A Secure Conference Key Protocol over ECC-based Grey Systems

Tzer-Long Chen
Department of Information Management
National Taiwan University
d97725005@ntu.edu.tw

Yu-Fang Chung
Department of Electrical Engineering
Tunghai University
yfchung@thu.edu.tw

Frank Y.S. Lin
Department of Information Management
National Taiwan University
yslin@im.ntu.edu.tw

ABSTRACT. *In the current environment, there are only a limited number of third-parties that general users can trust in terms of authentication and verification. Often, the self-acclaimed independent third-parties are the parties from where information outflow occurs. While current public key encryption systems have numerous algorithms that have been protecting confidential data for several years, these systems are often met with hardware difficulties for information protection on the Internet and commercial applications. In order to meet the various needs of the environment, often several cryptography modules are combined or merged to achieve the effect of covering each others' deficiencies. This is a very common practice. The proposed method in this article is applicable for preventing information outflow with the introduction of third parties during a bi-party communication, in circumstances where bi-party communication is met with network environment difficulties, and also when the third party is not a trusted controller, or there are no controllers at all. While current systems operate on the back of trusted third-party administrators as is a common security mechanism for managing the public key and confidential data, often even with management, there are still probabilities of insecurity that threaten system security on the whole. To prevent this and also adapt to environment needs, the proposed method combines the grey system theory with the ECC method. This*

method can verify the credibility of senders' identity when the legitimate third party is no longer trusted, thus preventing malicious third-party intrusions. The concept of this method is based on the well-known Digital Signature Algorithm (DSA) concept from which the Diffie-Hellman Key Agreement mechanism is derived to manage a common conference key in a mutual communication agreement. When the user can communicate mutually between themselves without the need for a third-party intermediary, the solution to intervention and theft of confidential data by third-parties becomes plausible. With flexibility in calculation, one can set his/her access protocol for the modules to confuse malicious users and increase the difficulty of acquiring the keys illegally. In addition, by combining the ECC public key system, with ECC's short and low computational properties, the proposed method improves on the encryption and decryption operation efficiency. This method is thus a system set to establish a secure and efficient conference key system by combining the properties of the ECC public key system with the grey system theory.

Keywords: Conference Key, Elliptic Curve Cryptosystem, Digital Signature Algorithm, Grey System.

1. Introduction. With the current increasing frequency of network intrusions, information security and protection issues have received increasing attention. The degree of importance for commercial secrets and personal privacy has also changed immensely. At present, companies educate their internal staff on improving information security through education management or by employing business information security controls. Therefore, information security has gained importance not only from the personal and individual aspect, but also from the commercial side, demanding development in the applications of encryption systems to be even cautious in information security issues.

Encryption systems are based on the difficulty of mathematics, such as DLP, ECDLP, and so on, and based on the difficulty are they applied to encryption systems, such as ElGamal, Diffie-Hellman, ECC, RSA, DSA, Schnorr, and so on. Since the solving or deciphering of these encryption systems require immense time and computation, they are relatively safe in security concerns, or at least are safe as of now.

The proposed method, which employs the ECC encryption system [1, 9], has low computational complexities and the feature of short keys [4, 10], which make it easy to be implemented from both aspects of the hardware and the development in software applications. The feature of short keys is particularly lauded. Compared with the RSA or DSA algorithms, the ECC's key length of 160 bits has the equivalent

security level to the RSA's 1024-bit length key. Therefore, the ECC has been a popular encryption system for the past two decades, with its applications in both wireless networks and network application software. What the RSA can do, the ECC can also achieve [6], such as digital signature, identity verification [21, 22, 23], and other applications within these related scope.

Next, ECC, the common algorithm for encryption systems employed in the basic public key structure, will be introduced. The symbols used in this article will first be introduced to explain the legal conditions for ECC system operations. U_1 and U_2 are two users, namely user1 and user2 who wish to communicate with each other. M_m represents a message, while SM_m represents a confidential message. Before transmission or communication takes place, both sides must select a valid ECC system, denoted by $E_P(a,b)$: $y^2 = x^3 + ax + b \bmod p$, $a, b \in N^+$ [5], $D = 4a^3 + 27b^2 \bmod p \neq 0$, where p is a large prime number, and G is the Basic Point [3] identified by both sides in the ECC cryptography system, and also $G \in E_p(a,b)$. As to the keys, k_{U_1} and P_{U_1} are the secret and public keys of U_1 respectively, while k_{U_2} and P_{U_2} are the secret and public keys of U_2 respectively. The following is the calculation of both public keys.

$$P_{U_1} = k_{U_1} \times G \tag{1.1}$$

$$P_{U_2} = k_{U_2} \times G \tag{1.2}$$

After the above parameters are set, the ECC system operates as follows. When U_1 wants to communicate with U_2, U_1 will send a message to the other party. Nonetheless, a secret parameter z must be firstly chosen; and, according to (1.3), the generation of T_1, which will be used to restore parameters in the future, is calculated.

$$T_1 = z \times G \bmod p \tag{1.3}$$

The message M_m is then divided into two parts, namely M_1 and M_2. Through U_2 public key encryption, M_1 and M_2 are encrypted to generate a secrete message SM_m, which are C_1 and C_2 respectively. As the points used in the ECC encryption are finite points, x and y represents a legitimate point in an elliptic curve as represented by the vector of x and y. The vector of x and y is further divided into two parts, while the message is

encrypted. Finally, along with the calculated encrypted text, C_1 and C_2 and the results of T_1 are sent to the receiver U_2 as calculated by the the following Equations (1.4) and (1.5) below.

$$C_1 = M_1 + z \times (P_{U_2})_x \bmod p \tag{1.4}$$

$$C_2 = M_2 + z \times (P_{U_2})_y \bmod p \tag{1.5}$$

When U_2 receives the cipher message (C_1, C_2, T_1), it will use its own cipher key k_{U_2} to restore the message. Before the message is restored, a parameter α, the redox factor, must be calculated according to Equation (1.6) below.

$$\begin{aligned} a &= (k_{U_2} \times T_1) \bmod p \\ &= k_{U_2} \times (z \times G) \bmod p \\ &= z \times (k_{U_2} \times G) \bmod p \\ &= z \times P_{U_2} \bmod p \end{aligned} \tag{1.6}$$

Next, the cipher message is received according to Equations (1.7) and (1.8), and the message is restored. The decryption process operates as follows.

$$\begin{aligned} C_1 - \alpha_x \bmod p &= (M_1 + z \times (P_{U_2})_x) - \alpha_x \bmod p \\ &= (M_1 + z \times (P_{U_2})_x) - (z \times (P_{U_2})_x) \bmod p \\ &= M_1 \end{aligned} \tag{1.7}$$

$$\begin{aligned} C_2 - \alpha_y \bmod p &= (M_2 + z \times (P_{U_2})_y) - \alpha_y \bmod p \\ &= (M_2 + z \times (P_{U_2})_y) - (z \times (P_{U_2})_y) \bmod p \\ &= M_2 \end{aligned} \tag{1.8}$$

According to the above Equations (1.4), (1.5), (1.7) and (1.8), the message can be decrypted successfully. The use of ECC algorithms [11] is advantageous during calculation, thus guaranteeing that, with this method, even if a malicious user steals the cipher message during network transmission, the attacker will fail to decrypt the

message during the safety period, thus assuring the safety and effectiveness of this method.

2. Data Generation and Model Generation. The grey system theory was proposed by a scholar from China, Professor Long Deng Ju, in 1982, to establish a system model, in which system analysis and model structuring employed forecasting and decision-making methods to explore and understand systems when the model was uncertain or its information was incomplete. The advantage lies in the ability to do a system forecast when the system faces incomplete or uncertain information, which provides a good method to arrive at prediction accuracy for research under limited data.

The fundamental idea of the grey system theory is to predict the probability of future events that may occur when only very limited information is available. This is done through the grey link of the grey theory and grey modeling to construct a simulation system that will predict the probability of possible future events. In fact, the grey system theory is like a large black box, which contains numerous methods for choices. Metaphorically, the known information to be inputted is white, while the unknown information that will be outputted is black. The grey system theory, then, is to construct models built from various methods and to select, by itself, the method to operate and calculate the probability or value of possible "black" events. The grey system theory is constructed with various mathematical equations with innumerous methods, where the most common method is grey link and grey modeling. Grey modeling [7, 8, 16] is the basis of the proposed method and will be introduced as follows.

2.1 Data Generation. Suppose that there is an original known series, whose set is x, expressed by Equation (2.1) as follows.

$$X = \{x_1,\ x_2,\ \cdots,\ x_n\} \tag{2.1}$$

Next, the grey model (1-AGO) cumulative computing method [2, 12] is used to generate $X^{(1)}$, the first power series of the original series, as represented in Equation (2.2).

$$X^{(1)} = \{x_1^{(1)},\ x_2^{(1)},\ \cdots,\ x_n^{(1)}\} \tag{2.2}$$

It should also satisfy the condition $\forall x_k^{(1)} \in X^{(1)}$,

$$x_k^{(1)} = \sum_{i=1,\ x_i \in X}^{k} x_i \tag{2.3}$$

The elements of the series are used to calculate in Equation (2.3), cumulative

computing algorithm, but the series of $X^{(1)}$ must satisfy Equation (2.4), and through Equation (2.5), and obtain two special solutions, *a* and *u*. These solutions are derived from matrix calculations of Equation (2.6). The matrix calculation of (2.7) and (2.8) is obtained as follows.

$$\frac{dx_1^{(1)}}{dt} + ax_1^{(1)} = u \tag{2.4}$$

$$\hat{x}_{k+1}^{(1)} = (x_1^{(0)} - \frac{u}{a})e^{-ak} + \frac{u}{a} \tag{2.5}$$

$$\begin{pmatrix} a \\ u \end{pmatrix} = \left(B^T B\right)^{-1} B^T Y_N \tag{2.6}$$

$$B = \begin{bmatrix} -\frac{1}{2}\left(x_1^{(1)} + x_2^{(1)}\right) & 1 \\ -\frac{1}{2}\left(x_2^{(1)} + x_3^{(1)}\right) & 1 \\ \vdots & \\ -\frac{1}{2}\left(x_{n-1}^{(1)} + x_n^{(1)}\right) & 1 \end{bmatrix} \tag{2.7}$$

$$Y_N = \left(x_2,\ x_3,\ \cdots,\ x_n\right)^T \tag{2.8}$$

According to the method proposed by D.J. Long in 1989, Equations (2.1) to (2.8) form the method of the grey modeling method of the grey system theory, from which Equation (2.9) is derived. With this equation, prediction is made for the next class of series or the next value.

$$\hat{x}_{k+1}^{(1)} = (x_1^{(1)} - \frac{u}{a})e^{-ak} \tag{2.9}$$

Through Equation (2.9), a series result represented in (2.10) is acquired to predict the future value. For $k = 1, 2, \cdots, m$, the following sequence is received from (2.9):

$$\overline{X} = \left(\alpha e^{-a},\ \alpha e^{-2a},\ \cdots,\ \alpha e^{-ma}\right) \tag{2.10}$$

Since only the whole value of the series (2.10) is used, the whole integer should be derived through $\alpha e^{-ja} = INT(\alpha e^{-ja})$. This process is called the sequence of data generation, where $\alpha e^{-ja} = INT(\alpha e^{-ja})$, $\alpha e^{-ja} \in \overline{X}$. Equation (2.10) is called the sequence of data generation of (2.1).

2.2 Model Generation. The above calculation will produce a number of series being used in Equation (2.11) to build the model. This is primarily used to comply with the ECC's encryption system condition that requires the prime number result to be

consistent with the system result in order to be legal and thus to meet the system requirement.

$$\left(\alpha e^{-a},\ \alpha e^{-2a},\ \cdots,\ \alpha e^{-ma}\right) \tag{2.11}$$

Supposing that *m* in the series is a legible large number, whose *p* result is consistent with the ECC system and complies with the system requirement. Next, using Equation (2.12), the series are individually calculated to obtain the series of (2.13). The resultant series complies with the system requirement, upon which one of the values will be taken up to be the cipher key.

$$\beta_j = \alpha e^{-ja} \bmod p \tag{2.12}$$

$$\beta = \{\beta_1,\ \beta_2,\ \cdots,\ \beta_m\} \tag{2.13}$$

Example 1. *This method primarily follows the flowchart of Figure1 to calculate the sequence of the grey model in order to obtain the class series model forecasts. A grey-theory system utilizes the accumulated generating sequence and the inverse accumulated generating sequence of the grey generating function to allow the system to have multiple levels of generating sequences. The proposed method thus uses such generating sequences to choose a key. The main purpose is to impose mathematical difficulties and to confuse the attackers who want to break the key. Furthermore, the grey theory also has the characteristics of mutually inclusive accumulated generating sequences and inverse accumulated generating sequences, from which the original key can still be restored. The operating process of the method can be explained below. When the user sends an encoded message, the grey-theory system is entered. After choosing the original array for the key, the system goes through the accumulated grey generating model, calculates the grey mathematical model, predicts grey elements of different levels, generates different arrays, and finally, through the generating arrays of various levels, chooses the key for communication.*

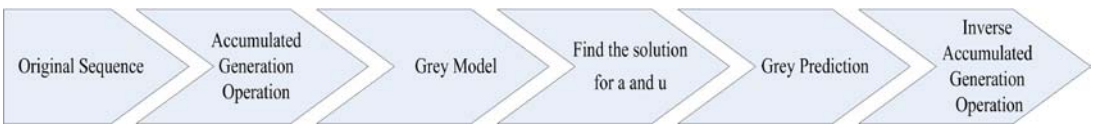

Figure 1: The flowchart of Grey Model and Grey Prediction.

The method also primarily uses the obtained forecasts series to obtain a value to be the cipher key. The following example illustrates how to set up a grey model. Assuming that there is a series $y^{(0)}$*=(383.378, 393.040, 399.363, 406.007, 414.62), after the cumulative power computation, the first power series is arrived at*

$y^{(1)}$=(383.378, 776.418, 1175.781, 1581.788), after many more cumulative computations, other power series, $y^{(2)}$, $y^{(3)}$, …, $y^{(n)}$ are generated, and after a customized computation for the average value, $z^{(1)}$=(579.898, 976.100, 1378.785) is obtained as the average. In order to obtain the values of a and u, the original series and the average value series are substituted in the grey differential equation as follows.

$$-579.898a + u = 393.040$$
$$-976.1a + u = 399.363$$
$$-1378.785a + u = 406.007$$

The linear equation is then converted into the matrix $B\tilde{\theta} = Y$

$$B = \begin{bmatrix} -579.898 & 1 \\ -976.100 & 1 \\ -1378.785 & 1 \end{bmatrix},\ \tilde{\theta} = \begin{bmatrix} a \\ u \end{bmatrix},\ \mathrm{Y} = \begin{bmatrix} 393.040 \\ 399.363 \\ 406.007 \end{bmatrix}$$

Therefore, using the least square method, a and u are obtained, as shown below.

$$\tilde{\theta} = \begin{bmatrix} a \\ u \end{bmatrix} = (B^T B)^{-1}\ B^T Y = \begin{bmatrix} -0.016 \\ 383.591 \end{bmatrix}$$

The whitening equation is:

$$\frac{dy^{(1)}(t)}{dt} - 0.016y^{(1)}(t) = 383.591$$

The whitening equation is solved as follows.

$$y^{(1)}(t) = 24357.8511 * e^{0.016(t-1)} - 23974.4375$$

$$\Rightarrow \text{according to formula (2.5)}\ \hat{x}_{k+1}^{(1)} = (x_1^{(0)} - \frac{u}{a})e^{-ak} + \frac{u}{a}$$

$$\Rightarrow y^{(1)}(t+1) = (383.378 + 383.591/0.016) * e^{0.016t} - 383.591/0.016$$

The result is generated with the cumulative series, which will have to be regressed to restore back to the original series as $\Rightarrow \hat{y}^{(0)}(t+1) = \hat{y}^{(1)}(t+1) - \hat{y}^{(1)}(t)$

$$\hat{y}^{(0)}(t+1) = y^{(1)}(t+1) - y^{(1)}(t)$$
$$= 386.668e^{0.016(t)}$$

From the above computation, the following result is acquired, as shown in Table1.

Table 1: Original values and model values

t	Original Value $y^{(0)}(t)$	Model Value $\tilde{y}^{(0)}(t)$
1	383.378	383.378
2	393.040	392.904
3	399.363	399.242
4	406.007	405.681

From the above, it can be derived that the next sequential value is $\tilde{y}^{(0)}(5) = 418.872$. *The values for* $\tilde{y}^{(0)}(6)$, $\tilde{y}^{(0)}(7)$, $\cdots$, $\tilde{y}^{(0)}(n)$ *can likewise, be derived and predicted, with their values converted into integer values and made as the system key. The grey prediction model works as follows.*

$$\tilde{y}^{(0)} = IAGO \circ GM(1,1) \circ AGO \circ y^{(0)}$$

3. Elliptic Curve Cryptosystems Using Conference Key $C_{U_1U_2}$**.** Since the proposed method is to facilitate a system that does not require, or trust, a third party management unit to manage the public key [18], a conference key [20] system is required to solve such problems. When two sides need to communicate, but would like to verify each other's identities before data transmission, the proposed method is used for this purpose.

The method proposed in the paper is a creation of a new type of cryptographic application that integrates mathematical grey theory with public key cryptography that can be applied to environments without a trusted third party by using the Diffie-Hellman key exchange concept. The proposed method is to be used in an environment without a trusted third party, or for two-party communication in insecure environments. In an insecure environment, the new conference key proposed can be a secure method for message exchange with advantages listed below:

1. Confidentiality: As this paper utilizes both the grey theory and the ECC method, the proposed scheme can guarantee message confidentiality. From characteristics of the grey theory, more difficulties are imposed on key deciphering for deciphers; in addition, by using ECC cryptography, deciphers will face the difficult ECDLP problem in their attempt to steal information.

Therefore, confidentiality is ensured during the exchange of message and information.

2. Safety: As mentioned above, all attempts to break or steal the key during message-exchange will face the ECDLP problem; therefore, the safety of secret messages or keys generated with the proposed method is assured.
3. Completeness: The information or message exchanged can be verified with the conference key to check for edits and changes. Completeness can thus be easily verified.
4. Flexibility: In the past, a trusted third party is required for managing the system members' keys. However, such trusted third parties may not be available for certain application environments, and moreover security concerns associated with the trusted third parties may end up undermining overall security. The method proposed in the paper thus offers another choice for environments without the need for a trusted thirty party, such as: in methods regarding sensor networks, where communication and safety for both senders and receivers are major concerns.
5. Low cost: ECC cryptography has characteristics of short keys and low computation costs, which makes the proposed method particularly applicable in limited-energy and/or low-computation- power environments, such as sensor networks.

Suppose that there is a need to construct a sensor network in an insecure environment and that the ad-hoc mode is adopted due to the environment's characteristics. Without a backbone communication infrastructure in such an ad-hoc mode, sensors need to communicate with each other directly. The sensor network now faces a public and insecure environment, and consequently, the sensors will require a secure communication mechanism among them. This is when the proposed method can protect the sensors' communication and can guarantee the message-exchange safety.

Supposing that U_1 and U_2 are two parties who want communication, both sides firstly select a valid ECC encryption system and a and b to be ECC's valid parameters. ECC's valid equation condition and computation are as follows.

$$E_P(a,b): y^2 = x^3 + ax + b \bmod p\ ,\quad a,b \in N^+\ ,\quad D = 4a^3 + 27b^2 \bmod p \neq 0\ ,\quad p \text{ is prime.}$$

G is the basic point, $G \in E_p(a,b)$.

Next, the formula derived from grey modeling is used in the encryption system [15]

for identification purpose. $X^{U_1} = \{x_1^{U_1}, x_2^{U_1}, ..., x_n^{U_1}\}$ is U_1's identification, while $X^{U_2} = \{x_1^{U_2}, x_2^{U_2}, ..., x_n^{U_2}\}$ is U_2's identification. When both sides have selected a system, they must exchange the public keys generated by each other to compute the conference key as follows.

3.1 U_1 **generates cipher key** k_{U_1} **and public key** P_{U_1}**.** Firstly, sender U_1 has to construct a generative class series (3.1) from $X^{U_1} = \{x_1^{U_1}, x_2^{U_1}, ..., x_n^{U_1}\}$. This series will use the equation computed from $\alpha e^{-ja} = INT(\alpha e^{-ja})$ to compute Equation (3.2) to become series (3.3). When computing (3.2), attention should be paid to the ECC's encryption legal terms being met. The prime number *p* generates the power series of (3.3), from which one of the values will be randomly chosen to be the cipher key of U_1 for the communication process, assigned as k_{U_1}. From $k_{U_1} = \beta_j^{U_1}$ and $\beta_j^{U_1} \in \beta^{U_1}$, along with Equation (3.4), the public key is calculated as follows.

$$\left(\alpha e^{-a}, \alpha e^{-2a}, \cdots, \alpha e^{-(m-1)a}, \alpha e^{-ma}\right) \tag{3.1}$$

$$\beta_i = \alpha e^{-ia} \bmod p \tag{3.2}$$

$$\beta^{U_1} = \{\beta_1^{U_1}, \beta_2^{U_1}, ..., \beta_m^{U_1}\} \tag{3.3}$$

$$P_{U_1} = k_{U_1} G \tag{3.4}$$

3.2 U_2 **generates cipher key** k_{U_2} **and public key** P_{U_2}**.** Next, like U_1, U_2 uses the same method to generate the parameters and series as $X^{U_2} = \{x_1^{U_2}, x_2^{U_2}, ..., x_n^{U_2}\}$(3.5).

$$\beta^{U_2} \{\beta_1^{U_2}, \beta_2^{U_2}, ..., \beta_m^{U_2}\} \tag{3.5}$$

From the series, a value will be randomly chosen for the cipher key. The public key is computed as follows.

$$P_{U_2} = k_{U_2} G \tag{3.6}$$

When both sides wish to communicate and have finished setting up the system, they can begin the mode for public key exchange and the calculation of the

conference key. First, U_1 and U_2 have to send their public keys to each other; then, the conference key $C_{U_1U_2}$ is calculated by Equation (3.7) as follows.

$$C_{U_1U_2} = (k_{U_1} k_{U_2})G \tag{3.7}$$

The factors that compose the conference key are formed with both parties' public and cipher keys. Therefore, there is no need for a third party to verify and manage the public keys, as illustrated in Figure 2.

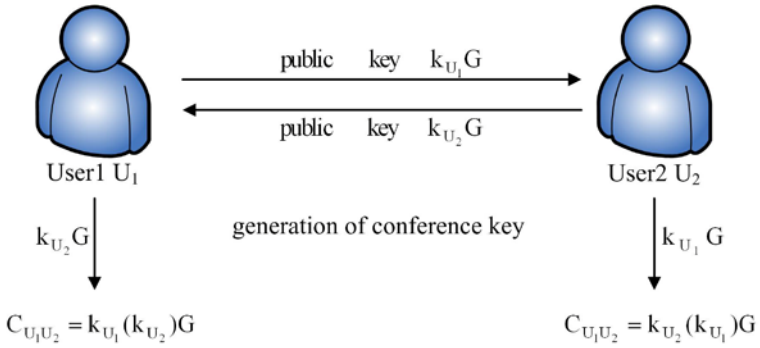

Figure 2: Public key exchanges and computation of conference keys

3.3 U_1 enciphers M_m to get SM_m and sends SM_m to U_2. When both sides have exchanged the public keys and also computed the conference key, transmission of information can begin. Supposing that U_1 needs to send a message M_m to U_2, the message M_m will be encrypted as cipher message SM_m in the following steps.

Step1: Firstly, U_1 calculates the conference key $C_{U_1U_2}$ according to the exchanged public keys. Calculated M_m in Equation (3.8), a cipher message SM_m is derived.

$$SM_m = C_{U_1U_2} + M_m \tag{3.8}$$

Step2: The cipher message SM_m is transmitted by U_1 to U_2.
Step3: END.

3.4 U_2 receives SM_m and deciphers SM_m to get M_m. When U_2 receives the cipher message SM_m from U_1, the conference key is calculated at the same time. Because the factors composing the conference key are made from both parties' public keys and U_2's personal cipher key, the message SM_m can thus be restored. The original message M_m can be restored in the following steps.

Step1: After receiving the cipher message SM_m, U_2 first calculates the conference key using Equation (3.9), and then remove the conference key from the cipher message.

$$M_m = SM_m - C_{U_1U_2} \tag{3.9}$$

Step2: END.

4. Elliptic Curve Cryptosystems Using Compound Conference Key $C'_{U_1U_2}$. Next, the second conference key approach described in this paper is introduced. The concept is similar to the first approach, where the encryption system is incorporated with the grey theory method. The constructed grey theory series is used to combine with the ECC method to further ensure the security of the key. At the same time, the values from the grey series are used to derive the key parameters from the first and second power series form the first part of the key. Firstly, U_1 chooses the values from the first power series $k_{U_1}^{(1)}$ and the second power series $k_{U_1}^{(2)}$ and the sum is divided by the prime number *p* selected by the ECC. This meets the ECC's legal terms and is made the cipher key. As with $N_{U_1}^* = k_{U_1}^{(1)} + k_{U_1}^{(n)} \bmod p$ to calculate $N_{U_1}^*$, where $N_{U_1}^*$ is one of the factors in the compound conference key; likewise, U_2 uses the same method to calculate $N_{U_2}^* = k_{U_2}^{(1)} + k_{U_2}^{(n)} \bmod p$, where the selected parameters are the same as those of U_1.

After the above parameters have been selected and computed, both sides send their individual $N_{U_1}^*$ and $N_{U_2}^*$. Before communication takes place between the two parties, the conference key $C'_{U_1U_2}$ is calculated by Equation (4.1).

$$C'_{U_1U_2} = (N_{U_1}^* N_{U_2}^*)G \tag{4.1}$$

U_1's $C'_{U_1U_2}$ is composed of $N_{U_1}^*$ and $N_{U_2}^* G$, while $C'_{U_1U_2}$ of U_2 is composed of $N_{U_2}^*$ and $N_{U_1}^* G$. As illustrated in Figure 3 below, $C'_{U_1U_2}$ calculated by both sides will be the same. At the same time, $C'_{U_1U_2}$ is used as the conference key.

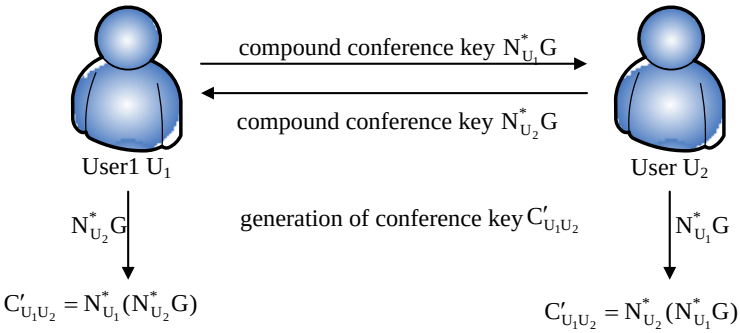

Figure 3: Computation of conference key $C'_{U_1U_2}$

4.1 U_1 enciphers M_m to get SM_m and sends SM_m to U_2. With the results calculated above, the message transmission stage is begun, according to the following steps.

Step1: U_1 computes the conference key $C'_{U_1U_2}$. A whole number *k* and a basic point *G* are chosen. The message M_m to be sent is encrypted by Equation (4.2) to form cipher message SM_m, where

$$SM_m = \{kG, M_m + kC'_{U_1U_2}\} \tag{4.2}$$

Step2: The cipher message SM_m is sent to the receiver.

Step3: END.

4.2 U_2 receives SM_m and deciphers SM_m to get M_m. Because both sides communicate through an encrypted conference key $C'_{U_1U_2}$, when U_2 receives the cipher message SM_m, the conference key is used again for decryption. Here, with the use of the receiver's $N^*_{U_2}$, the conference key can be decrypted, where restoration of the original message M_m can also begin.

Step1: After U_2 receives the cipher message SM_m, the conference key is firstly calculated. The received cipher message will contain two parts, the first being $SM_{m1} = kG$ and the second being $SM_{m2} = M_m + kC'_{U_1U_2}$. Using Equation (4.3), the original message M_m can be restored.

$$
\begin{aligned}
SM_{m2} - N^*_{U_2} SM_{m1} &= M_m + kC'_{U_1U_2} - N^*_{U_2}(kG) \\
&= M_m + kC'_{U_1U_2} - k(N^*_{U_2} G) \\
&= M_m + kC'_{U_1U_2} - kC'_{U_1U_2} \\
&= M_m
\end{aligned} \tag{4.3}
$$

Step2: END.

5. An Elliptic Curve Example Using Compound Conference Key $S'_{U_1U_2}$. The proposed method can be applied under insecure environments, for example, ad-hoc sensor networks. Sensors then can securely communicate and exchange information and can mutually verify each other' s identity, satisfying the three needs of confidentiality, completeness, and usability. When we apply the grey theory in the proposed method to the sensors in a sensor network, before spreading the sensors, by setting the original array of grey mathematics and the choice of keys, we can have different agreements: such as, time-difference, and general agreement between internal members of the sensor network about the password of different levels, which the attacker will not be able to calculate even with one legitimate password, nor the original array of grey mathematics. And when we incorporate the ECC public key cryptography system, the attacker will then have to face the ECDLP problem. Breaking the key thus becomes extremely difficult.

Supposing that two parties U_1 and U_2 of an ad-hoc sensor network are going to communicate, before communicating, they have to firstly choose an agreed legal ECC encryption system to be used as the basis for communication. Supposing that U_1 initiates communication and uses the parameters in the ECC system, the message M_m is encrypted to become SM_m, which is transmitted to U_2. The following is an example of ECC based on $E_{29}(2,3)$.

$$y^2 = x^3 + 2x + 3 \bmod 29,$$

$$D = 4a^3 + 27b^2 (\bmod 29) \neq 0$$

The set of points satisfying $E_{29}(2,3)$ is {(1, 8), (1, 21), (3, 6), (3, 23), (5, 14), (5, 15), (6, 12), (6, 17), (8, 3), (8, 26), (9, 5), (9, 24), (11, 14), (11, 15), (13, 14), (13, 15), (14, 7), (14, 22), (16, 10), (16, 19), (17, 7), (17, 22), (18, 10), (18, 19), (22, 9), (22, 20), (23, 6), (23, 23), (24, 10), (24, 19), (26, 12), (26, 17), (27, 7), (27, 22), (28, 0)}. The point O is the infinite point of $E_{29}(2,3)$. G = (9, 5) is chosen from $E_{29}(2,3)$ by both U_1 and U_2. The order is n = 36. M_m= (3, 6) = 4G is assumed.

$E_{29}(2,3)\ y^2 = x^3 + 2x + 3 \bmod 29$									
G	(9, 5)	$2G$	(24, 19)	$3G$	(26, 12)	$4G$	(3, 6)	$5G$	(13, 15)
$6G$	(6, 17)	$7G$	(1, 21)	$8G$	(23, 23)	$9G$	(17, 22)	$10G$	(27, 22)
$11G$	(16, 19)	$12G$	(8, 26)	$13G$	(18, 10)	$14G$	(22, 20)	$15G$	(11, 15)
$16G$	(5, 15)	$17G$	(14, 22)	$18G$	(28, 0)	$19G$	(14, 7)	$20G$	(5, 14)
$21G$	(11, 14)	$22G$	(22, 9)	$23G$	(18, 19)	$24G$	(8, 3)	$25G$	(16, 10)
$26G$	(27, 7)	$27G$	(17, 7)	$28G$	(23, 6)	$29G$	(1, 8)	$30G$	(6, 12)
$31G$	(13, 14)	$32G$	(3, 23)	$33G$	(26, 17)	$34G$	(24, 10)	$35G$	(9, 24)

U_1 chooses, from the first power series, a value $n_{U_1}^{(1)} = 5$ to be the first cipher key, while the second cipher key $n_{U_1}^{(2)} = 5$ is selected from the second series. The two cipher keys are added and then divided by $p = 29$. The compound cipher key of U_1 is $N_{U_1}^* = (5 + 5 \bmod 29) = 10$.

Likewise, U_2 chooses a value $n_{U_2}^{(1)} = 5$ from the series to be the first cipher key, while the second key $n_{U_2}^{(2)} = 7$ is chosen from the second power series. The two are added and then divided by $p = 29$. The compound cipher key of U_2 obtains the compound cipher key of B to be $N_{U_2}^* = (5 + 7 \bmod 29) = 12$. $N_{U_1}^*$, $N_{U_2}^*$, and G are calculated to be the conference key which both sides can use. $C'_{U_1U_2}$ of U_1 and U_2 can be computed as follows.

$$\begin{aligned} C'_{U_1U_2} &= N_{U_2}^* (N_{U_1}^* G) \bmod 36 \\ &= (n_{U_2}^{(1)} + n_{U_2}^{(2)} \bmod p)(n_{U_1}^{(1)} + n_{U_1}^{(n)} \bmod p)\ G \bmod 36 \\ &= (10)((12)\ G) \bmod 36 \\ &= 12G \bmod 36 \\ &= (8,\ 26) \end{aligned}$$

5.1 U_1 enciphers M_m to get SM_m and sends SM_m to U_2. When U_1 exchanges messages with U_2, the above $C'_{U_1U_2}$ can be treated as the key. The following processes allow SM_m to be transmitted to U_2。

Step1: U_1 firstly computes $C'_{U_1U_2}$, the conference key of U_1 and U_2. Then U_1 chooses a positive integer k = 4 and a basic point G = (9, 5) for enciphering plaintext M_m to get ciphertext SM_m, where

$$\begin{aligned} SM_m &= \{kG,\ M_m + kC'_{U_1U_2}\} \\ &= \{4G,\ 4G + 4(12G)\} \\ &= \{4G,\ 16G\} \\ &= \{(3,6),(5,15)\} \end{aligned}$$

Step2: U_1 sends SM_m to U_2.

Step3: END.

5.2 U_2 receives SM_m and deciphers SM_m to get M_m. When U_2 receives SM_m from U_1, the following processes are proceeded to revert to the original M_m.

Step1: U_2 firstly computes $C'_{U_1U_2}$, the conference key of U_1 and U_2, and then takes SM_m's second term $SM_{m2} = M_m + kC'_{U_1U_2}$, the product of SM_m's first term $SM_{m1} = kG$, and U_2's two cipher keys $N^*_{U_2}$ to decipher the cipher message SM_m to get plaintext M_m.

$$\begin{aligned} SM_{m2} - N^*_{U_2} SM_{m1} &= M_m + kC'_{U_1U_2} - N^*_{U_2}(kG) \\ &= 16G - 12(4G) \bmod 36 \\ &= 16G - [48G \bmod 36] \bmod 36 \\ &= 16G - 12G \bmod 36 \\ &= 4G \bmod 36 \\ &= M_m \end{aligned}$$

Step2: END.

6. Analysis. The progress in networks and computational abilities has improved decryption or hacking methods, which threatens the current environment of encryption systems with solutions to cracking them, and therefore increasingly challenges the security offered by the systems. Regardless the key length being forced to grow in length, new and special ways, which cannot be mentioned one by one, continue to decrypt and crack current systems. However, there has not been one effective method for attacks to tackle the difficult ECDLP of ECC, allowing key

length to avoid rapid growth in size in contrast with other known cryptosystems, e.g., RSA. The ECDLP is also based on the DLP problem, which is recognized to be more secure than DLP. The following function is constructed by the computation of the key encryption process using cipher key x and public key y.

$$y = g^x \bmod p$$

If the chosen prime number p is large enough, even when y, g, and p are known, it is still very difficult to use discrete logarithm to obtain the private key x. With this security feature that trumps other cryptosystems and the fact that most attacks are carried out against keys, the ECDLP is relatively effective in security protection. However, should there come up a way to effectively solve this difficult problem, the ECC encryption system will no longer be safe. The proposed method then combines the grey theory method with ECC cryptography because when the class series computed from the grey theory [13, 14] are rounded up as an approach to form new series, during the computation of the series, some commonly used constants will confuse attackers. In addition, by incorporating the average value calculation approach in the series calculation, many computational choices can be chosen, which causes difficulties in attacks. Only the original series have to be saved for re-computation to prevent internal security incidents. In addition, by combining with the ECC cryptography, the proven difficulty of ECDLP will be faced when one desires to crack. Together with ECC cryptography features of short key length and low computational load, the ECC method presents better security and efficiency than other cryptosystems that are based on difficulties of solving DLP or other difficult problems. These explain how the proposed method is an effective and secure mechanism.

7. Conclusion. The network environment is an open public environment that is not safe. When users want to exchange confidential message or information through the network, they can be easily attacked or eavesdropped. At times, it is the third-party verifiers, who are not entrusted, leading to frequent information security incidents. To prevent the third party from leaking confidential data, the best way is to avoid using a third party and to manage the communication process carefully all by oneself. This is a more conservative approach.

In order to solve such a problem and meet environment needs, the proposed method combines the grey modeling approach in the grey theory to derive a class of series and through the use of different averaging methods, so as to protect the system from malicious attacks. At the same time, by using integers and the values from the forecasted series to create the cipher key for ECC's encryption process, internal

security incidents are prevented. In addition, this method integrates the concepts of ECC and H-B to build a new conference key encryption system. This system only requires the communicators to initiate the encryption of the complex mathematical computations to assure its security in the network, avoiding the need for a third party to verify and manage the public key or other items of identification. This not only protects the system from malicious external attacks, but also effectively eliminates trust concerns regarding the management. It is also applicable in environments that do not have managerial parties. This can be thought as two computers which would like to initiate a wireless communication with the ad-hoc approach, without the security concerns on AP's (Access Point) access to information. Through the proposed method, even when attackers would like to steal the cipher key during an information transmission, while facing ECDLP, it is impossible to solve cipher message within the effective period. Through the security analyses, the method cuts back on many unnecessary exhaustive computations, while at the same time maintains or exceeds the security level of the RSA method. This proves that the proposed method is efficient and secure.

Acknowledgement

This work was supported partially by National Science Council of Republic of China under Grants NSC 99-2221-E-029 -023.

REFERENCES

[1] N. Koblitz, "Elliptic Curve Cryptosystems," *Mathematics of Computation*, Vol. 48, No. 17, pp. 203-209, 1987.

[2] D.J. Long, "Introduction to Grey System Theory," *The Journal of Grey System*, Vol. 1, No. 1, pp. 1-24, 1989.

[3] A.J. Menezes and S.A. Vanstone, "Elliptic Curve Cryptosystem and Their Implementation," *Journal of Cryptology*, Vol. 6, No. 4, pp. 209-224, 1993.

[4] S. Vanston, "Elliptic Curve Cryptosystem - The Answer to Strong," *Fast Public-Key Cryptography for Securing Constrained Environments*, *Elsevier Information Security Technical Report*, Vol. 2, No. 2, pp. 78-87, 1997.

[5] A. Jurisic and A. J. Menzes, "Elliptic Curves and Cryptography," *Dr-Dobb's Journal*, pp. 26-35, 1997.

[6] W. Caelli, E. Dawson and S. Rea, "PKI, Elliptic Curve Cryptography and Digital Signatures," *Elseiver Computer and Security*, Vol.18, No. 1, pp. 47-66, 1999.

[7] T. S. Chen and K. Q. Shi, "The Grey Generation Lock and its Password Encryption System (I),"

Journal of Grey System, Vol. 13, No. 3, pp. 237-247, 2001.

[8] K.Q. Shi and T.S. Chen, "The Grey Generation Lock and its Password Encryption System (II)," J*ournal of Grey System*, Vol. 13, No. 3, pp. 269-276, 2001.

[9] V.S. Miller, "Use of Elliptic Curves in Cryptography," *Advances in Cryptology: Proceedings of Crypto '85*, Vol. 218, pp. 417-426, 1986.

[10] S.T. Wu, "Authentication and Group Secure Communications Using Elliptic Curve Cryptography," *Doctoral Dissertation*, National Taiwan University of Science and Technology, Taipei, 2005.

[11] C.W. Shieh, "An Efficient Design of Elliptic Curve Cryptography Processor," *Master Thesis*, Tatung University, Taipei, 2006.

[12] N. Xie and S. Liu, "Research on Discrete Grey Model and Its Mechanism," *Systems, Man and Cybernetics, IEEE International Conference*, Vol. 1, pp. 606-610, 2005.

[13] L. Yi and S. Liu, "A Historical Introduction to Grey Systems Theory," *Systems, Man and Cybernetics, 2004 IEEE International Conference*, Vol. 3, pp. 2403-2408, 2004.

[14] T. Yao, S. Liu and N. Xie, "On The Properties of Small Sample of *GM*(1,1) Model," *Applied Mathematical Modelling*, Vol. 33, No. 4, pp. 1894-1903, 2009.

[15] R.L. Shen, Y.F. Chung, and T.S. Chen, "A Novel Application of Grey System Theory to Information Security (Part I)," *Computer Standards and Interfaces*, Vol. 31, No. 1, pp. 277-281, 2009.

[16] C. Wang and W. Chen, "Novel Data Processing Mechanism of Grey Control Model," *2009 International Conference on Artificial Intelligence and Computational Intelligence*, Vol. 4, pp. 224-227, 2009.

[17] Y.M. Tseng, "A Communication-Efficient and Fault-Tolerant Conference-Key Agreement Protocol with Forward Secrecy," *Journal of Systems and Software*, Vol. 80, No.7, pp. 1091-1101, July, 2007.

[18] N.C. Wang and S.Z. Fang, "A Hierarchical Key Management Scheme for Secure Group Communications in Mobile Ad Hoc Networks," *Journal of Systems and Software*, Vol. 80, pp. 1667-1677, October, 2007.

[19] S. Lee, J. Kim and S.J. Hong, "Security Weakness of Tseng's Fault-Tolerant Conference-Key Agreement Protocol," *Journal of Systems and Software*, Vol. 82, No.7, pp. 1163-1167, July 2009.

[20] H.F. Huang, C.W. Chan, C.H. Lin and H.W. Wang, "A Low-Computation Conference Key System for Mobile Communications," *International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 2, pp. 461-466, 2009.

[21] Y.M. Tseng, T.Y. Wu and J.D. Wu, "An Efficient and Provably Secure ID-Based Signature Scheme with Batch Verifications," *International Journal of Innovative Computing, Information and Control*, Vol. 5, No. 11(A), pp. 3911-3922, 2009.

[22] M.S. Hwang, S.F. Tzeng and S.F. Chiou, "A Non-Repudiable Multi-Proxy Multi-Signature Scheme," *ICIC Express Letters*, Vol. 3, No. 3(A), pp. 259-264, 2009.

[23] M. Wang, H. Hu and G. Dai, “An Identity-Based Signature Scheme for Mobile Business,” *ICIC Express Letters*, Vol. 4, No. 2, pp. 565-570, 2010.