韓國IT서비스學會誌
第19卷 第1號
2020年 2月, pp.145-158

Journal of Information Technology Services
https://doi.org/10.9716/KITS.2020.19.1.145

소비자 프라이버시 보호에 관한 다항식 기반 연구

박연희* · 김민지**

A Polynomial-based Study on the Protection of Consumer Privacy

Yanji Piao* · Minji Kim**

■ Abstract ■

With the development and widespread application of online shopping, the number of online consumers has increased. With one click of a mouse, people can buy anything they want without going out and have it sent right to the doors. As consumers benefit from online shopping, people are becoming more concerned about protecting their privacy. In the group buying scenario described in our paper, online shopping was regarded as intra-group communication. To protect the sensitive information of consumers, the polynomial-based encryption key sharing method (Piao et al., 2013; Piao and Kim, 2018) can be applied to online shopping communication.

In this paper, we analyze security problems by using a polynomial-based scheme in the following ways : First, in Kamal's attack, they said it does not provide perfect forward and backward secrecy when the members leave or join the group because the secret key can be broken in polynomial time. Second, for simultaneous equations, the leaving node will compute the new secret key if it can be confirmed that the updated new polynomial is recomputed. Third, using Newton's method, attackers can successively find better approximations to the roots of a function. Fourth, the Berlekamp Algorithm can factor polynomials over finite fields and solve the root of the polynomial. Fifth, for a brute-force attack, if the key size is small, brute force can be used to find the root of the polynomial, we need to make a key with appropriately large size to prevent brute force attacks. According to these analyses, we finally recommend the use of a relatively reasonable hash-based mechanism that solves all of the possible security problems and is the most suitable mechanism for our application. The study of adequate and suitable protective methods of consumer security will have academic significance and provide the practical implications.

Keyword : Online Shopping, Consumer Privacy, Security Problems, Polynomial-based Study

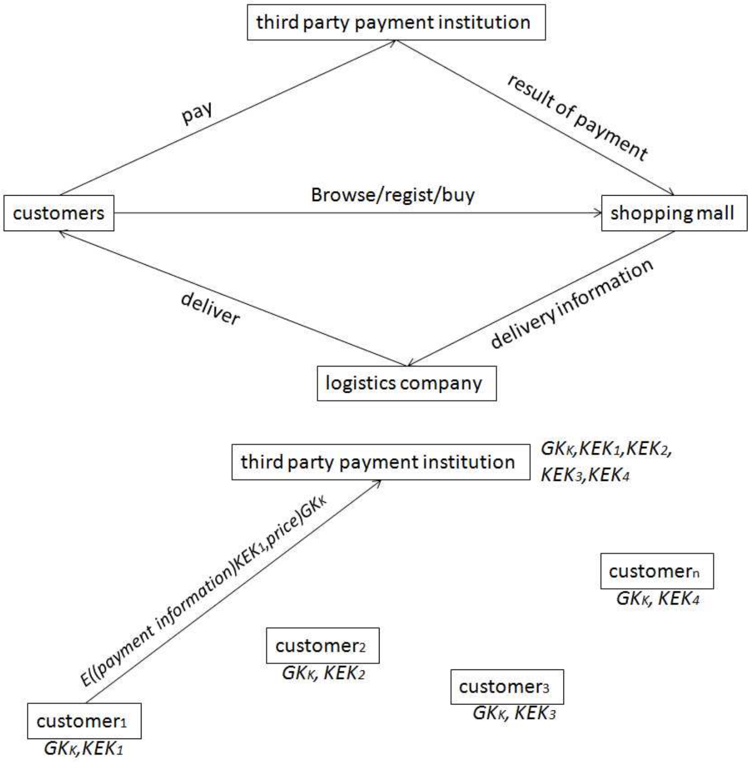
Submitted : December 21, 2019　　1st Revision : January 23, 2020　　Accepted : January 25, 2020

* Lecturer, Yanbian University, College of Economics and Management
** Full-time Lecturer, Seoul National University, Business School, Corresponding Author

1. Introduction

Service science is an emerging field and one of the main research problems in the service is management of Information and Communication Technologies (ICT) (Stuart et al., 2009). The application of service science in the e-commerce has become a very common way for people to do online trading (Hwang and Jeong, 2016; Jo et al., 2013). The popularity of online shopping is high because it makes people's lifestyles more convenient and comfortable. However, online shopping systems transmit consumers'payment data through networks, and if the payment information is exposed, there will be disclosure of sensitive information about the consumers. Therefore, the security of data transmission has become an important market environment condition (Anthony and Ana, 2005; Chen et al., 2017).

Online shopping was regarded as intra-group communication, for instance, group buying, auctions, and Chinese Taobao snap up. The customers bundled together enjoy the group purchase, because the price is cheap when you join group buying. Some customers voluntarily organized membership to purchase the products. Based on the example of a membership purchasing system in group buying shown in [Figure 1], we consider group buying to be a form of group communication. Group communication is a relationship between three or more individuals who want to accomplish a common goal. The authorized party is the group controller, and the



[Figure 1] Membership Group Purchase System online consumers are called group members. Data encryption is the basic method of protecting information messages on the Internet. When a member customer 1 in the group sends a payment message to the payment institution, the message must be encrypted with the key GK_K (which will be described in the related works section) to prevent data leakage. In order to prevent data falsification and loss in purchase system we can use hash function and digital signature as well, but it is not mentioned in this paper. We only consider the step of pay in [Figure 1]. Only the members in the group will be able to recover the price message, and only the group controller will be able to recover the payment message.

What will happen if there is no verification and no encryption? First, if there is no sender verification, it is possible to impersonate the sender. Attackers can impersonate a member of the group and forge the payment messages to the recipient. We proposed verification solutions in our previous paper (Piao and Kim, 2018). Second, encryption is a method used to protect data from others, and only the sender and receivers can read the data. What will happen if the consumer sends the payment messages in plaintext without adopting any encryption method? Obviously, it will be exposed to all the malicious users. Hence, it should be protected from malicious users, and it should be encrypted with a secured secret key that is shared between the sender and the recipient. The traditional encryption schemes have a disadvantage : the more consumers need to send payment messages, the more communication overhead there is, and the costs for the group controller increase. To make up for the weak points in traditional encryption schemes, it can adopt our previous polynomial-based encryption method (Piao et al., 2013). In this paper, we will analyze the polynomial-based method from a security perspective and recommend a relatively reasonable hash-based mechanism.

2. Related Works

Protection of the consumers personal information is the increasingly serious research area (Gurung and Raja, 2016; Kahn and Liñares-Zegarra, 2016; Janse et al., 2017), and data encryption is the mostbasic method (Diffie and Hellman, 1976; Harney and Muckenhirn, 1997; Wallner et al., 1999; Wong et al., 1998) of protecting information on a network. There are a couple of approaches to address the security issues of internet shopping consumers. Traditional method is symmetric method, the consumer and the receiver share a secret key to protect the secret message. The disadvantage is the controller will be overwhelmed by the communication overhead for spreading the shared keys to each of consumers. Besides, several methods are proposed to protect the information based on the theory of non-symmetric. The most typical method is (Diffie and Hellman, 1976), but it involves exponential computation. In order to make up for the weak points of traditional methods Piao and Kim (2018) proposed a polynomial-based privacy-preserving scheme that is suitable for online shopping environments.

A polynomial-based scheme was first used to implement threshold secret sharing (Shamir, 1979). A dealer D distributes a secret s to n players, and at least k participants are required to construct a secret s. Staddon et al. (2002) and Liu et al. (2003) proposed a self-healing group key distribution mechanism with a revocation capability. The group controller uses a bivariate polynomial as a masking function to privately transmit messages to the group members.

To ensure secure intergroup communication, Wang and Stransky (2007), Wang and Bhargava (2005) and Wang and Wang (2008) proposed a polynomial-based encryption scheme in which the authors adopted polynomials to provide the distribution of personal key shares. They use the t-degree polynomial $H(x)$ to establish the personal key shares and protect one-to-many multicast traffic. $H_{2,1}(v)$ is used to encrypt data from v in group one ($G1$) for members of group two ($G2$) (called a personal key share). $H_{2,1}(x)$ is a polynomial to determine the keys for decrypting the data from a node in $G1$ for the members of $G2$. Node v in $G1$ can obtain $H_{2,1}(v)$ from the group controller, and v encrypts the message using personal key share $H_{2,1}(v)$ and sends the encrypting message to $G2$. At this time, the nodes in $G2$ already have $H_{2,1}(x)$ from the group controller, and they can be aware that the message is coming from v, so the nodes in $G2$ can derive $H_{2,1}(v)$ and decrypt the message from v. For example, with $H_{2,1}(x) = 5x+8$, all the members in $G2$ keep $H_{2,1}(x)$ if the key value of node v is 5, the personal key share can be calculated as $H_{2,1}(v) = 5\times5+8=33$. Therefore, only the sender v and all the members in $G2$ can easily able read the message encrypted by the secret key 33 because other members cannot obtain the polynomial value. Here, the polynomial $H(x)$ is generated and sent by the group controller, so the group controllers consume time and waste energy not only for generating the polynomials but also for sending it to group members.

We have redesigned the intergroup polynomial-based mechanism (Piao et al., 2013) inspired by Wang and Stransky (2007), Wang and Bhargava (2005) and Wang and Wang (2008). In a previous paper (Piao and Kim, 2018), we explained how to share an encryption key that achieves sender anonymity and confidentiality if an internet consumer sends a secret message to the other group.

In this paper, we only focus on an intragroup key management scheme. In the previous proposed scheme (Piao et al., 2013), we adopted a polynomial-based mechanism to derive the intra-group key. Assume that every node is uniquely identified by a node *ID* i, where $i\in\{1\cdots n\}$ and n is the total number of nodes in the group.

1) The group controller shares the keys KEK with every member i (i = 1 ⋯ n) through a secure channel. In our application, we can protect payment information like *ID* number and card number using KEK_i. The payment information is only known by consumer and authorized third party.
2) The group controller generates a polynomial P that is made by all the secret keys KEK_i, i = 1 ⋯ n. The group controller broadcasts P, the main advantage of using polynomial P is they share the intra-group key without any encryption/decryption. The group controller generates the group key GK_K of the group GK and broadcasts the expanded polynomial P to the members who want to join group buying through a public channel. GK_K is used for protecting the price from people who did not participate the group buying. Certainly, consumers access the group purchase system after authorizing their identity.

$$P = (x-KEK_1)(x-KEK_2)\cdots (x-KEK_n)+GK_K \tag{1}$$

In the equation (1), P is a polynomial function which is used for deriving intra-group key GK_K, and x is secret keys KEK_i, i = 1 ⋯ n.

3) When a user Ui in the group receives P, the user Ui can figure out the group key GK_K.

When a new member w joins the group, the intra group key GK_K should be regenerated, and the group controller broadcasts P' to the members.

$$P' = (x - KEK_1)(x - KEK_2) \cdots (x - KEK_n)(x - KEK_w) + GK_K' \tag{2}$$

In the case in which a user Uj leaves the group, the encryption key sharing process is almost the same. The group key GK_K should be updated by the new intra group key GK_K, and the polynomial $P'(x)$ is sent to all the remaining members. They can obtain the group key by calculating $P'(KEK_i)$.

Based on the approach of Piao et al. (2013), Patsakis and Solanas (2013) proposed that the group controller picks $m+1^{\text{th}}$ random values and calculates the following polynomial :

$$P(x) = \prod_{i=1}^{m+1} (x - K_i) + GK_k \bmod n$$

The scheme has the additional key K_{m+1}, and it does not belong to any user. Although there is an $m+1^{\text{th}}$ additional key, it can apply a simultaneous equation, as mentioned in section 3.2, and the leaving node derives the group keys of the next session. Patsakis and Solanas (2013) argue that the scheme is shown to be secure against the collusion attack. However, in the worst-case scenario, m-1 members may collude to expose the key of m^{th} member, and then they can calculate the polynomial :

$$G(x) = \prod_{i=1}^{m+1} (x - K_i) \bmod n$$

To recover the key of m^{th} member, they factor the polynomial as shown below :

$$g(x) = \frac{P(x) - GK_k}{G(x)} = \frac{\Pi_{i=1}^{m+1}(x - K_i)}{\Pi_{i=1}^{m-1}(x - K_i)} = (x - K_s)(x - K_m)$$

As seen from the above equation $(x - K_s)$, $(x - K_m)$, the probability of guessing the key of m^{th} member K_m is 50% in general. Therefore, C. Patsakis's scheme (Patsakis and Solanas, 2013) is not sufficiently secure against collusion attacks.

In the following section, we will analyze the various valid security problems for the mentioned polynomial-based method.

3. Security Analysis

In this section, we analyze security problems by using the original polynomial-based scheme which proposed in our previous paper (Piao et al., 2013).

3.1 Kamal's Attack

Although the scheme (Piao et al., 2013) is very efficient in terms of scalability, it does not satisfy perfect forward and backward secrecy when the group members leave or join (Kamal, 2013). It can be broken in polynomial time because of a mathematical problem. The leaving node can easily access the new intra-group key based on its previous keys. Similarly, the joining node can discover the previous intra-group keys using its current key.

3.1.1 No Backward Secrecy

When a new member W joins the group, W receives the new polynomial P' from the group controller.

$$P' = (x-KEK_1)(x-KEK_2)\cdots (x-KEK_w)(x-KEK_n)+GK_K' \tag{3}$$

From equation (3), w can calculate :

$$(P'-GK_K')/(x-KEK_w) = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_n) \tag{4}$$

Thus, w can deduce the previous intra-group key :

$$GK_K = P-(x-KEK_1)(x-KEK_2)\cdots(x-KEK_n) = P-(P'-GK_K')/(x-KEK_{w)} \tag{5}$$

In the security problem, the new member w should not connect previous session. However, from equations (4) and (5), w can easily deduce the previous encryption key GK_K, and it can easily access the previous messages that were encrypted by GK_K.

3.1.2 No Forward Secrecy

Similarly, when a member i leaves, the polynomial P must be updated to a new polynomial P′,

$$P' = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_{i-1})(x-KEK_{i+1})\cdots(x-KEK_n)+GK_K' \tag{6}$$

From equation (1), i can calculate:

$$(P-GK_K)/(x-KEK_i) = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_{i-1})(x-KEK_{i+1})\cdots(x-KEK_n) \tag{7}$$

Then, i can easily derive the new intragroup key :

$$GK_K' = P'-(P-GK_K)/(x-KEK_i) \tag{8}$$

Therefore, the leaving member i can easily access the new session. To make up for the weak points (Kamal, 2013) of intragroup key management in our previous work, we have tried adopting a dummy member in the group when generating the polynomial P. First, the dummy member shares KEK_{dum} with a group controller, and KEK_{dum} is the dependent value of all of the members. KEK_{dum} is exclusive OR of all the members' KEK_i in the group. Hence, when a join or leave operation happens, KEK_{dum} should be changed as well. Second, the group controller generatesa polynomial P using the secret key KEK_i and the dummy key KEK_{dum} and then broadcasts an expanded polynomial to the members through a public channel. Finally, each group member has to derive the intra-group key GK_K by themselves. The polynomial P is :

$$P = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_n)(x-KEK_{dum})+GK_{K,}\, i=1\cdots n,\ KEK_{dum} = KEK_1 \oplus KEK_2 \oplus \cdots \oplus KEK_n \tag{9}$$

3.1.3 Member Join

Assume that a new member w wants to take part in the group Gk. The group key GK_K must be renewed by GK_K to prevent w from getting access to the previous session messages.

The new node w shares KEK_w with the group controller.

1) KEK_{dum} of dummy member will be changed by :

$$KEK_{dum}' = KEK_1 \oplus KEK_2 \oplus \cdots \oplus KEK_w \oplus KEK_n \tag{10}$$

2) The group controller generates a new polynomial P and broadcasts it to the current available members.

$$P' = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_w)(x-KEK_n)(x-KEK_{dum}')+GK_K' \tag{11}$$

3) All the available members, including w, can derive the updated group key GK_K using their own KEK_i.

Even though the new member w can calculate $(P'-GK_K')/(x-KEK_w)$, it cannot obtain the old group key GK_K by adding the dummy key KEK_{dum}. The dummy key is totally dependent on all of the members of KEK_i in the same group. When a member w takes part in the group, KEK_{dum} must be changed into $KEK_{dum}^{'}$. It solves the group backward secrecy problem, which is mentioned in a paper by Kamal (2013).

3.1.4 Member Leave

Assume that a member i leaves the group, GK_K should be updated by the new key $GK_K^{'}$, and at the same time, the dummy key KEK_{dum} should be changed by :

$$KEK_{dum}^{'} = KEK_1 \oplus KEK_2 \oplus \cdots \oplus KEK_{i-1} \oplus KEK_{i+1} \oplus \cdots \oplus KEK_n \tag{12}$$

The group controller regenerates a new P′ and broadcasts it to the current available members, except for the leaving member i.

$$P' = (x-KEK_1)(x-KEK_2)\cdots(x-KEK_{i-1})(x-KEK_{i+1})\cdots(x-KEK_n)(x-KEK_{dum}^{'}) + GK_K^{'}\ ,i=1\cdots n \tag{13}$$

All of the members in the group, except the leaving node i, can derive $GK_K^{'}$. In the same way, this approach solves the group forward secrecy problem, which was mentioned in a paper by Kamal (2013).

3.2 Simultaneous Equations

Assume that there are three members in the group and the polynomial P is :

$$P = (x-KEK_1)(x-KEK_2)(x-KEK_3)(x-KEK_{dum1}) + GK_1 \tag{14}$$

Member 2 (called $M2$) can easily derive equation (15) using the polynomial P, group key GK_1 and its own KEK_2.

$$\begin{aligned}&(x-KEK_1)(x-KEK_3)(x-KEK_{dum1})\\&=(P-GK_1)/(x-KEK_2)\\&=x^3-(KEK_{dum1}+KEK_3+KEK_1)x^2\\&\quad+(KEK_3KEK_{dum1}+KEK_1KEK_{dum1}\\&\quad+KEK_1KEK_3)x-KEK_1KEK_{dum1}KEK_3\end{aligned} \tag{15}$$

When $M2$ leaves the group, the group controller should generate a new polynomial P_{new} :

$$\begin{aligned}P_{new} &= (x-KEK_1)(x-KEK_3)(x-KEK_{dum2})\\&\quad+GK_2 = x^3-(KEK_{dum2}+KEK_{3+}KEK_1)x^2\\&\quad+(KEK_3KEK_{dum2}+KEK_1KEK_{dum2}\\&\quad+KEK_1KEK_3)x-KEK_1KEK_{dum2}KEK_3+GK_2\end{aligned} \tag{16}$$

Because the polynomial is expanded but not encrypted, the leaving member $M2$ also knows the P_{new}. Then, $M2$ can calculate (15)-(16) :

$$\begin{aligned}&(15)-(16)\\&=(KEK_{dum2\,-}KEK_{dum1})x^2+(KEK_1+KEK_3)\\&\quad(KEK_{dum1\,-}KEK_{dum2})x-GK_2\end{aligned} \tag{17}$$

From equation (17), $M2$ knows the coefficient of x^2.

The coefficient of x^2 is :

$$KEK_{dum2}-KEK_{dum1} \tag{18}$$

The coefficient of x is :

$$(KEK_{1+}KEK_3)(KEK_{dum1\,-}KEK_{dum2}) \tag{19}$$

From equation (18) and equation (19), $M2$ can derive,

$$KEK_1+KEK_3 \tag{20}$$

From equation (16), $M2$ knows the coefficient of x^2,

$$KEK_{dum2}+KEK_1+KEK_3 \tag{21}$$

M2 finally derives (21)-(20) $= KEK_{dum2}$

Therefore, the updated new group key GK_2 will leak through the leaving member $M2$. Even if add the dummy member, the expelled member will leak the new group key.

3.3 Newton's Method

In mathematics, Newton's method is an interactive method for finding successively better approximations to the roots of a function, and fis a given function that is differentiable in an open interval. The process is shown as follows :

$$X_{n+1} = X_n - (f(X_n)/f'(X_n)) \tag{22}$$

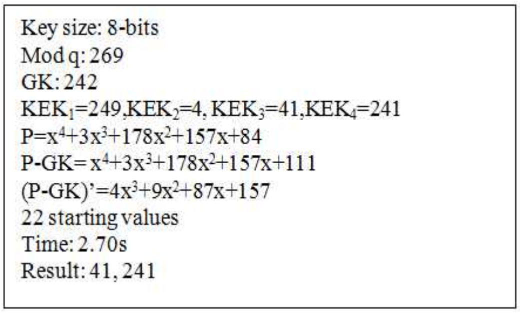
An attack that occurs within a set of group members is called an insider attack. That is, the malicious user in the group will be able to derive others' KEK when the key size is small. Therefore, as long as the attacker knows the others' secret key, he/she can derive the group key. We assume there are n members in the group, so the polynomial P is :

$$P = (x - KEK_1)(x - KEK_2)\cdots(x - KEK_n)(x - KEK_{dum}) + GK_K \tag{23}$$

The members in the group can obtain both the expended polynomial P, and therefore, for GK_K, each member derives :

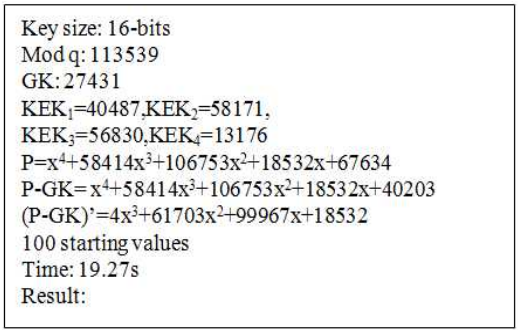
$$P - GK_K = (x - KEK_1)(x - KEK_2)\cdots(x - KEK_n)(x - KEK_{dum}) \tag{24}$$

Even though $P - GK_K$ is expanded, each node can derive the approximate value of the polynomial $P - GK_K$ using Newton's method. The secret key KEK will be exposed by the group members because KEK is the integer value. If the function is differentiable, it can apply Newton's method. An attacker obtains the personal key share KEK_s of others who share the current session with him/her.



```
Key size: 8-bits
Mod q: 269
GK: 242
KEK_1=249,KEK_2=4, KEK_3=41,KEK_4=241
P=x^4+3x^3+178x^2+157x+84
P-GK= x^4+3x^3+178x^2+157x+111
(P-GK)'=4x^3+9x^2+87x+157
22 starting values
Time: 2.70s
Result: 41, 241
```

[Figure 2] Newton's Mthod with a Key Size of 8-bits



```
Key size: 16-bits
Mod q: 113539
GK: 27431
KEK_1=40487,KEK_2=58171,
KEK_3=56830,KEK_4=13176
P=x^4+58414x^3+106753x^2+18532x+67634
P-GK= x^4+58414x^3+106753x^2+18532x+40203
(P-GK)'=4x^3+61703x^2+99967x+18532
100 starting values
Time: 19.27s
Result:
```

[Figure 3] Newton's Method with a Key Size of 16-bit

[Figure 2] and [Figure 3] show examples of determining the secret key of a modular polynomial using Newton's method with JAVA programming. We assume that there are four members in the groups. If the key size is 8 bits, we find two secret keys in 2.70 seconds with 22 starting values, as shown in [Figure 2]. [Figure 3] shows that there is no result with the key size 16 bits and 100 starting values. The malicious users will find the approximate value, but that could just be a lucky attack. Based on our simulation, there is no result with a key size of 128 bits and 3000 starting values. Therefore, it is rather difficult to find the secret key if the key size is larger than 128 bits.

3.4 Berlekamp Algorithm

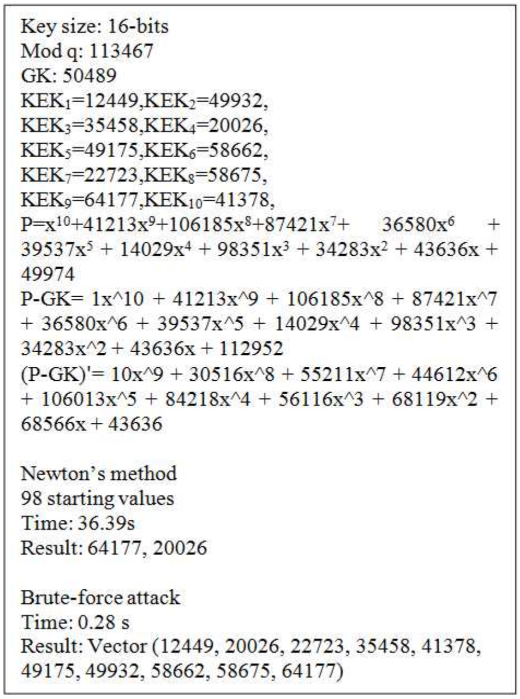
The Berlekamp algorithm is a method for factoring polynomials over finite fields (Berlekamp, 1970). The big prime Berlekamp algorithm for factoring the polynomial P of degree n in domain $GF(q)$ has complexity $O(n^3 \times \log(q) \times \log(n))$ (Liu et al., 2013).

Through an insider attack, the malicious member u has received the polynomial P and member u retrieved the intra-group key GK, so u can deduce polynomial $F(x) = (P - GK_k)/(x - KEK_u) = (x - KEK_1)(x - KEK_2) \cdots (x - KEK_{u-1})(x - KEK_{u+1}) \cdots (x - KEK_n)$. It is not hard to obtain the secret key KEK that is shared between the members and the group controller from $F(x)$. The polynomial can be factorized by using any of the algorithms (Berlekamp, 1970; Cantor and Zassenhaus, 1981; Shoup, 1990), then, the malicious member u calculates the $KEKs$ of other members in the group. In conclusion, it is possible to solve the root of the polynomial P. Therefore, changing the secret key KEK in every session can solve the problem.

3.5 Brute-Force Attack

We assume that there are ten members in the group. In [Figure 4], using Newton's method, the attacker finds two secret keys in 36.39 seconds with a key size of 16 bits. In contrast, a brute force solution only requires 0.28 seconds to determine all the values of the polynomial.

After repeated simulations, it did not determine any results for a key size of 256 bits. Therefore, it needs to make keys with an appropriately large size to prevent this kind of attack.



Key size: 16-bits
Mod q: 113467
GK: 50489
KEK_1=12449,KEK_2=49932,
KEK_3=35458,KEK_4=20026,
KEK_5=49175,KEK_6=58662,
KEK_7=22723,KEK_8=58675,
KEK_9=64177,KEK_{10}=41378,
$P=x^{10}+41213x^9+106185x^8+87421x^7+ 36580x^6 + 39537x^5 + 14029x^4 + 98351x^3 + 34283x^2 + 43636x + 49974$
P-GK= 1x^10 + 41213x^9 + 106185x^8 + 87421x^7 + 36580x^6 + 39537x^5 + 14029x^4 + 98351x^3 + 34283x^2 + 43636x + 112952
(P-GK)'= 10x^9 + 30516x^8 + 55211x^7 + 44612x^6 + 106013x^5 + 84218x^4 + 56116x^3 + 68119x^2 + 68566x + 43636

Newton's method
98 starting values
Time: 36.39s
Result: 64177, 20026

Brute-force attack
Time: 0.28 s
Result: Vector (12449, 20026, 22723, 35458, 41378, 49175, 49932, 58662, 58675, 64177)

[Figure 4] Newton's Method and a Brute-Force Attack with a Key Size of 16-bits

4. Discussion and Result

4.1 XOR and Hash-based Scheme

There are two kinds of main security problems for the previous polynomial-based scheme. One is that a group member can obtain the KEK of other members that are shared with the group controller. The other one is that the method cannot achieve both forward and backward secrecy.

The group controller generates a polynomial P using modulus N (i.e., N = pq, where p and q are large primes) :

$$P = (x - KEK_1 \oplus C_1)(x - KEK_2 \oplus C_2) \cdots (x - KEK_N \oplus C_n) + GK_k \qquad (25)$$

A mark C_i is a random number chosen by each member. The group controller sends the authentication message Auth = h(GK_K) along with polynomial P to the members, and GK_K is hashed by the secure one-way hash function h(·). Every member retrieves the intra-group key by computing $P(KEK_t \oplus C_t)$ and checks whether the authentication message is valid or not.

4.2 Hash-Based Scheme

Liu et al. (2013) simply mentioned an improved mechanism for solving the above attacks that changes $x-KEK_i$ to $x-h(KEK_i \| u)$. The value u is public and different in each session, so the group controller broadcasts polynomial P and value u to the members. The mark || means there is a concatenation of KEK and u.

$$P=(x-h(KEK_1\|u))(x-h(KEK_2\|u)) \cdots (x-h(KEK_n\|u))+GK_k \tag{26}$$

Equation (26) can solve all of the problems which mentioned in section 2. It can even solve the root of the polynomial, and the malicious user cannot obtain the KEK of other group members. Therefore, the attacker cannot deduce the intra-group key using an old/new polynomial. The secret key KEK will be changed for every session, and the group controller have to regenerate the polynomial all the time when a member joins or leaves the group. The improved scheme overcomes the security drawbacks that exist in the original by embedding a hash function, and it is the most suitable mechanism for our application.

4.3 Result

The comparison of re-keying overhead, storage overhead and communication overhead of the polynomial scheme and other key management schemes already described in our previous paper (Piao et al., 2013). We now compare the original polynomial-based scheme and improved polynomial scheme. In <Table 1> we compare the schemes against the five differents criteria : Kamal's Attack, Simultaneous Equations, Newton's Method, Berlekamp Algorithm, Brute-force Attack. Studying the result in <Table 1>, the improved scheme can solve Kamal's attack, simultaneous equations and berlekamp algorithm. When the key size is larger than 256 bits, both the original and the improved scheme solve Newton's method and brute-force attack.

5. Conclusions

With the popularization of the internet, the exploitation of Information and Communication Technologies in IT service becomes the focus of research. In online shopping environment people are more concerned with the protection

〈Table 1〉 Comparison of the original and improved polynomial scheme

protocol	Kamal's Attack	Simultaneous Equations	Newton's Method	Berlekamp Algorithm	Brute-force Attack
original polynomial scheme	unsolved	unsolved	solved (key size is larger than 128-bits)	unsolved	solved (key size is larger than 256-bits)
improved polynomial scheme	solved	solved	solved (key size is larger than 128-bits)	solved	solved (key size is larger than 256-bits)

of their privacy. To increase security for online consumers, we can apply a polynomial-based encryption method to online shopping communications system, the reason for adopting polynomial-based method in the encryption stage instead of traditional encryption method is that the traditional schemes increase the communication overhead when the sender and receiver share the secret key, the comparison of the storage overhead number of re-keying message and communication overhead with the traditional schemes are mentioned in our previous paper. In this paper, we mainly analyze the security problems against the mentioned polynomial-based method using Kamal's attack, simultaneous equations, Newton's method, the Berlekamp algorithm, and a brute-force attack. According to security analyses, we finally recommend the most suitable hash-based method based on our previous polynomial scheme which can solve all of the possible security problems. Taken together, it will help strengthen security for consumer data, such as payment information and logistics data for online communication when we adopt the improved method. The purpose of the current study was to make the encryption method more light weight and more secure in online shopping, and the findings of this study have a number of important implications for encryption and authentication technology in online communication.

An issue that was not addressed in this study is that the more consumers there are in the group, the more computation overhead can be incurred by changing the secret key *KEK*. Further research can be undertaken in the following areas : First, we will further adopt efficient expansion of the mathematical methods in the polynomial expansion stage as a future work. Second, we will further do a simulation for making a comparison of the computation overhead between a traditional encryption method and a polynomial-based method in the future.

References

Anthony, D.M. and F. Ana, "Consumer Perceptions of Privacy and Security Risks for Online Shopping", *Journal of Consumer Affairs*, Vol.35, No.1, 2005, 27-44.

Berlekamp, E.R., "Factoring polynomials over large finite fields", *Mathematics of Computation*, Vol.24, No.111, 1970, 713-735.

Blundo, C., F. Orciuoli, and M. Parente, "An AmI-based and privacy-preserving shopping mall model", *Human-centric Computing and Information Sciences*, Vol.7, No.1, 2017, 1-28.

Cantor, D.G. and H. Zassenhaus, "A new algorithm for factoring polynomials over finite fields", *Mathematics of Computation*, Vol.36, No.154, 1981, 587-592.

Chang, C.C., L. Harn, and T.F. Cheng, "Notes on 'Polynomial-based key management for secure intra-group and inter-group communication' ", *International Journal of Network Security*, Vol.16, No.2, 2014, 165-170.

Chen, H., C.E. Beaudoin, and T. Hong, "Securing online privacy : An empirical test on Internet scam victimization, online privacy concerns, and privacy protection behaviors", *Computers in Human Behavior*, Vol.70, 2017, 291-302.

Diffie, W. and M.E. Hellman, "New directions in cryptography", *IEEE Transactions on Information Theory*, Vol.22, No.6, 1976, 644-654.

Döbelt, S., M. Jung, M. Busch, and M. Tscheligi, "Consumers' privacy concerns and implications for a privacy preserving Smart Grid architecture—Results of an Austrian study", *Energy Research and Social Science*, Vol.9, 2015, 137-145.

Galup, S.D., R. Dattero, J.J. Quan, and S. Conger, "An overview of it service management", *Communications of the Acm*, Vol.52, No.5, 2009, 124-127.

Gurung, A. and M.K. Raja, "Online privacy and security concerns of consumers", *Information and Computer Security*, Vol.24, No.4, 2016, 348-371.

Haddad, G.E., E. Aïmeur, and H. Hage, "Understanding trust, privacy and financial fears in online payment", *Security And Privacy In Computing and Communications/12th IEEE International Conference On Big Data Science And Engineering*, 2018, 28-36.

Harney, H. and C. Muckenhirn, "Group key management protocol(GKMP) Specification", RFC 2093, 1997, Available at https://datatracker.ietf.org/doc/rfc2093/.

Hwang, Y. and J. Jeong, "Electronic Commerce and Online Consumer Behavior Research : A Literature Review", *Information Development*, Vol.32, No.3, 2016, 377-388.

Janse, N., C.X. Ou, Angelopoulos, J., S., Davison, R.M., and J.W. Jia, "Do security breaches matter to consumers?", ICEB 2017 Proceedings, 2017, Available at https://aisel.aisnet.org/iceb2017/50.

Jo, H. and J.M. Lee, "A Study on Antecedents of WOM in the Context of Internet E-Commerce", *Journal of Information Technology Services*, Vol.12, No.2, 2013, 231-242.

Kahn, C.M. and J.M. Liñares-Zegarra, "Identity theft and consumer payment choice : Does security really matter?", *Journal of Financial Services Research*, Vol.50, No.1, 2016, 121-159.

Kamal, A.A., "Cryptanalysis of a polynomial-based key management scheme for secure group communication", *International Journal of Network Security*, Vol.15, No.1, 2013, 68-70.

Liu, D., P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability", *in Proceedings of the 10th ACM conference on computer and Communications Security*, 2003, 231-240.

Liu, N., S. Tang, and L. Xu, "Attacks and comments on several recently proposed key management schemes", 2013, Available at https://eprint.iacr.org/2013/100.

Mou, J., D.H. Shin, and J.F. Cohen, "Trust and risk in consumer acceptance of e-services", *Electronic Commerce Research*, Vol.17, No.2, 2017, 255-288.

Newton's Method, Available at https://en.wikipedia.org/wiki/Newton's_method.

Patsakis C. and A. Solanas, "An efficient scheme for centralized group key management in collaborative environments", 2013, Available at http://citeseerx.ist.psu.edu/viewdoc/summary?.

Piao, Y. and M.J. Kim, "A study on the protection of consumers' personal information in online shopping", *Academic Society of Global Business Administration*, Vol.15, No.5, 2018, 209-223.

Piao, Y., J.U. Kim, U. Tariq, and M. Hong, "Polynomial-based key management for secure intra-group and inter-group communication", *Computers and Mathematics with*

Applications, Vol.65, No.9, 2013, 1300-1309.

Shamir, A., “How to share a secret”, *Communications of the ACM*, Vol.22, No.11, 1979, 612-613.

Shoup, V., “On the deterministic complexity of factoring polynomials over finite fields”, *Information Processing Letters*, Vol.33, No.5, 1990, 261-267.

Staddon, J., S. Miner, M. Franklin, D. Balfanz, M. Malkin, and D. Dean, “Self-healing key distribution with revocation”, *IEEE Symposium on Security and Privacy*, 2002.

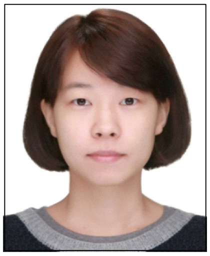
Wang, W. and B. Bhargava, “Key distribution and update for secure inter-group multicast communication”, *SASN ’05 Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*, 2005, 43-52.

Wang, W. and T. Stransky, “Stateless key distribution for secure intra and inter-group multicast in mobile wireless network”, *Computer Networks*, Vol.51, No.15, 2007, 4303-4321.

Wang, W. and Y. Wang, “Secure group-based information sharing in mobile ad hoc networks”, *IEEE International Conference on Communications*, 2008, 1695-1699.

Wong, C.K., M. Gouda, and S.S. Lam, “Secure group communications using key graphs”, *IEEE/ACM Transactions on Networking*, Vol.8, No.1, 2000, 68-79.

◈ About the Authors ◈



박 연 희 (piaoyanji@ybu.edu.cn)

북경공업대학교 컴퓨터공학과를 졸업하고, 아주대학교 정보통신전문대학원에서 석사 박사를 졸업하고, 현재 중국 연변대학 정보관리 및 정보시스템 학과에 재직하고 있다. 주요 관심분야는 정보관리, 전자상거래 등이다.

김 민 지 (kittybus@snu.ac.kr)

현재 서울대학교 경영대학 시간강사로 재직 중이다. 전북대학교 상과대학에서 경영학을 전공하였으며, 동 대학에서 경영학석사 및 경영학박사를 취득하였다. 박사학위 취득 이후에는 한국연구재단의 지원을 받아 신진연구자로서 활발히 연구를 진행 중이다. 주요 연구분야는 마케팅, 소비자 행동, 소비 심리 등이다.