Computer Science and Information Systems 11(3):1091–1112 DOI: 10.2298/CSIS130924066C

# A Secure E-Mail Protocol Using ID-based FNS Multicast Mechanism

Hsing-Chung Chen[1], Cheng-Ying Yang[2], Hui-Kai Su[3], Ching-Chuan Wei[4], and Chao-Ching Lee[1]

[1] Department of Computer Science and Information Engineering,
Asia University, Taichung 413, Taiwan
shin8409@ms6.hinet.net, cdma2000@asia.edu.tw
[2] Department of Computer Science, University of Taipei,
Taipei 100, Taiwan
cyang@uTaipei.edu.tw
[3] Department of Electrical Engineering,
National Formosa University, Yunlin 632, Taiwan
hksu@nfu.edu.tw
[4] Department of Information and Communication Engineering,
Chaoyang University of Technology, Taichung 413, Taiwan
ccwei@cyut.edu.tw

**Abstract.** Electronic mail (e-mail) has been used to transfer various types of electronic data in Internet. Usually, a user has to send an e-mail to a specific group of users with a secure delivery mechanism. In this paper, a novel and feasible e-mail delivery mechanism using the secure multicast protocol with an ID-based factorial number structure (FNS) is proposed in the multicast system. In the proposed e-mail delivery mechanism, the e-mail is required to be encrypted before sending out in order to safeguard the message via a public channel, such as wire public switching communication links and wireless communication systems. Without loss generality, the public-key system is adopted in the proposed secure multicast system for a convenient and easy key management. The proposed scheme outperforms the existing methods for more easily to construct secure e-mail system. Furthermore, the security of the proposed scheme is analyzed, including replay attack, sender impersonation attack, unknown key-share attack, forgery attack and insider attack. Finally, the computation complexities of the proposed mechanism are discussed. The result shows that the proposed scheme outperforms the CRT-based secure e-mail scheme.

**Keywords:** factorial number structure, e-mail, security, cryptography.

## 1. Introduction

People widely use electronic mails (e-mails) to communicate with each other in Internet. Delivering an e-mail in Internet, people could exchange not only normal text-based letter, but also sensitive rich electronic files. Because of the popularity, e-mail systems become an adversary's or a malicious user's targets. Among the e-mail security issues, basic and primary concerns are the confidentiality and authentication for the e-mails [1].

Some data cryptosystems [2] can satisfy those concerns. Users can utilize a specific interactive key to encrypt and to verify their e-mails. However, the e-mail system is a kind of store-and-forward system in which e-mail servers act as a proxy to accept, forward, and store users' e-mails. User does not need continuously on-line to connect with an e-mail server. When a user wants to get the emails that are received and stored in the server, he/she has to access the email server first. For example, sender $B$ intends to send an e-mail to receiver $A$. Sender $B$ firstly sends the e-mail to the mail server $S_B$, and then the mail server $S_B$ forwards the e-mail to receiver $A$ 's mail server $S_A$. Following, the mail server $S_A$ stores the e-mail in the storage. As receiver $A$ connects to the e-mail server $S_A$, receiver $A$ sends a request for new e-mails, and the mail server $S_A$ forwards the stored e-mail to receiver $A$. Obviously, e-mail users are not always on-line. However, the e-mail users could not exchange the session key in time within a secure on-line system. To solve this difficulty, there are several challenges, such as authentication and secure key distribution [2], to mail server. Public key systems could provide a solution but need much time to deal with encrypt or decrypt. The hybrid cryptosystems to prevent the high computation is also provided [3]. Another more efficient solution is provided by Pretty Good Privacy (PGP) protocol.

PGP was designed and implemented for distributed networks in 1991. It is a well-known secure e-mail protocol that provides confidential data between senders and receivers. It is available on almost any platform which aims to be used within existing e-mail systems [4], [5], [6], [7]. PGP protocol [8] utilizes the idea in the hybrid cryptosystems to securely transfer a session key to both of the corresponding sender and receiver. A sender in the PGP system is given a certificated public key. The certificated public key can be applied to a secure channel to transfer the session key within the session key is used for encrypting the emails between the sender and the receiver. A user cannot verify the validity of PGP keys for each other. However, under many circumstances, a sender needs to send a single email to each other. Hence, how to transfer a session key to multi-receivers is a challenge for securing e-mail systems. Hung-Min Sun et.al. [9] proposed two novel e-mail protocols to provide a perfect forward secrecy. The basic protection in an e-mail system is to encrypt the bulk mail using a conventional cryptosystem with a short-term key and to protect the short-term key using a public-key cryptosystem with the receiver's public key. Amna Joyia, et.al. [10] found that an attacker can easily track from email header which are normally transported in clear text. Furthermore, this information can be manipulated for malicious purposes like sending spam messages to the extracted user identities, analyzing traffic to extract the behavior of both sender and receiver. All these attacks lead to vivid threat to the user's privacy. Then, he designed and implemented a secure and privacy enhanced email system which provided the solution to ensure the privacy of e-mail users. However, in the multicasting system, it uses PGP scheme to send e-mail for lots of specific receivers. It has to send the e-mail one-by-one. For example, as a user usually needs to send an e-mail to a group of users, in the exiting e-mail protocols such as Simple Mail Transfer Protocol (SMTP), the e-mail server forwards the copies of this e-mail to the receivers. Intending to deliver an e-mail to receivers $A$, $C$ and $D$, receiver $B$ initially sends an e-mail to the mail server $S_B$. Then, the mail server $S_B$ forwards the copies of this e-mail to the mail servers $S_A$, $S_C$ and $S_D$ for

receivers, respectively. Next, the mail servers $S_A$, $S_C$ and $S_D$ wait for the request for the new e-mails from the receivers. For example, if $S_C$ receives a request sent by the receiver $C$, $S_C$ forwards the copy of the e-mail to the receiver $C$. In the repeatedly transmission, there exists a redundant computation which causes a significant delay. Hence, to send e-mails in the multicast system, it has to look for another efficient solution.

In 1985, the Identity-Based Cryptosystems and Signature Schemes were first proposed by Adi Shamir [11]. A novel type of cryptographic scheme was proposed to enable any pair of users to communicate securely. In 2005, McCullagh, N. [12] proposed another solution for secure e-mail with identity-based encryption. It could allow an arbitrary string of characters and numbers to serve as a public key. It had some effects in simplifying public-key encryption. In 2010, Anastasios Kihidis et.al. [13] presented a complete implementation of a practical Identity Based Encryption (IBE) infrastructure for secure e-mail communication. It attempted to simultaneously provide a fully functional and user-friendly IBE system. A packet construction mechanism using an ID-based factorial number structure (FNS) was proposed by Chen H.C. [14], [15], [16] for a secure system to provide a feasible solution for a secure multicast system. In 2010, Zhang M.Q. et. al. [17] presented a secure and efficient ID-based fair multi-party exchange protocol with off-line semi-trusted third party. Application of multi-receiver identity-based encryption. In 2013, Mingwu Zhang et.al. [18] proposed an efficient anonymous multi-receiver encryption scheme to achieve the security properties of confidentiality and anonymity. The anonymity of the proposed scheme could securely against outer attackers and inner attackers simultaneously, and also presented a dual-anonymous multi-receiver encryption that could support the security properties such as identity privacy of both sender and receiver.

In 2013, Chen H.C. [15] proposed a secure multicast protocol for e-mail systems. A user usually needs to send an e-mail to a group of users. The proposed secure multicast protocol [15] for e-mail systems could provide perfect forward secrecy to ensure confidentiality and authentication. The protocol [15] employs the Chinese Remainder Theorem (CRT), RSA public key cryptosystems, and one-way hash functions. The protocol can save redundant key materials used for the e-mails. However, CRT will take a very long time in the calculation to factor for a large integer. In this paper, a secure multicast key protocol is proposed a solution to the e-mail systems for distributing a session key to the specific group. Due to the concerning for the securely transferring the session key, the proposed protocol adopts ID-based FNS [14] to replace CRT [15] is proposed. The scheme is based on ID-based FNS [14] with the hybrid cryptographic algorithms of public-key and secret-key system [19-25]. In the manner, not only the e-mail construction in multicast system can be efficiently retained, but also the easy key management and fast computation [21], [22], [23], [24], [25] to process a multiple secure e-mail delivery can be proficiently achieved. The proposed protocol benefits for an excellent secure broadcast e-mail system [25]. The rest of this paper is organized as the followings, the fundamental theory of the ID-based FNS are addressed in Section 2. Two scenarios consist of corresponding schemes are proposed in Section 3. Security and complexity analyses are described in Section 4. Finally, conclusions are given in Section 5.

## 2. Fundamental Theory of the ID-based FNS

ID-based FNS [15] in a secure multicast key scheme begins with Lemma 1.

**Lemma 1.** $P^*_{(i,0)}, P^*_{(i,1)}, \ldots, P^*_{(i,j)}, \ldots, P^*_{(i,k)}, \ldots, P^*_{(i,m-1)}$ be positive integers, where $P^*_{(i,j)} \neq P^*_{(i,k)} \neq 0$, $0 \leq j$, $k \leq m-1$, $j \neq k$. The values of $P_{(i,0)}, P_{(i,1)}, \ldots, P_{(i,m-1)}$ are gotten as the followings, $P_{(i,o)} = \sum_{j=0}^{m-1} p^*_{(i,j)}$, $P_{(i,1)} = \sum_{j=1}^{m-1} p^*_{(i,j)}$, …, $P_{(i,m-1)} = \sum_{j=m-1}^{m-1} p^*_{(i,j)} = p^*_{i,m-1}$ such that the inequality relation of $P_{(i,0)} > P_{(i,1)} > \ldots > P_{(i,m-2)} > P_{(i,m-1)}$ is satisfied.

□

**Theorem 1.** Let $P^*_{(i,0)}, P^*_{(i,1)}, \ldots, P^*_{(i,m-1)}$ be positive integers, where $P^*_{(i,j)} \neq P^*_{(i,k)} \neq 0$. And, the values of $P_{(i,0)}, P_{(i,1)}, \ldots, P_{(i,m-1)}$ are obtained by Lemma 1, respectively. There exists a positive integer, $Z_i = \sum_{j=0}^{m-1} \alpha_{(i,j)} p_{(i,j)}$, such that the individual positive integer can be retrieved by the equation,

$$\begin{aligned} p^*_{(i,j)} &= p_{(i,j)} - p_{(i,j+1)} \\ &= \left\{ \left[ \frac{Z_i}{\alpha_{(i,j)}} \right] mod(T_i - x_{(i,j-1)}) \right\} - \left\{ \left[ \frac{Z_i}{\alpha_{(i,j+1)}} \right] mod(T_i - x_{(i,j)}) \right\}, \end{aligned} \tag{1}$$

where some notations are defined as followings.

$T_i = max\{P_{(i,0)}, P_{(i,1)}, \ldots, P_{(i,m-1)}\}$, $\alpha_{(i,0)} = \prod_{j=m-2}^{0} (T_i - x_{(i,j)})$, $\alpha_{(i,1)} = \prod_{j=m-2}^{1} (T_i - x_{(i,j)})$, … , and $\alpha_{(i,m-2)} = \prod_{j=m-2}^{m-2} (T_i - x_{(i,j)})$, $\alpha_{(i,m-1)} = 1$,

$I_0, I_1, \ldots, I_i, \ldots, I_{m-1}$ : The Identity numbers that are corresponding to the positive integers $P^*_{(i,0)}, P^*_{(i,1)}, \ldots, P^*_{(i,m-1)}$ respectively. The numbers of $I_i, i = 0,1,\ldots,m-1$, are pre-sorted by decreasing order as the relations: $I_0 > I_1 > \ldots > I_i > \ldots > I_{m-1}$.

$x_{(i,-1)} = -1$ , $x_{(i,0)} = \sum_{j=0}^{m-1} I_j$ , $x_{(i,1)} = \sum_{j=1}^{m-1} I_j$ , …, and $x_{(i,m-1)} = \sum_{j=m-1}^{m-1} I_j$ that satisfy $(p_{(i,0)} - x_{(i,j)}) >> p_{(i,j)}$ for $j \in \{1,2,\ldots m-1\}$.

As observed Theorem 1, the list of generated $p^*_{(i,j)}$, $j = 0,1,2,\ldots m-1$ is shown as the followings,

$$p^*_{(i,0)} = p_{(i,0)} - p_{(i,1)} = \sum_{j=0}^{m-1} p^*_{(i,j)} - \sum_{j=1}^{m-1} p^*_{(i,j)},$$

$$p^*_{(i,1)} = p_{(i,1)} - p_{(i,2)} = \sum_{j=1}^{m-1} p^*_{(i,j)} - \sum_{j=2}^{m-1} p^*_{(i,j)},$$

$$\vdots$$

$$p^*_{(i,m-2)} = p_{(i,m-2)} - p_{(i,m-1)} = \sum_{j=m-2}^{m-1} p^*_{(i,j)} - \sum_{j=m-1}^{m-1} p^*_{(i,j)},$$

$$p^*_{(i,m-1)} = p_{(i,m-1)}.$$

□

The fact of *Theorem 1* can be seen in the Appendix of Ref. [15]. Let ID-based FNS be more easily readable and, therefore, Example 1 be given as below.

**Example 1.** Assume that there exists five identical numbers which are sorted by the decreasing order, $I_0 = 31$, $I_1 = 29$, $I_2 = 23$, $I_3 = 12$ and $I_4 = 9$, where these numbers are the published identification numbers for the users, $u_0$, $u_1$, $u_2$, $u_3$ and $u_4$, respectively, in the communication group. Assume that participant $u_0$ whose identical number is $I_0$ wants to send a secure multicast key to $u_1$, $u_2$, $u_3$ and $u_4$ by a broadcast mechanism. Following, $u_0$ will choose the positive integers $p_0^* = 98$, $p_1^* = 123$, $p_2^* = 65$, $p_3^* = 72$ and $p_4^* = 132$ corresponding to $I_0$, $I_1$, $I_2$, $I_3$ and $I_4$, respectively. Then, according to *Lemma 1*, $u_0$ computes the values *of* $P_0^*, P_1^*, ..., P_4^*$ *as the followings,* $p_0 = \sum_{i=0}^{4} p_i^* = 490$, $p_1 = \sum_{i=1}^{4} p_i^* = 392$, $p_2 = \sum_{i=2}^{4} p_i^* = 269$, $p_3 = \sum_{i=3}^{4} p_i^* = 204$, $p_4 = \sum_{i=4}^{4} p_i^* = 132$ individually, such that $p_0 > p_1 > p_2 > p_3 > p_4$ is satisfied. In order to pack the five numbers, $p_0, p_1, p_2, p_3, \text{and } p_4$, into a fixed integer $Z_0$, the accumulative operation in the decreasing order is launched. Therefore, $u_0$ obtains $x_0 = \sum_{i=0}^{4} I_i = 104$, $x_1 = \sum_{i=1}^{4} I_i = 73$, $x_2 = \sum_{i=2}^{4} I_i = 44$, $x_3 = \sum_{i=3}^{4} I_i = 21$, $x_4 = \sum_{i=4}^{4} I_i = 9$, respectively.

Moreover, $u_0$ calculates $T = max\{p_0, p_1, p_2, p_3, p_4\} = 490$. The $\alpha_i$ for $i = 0, 1, 2, 3, 4$ is defined by Equation (1) and found as the follows:

$$\alpha_0 = \prod_{i=3}^{0} (T - x_i) = 33669065388,$$

$$\alpha_1 = \prod_{i=3}^{1} (T - x_i) = 87225558,$$

$$\alpha_2 = \prod_{i=3}^{2} (T - x_i) = 209174,$$

$$\alpha_3 = \prod_{i=3}^{3} (T - x_i) = 469,$$

and $\alpha_4 = 1$.

According to the given results: $\alpha_i$'s and $p_i$'s values for $i = 0, 1, 2, 3, 4$, the fixed integer $Z = \sum_{i=0}^{4} \alpha_i p_i = 16532090822347$ is constructed. Then, sender $u_0$ sends the packet $\{16532090822347 \,||\, 490\}$ to $u_1$, $u_2$, $u_3$ and $u_4$ by using a broadcast mechanism.

Next, according to *Theorem 1*, each one of the participants calculates the values for $x_{-1}, x_1, x_2, x_3$ and $x_4$ by using the published identical numbers and attempts to directly extract the $p_i$ values from the summed $Z_0$ by using Equation (1).

$$p_0 = \left\lfloor \frac{Z}{\alpha_0} \right\rfloor mod(T - x_{-1}) = 490,$$

$$p_1 = \left\lfloor \frac{Z}{\alpha_1} \right\rfloor mod(T - x_0) = 392,$$

$$p_2 = \left\lfloor \frac{Z}{\alpha_2} \right\rfloor mod(T - x_1) = 269,$$

$$p_3 = \left\lfloor \frac{Z}{\alpha_3} \right\rfloor mod(T - x_2) = 204,$$

$$p_4 = \left\lfloor \frac{Z}{\alpha_4} \right\rfloor \mathrm{mod}(T - x_3) = 132.$$

$$p_0 - p_1 = 490\text{-}392 = 98 = p_0^*,$$

$$p_1 - p_2 = 392\text{-}269 = 123 = p_1^*,$$

$$p_2 - p_3 = 269 - 204 = 65 = p_2^*,$$

$$p_3 - p_4 = 204 - 132 = 72 = p_3^*,$$

$$p_4 = p_4^* = 132.$$

When the resulting $p_i^*$ values are recovered from the original ones.

## 3. Proposed Scheme

Some notations are defined and listed in Table 1. Two scenarios and the corresponding schemes are described and designed in Section 3.1 and 3.2, respectively. The first scenario deals with that a sender sends an e-mail to one recipient. For the multicast concerning, the second scenario scopes with that a sender sends an e-mail to specific recipients.

The following notations are used to describe the security protocol and cryptographic operations in this paper.

**Table 1.** Notations

| Notations | Descriptions |
|---|---|
| $U_i$ | The $i$ -th user in the e-mail system |
| $TC$ | The trust center |
| $S$ | The mail server |
| $M$ | A plain-text content of the e-mail |
| $K_c$ | The communication key is randomly generated by the e-mail sender |
| $PK_i$ | A user $U_i$ 's public key |
| $SK_i$ | A user $U_i$ 's secret key corresponding to the $PK_i$ |
| $ID_j$ | A uniquely identifies user $U_i$ where $ID_1 > ID_2 > \cdots > ID_n$ |
| $E_k(M)$ | A asymmetric encryption algorithm using to encrypt the e-mail message $M$ via a secret key $k$ |
| $D_k(C)$ | A asymmetric decryption algorithm using to decrypt the encrypted e-mail message $C$ via a key $k$ |
| $Sig_k(m)$ | A signature algorithm used to generate signature of the message $m$ using the secret key $k$ |
| $h(\cdot)$ | A cryptographically secure one-way hash function |
| $\|\|$ | A catenation symbol |
| $A \rightarrow B$ | A symbol indicates that the certain message sent from the entity $A$ to the entity $B$ |

### 3.1. Scenario I: A sender sends an e-mail to one recipient

A sender sends an e-mail to one recipient. In Fig. 1, it shows that an e-mail is sent from sender B to receiver A, individually. There are three parts in this scenario. The first one is Pre-computation that consists steps, S1 and S2. Another one is Sending phase that describes the steps from S3 to S13. The other one is Receiving phase that illustrates the steps from S14 to S23.

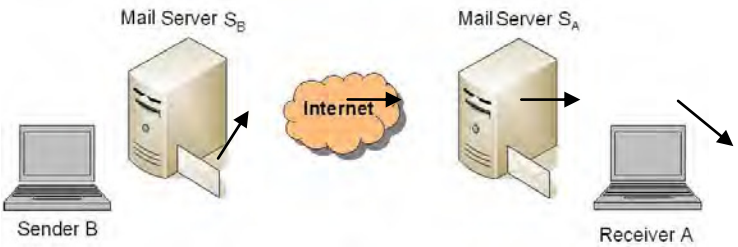


**Fig. 1.** The scenario of an e-mail sent from a sender B to a single receiver A [15]

1) Pre-computation

Step S1: $TC \rightarrow U_i$: $g$, $n$. $TC$ generates randomly a number $g$, and chooses a big prime $n$ sent to the $U_i$. The sender chooses a secret key $k_i$ and computes the public key $e_{k_i} = g^{k_i} \bmod n$. Then, the receiver also chooses a secret key $k_j$ and computes the public key $e_{k_j} = g^{k_j} \bmod n$.

Step S2: $U_i \rightarrow S$: $e_{k_i}$, $e_{k_j}$, $Sig_{SK_i}(e_{k_i})$, $Sig_{SK_i}(e_{k_j})$, $ID_j$. A user $U_i$ generates another pair of public key and secret key $(e_{k_i}, k_i)$ and $(e_{k_j}, k_j)$. This pair of public key and secret key are not related to the pair of public key $PK_i$ and secret key $SK_i$ pre-distributed by the system. The user $U_i$ sends $e_{k_i}$, $e_{k_j}$ and $Sig_{SK_i}(e_{k_i})$, $Sig_{SK_i}(e_{k_j})$ to the e-mail server. Note that this procedure is executed after the user $U_i$ finished receiving an e-mail. Then e-mail server arranges all the $ID_j$ where $ID_1 > ID_2 > \cdots > ID_n$.

2) Sending Phase

Step S3: $S \rightarrow U_1$: $e_{k_1}, e_{k_2}$, $Sig_{SK_1}(e_{k_1}), Sig_{SK_2}(e_{k_2})$, $ID_1, ID_2$.

Step S4: $U_1$ randomly generates the communication key $K_c$.

Step S5: The encrypted e-mail message $C = E_{K_c}(M)$ is encryption under the chosen key $K_c$, where $M$ is the content message of the e-mail.

Step S6: The $p^*_{i,j}$ for each receivers is computed by applying $p^*_{i,j} = E_{k_{i,j}}(K_c)$ for all $j = 1, 2$. The generation of $k_{i,j}$ will follow the rule of $k_{i,j} = (e_{k_j})^{k'_i} \bmod n = (g^{k'_j})^{k'_i} \bmod n = g^{k'_i k'_j} \bmod n$.

Step S7: Each $p^*_{i,j}$ for all $j = 1, 2$ is computing using the following equations, $p_{i,1} = \sum_{j=1}^{2} p^*_{i,j}$, $p_{i,2} = \sum_{j=2}^{2} p^*_{i,j}$, such that the decreasing order relation $P_{i,1} > P_{i,2}$ is satisfied. Moreover $T = p_1$ is set, which the maximal value of the set is of $\{P_{i,1}, P_{i,2}\}$. A polynomial $f(x)$ is then

constructed by the originator as the followings, $f(x)=T+(x-k_{i,1})\times(x-k_{i,2})$.

Step S8: Then set $\{P_{i,1},P_{i,2}\}$ is encrypted to be a sub-packet $\Gamma$ by the way of $\Gamma=E_T(p_{i,1}||p_{i,2})$.

Step S9: Sum up $x_{i,j}=\sum_{j}^{n} ID_j$. Define the initial value $x_{-1}=-1$. Compute $x_{i,1}=\sum_{j=1}^{2} ID_j$, $x_{i,2}=\sum_{j=2}^{2} ID_j$.

Step S10: Compute $\alpha_{i,j}$'s for $j=1$ to $j=2$ using the following equations, $\alpha_{i,1}=\prod_{j=2-1}^{1}(T-x_{i,j})$, and $\alpha_2=1$.

Step S11: Construct a basic e-mail packet lock $Z$ as the format of $Z=\sum_{j=1}^{2}\alpha_{i,j}p_{i,j}$.

Step S12: Compute a varied e-mail packet lock in bit-wise exclusive-or operation of follow: $L=Z\oplus E_T(T)$.

Step S13: $U_1\rightarrow S$ : $C$, $L$, $f(x)$, $\Gamma$, $Y$, $t$, where $Y=Sig_{PK_1}(h(ID_1||ID_2||M||t))$. The parameter $t$ is a timestamp at that time.

3) Receiving Phase

Step S14: $S\rightarrow U_i$: $C$, $L$, $f(x)$, $\Gamma$, $Y$, $t$, $ID_1, ID_2$.

Step S15: Find the maximal sub-packet by computing $f(k_{i,j})=T$, and let $\zeta=E_T(T)$.

Step S16: Decrypt the set $\{P_{i,1},P_{i,2}\}$ by using the following equation: $D_T(\Gamma)=(P_{i,1}||P_{i,2})$.

Step S17: Find the e-mail packet lock $Z$ by computing $L\oplus\zeta=(Z\oplus E_T(T))\oplus\zeta=Z$.

Step S18: Sum up $x_{i,j}=\sum_{j}^{n} ID_j$. Let the initial value be $x_{-1}=-1$. Compute $x_{i,1}=\sum_{j=1}^{2} ID_j$, $x_{i,2}=\sum_{j=2}^{2} ID_j$.

Step S19: Compute the $\alpha_{i,j}$'s for $j=1$ to $j=2$ using the following equations, $\alpha_{i,1}=\prod_{j=2-1}^{1}(T-x_{i,j})$, and $\alpha_2=1$.

Step S20: Compute the sub-packet $p_{i,j}^{*}$ as per following formula,

$$
\begin{aligned}
p_{i,j}^{*} &= p_{i,j} - p_{i,j+1} \\
&= \left\{ \left[ \frac{Z}{\alpha_{i,j}} \right] mod(T - x_{i,j-1}) \right\} \\
&\quad - \left\{ \left[ \frac{Z}{\alpha_{i,j+1}} \right] mod(T - x_{i,j}) \right\},
\end{aligned}
$$

where $j = 1, 2$. $p_{i,1}^{*} = p_{i,1} - p_{i,2} = \sum_{j=1}^{2} p_{i,j}^{*} - \sum_{j=2}^{2} p_{i,j}^{*}$, $p_{i,2}^{*} = p_2$.

Step S21: Decrypt communication key $K_c = D_{k_{i,j}}(p_{i,j}^{*})$.

Step S22: Recover the original content message $M = D_{K_c}(C)$.

Step S23: The $U_2$ computes the value $Y' = Sig_{PK_i}(h(ID_1 \,||\, ID_2 \,||\, M \,||\, t))$ and checks if $Y'$ equals to the value in the signature $Y$.

### 3.2. Scenario II: A sender sends an e-mail to multiple recipients

It shows a sender sends an e-mail to multiple recipients. Fig. 2 shows that the scenario that an e-mail is sent from sender B to the multiple receivers A, C, and D. Similarly, there are three parts in this scenario. The first one is Pre-computation that consists steps, M1 and M2. Another one is Sending phase that describes the steps from M3 to M13. The other one is Receiving phase that illustrates the steps from M14 to M23.

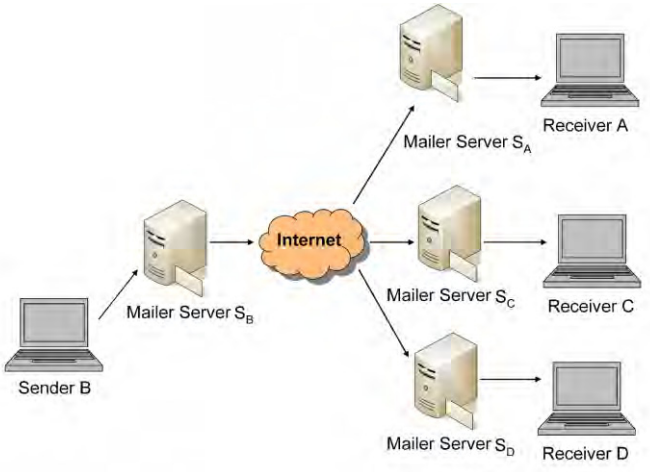


**Fig. 2.** The scenario of an e-mail sent from sender B to the multiple receivers A, C, and D [15, 16].

1) Pre-computation

Step M1: $TC \rightarrow U_i$ : $g$ , $n$ . Note that this step is similar to S1.

Step M2: $U_i \rightarrow S$ : $e_{k_i}$ , $e_{k_j}$ , $Sig_{SK_i}(e_{k_i})$ , $Sig_{SK_i}(e_{k_j})$ , $ID_j$ . Note that this step is similar to S2.

2) Sending Phase

Step M3: $S \rightarrow U_1$ : $e_{k_1}, e_{k_2}, \cdots, e_{k_n}$ , $Sig_{SK_1}(e_{k_1}), Sig_{SK_2}(e_{k_2}), \cdots, Sig_{SK_n}(e_{k_n})$ , $ID_1, ID_2, \cdots, ID_n$ .

Step M4: $U_1$ randomly generates the communication key $K_c$ .

Step M5: The encrypted e-mail message $C = E_{K_c}(M)$ is encryption under the chosen key $K_c$ , where $M$ is the content message of the e-mail.

Step M6: The $p^*_{i,j}$ for each receivers is computed by applying $p^*_{i,j} = E_{k_{i,j}}(K_c)$ for all $j = 1, 2, \cdots, n$ . The generation of $k_{i,j}$ will follow the rule of $k_{i,j} = (e_{k_i})^{k'_j} \bmod n = (g^{k'_i})^{k'_j} \bmod n = g^{k'_i k'_j} \bmod n$ .

Step M7: Each $p_{i,j}$ for all $j = 1, 2, \cdots, n$ is computing using the following equations, $p_{i,1} = \sum_{j=1}^{n} p^*_{i,j}$ , $p_{i,2} = \sum_{j=2}^{n} p^*_{i,j}$ , $\cdots$, and $p_{i,n} = \sum_{j=n}^{n} p^*_{i,j} = p^*_{i,n}$ , such that the decreasing order relation $P_{i,1} > P_{i,2} > P_{i,3} > \cdots > P_{i,n-1} > P_{i,n}$ is satisfied. Moreover $T = p_1$ is the maximal value in the set of $\{P_{i,1}, P_{i,2}, P_{i,3}, \cdots, P_{i,n-1}, P_{i,n}\}$ . A polynomial $f(x)$ is then constructed by the originator as follows, $f(x) = T + (x - k_{i,1}) \times (x - k_{i,2}) \times \cdots \times (x - k_{i,n})$ .

Step M8: Then set $\{P_{i,1}, P_{i,2}, P_{i,3}, \cdots, P_{i,n-1}, P_{i,n}\}$ is encrypted to be a sub-packet $\Gamma$ by the way of $\Gamma = E_T(P_{i,1} \,||\, P_{i,2} \,||\, P_{i,3} \,||\, \cdots \,||\, P_{i,n-1} \,||\, P_{i,n})$ .

Step M9: Sum up $x_{i,j} = \sum_{j}^{n} ID_j$ . Define the initial value $x_{-1} = -1$ . Compute $x_{i,1} = \sum_{j=1}^{n} ID_j$ , $x_{i,2} = \sum_{j=2}^{n} ID_j$ , $\cdots$, and $x_{i,n} = \sum_{j=n}^{n} ID_j = ID_j$ .

Step M10: Compute $\alpha_{i,j}$ 's for $j = 1$ to $j = n$ using the following equations, $\alpha_{i,1} = \prod_{j=n-1}^{1} (T - x_{i,j})$ , $\alpha_{i,2} = \prod_{j=n-1}^{2} (T - x_{i,j})$ , $\cdots$ , $\alpha_{i,n-1} = \prod_{j=n-1}^{n-1} (T - x_{i,j})$ , and $\alpha_{i,n} = 1$ .

Step M11: Construct a basic e-mail packet lock $Z$ as the format of $Z = \sum_{j=1}^{n} \alpha_{i,j} p_{i,j}$ .

Step M12: Compute a varied e-mail packet lock in bit-wise exclusive-or operation of follow: $L = Z \oplus E_T(T)$ .

Step M13: $U_1 \rightarrow S$ : $C$ , $L$ , $f(x)$ , $\Gamma$ , $Y$ , $t$ , where $Y = Sig_{PK_1}(h(ID_1 \| ID_2 \| \ldots \| ID_n \| M \| t))$ . The parameter $t$ is a timestamp at the time which the e-mail is sent form sender $U_1$ to his e-mail server $S$ .

3) Receiving Phase

Step M14: $S \rightarrow U_i$: $C$ , $L$ , $f(x)$ , $\Gamma$ , $Y$ , $t$ , $ID_1, ID_2, \cdots, ID_n$ .

Step M15: Find the maximal sub-packet by computing $f(k_{i,j}) = T$ , and let $\zeta = E_T(T)$ .

Step M16: Decrypt the set $\{P_{i,1}, P_{i,2}, P_{i,3}, \cdots, P_{i,n-1}, P_{i,n}\}$ by using the following equation, $D_T(\Gamma) = (P_{i,1} \| P_{i,2} \| P_{i,3} \| \cdots \| P_{i,n-1} \| P_{i,n})$ .

Step M17: Find the e-mail packet lock $Z$ by computing $L \oplus \zeta = (Z \oplus E_T(T)) \oplus \zeta = Z$ .

Step M18: Sum up $x_{i,j} = \sum_{j}^{n} ID_j$ . Let the initial value be $x_{-1} = -1$ . Compute

$$x_{i,1} = \sum_{j=1}^{n} ID_j \text{ , } x_{i,2} = \sum_{j=2}^{n} ID_j \text{ , } \cdots \text{, and } x_{i,n} = \sum_{j=n}^{n} ID_j = ID_j \text{ .}$$

Step M19: Compute the $\alpha_{i,j}$ 's for $j = 1$ to $j = n$ using the following equations,

$$\alpha_{i,1} = \prod_{j=n-1}^{1}(T - x_{i,j}) \text{ , } \alpha_{i,2} = \prod_{j=n-1}^{2}(T - x_{i,j}) \text{ , } \cdots \text{ , } \alpha_{i,n-1} = \prod_{j=n-1}^{n-1}(T - x_{i,j}) \text{ , and}$$

$\alpha_{i,n} = 1$ .

Step M20: Compute the sub-packet $p_{i,j}^*$ as per following formula,

$$\begin{aligned} p_{i,j}^* &= p_{i,j} - p_{i,j+1} \\ &= \left\{ \left[ \frac{Z}{\alpha_{i,j}} \right] mod(T - x_{i,j-1}) \right\} \\ &\quad - \left\{ \left[ \frac{Z}{\alpha_{i,j+1}} \right] mod(T - x_{i,j}) \right\}, \end{aligned}$$

where $j = 1, 2, \cdots, n$ .

$$p_{i,1}^* = p_{i,1} - p_{i,2} = \sum_{j=1}^{n} p_{i,j}^* - \sum_{j=2}^{n} p_{i,j}^* \text{ ,}$$

$$p_{i,2}^* = p_{i,2} - p_{i,3} = \sum_{j=2}^{n} p_{i,j}^* - \sum_{j=3}^{n} p_{i,j}^* \text{ ,}$$

$$\vdots$$

$$p^*_{i,n-1} = p_{i,n-1} - p_{i,n} = \sum_{j=n-1}^{n} p^*_{i,j} - \sum_{j=n}^{n} p^*_{i,j} ,$$

$$p^*_{i,n} = p_{i,n} .$$

Step M21: Decrypt communication key $K_c = D_{k_{i,j}}(p^*_{i,j})$.

Step M22: Recover the original content message $M = D_{K_c}(C)$.

Step M23: The $U_i$ computes the value $Y' = Sig_{PK_I}(h(ID_1 || ID_2 || \ldots || ID_n || M || t))$ and checks if $Y'$ equals to the value in the signature $Y$.

## 4. Security and Complexity Analysis

The security of the proposed scheme is analyzed, including replay attack, sender impersonation attack, unknown key-share attack, forgery attack and insider attack. Then, the computation complexity of the proposed scheme is discussed.

### 4.1. Security Analysis

**Replay Attack.** The replay attack on e-mail systems means that a certain user who previously established a common key with the sender exploits the preceding key materials to evade victim users' verification procedures. Then the victim users will receive the bogus information from this malicious user without discovering the misbehavior. In the proposed scheme, the messages in Step S14 and M13 contain the time stamp $t$. The sender and receivers can find out this time stamps in their memory or storage device. When a repeated time stamp is found on the received message, receiver can find out this misbehavior and discard the received messages.

**Sender Impersonation Attack.** The sender impersonation attack means that an adversary impersonates a legitimate sender to send a forged message to a receiver. In the proposed scheme, the receiver checks the signature $Y$ signed on by the sender in Step S13 and M13. Due to the properties of cryptographically secure one-way hash function, it is hard to find a collision corresponding to the forged content. In addition, an adversary who does not learn the sender's secret key cannot produce a correct signature for the forged message. Therefore, the sender impersonation attack cannot be engaged successfully.

**Unknown Key-Share Attack.** This attack can be considered as a special case of impersonation attacks. An adversary makes duplicates of the preceding authentication message transmitted between the sender and receiver to cheat a victim user to construct a short-term key. Then, the victim user considers the adversary as an authorized user and

sends him messages, confined to specific authorized users. In the proposed scheme, the sender signs on a digest related to the e-mail in Step S13 and M13. The input value of the signature $Y$ includes the sender's and receiver's identifications, the content in the e-mail, and the timestamp $t$. According to the properties of a cryptographically secure one-way hash function, it is hard to reversely derive the input and find a collision. Moreover, the short-term session key is encrypted by the receiver's public key. If an adversary tries to impersonate the sender with the preceding authentication message, users can check the signature $Y$ to discover the adversary.

**Forgery Attack.** The forgery attack on e-mail systems means that an adversary sends bogus message for authentication. In the proposed scheme, the sender sends the message in Step S13 and M13, which are signed on by the sender's secret key. The receiver can check the validity of the message through the sender's public key. Hence, any adversary cannot successfully engage a forgery attack in the proposed scheme.

**Insider Attack.** The insider attack means that malicious operators of e-mail servers can learn the short-term session key shared between the sender and the receiver. The malicious node can use the short-term session key to eavesdrop the e-mail content or send the bogus message. In the proposed scheme, the short-term session key is only known to the sender and the receiver. Even if a malicious operator of the e-mail server collects the messages transmitted between the sender and the receiver, he cannot derive the short-term session key.

## 5. Computation Complexity

The ratio of average time consumption $\alpha$ is defined in the known cryptographic algorithms [2], [25], i.e. the secret-key systems, DES, Triple DES, and AES, and public-key system, RSA. Suppose that $m$ is the number of e-mail receivers. According to the results in [14], the time consumption results in RSA are around 80 times of that in Triple-DES. Also, it takes the time even around 258 times slower than that in AES. Therefore, the ratio of average time consumption $\alpha_1$ for RSA and Triple DES equals 80,

$$\alpha_1 = \frac{\text{Average time consumption of RSA}}{\text{Average time consumption of Triple DES}} = 80,$$

and the ratio of average time consumption $\alpha_2$ for RSA and AES equals 258,

$$\alpha_2 = \frac{\text{Average time consumption of RSA}}{\text{Average time consumption of AES}} = 258.$$

The results with the scheme in [15] is compared to the results with the proposed scheme in this paper, the comparison for the average time consumption, the number of rounds for modular operation, one-way hash function operation, XOR operation are given in Table 2. For example, m is the number of receivers equals to 50. The result of the average time consumption in Sending Phase by using the method from the CRT-based scheme [15] equals to 4160, the other comparisons are given in Table 3 and Figure 3. The result of the average time consumption in Receiving Phase by using the method

from the CRT-based scheme equals to 240. On the contrary, the result of the average time consumption in both Sending Phase and Receiving Phase by using the proposed scheme also equals to 53, the other comparisons are given in Table 3 and Figure 3. The other comparisons are given in Table 4, Table 5, Table 6, Figure 4, Figure 5 and Figure 6. Therefore, the proposed scheme outperforms the CRT-based secure e-mail scheme [15].

**Table 2.** Computation comparison of the e-mail security protocols

| Compared Items \ Protocols | | The scheme of previous works in [15] | | The proposed scheme | |
|---|---|---|---|---|---|
| Communication Phases | | Sending Phase | Receiving Phase | Sending Phase | Receiving Phase |
| The average time consumption | $\alpha_1 = 80$ | $80 \times (m+2)$ | 240 | $m+3$ | $m+3$ |
| | $\alpha_2 = 258$ | $258 \times (m+2)$ | 774 | m+3 | m+3 |
| The number of rounds for modular operation | | $m+4$ | 4 | $m+1$ | $2m+1$ |
| The number of rounds for one-way hash function operation | | 1 | 1 | 1 | 1 |
| The number of rounds for *XOR* operation | | 0 | 0 | 1 | 1 |

Note that α is the ratio of average time consumption of the known cryptographic algorithms [14], and m is the number of receivers, and m is the number of receivers.

**Table 3.** The ratios of average time consumptions using $\alpha_1 = 80$ are compared in Sending Phase

| Compared Items \ Schemes | The scheme of previous works in [15] | The proposed scheme |
|---|---|---|
| $m$=1 | 240 | 4 |
| $m$=10 | 960 | 13 |
| $m$=15 | 1360 | 18 |
| $m$=20 | 1760 | 23 |
| m=25 | 2160 | 28 |
| m=30 | 2560 | 33 |
| m=35 | 2960 | 38 |
| m=40 | 3360 | 43 |
| m=45 | 3760 | 48 |
| m=50 | 4160 | 53 |

Note: $m$ is the number of receivers.

In Sending Phase, the ratios of average time consumptions using $\alpha_1 = 80$ are compared in Table 3, and the comparison results are depicted in Fig. 3.

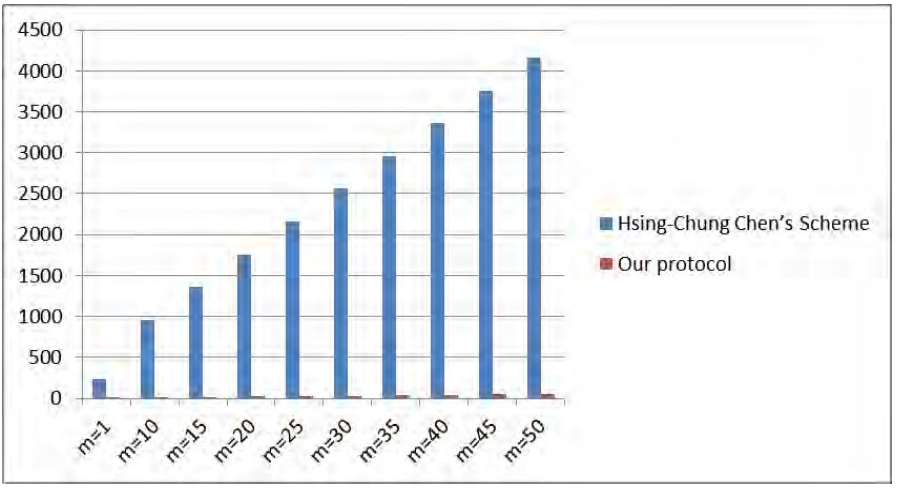


**Fig. 3.** The ratios of average time consumptions using $\alpha_1 = 80$ are compared in Sending Phase

In Receiving Phase, the ratios of average time consumptions using $\alpha_1 = 80$ are compared in Table 4, and the comparison results are depicted in Fig. 4.

**Table 4.** The ratios of average time consumptions using $\alpha_1 = 80$ are compared in Receiving Phase

| Protocols / Compared Items | The scheme of previous works in [15] | The proposed scheme |
|---|---|---|
| m=1 | 240 | 4 |
| m=10 | 240 | 13 |
| m=15 | 240 | 18 |
| m=20 | 240 | 23 |
| m=25 | 240 | 28 |
| m=30 | 240 | 33 |
| m=35 | 240 | 38 |
| m=40 | 240 | 43 |
| m=45 | 240 | 48 |
| m=50 | 240 | 53 |

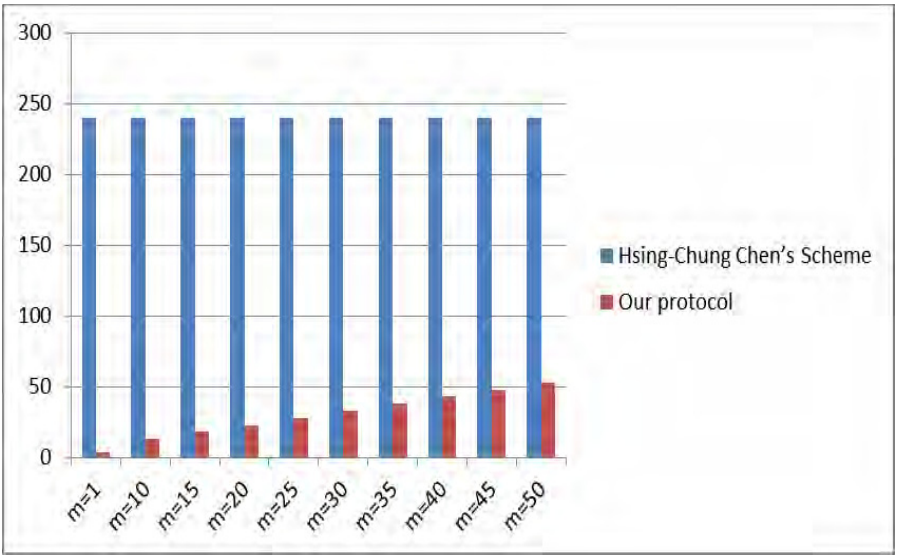


**Fig. 4.** The ratios of average time consumptions using $\alpha_1 = 80$ are compared in Receiving Phase

In Sending Phase, the numbers of modular operation round are compared in Table 5, and the comparison results are depicted in Fig. 5.

**Table 5.** The comparison results of number of modular operation in Sending Phase

| Schemes<br>Compared Items | The scheme of previous works in [15] | The proposed scheme |
|---|---|---|
| m=1 | 5 | 2 |
| m=10 | 14 | 11 |
| m=15 | 19 | 16 |
| m=20 | 24 | 21 |
| m=25 | 29 | 26 |
| m=30 | 34 | 31 |
| m=35 | 39 | 36 |
| m=40 | 44 | 41 |
| m=45 | 49 | 46 |
| m=50 | 54 | 51 |

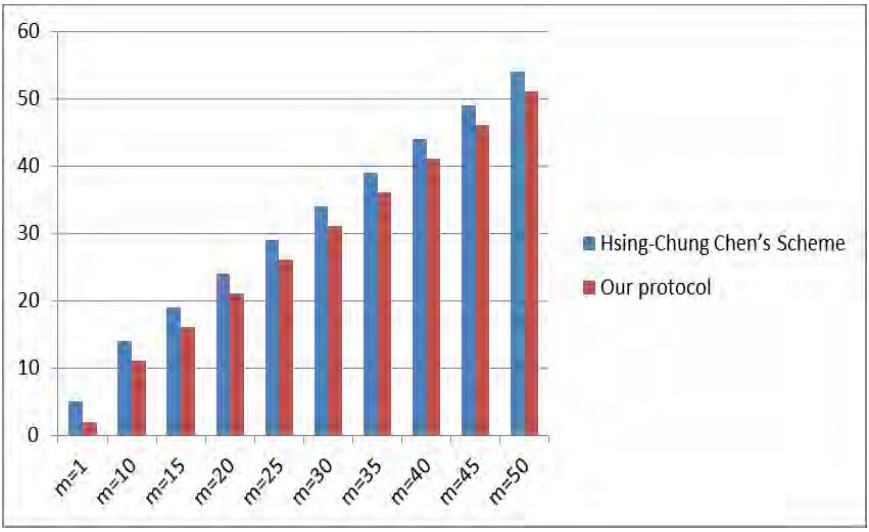


**Fig. 5.** The comparison results of number of mod operation in Sending Phase

In Receiving Phase, the numbers of modular operation round are compared in Table 6, and the comparison results are depicted in Fig. 6.

**Table 6.** The comparison results of number of modular operation in Receiving Phase

| Schemes<br>Compared Items | The scheme of previous works in [15] | The proposed scheme |
|---|---|---|
| m=1 | 4 | 3 |
| m=10 | 4 | 21 |
| m=15 | 4 | 31 |
| m=20 | 4 | 41 |
| m=25 | 4 | 51 |
| m=30 | 4 | 61 |
| m=35 | 4 | 71 |
| m=40 | 4 | 81 |
| m=45 | 4 | 91 |
| m=50 | 4 | 101 |

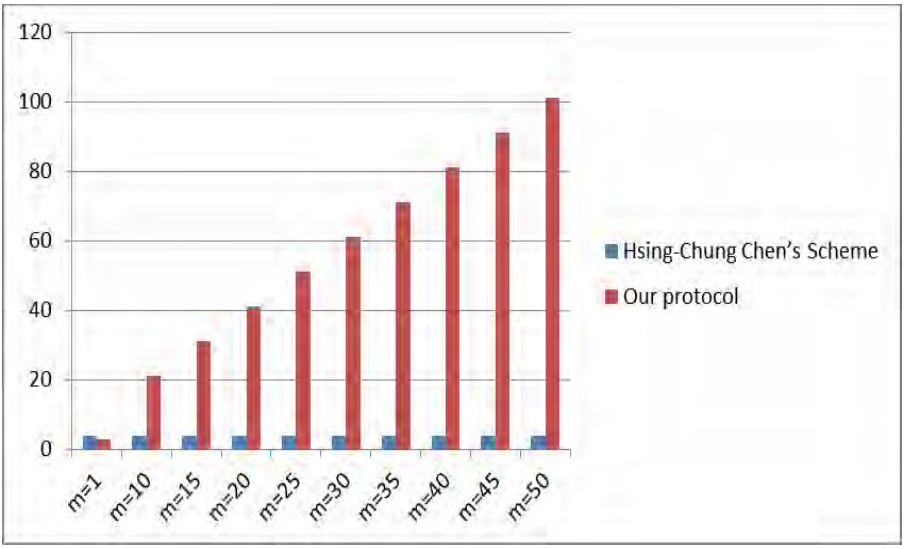


**Fig. 6.** The comparison results of number of modular operation in Receiving Phase

Finally, In Table 2, the number of rounds for one-way hash function operation between both comparison schemes is same. The number of rounds for XOR operation in the proposed scheme equals one, and the number of rounds for XOR operation in the scheme of previous works in [15] equals zero. The values of the last two items in the comparison, Table 2, are too small to be ignored.

## 6. Conclusions

In this paper, a novel secure e-mail system is proposed. The protocol is constructed by ID-based FNS Multicast mechanism with the hybrid cryptographic algorithms of public-key and secret-key system. A secure multicast key protocol is proposed a solution to the e-mail systems for distributing a session key accompanied the sent e-mail to the specific group. Due to the concerning for the securely transferring the session key, the proposed protocol adopts ID-based FNS to replace CRT is proposed. In the manner, not only the e-mail construction in multicast system can be efficiently retained, but also the easy key management and fast computation to process a multiple secure e-mail delivery can be proficiently achieved. The results with the CRT-based secure e-mail scheme is compared to the results with the proposed scheme in this paper, the comparison for the average time consumption, the number of rounds for modular operation, one-way hash function operation, XOR operation are given. According to the results of comparisons in Table 3, Table 4, Table 5, Table 6, Figure 3, Figure 4, Figure 5 and Figure 6, the proposed scheme outperforms the CRT-based secure e-mail scheme.

**Acknowledgments.** This work was supported in part by Asia University, Taiwan, under Grant 101-asia-28, also by the National Science Council, Taiwan, Republic of China, under Grant NSC 102-2221-E-468-007.

## References


1. Basagiannis S., Petridou S., Alexiou N., Papadimitriou G., Katsaros P.: Quantitative analysis of a certified e-mail protocol in mobile environments: A probabilistic model checking approach. Computers & Security, Vol. 30, 257-272. (2011)
2. Chen H.C., Marsha A.V., Weng C.E. Kung T.L.: Cognitive RBAC in Mobile Heterogeneous Networks. Computer Science and Information Systems, Vol. 10, No. 2, 779-806. (2013)
3. Fujisaki E., Okamoto T.: Secure Integration of Asymmetric and Symmetric Metric Encryption Schemes. Advances in Cryptology –CRYPTO'99, LNCS, Vol. 1666, 537-554. (1999)
4. Atkins D., Stallings W., Zimmermann P.: PGP Message Exchange Formats. Internet Draft. (1995)
5. Balenson D.: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers. RFC 1423. (1993)
6. Galvin J., Murphy G., Crocker S., Freed N.: MIME Object Security Services. RFC 1848. (1995)
7. Elkins M.: MIME Security with Pretty Good Privacy (PGP). Internet Draft, 1995.
8. Schneier B.: E-mail Security with PGP and PEM: How to Keep Your Electronic Mail Private. (1995)
9. Sun H.M., Hsieh B.T., Hwang H.J.: Secure E-mail protocols providing perfect forward secrecy. IEEE Communications Letters, Vol. 9 , No. 1, 58 – 60. (2005)
10. Joyia, A., Ghafoor, A., Sajjad, M., Choudhary, M.Q.: Secure and privacy enhanced email system as a cloud service. In Proceedings of 2013 Eighth International Conference on Digital Information Management (ICDIM), 73–78. (2013)
11. Shamir A.: Identity-Based Cryptosystems and Signature Schemes. Lecture Notes in Computer Science Volume 196, 47-53. (1985)
12. McCullagh, N.: Securing e-mail with identity-based encryption. IT Professional, Vol. 7, No. 3, 64, 61 – 63. (2005)
13. Kihidis, A., Chalkias, K., Stephanides, G.: Practical Implementation of Identity Based Encryption for Secure E-mail Communication, In Proceedings of 2010 14th Panhellenic Conference on Informatics (PCI 2010), 101 – 106. (2010)
14. Chen H.C., Wang, S.J., Wen J.H.: Packet Construction for Secure Conference Call Request in Ad Hoc Network Systems. Information Sciences, Vol. 177, Issue 24, 5598–5610. (2007)
15. Chen H. C.: Secure multicast key protocol for electronic mail systems with providing perfect forward secrecy. Security and Communication Networks, Vol. 6, No. 1, 100–107. (2013)
16. Chen H. C. et. al.: Secure Multicast Key Protocol for E-Mail System Using Factorial Number Structure. In Proceedings of 2013 Seventh International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS 2013), 611-616. (2013)
17. Zhang M.Q., Xiao H.Y., Yang X.Y.: ID-Based Fair Multi-party Exchange Protocol. 2010 International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), Volume 2, 402 – 405. (2010)
18. Zhang M., Takagi, T.: Efficient Constructions of Anonymous Multireceiver Encryption Protocol and Their Deployment in Group E-mail Systems with Privacy Preservation. IEEE Systems Journal, Vol. 7, No. 3, 410 – 419. (2013)
19. Denning D.E.: Cryptography and Data Security. Addison-Wesley, Reading, Mass. (1982)
20. Kent S. T.: Security Requirements and Protocols for a Broadcast Scenario. IEEE Trans. Communications, Vol. 29, No. 6, 778-786. (1981)
21. Phan R.C.W.: Cryptanalysis of E-mail Protocols Providing Perfect Forward Secrecy. Computer Standards & Interfaces, Vol. 30, No. 3, 101-105. (2008)

22. Yoon E.J., Yoo K.Y.: Cryptanalysis of Robust E-mail Protocols with Perfect Forward Secrecy. IEEE Communication Letter, Vol. 11, No. 5. (2007)
23. Menezes A.J., Van Oorschot P.C., Vanstone S.A.: Handbook of Applied Cryptography, CRC Press. (1997)
24. Chang C.C., Wu Y.C., Chang S.C.: A Novel E-mail Protocol Using Three-party Password-authenticated Key Exchange, In Proceedings of International Conference on Security Technology (SECTECH'08), 150-154. (2008)
25. Wang Y., Hu M.: Timing evaluation of the known cryptographic algorithms," In Proceedings of International Conference on Computational Intelligence and Security. (2009)

**Hsing-Chung Chen (Jack Chen)** received the Ph.D. degree in Electronic Engineering from National Chung Cheng University, Taiwan, in 2007. During the years 1991-2007, he had served as a Mobile Communication System Engineer at the Department of Mobile Business Group, Chunghwa Telecom Co., Ltd. From Feb. 2008 to Feb. 2013, he was the Assistant Professor of the Department of Computer Science and Information Engineering at Asia University, Taiwan. Since February 2013–present, he is the Associate Professor at the same University. He is also the Research Consultant of Department of Medical Research at China Medical University Hospital, China Medical University Taichung, Taiwan. Currently, he is interested in Information Security, Cryptography, Role-based Access Control, Computer Networks and Wireless Communications. He was Program Co-Chair of numerous conferences. Dr. Chen was the Editor-in-Chief of Newsletter of TWCERT/CC from July 2012 to June 2013.

**Cheng-Ying Yang** received the M.S. degree in electronic engineering from Monmouth University, New Jersey in 1991, and Ph.D. degree from the University of Toledo, Ohio in 1999. He is a member of IEEE Satellite & Space Communication Society. Currently, he is employed as an associate professor with the Department of Computer Science, University of Taipei, Taiwan. His research interests are performance analysis of digital communication systems, error control coding, signal processing, and computer security.

**Hui-Kai Su** received the B.S degree from I-Shou University, Taiwan, in 1999. He received the M.S. degree and the Ph.D. degree from National Chung-Cheng University, in 2001 and 2006 respectively. He was an Assistant Professor at the department of computer science and information engineering, Nanhua University, Taiwan, during 2006 and 2009. He joined the department of electrical engineering, Formosa University, in the spring of 2009. Currently he is an Associate Professor in the department. His research interests include multimedia network applications, P2P network applications, IP/MPLS network survivability, network QoS control and management, embedded systems, etc.

**Ching-Chuan Wei** was born in Taiwan in 1966. He received his B.S., M.S. and Ph.D. degrees from the Department of Communication Engineering, National Chiao Tung University, Taiwan. Currently, he is a Professor serving for the Department of Information and Communication Engineering, Chaoyang University of Technology. His research interests focus on the biomedical signal analysis and processing.

**Chao-Ching Lee** received the BS degree in Information System from Asia University, Taiwan, in 2011, and the MS degree in Computer Science and Information Engineering from Asia University, Taiwan, in 2013. His research interests include Information Security, Computer Network and Mobile Computing.

*Received: September 24, 2013; Accepted: January 28, 2014.*