International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.419-428
http://dx.doi.org/10.14257/ijsia.2015.9.12.37

Public Key Generation and Encryption Mechanism Using the Elliptic Curve in Smart Phones

Seung-Ho Shin[1] and Hee-Ju Eun[2]

Department of Computer Science, Kangwon National University 1
Kangwondaehak-gil, Chuncheon, Korea
michael@kangwon.ac.kr[1]
Department of Computer Engineering, Chonbuk National University 567
Baekje-daero, DuckJin-Gu, Jeonju, Korea
Corresponding Author, Hee-Ju Eun, hjeun@jbnu.ac.kr[2]

Abstract

Personal information stored in mobile devices can be unexpectedly exposed to others when users make use of mobile banking, Internet shopping and etc. Because of the important personal information that can be easily exposed in the mobile environment, it becomes more important to have a reliable security system. It is strongly required for this mobile security system to have a small memory size and a high processing speed as its components' characteristics. Considering these characteristics of the mobile security system, this paper aims at proposing a public key generation and an encryption mechanism that generates a hidden key using the Newton-Raphson method and applies the Diffie-Hellman key-exchange method to authenticate the peer. This mechanism uses an elliptic curve resulting in a small size of encryption key and a high security level.

Keywords: *Public key generation, Mobile Security, Encryption key, Public key, Security system, Newton-Raphson method, Diffie-Hellman Algorithm, Elliptic Curve Cryptography*

1. Introduction

In contemporary society, mobile systems are used for computer processing such as downloading music files or games, real time traffic information, e-commerce and banking business, and mobile phone processing at the same time. The mobile system is portable, operated by a small memory size, and high stability and fast speed are ensured in wireless information processing. However, as this characteristic is considerably limited in encrypting personal information, an encryption system of powerful and fast processing speed with small memory consumption while using small key size is required.

In this study, in order to suggest an encryption system fit for mobile systems having small memory size, elliptic curve formula and Newton-Raphson formula ensuring high stability by small size key value only were used. In addition, in order to transmit information stably in wireless information exchange (communication), Diffle-Hellman key exchange algorithm was used and in order to ensure fast arithmetic operation, additional operation by discrete logarithm was utilized.

The elliptic curve encryption system is convenient for safe encryption design and enables a smaller key for providing safety. In addition, as addition operation in elliptical curve includes an operation in finite field, it is easy to implement it by hardware and software.

ISSN: 1738-9976 IJSIA

2. Relevant Research

2.1. Encryption Technique

As mobile e-commerce environment through application of smart phone is being developed, the use of mobile credit cards is generalized. However, due to malicious approaches to smart phone data, exposure of credit card information being entered/saved/used without coping measures (countermeasure) such as encryption increases the risk of financial accidents. Under this situation, in this section, encryption method of private key and public key that is basis of encryption technique and its certification will be explained.

The security of private key encryption system relies on two elements. First, cryptography algorithm is required to be powerful enough not to be able to decipher message by cipher text itself only. Second, security depends on the confidentiality of the key, not that of the algorithm. In other words, even though cipher text, cryptography/decoder algorithm should be presented, decoding of message is assumed to be impossible. [Figure 2.1] shows private key encryption system process [1-2].

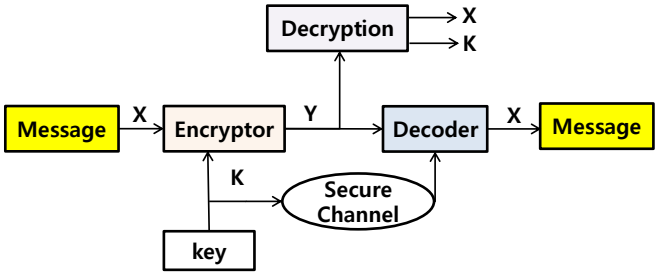

Figure 2.1. Private Key Encryption System Model

Encryption of public key was attempted in order to solve the problem that occurred in private key cryptography.

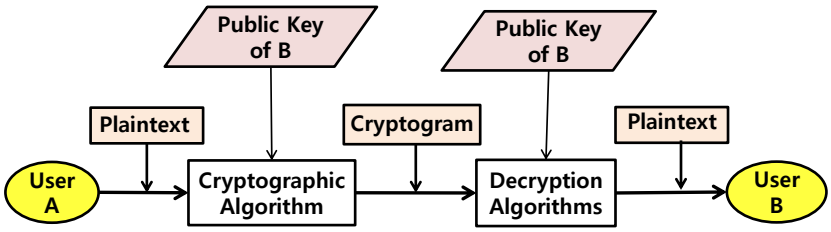

Figure 2.2. Brief Model of Public Key Encryption

Public key encryption process is as shown on [Figure 2.2].
First, generate a pair of keys being used for encryption and decoding of message to be received by each system in network. Second, the system makes the coded key (public key) public in public records or files, and the other key is kept by individuals as a private key. Third, if A wishes to transmit a message to B, the message is transmitted by coding a message using public key of B. Fourth, when B receives coded text, cipher text is decoded by using private key of B. As any other receiver is unable to know private key of B, such cipher text could not be decoded. [3-4].

2.2. Elliptic Curve Encryption System

Elliptic curve cryptography (ECC) is a cryptography algorithm based on difficulty of discrete logarithm of elliptic curve, and its safety level is ensured while using a much shorter key than that of other public key cryptography algorithms. Elliptic curve is defined on point O and a field K called 'point at infinity', and it is a set comprising points satisfying Weierstrass equation of which discriminant is not 0. Where, field K could be defined as follows. [5- 6]

$$E(K) = \left\{(x, y) \in K^2 \middle| y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a6\right\} \cup 0 \quad \text{-----<Formula 2.1>}$$

K: real number, rational number, complex number, finite field, *etc*.

When elliptic curve cryptography was announced, it was not widely used due to a problem in the reliability of safety, however, later its using range has been expanded as safety analysis was performed sufficiently and, in the case of signature algorithm using elliptic curve, its standardization work was completed at home and abroad. However, an environment where elliptic curve cryptography could not be applied exists still, and sensor network falls under this category. As most of sensor networks are based on wireless communication, importance of security is highly required but in reality, due to limitation of resources, public key-based cryptography algorithm is unable to be used. [7-9]

In this sensor network, an alternative key exchange method is researched but it does not ensure the stability level of public key-based algorithm. Therefore, in this study, key generation and encryption mechanism using elliptic curve cryptography improving security stability and fit for mobile system is suggested.

2.3. Diffie-Hellman Key Exchange

Diffie-Hellman key exchange algorithm is a public key-based key exchange algorithm. A method of exchanging private keys by using difficulty of obtaining discrete logarithm on Galois field F_p (GF(p)) was suggested. A method of mutually exchanging private keys by calculating $g^{ab} \bmod p$ with $g^a \bmod p$ and $g^b \bmod p$ was developed. In Diffie-Hellman algorithm, user A and B exist and these two know public variable (p & g). Where, p is prime number and g as primitive root, is smaller than p. Next, A and B select their personal key $X_a, X_b \in \{2, \cdots, p-1\}$ and calculate public key ($y_a = g^{X_a} \bmod p$, $y_b = g^{X_b} \bmod p$). And when mutually exchanging public key, A and B could obtain sharing key (symmetric key) $K = y_a^{X_a} \bmod p = y_b^{X_a} \bmod p = g^{X_aX_b} \bmod x$ by using counterpart key and their own inherent personal key. [10-12]

In the case of Diffie-Hellman's key exchange algorithm, public keys of key exchange algorithm is open, but it is safe until a discrete logarithm problem of finite field is solved even though the attacker knows this and so, if p size is big enough, its advantage is that the possibility of a private key being exposed is almost nil.

3. Mobile Security System based on Elliptic Curve

3.1. Security System Mechanism

The total structure of public key generation and encryption mechanism by using elliptic curve being suggested in this study is comprised of user, security server

certification institution (CA), certificate information registration, requested certificate management function, and certificate inquiry function.

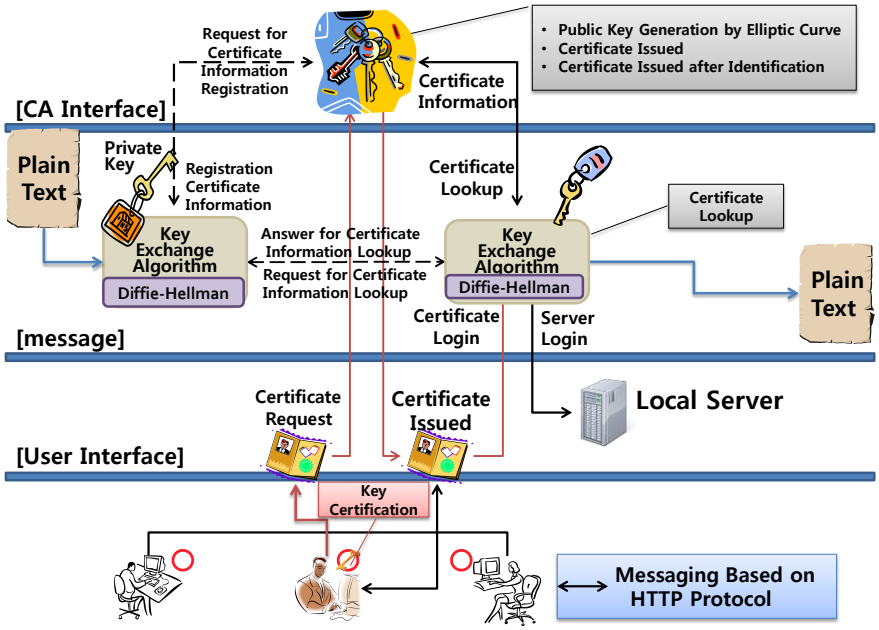

Figure 3.1. Elliptic Curve-Based Mobile Security System

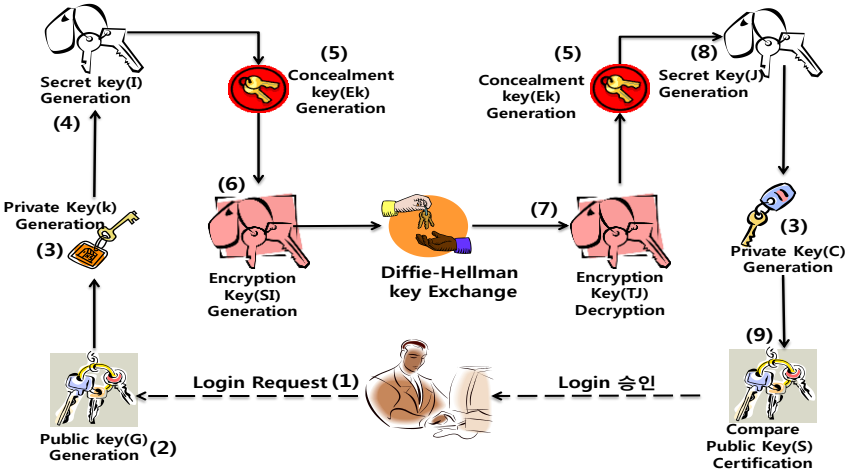

Figure 3.2. Key Generation Certification Process

Certification process of key generation is as shown on Figure 3.2. Input of certificate password and user ID by user (1) ⇒ Generation of public key by utilizing elliptic curve formula (2) ⇒ Request for registration by preparing user certificate password and certification public key as message in order to register public key information being generated by public key generation module in certification management server. Generation of individual personal keys arbitrarily selected by client and server (3) ⇒ Generation of private keys by selecting arbitrary personal key of client and server (4) ⇒ Generation of concealed keys by client and server at the same time based on approximate value by using Newton-Raphson method that is

non-linear numerical solution (5) ⇒ Generation of cryptography keys of the client and server using concealed key (6) ⇒ Exchange of Diffie-Hellman key (7) ⇒ Decoding cryptography key using concealed key (8) ⇒ Decoding public key by using personal key and private key (9).

3.2. Mobile Security System Algorithm

Public keys being generated by using elliptic curve formula based on Diffie-Hellman encryption mechanism algorithm obtain points of coordinates value in algebraic method by substituting arbitrary coefficient and constant in elliptic curve formula jointly by client and server.

3.2.1. Generation of Public Key by Using Elliptic Curve Formula: From elliptic curve formula $y^2 = x^3 + ax + b \pmod{p}$, x coordinates where $x^2 \pmod{p}$ and $y^2 \pmod{p}$ are same and set finite field F_p that is $y^2 \pmod{p}$ are obtained. (But $a, b \in$ integer, $p \in$ prime number : number of points comprising curve) By arbitrarily selecting one value among these, $G \in F_p$ is designated as public key. In other words, $G = (x_k, y_k)$. But k is integer.

Where, in order to protect public key, discard coordinate value G that was used once and designate new value as public key.

3.2.2. Encryption and Decoding Using Diffie-Hellman: 1) Generation of private key by using Diffie-Hellman. Client and server obtain private key as follows by using public key $G = (x_k, y_k)$ after selecting constant value k and c by using arbitrary personal key.

$$I = k * G \pmod{p} \quad \text{---- <Formula 3. 1>}$$

$$J = c * G \pmod{p} \quad \text{---- <Formula 3. 2>}$$

At this time, in case that a value calculated by applying algebraic addition exceeds p that is mod value, obtain client private key $I = (x_i, y_j)$ and server private key $J = (x_i, y_j)$ by applying $\bmod p$

2) Generation of Concealed Key by Using Newton-Raphson Numerical Solution. Integer of approximate solution (x_1, x_2) value is taken as concealed key by using Newton-Raphson method that is non-linear numerical solution based on client private key $I = (x_i, y_j)$ and server private key $J = (x_i, y_j)$ obtained from <Formula 3. 1> and **<Formula 3. 2>**

$$f(x) = \alpha x^3 + \beta x^2 + \delta x + \gamma, \quad \text{(initial value } \rho_0\text{)}$$

But, $\alpha, \beta, \delta, \gamma$ take each coefficient of elliptic curve formula as

$$\alpha = \gamma = a, \beta = \delta = b \quad x_0 = \rho_0.$$

3) Generation of Private Key by Using Concealed Key. As concealed key is subject to exposure, generate cryptography key of client and server based on following **<Formula 3.3>** and **<Formula 3.4>** by using concealed keys separately obtained through Newton-Raphson calculation formula.

$SI = I \ XOR \ Ek$ **---- <Formula 3. 3>**
$TJ = J \ XOR \ Ek$ **---- <Formula 3. 4>**

3.2.3. Certification by using Diffie-Hellman: As a certification procedure, after decoding private keys and personal keys by using generated cryptography key and Diffie-Hellman algorithm, certification status is determined by comparing such keys.

1) Decoding Private Key

Obtain private key I & J of client and server by calculating concealed key Ek based on **<Formula 3.5>** and **<Formula 3.6>** using cryptography key SI and TJ

$I = SI \ XOR \ Ek$ **---- <Formula 3. 5>**
$J = TJ \ XOR \ Ek$ **---- <Formula 3. 6>**

2) Decoding Public Key and its Certification

Certification procedure of user after generating a public key is progressed by obtaining S and T that are new certification value based on <Formula 3. 7>and <Formula 3. 8> after multiplying private key J and I that exchanged arbitrary constant k and c held by client and server.

$S = k * J \pmod{p}$ **---- <Formula 3. 7>**
$T = c * I \pmod{p}$ **---- <Formula 3. 8>**

At this time, in case a value calculated by app

Certification process of key generation is as shown on [Figure 3.2]. Input of certificate password and user ID by user (1) ⇒ Generation of public key by utilizing elliptic curve formula (2) ⇒ Request for registration by preparing user certificate password and certification public key as message in order to register public key information being generated by public key generation module in certification management server. Generation of individual personal keys arbitrarily selected by client and server (3) ⇒ Generation of private keys by selecting arbitrary personal key of client and server (4) ⇒ Generation of concealed keys by client and server at the same time based on approximate value by using Newton-Raphson method that is non-linear numerical solution (5) ⇒ Generation of cryptography keys of the client and server using concealed key (6) ⇒ Exchange of Diffie-Hellman key (7) ⇒ Decoding cryptography key using concealed key (8) ⇒ Decoding public key by using personal key and private key (9)

3.2. Mobile Security System Algorithm

Public keys being generated by using elliptic curve formula based on Diffie-Hellman encryption mechanism algorithm obtain points of coordinates value in algebraic method by substituting arbitrary coefficient and constant in elliptic curve formula jointly by client and server.

3.2.1. Generation of Public Key by Using Elliptic Curve Formula: From elliptic curve formula $y^2 = x^3 + ax + b \pmod{p}$, x coordinates where $x^2 \pmod{p}$ and $y^2 \pmod{p}$ are same and set finite field F_p that is $y^2 \pmod{p}$ are obtained. (But $a, b \in$ integer, $p \in$ prime number : number of points comprising curve) By arbitrarily

selecting one value among these, $G \in F_p$ is designated as public key. In other words, $G = (x_k, y_k)$. But k is integer.

Where, in order to protect public key, discard coordinate value G that was used once and designate new value as public key.

3.2.2. Encryption and Decoding Using Diffie-Hellman: 1) Generation of private key by using Diffie-Hellman. Client and server obtain private key as follows by using public key $G = (x_k, y_k)$ after selecting constant value k and c by using arbitrary personal key.

$$I = k * G \pmod{p} \quad \text{---- <Formula 3. 1>}$$

$$J = c * G \pmod{p} \quad \text{---- <Formula 3. 2>}$$

At this time, in case that a value calculated by applying algebraic addition exceeds p that is mod value, obtain client private key $I = (x_i, y_j)$ and server private key $J = (x_i, y_j)$ by applying $\bmod p$

2) Generation of Concealed Key by Using Newton-Raphson Numerical Solution

Integer of approximate solution (x_1, x_2) value is taken as concealed key by using Newton-Raphson method that is non-linear numerical solution based on client private key $I = (x_i, y_j)$ and server private key $J = (x_i, y_j)$ obtained from <Formula 3. 1> and <Formula 3. 2>

$$f(x) = \alpha x^3 + \beta x^2 + \delta x + \gamma, \quad \text{(initial value } p_0\text{)}$$

But, $\alpha, \beta, \delta, \gamma$ take each coefficient of elliptic curve formula as

$$\alpha = \gamma = a, \beta = \delta = b \quad x_0 = p_0.$$

3) Generation of Private Key by Using Concealed Key

As concealed key is subject to exposure, generate cryptography key of client and server based on following **<Formula 3.3>** and **<Formula 3.4>** by using concealed keys separately obtained through Newton-Raphson calculation formula.

$$SI = I \ XOR \ Ek \quad \text{---- <Formula 3. 3>}$$

$$TJ = J \ XOR \ Ek \quad \text{---- <Formula 3. 4>}$$

3.2.3. Certification by using Diffie-Hellman: As a certification procedure, after decoding private keys and personal keys by using generated cryptography key and Diffie-Hellman algorithm, certification status is determined by comparing such keys.

1) Decoding Private Key

Obtain private key I & J of client and server by calculating concealed key Ek based on **<Formula 3.5>** and **<Formula 3.6>** using cryptography key SI and TJ

$$I = SI \ XOR \ Ek \quad \text{---- <Formula 3. 5>}$$

$$J = TJ \ XOR \ Ek \quad \text{---- <Formula 3. 6>}$$

2) Decoding Public Key and its Certification

Certification procedure of user after generating a public key is progressed by obtaining S and T that are new certification value based on <Formula 3. 7>and <Formula 3. 8> after multiplying private key J and I that exchanged arbitrary constant k and c held by client and server.

$$S = k * J \pmod{p} \text{ ---- <Formula 3. 7>}$$

$$T = c * I \pmod{p} \text{ ---- <Formula 3. 8>}$$

At this time, in case a value calculated by applying algebraic addition exceeds mod value p, obtain client certification key $S = (x_s, y_s)$ and server certification key $T = (x_t, y_t)$ by applying $\mod p$.

4. System Evaluation

In this section, characteristics of research relevant to mobile security systems and 3rd stage mobile security systems being suggested in this study are comparatively analyzed and its performance is evaluated. Target of comparative analysis is research relevant to mobile security explained in relevant research of Chapter 2 and performance is evaluated based on system response speed between similar security technique and suggested system.

4.1. Comparative Analysis of System Features

Comparative analysis and evaluation were performed in terms of functionality and reliability based on existing security related research and suggested security technique. When comparatively analyzing in terms of compatibility and expandability for functionality, as server security systems by using identification information generates personal key by combining its own inherent identification information with security code being provided basically, compatibility and expandability are limited but as 2 stage security technique is applied, safety against certificate plagiarism and hacking is quite high. As the technique suggested in this study generates and restores keys based on an elliptic curve, Diffie-Hellman and Newton-Raphson method, it could be applied to diversified systems and its compatibility and expandability are relatively high.

In addition, as comparative analysis for safety as to how much the suggested technique is safe against certificate plagiarism and hacking compared to other techniques passes through 3 stages of verification compared with existing system, its response speed is fair, although countermeasures against certificate plagiarism and hacking is relatively outstanding and its safety is analyzed to be high.

4.2. Comparison of Response Speed

In this chapter, in order to compare log-in response speed by targeting suggested system, comparative analysis was performed quantitatively by performing log-in for 100, 1,000 and 10,000 times and based on this result, response speed of similar security techniques was compared.

In case of performing login for 100, 1,000 and 10,000 times, respectively, 1 time login response speed of certification system for personal users is 0.0162695 seconds, 0.0167195 seconds and 212.195 seconds, respectively.

As a result of measuring the response speed between the suggested system and similar security techniques through a simulation, it could be seen that the response speed is somewhat slower than 2-stage system of similar security techniques in the existing study.

[Figure 4-1] shows the result of comparison between response speed among similar security techniques. When observing this result, it could be seen that in case of low login frequency, there was no difference in response speed but when login was performed for more than 1,000 times, difference was represented in response speed.

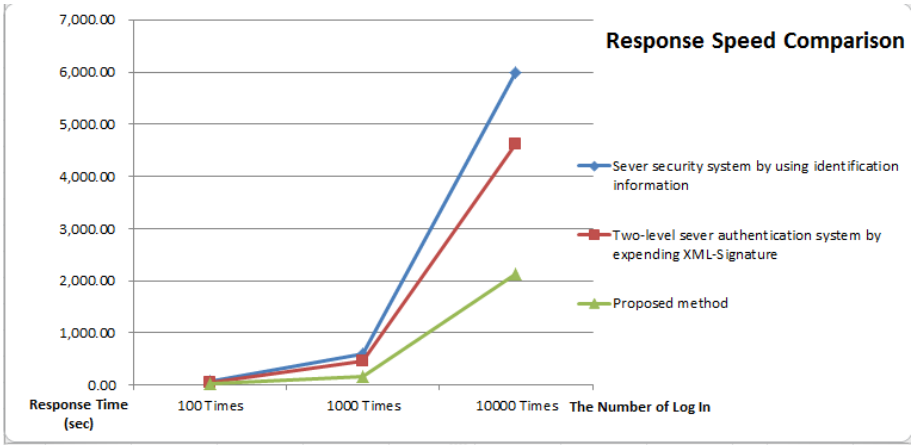

Figure 4.1. Comparison of Response Speed AmongSimilar Security Techniques

In addition, as a result of evaluating the performance in terms of safety, countermeasures against certificate plagiarization and hacking was high and in terms of expandability, as it was based on mobile environment, its expandability and compatibility were analyzed to be relatively high.

5. Conclusion

Mobile Internet systems could access the Internet at any time and place and without cable connection, and it could also exchange information and data by using wireless communication devices like mobile phones or PDA. In view of the features of a mobile system that uses a memory size of certain capacity, the key size required for encryption should be small in encryption systems being used in mobile device. However, in encryption systems using mobile device requiring fast speed in information transmission through encryption, key size is one of important factors.

In this study, in order to suggest a more reinforced elliptic curve encryption mechanism fit for mobile system, an encryption mechanism fit for hybrid mobile systems was designed by using Newton-Raphson algorithm and Diffie-Hellman key exchange method based on calculation method of elliptic curve encryption.

For this objective, first, an elliptic curve formula was applied in order to use small sized memory and was used in order to effectively perform encryption in mobile device that is limited by key size. Second, in order to ensure stability of information transmission by exchanging information through radio, generation of public keys and encryption systems using elliptic curve were used in Diffie-Hellman key exchange algorithm. Third, in order to ensure fast speeds in information transmission while using small sized mobile devices, an additional method of discrete logarithm having fast operation rather than numerical solution by multiplication was used in order to utilize elliptic curve function using a small sized

key. It is considered that this method is suitable for memory use and its encryption power is excellent while using smaller keys than public keys.

A mobile system using elliptic curve formula and Newton-Raphson formula satisfying the above 4 considerations being suggested in this study was designed and in order to use small sized memory, utilize encryption system using elliptic curve formula, and ensure stable information transmission in exchanging information by radio, the Diffie-Hellman key exchange system was used and for fast arithmetic operation, an additional operation by discrete logarithm was utilized.

References

[1] SK HafizulIslam, G.P Biswas "Design of improved password authentication and update scheme based on elliptic curve cryptography"Mathematical and Computer Modelling, vol. 57, no.11-12, **(2011)**, pp. 2703-2717.
[2] E-HeeGoo, S-DaeLee , "Reconfigurable real number field elliptic curve cryptography to improve the security, Journal of Computer Virology and Hacking Techniques, vol 11, no. 3, **(2014)**, pp. 123-128 .
[3] Z Shihua, W. Ziqi, "Encryption method based on a new secret key algorithm for color images" International Journal of Electronics and Communications **(2015)**.
[4] M. Babaei, "A novel text and image encryption method based on chaos theory and DNA computing" Natural Computing, vol. 12, no. 1, **(2012)** , pp101-107 .
[5] Z. Xing, "A New Public Key Encryption Scheme based on Layered Cellular Automata" KSII Transactions on Internet and Information Systems, vol 8, no10, **(2014)**, pp. 3572-3590.
[6] S. Zhi-Yi, Y. Bo, "On security against the server in designated tester public key encryption with keyword search", Information Processing Letters, vol. 115, no. 12, **(2015)**, pp. 957-961.
[7] L. Junzuo, K. Weidong, C. Kefei, "Self-generated-certificate public key encryption without pairing and its application, Information Sciences, vol. 181, no. 11, **(2011)**, pp. 2422-2435.
[8] R. Hyun Sook, P. Jong Hwan, L. Dong Hoon, "Generic construction of designated tester public-key encryption with keyword search", Information Sciences, vol. 205, **(2012)**, pp. 93-109.
[9] S.K. Islam Hafizul, "An improved three party authenticated key exchange protocol using hash function and elliptic curve cryptography for mobile-commerce environments, Journal of King Saud University-Computer and Information Sciences **(2015)**.
[10] S. K. HafizulIslam, "Dynamic ID-based remote user mutual authentication scheme with smartcard using Elliptic Curve Cryptography Journal of electronics, vol. 31, no. 5 **(2014)**.
[11] X. HungLe, "An energy-efficient access control scheme for wireless sensor networks based on elliptic curve cryptography", Journal of Communications and Networks, vol. 11, no. 6, **(2009)**, pp. 599-606.
[12] R. Kishore, "A Secure Key Predistribution Scheme for WSN Using Elliptic Curve Cryptography" ETRI Journal vol. 33, no. 5, **(2011)**, pp. 791-801.
[13] S. K. Ghosh, "Secured wireless medical data transmission using modified elliptic curve cryptography, Proceedings of the 3rd ACM MobiHoc workshop **(2013).**

