks using Elliptic Curve Cryptography over GF (p)", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, vol3 issue 5, May 2013.

[6] Ruchika Markan and Gurvinder Kaur, "An efficient SDRP with Elliptic Curve Integrated Encryption Scheme", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, vol 3 issue 11, November 2013.

[7] Ruchika Markan and Gurvinder Kaur, "Literature survey on Elliptic Curve Encryption Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, vol 3 issue 9, September 2013.

[8] Kaalidoss Rajamani and Dr. A. Arul L. S, "Survey: Elliptic Curve Cryptography using scalar multiplication algorithms", International Journal of Innovative Research in Advanced Engineering, ISSN: 2278-231, vol 1 issue 1, March 2014.

[9] Neha Gupta, Harsh Kumar Singh, Anurag Jain, "An efficient implementation for key management technique using smart card and ECIES cryptography", International Journal of Control Theory and Computer Modeling, ISSN 2013.3603,vol 3 no 6, November 2013.

[10] Ruchika Markan and Gurvinder Kaur, "Review on secure and distributed reprogramming protocol", International Journal of Engineering and Computer Science, ISSN 2319-7242, vol 2 issue 8, August 2013.