A Security Refreshing Algorithm of Dynamic Node based on Fast Group-Blind Signature

Hongbin Fan and Jiamin Rao *

College of software and communication engineering, XiangNan University,Chenzhou,423000, China.
Email: xnxyacm@126.com

Abstract. In the contemporary society, electronic payment becomes a part of people's life. It can make people's life more convenient and faster. At the same time, security's problem and efficiency's problem in the electronic payment arouse the attention of many researchers. In this paper, we study group-blind signature algorithms in digital signature technology. We take LR98 group-blind signature algorithm as the research object and analyze its problems. The algorithm put the fixed value l as security parameter, which results in the low efficiency of algorithm. In this paper, new security parameters are adopted, and take blind signature method of Boldyreva into consideration, a new group-blind method is proposed, CL-LR98. New method is applied to wireless communication network (WSN). A number of communication nodes (AP) and user terminal (UE) are built, which is used as the experimental environment. New group-blind signature method is applied to dynamic refreshing of WSN nodes, which includes anonymous communication, data transmission. In the process of experiments, new group-blind method has excellent characteristics, it has short signature character length, it can be simply realized and it has better encryption performance. In the node joining part and revocation part of communication process, these excellent characteristics make computation small, make node refresh efficiency high, and it will not cause frequent movement of other communication nodes.

1. Introduction

With the continuous development of Internet, life way of people is gradually transforming into way of information and way of network. As a new technology, e-business technology change the way of people's living. E-commerce[1] breaks traditional business model, and people can do a lot of economic activities at home or at other offices. The influence of electronic commerce has been attracted strong interest of all countries and many countries have made development strategy[2] of e-commerce. Some countries think that e-commerce can give new technological revolution to human and it can benefit the further development of productive forces.

Traditional commodity trading methods include cash payment[3] and bank card transfer[4]. There are many problems in these ways, which include the inconvenience of carrying, the loss of storage, the liquidity of fake currency. The bank's recycling of money needs a lot of human resources and material resources, and way of cash transactions is not good to trans-regional transactions. Electronic payment can help people achieve trans-regional transactions, and it do not need to store large amounts of cash. It is also an important part of e-commerce. Electronic payment is divided into 3 sub categories, which includes credit-card payment, online-check payment and paperless cash payment[5]. Among these electronic payment methods, credit-card payment is not applicable to off-line payment, it needs many supports, which includes shops, users, banks and card agencies, these departments need online to carry out data transmission and complete the transaction, but this kind of transaction is not anonymous,
which pay high cost for small payment; online-check payment can be used for off-line payment and it also be used for small payments, but it cannot prevent user's overdraft consumption, which is unsafe; paperless cash payments can be used as our cash, paperless cash can circulate and trade in different areas of life, this transaction way is used for off-line payment, the information of both sides in the transaction is confidential. Therefore, paperless cash payment has become an important means of electronic payment.

Paperless cash needs to rely on wireless communication nodes, which are used for data exchange and information authentication. The essence of e-commerce is to carry out trading activities of virtual currency under network environment, but the security problem is also showing an increasing trend. In 2010, a Trojan virus attacked the Iran Scher nuclear power station[6]; in 2011, hackers successfully entered a hydropower plant in Illinois[7], United States, by attacking the system's access mode, which caused a large number of water supply accidents; related organizations of U.S reported[8] that network security problems caused rising trend of network attacks. As a part of network environment, wireless communication environment affects people's lives and it is easily attacked by illegal elements, which results in economic losses. In the wireless communication environment, there are many nodes, data need to be transmitted among multiple nodes. Most people store their privacy and confidential data in the mobile phone, which cause the high probability of information disclosure. According to domestic manufacturers' research, in 2014, based on the Android platform[9], they found about 1000000 virus packages, which 40% of these packages were used to steal user's privacy information; Bucknell University also mentioned that more than 70% of iPhone applications had the risk of information disclosure. Under the network environment, information is easily altered, and digital signature technology[10] is a major security technology under current network environment. It can authenticate each layer of electronic data transmission. Digital signatures will be affected by different parameters, the same person signatures different messages, and its signature results are different; in different applications, the signatures of same message will produce different signature results. The scheme of digital signature includes blind signature, group signature, threshold signature and forward secure signature. The digital signature we study is group-blind signature.

Group-blind signature is a combination of group signature and blind signature. The signature method can be traced back to 1991, D. Chaum and Evan Heyst[11] proposed the first group signature scheme in the world. Chen put bilinear of identity into the group signature scheme, so that the scheme can effectively solve the key management problem. In 1982, on the basis of group signature scheme, D. Chaum put it into the paperless cash field and proposed the first electronic payment system. Some experts further improved the electronic payment system, they converted information invisibility into partial visibility of information, but all the electronic payment systems were based on the "single point" model, that means, there is only one user terminal, and multiple communication nodes must communicate by this user terminal. Multiple user terminals mean a number of network banks. In 1998, Lysyanskaya and Z. Ramzan[12] proposed a new group-blind signature. The signature method was close to the communication model of multiple communication nodes. The length of signature group key was nonlinear related to different communication nodes, but there were still many problems in this way, which included the low efficiency of executing, the complexity of computation, and the inadmissibility of joint attack.

In this paper, we learn group-blind signature algorithm in digital signature technology, analyzes the existing algorithms and selects LR98 group-blind signature algorithm as the research object. The algorithm takes the fixed value 1 as a security parameter, which makes the length of group key get linear relation with group size, then improves the computation of public key, increases the cost of data communication, so cause the efficiency of algorithm is not high. We improves LR98 group-blind signature algorithm, put the blind signature method of Boldyreva[13] into new method, proposes a new group-blind method, CL-LR98, a number of communication nodes (AP) and user terminal (UE) are built, which is used as the experimental environment. We analyze the security of communication node (Access Points, APs), which include anonymous communication and data transmission. In the process of experiments, new group-blind method has excellent characteristics, it has short signature character length, it can be simply realized and it has better encryption performance. In the node joining part and revocation part of communication process, these excellent characteristics make computation
small, make node refresh efficiency high, and it will not cause frequent movement of other communication nodes.

2. Analysis of Lr98 Group-Blind Signature Scheme

The LR98 group-blind signature scheme is proposed by Lysyanskaka and Z. Ramzan. The scheme is divided into 4 steps: (1) select the data analysis problem with large amount of computation; (2) apply the knowledge signature to the problem of data analysis; (3) blind process of knowledge signature; (4) a group-blind signature scheme is designed based on the blind process. The LR98 group-blind method has 3 blind ideas, which are blind knowledge signature of discrete logarithm(BSKLOG), blind knowledge signature of double-discrete logarithm(BSKLOGLOG) and blind knowledge signature of discrete logarithm multiple square root(BSKROOTLOG). The implementation steps of 3 blind ideas are roughly the same, they include: (1) send a message signature application; (2) the signer selects random number sequence to the user; (3) the signature blind; (4) the signer encrypts the user's key; (5) the user decrypts the encrypted information of the receiving, and the specific process is as follows:

(1) The user needs to sign the message $A_1$, so it is necessary to send out a signature application to the signer;

(2) The signer needs to select a sequence of random numbers, and specific implementation steps are:

$$\begin{align*}
p_i &\in \mathbb{Z}_{n(R)}, \quad 1 \leq i \leq l \\
q_i &:= v f^{p_i}, \quad 1 \leq i \leq l
\end{align*}$$

(1)

In accordance with the above criteria, we choose random sequence $\{q_i\}$ and send the sequence to users;

(3) Users blind the data based on the random sequence that send by the signer. The blind process includes the replacement of random sequences, 2-encryption based on random variables, the vectorization of message-password variables, the inverse of the vectorization, and sending inverse vector to the signer. In this process, the replacement of random sequences and 2-encryption based on random variables are important. This two steps realize the encryption of data sequence, and the encryption needs to ensure the existence of unique decryption method. If the encryption method is wrong, the data cannot be decrypted. The two steps are as follows:

$$\begin{align*}
u : \{1,\ldots,l\} &\rightarrow \{l,\ldots,1\}, \quad E_i := q_{ci} \\
\text{Random series} : w_1, w_2, \ldots, w_n, \quad V_i := E_i q^{wi}
\end{align*}$$

(2)

(4) The signer encrypts the key of user, design the decrypting key based on structure of encrypting key. In general, the key structure of user is the type of logarithm-exponent, the signer sends decryption key to the user, and the decryption key is as follows:

$$\begin{align*}
cf_i \\
cfi - j (\text{mod } n)
\end{align*}$$

(3)

In formula (3), we find that there are 2 decrypting keys. According to the length of encrypted data, we set different decrypting keys respectively, in which, the longer encrypting data, its corresponding decrypting key is expressed as $cf_i$; the shorter encrypting data, its corresponding decryption key is $cf_i - j (\text{mod } n)$.

(5) According to the decryption key that be sent by the signer, user decrypts the data, so can obtain the signature of the message $A_i$, as shown in Figure 1:
User need to sign the message $A_1$, which requires signature application.

Signer needs to send $\{q_i\}$ to users and commit to $\{q_i\}$.

If $(j=\log_2 c)$, calculate $f(j, b, n)$

Out of blindness

Random permutation, $E_i = qci$

Select random variables, $w_1, w_2, w_3, ..., V_i = E_q u_i$

$x = F(A_1 || y || q_i || V_1 || .. || V_i)$

Validate $q_i$

Calculate $F(j, b_i, n) + k_i \mod n$

Output signature of the message $A_1$

**Figure 1.** Blind idea of knowledge signature

In Figure 1, we see that the content is about the process of breaking off blind in the lower left corner of graph. The user needs to confirm whether the decryption method of signer sending corresponds to sending message, the data is restored based on the decrypting information, and the digital signature of message $A_1$ is finally obtained.

Base on blind idea of knowledge signature, the implementation process of LR98 group-blind signature method includes: (1) system establishment; (2) member joining; (3) signature function and verification function; (4) open protocol. The process of system establishment is described as follows:

**Figure 2.** System establishment phase

In Figure 2, we see that system establishment phase is divided into 4 steps, it requires a pair of public keys $(r, d)$, which the length of the $r$ is greater than the $2^d$ bit; for the more complex part, a $r$-order cyclic group is applied, which is helpful to simplifying problem; a variable $al$ is selected and the main factor of variable can support multiplication; installing the parameter of private key's length is $\eta$, which is expressed as the upper limit of length, and the value is a constant. Therefore, we can set public key of group signature to $(r, d, G, g, al, m, \eta)$, that means, the number of passing parameter is at least 7, so we need to reduce the number of parameters.

The process of member joining is described as follows:
Join of member

Choose a private key \( r \), \( r \) is in the \( \{0, 1, \ldots, 2^n - 1\} \)

Calculate \((b, c)\),
\[
\begin{align*}
b &= op \pmod{n} \\
c &= q_i^3
\end{align*}
\]

Output \((b, c)\) to group administrator

Generate a member certificate to the member

---

**Figure 3.** Member joining phase

In Figure 3, we see the stage of member joining, we need to select their own private key in a certain standard, and then calculate \((b, c)\), send it to group signature administrator, the administrator decrypts it, and determines that members know their private key; administrator sends a member certificate, and this certificate is also a signature function.

Signature function and verification function are described as follows:

---

**Figure 4.** Signature function and verifying function

In Figure 4, we see that we need to implement two processes in the phase, signature and verification. At the signature stage, we need to select appropriate random number, and apply the SKLOGLOG protocol and the SKROOTLOG protocol into indexing of parameters, realize the encryption of data, get \( q_i^{SKLOGLOG} \) and \( q_i^{SKROOTLOG} \), take it as a part of encrypting information, and send it to the user; the user decrypts the encrypted information that is sent by the signer, so can get the signature value of parameter \((pi, Z, T_1, T_2)\), it can be verified the correctness of signature by \( T_1 \) and \( T_2 \).

2.1. Security Analysis of LR98 Scheme

The LR98 group-blind signature scheme is based on the calculation of member's certificate, made corresponding plans, security measures are adopted logarithmic method, which include discrete logarithm, double-discrete logarithm and discrete logarithm multiple square root. At the same time, Schnorr signature scheme[14] and RSA signature scheme[15] are used for reference, and some
researchers did analysis of safety for these signature schemes, which was applied to LR98 group-blind signature scheme.

2.2. Executive Efficiency of Lr98 Scheme
LR98 group-blind signature scheme needs to set up a security parameter, which is a constant. The group-blind signature scheme involves system establishment phase, member joining phase, signature-verification stage. In these stages, generation of each step is linear with the security parameters.

The process of opening signature requires a large amount of time, and time is linear with the size of group. At the same time, the space of signature is also linear with the size of group. We can further find that the public key length of group signature is linearly related to group size in the LR98 group-blind signature scheme. The computational complexity of signature and the spatial complexity of signature are all related to security parameters, and the total computation is positively correlated with the security parameters, which leads to the low execution efficiency of LR98 group-blind signature scheme.

3. Improved Group-Blind Algorithm
The LR98 group-blind signature scheme is constrained by the security parameters, which leads to the large calculation of public key and private key. We analyze the parameter design method of Boldyreva group signature scheme and improve LR98 group-blind scheme, a new group-blind method is proposed, CL-LR98. Before we carry out the algorithm, we need to set some public parameters:

\[
\begin{align*}
\text{parameter: } & re > 1, \ wq, \ rt \\
\text{bit length: } & \beta_1, \ \beta_2, \ \eta_1, \ \eta_2 \\
\beta_1 & > re(\beta_2 + wq) + 2, \ \beta_2 > 4. rt \\
\eta_1 & > re(\eta_2 + wq) + 2, \ \eta_2 > \eta_1 + 2
\end{align*}
\] (4)

In the formula (4), we define the parameters and describe the range of upper limit and lower limit. Therefore, the security parameter is no longer a fixed value, and the corresponding range is expressed as:

\[
(Down\_value, \ Upper\_value) = \begin{cases} (2^{\beta_1} - 2^{\beta_2}, \ 2^{\beta_1} + 2^{\beta_2}) \\ (2^{\eta_1} - 2^{\eta_2}, \ 2^{\eta_1} + 2^{\eta_2}) \end{cases}
\] (5)

In formula (5), upper limit and lower limit of the range are expressed in the way of interval. The interval can effectively change the length of range, and calculation of the public key and the private key will be reduced accordingly.

3.1. Implementation of Algorithm
In the system establishment phase, the group administrator (GM) randomly selects a \( rt \) bits of prime number \((ad', ac')\). Based on the definition of prime number, it can be deduced that \( 2ad' + 1, 2ac' + 1 \) are prime numbers. When we carry out the calculation of modulus, the size of modulus is no longer a constant \( n \), it is set to \( (2ad' + 1)(2ac' + 1) \), and the specific steps of this stage are such as below:
System establishment

The size of N: \((2^{ad'}+1)(2^{ac'+1})\)

Choose a series of random numbers \((e, e_0, pe, ph)\)

Choose a random number \(M, M\) is the range of \((2^{ad'}+1)(2^{ac'+1})\)

\(Ve = pe^M \mod N\)

Public key of group is \((N, e, e_0, Ve, pe, ph)\)

Figure 5. System establishment phase of new algorithm

In Figure 5, we select 4 random numbers as parameters, and their range is \((2^{ad'}+1)(2^{ac'+1})\). In this range, we select the random number \(M\) and calculate \(Ve = pe^M \mod N\), then the public key of GM can be expressed as \((N, e, e_0, Ve, pe, ph)\), the private key of GM can be expressed as \((ad', ac', M)\).

In the process of member joining, we assume that communication channels of user \(Ti\) and GM are secure. The specific steps include: (1) the user \(Ti\) generates a secret index \(aq\), which value range is \([0, 2^{\beta_2}]\); (2) selects a random integer \(te\), and its value range is \([0, (2^{ad'}+1)(2^{ac'+1})^2]\); (3) Calculating \(C_1\), we proves that \(C_1\) is an expression based on \((pe, ph)\) and tells the process to GM, the expression of \(C_1\) is denoted as:

\[
C_1 = pe^{aq} ph^{te} \tag{6}
\]

GM checks whether \(C_1\) is in the range. GM selects two parameters \((k_i, j_i)\), the parameters are in the range of \([0, 2^{\beta_2}]\), send pairs of parameters to users and users do the calculation:

\[
aq_i = 2^{\beta_1} + (k_i aq + j_i \mod 2^{\beta_2}) \tag{7}
\]

The user do the calculation, \(C_2 = e^{aq^2} \mod N\), sends the result to GM, and proves to GM: (1) the discrete logarithm of \(C_2\) is located in \((2^{\beta_1} - 2^{\beta_2}, 2^{\beta_1} + 2^{\beta_2})\); (2) put \(eu\) in the range of \((-2^{\beta_2}, 2^{\beta_2})\), \(ev = C_2 / e^{\beta_2}\), then the following deduction is made:

\[
C_1^{k_i} pe^{j_i} = pe^{eu} (pe^{\beta_2^2})^{ev} ph^{ev} \tag{8}
\]

In formula 8, the user's private key \(aq = \log_e C_2\), it can be obtained by computing variables \(C_1, k_i, j_i\). GM checks whether \(C_2\) is correct, and then sends member certificates to the user.

After the user gets member certificate, it needs to be blind to message. We need to send a signature request and calculate the initial parameters by \(mod\). Here we take a linear method to blind it. The specific implementation steps are as follows:

Figure 6. Blindness phase of new algorithm
In Figure 6, the blind process is further simplified to the sum of linear functions. The user needs to message of signing, which is range of \( \{0, 1\}^* \), user selects the parameter \( RT \), and its value range is \([0, (2ad^2+1)(2ac^2+1)]\), the calculated function is \( f(\text{message}) \), which is expressed as \( f(\text{message})=Ve(\text{message})+RT,pe, f(\text{message}) \) is sent to the other members in the group.

3.2. Security's Analysis of Algorithm

The algorithm is based on the improvement of LR98 group-blind signature, and the design concept of Boldyreva group signature scheme is applied. The new group-blind signature scheme is based on the random prediction model. The model emphasizes the RSA method and the Diffie-Hellman hypothesis, security performance of algorithm is the same as Boldyreva group signature scheme. According to some studies, the security performance of Boldyreva group signature scheme is reliable.

Compared to LR98 group-blind signature scheme, the new group blind signature scheme, CL-LR98, changes setting of security parameters and transforms the expression of group public key \((r, d, G, g, al, m, \eta)\) into \((N, e, e_0, pe, ph)\), there is a positive correlation between the length of group public key and the number of group members, which reduces the computational complexity of algorithm; the scheme takes computing methods of discrete logarithm and double-discrete logarithm, the new group blind signature scheme, it combines mod computing with linear computing, further improves the operation efficiency.

4. Node Refreshing System Based on Improved Group-Blind Signature Algorithm

In the process of wireless network communication, communication nodes (AP) can speculate sender and receiver of the data by traffic analysis and data packet decryption, information exchange between communication nodes (AP) and user terminal (UE) is easy to leak; internal signal source can also speculate sender and receiver of the data by data packet decryption and joint attack, which leads the leak of communication data.

The communication mode between communication node (AP) and user terminal (UE) can be either anonymous communication mode or reverse transmission mode. If someone want to adopt the anonymous communication mode, the secret key management is complex and the computational complexity is large; if someone want to adopt the reverse transmission mode, the anonymous communication mode can be improved. We apply the proposed algorithm to the two modes mentioned above, and analyze the signature process of communication node (AP)-user terminal (UE) security authentication.

4.1. Anonymous Communication Model of Communication Nodes

In the process of anonymous communication, the information between nodes(APs) is constantly refreshed. We define the model as 4 parts, which includes the sender (Provider), the receiver (Receive), the group network (G-Network) and the group-blind signature strategy (Blind-Signature). The sender divides the data into multiple split, generates multiple sub-host nodes, each sub-host node has a split; the receiver integrates multiple splits, information encoding and data recovery; the group network is composed of multiple communication nodes, and the communication nodes temporarily store and forward the data, in the range, the node transmission is effective; secure transmission mechanism, we apply the proposed group-blind signature algorithm, do the digital signature for IO of node data, make sure security of data. The wireless network anonymous communication model can be described as:
In Figure 7, the signal sender needs to be defined as a group (G-Provider), the receiver of data needs to be defined as a group (G-Receive), the group signature of signal sender is set to $\operatorname{Sig}_{\text{Pro}}$, the group signature of signal receiver is set to $\operatorname{Sig}_{\text{Rec}}$, the group-blind signature of node communication is set to $\operatorname{Sig}_{\text{Mid-store}}$, and we describe the process from Provider to Receive03:

1. Provider randomly selects number $M$, calculates $V_e = p e^M \mod N$, sends $V_e$ to Node01;
2. Node01 calculates $e = H(V_e || \text{port})$ (Port represents the output port), sends $e$ to Node$i$, Node$i$ is closest to Receive03;
3. Node05 calculates $aw = (p h - p e).e$ and sends $aw$ to Node01;
4. Node01 needs to verify whether $qi(aw, P) = qi(e, \beta \cdot \text{Node05})$ is established, if the expression is established, the identity of the user is real;
5. The communication process from Node05 to Node08 is the same as (1) - (4);
6. The identity of Provider has been proved, and Receive03 will get corresponding communication data from Node08;
7. The information is blocked by Node08, which includes the transmitted path M-Route and the sending Data, that is, $C_1 = f(M\text{-Route}, \text{Data})$, Node08 do the blind for $C_1$, $C_1$ is converted to $C_2$, and $C_2$ is sent to Receive03;
8. Receive03 carries out group signature on $C_2$, gets $\operatorname{Sig}_{\text{Rec}}(C_2)$, and sends $\operatorname{Sig}_{\text{Rec}}(C_2)$ to Provider;
9. Provider do relieving of blindness for $\operatorname{Sig}_{\text{Rec}}(C_2)$ and gets $\operatorname{Sig}_{\text{Rec}}(C_1)$.

4.2. Reverse Transmission Model of Communication Node

Katti introduced the information segmentation into the anonymous communication field. The method does not need any encryption means. The message is divided by the source node, so that the split information can be forwarded to different paths at the same time. Finally, the data is collected at the destination, and then the complete information is decoded. In anonymous group networks, every forwarding path is likely to be breaked, and nodes can get information of data source by acquiring some fragments of information.

Katti further applied the security mechanism of split data, that is, to mark the intercepted splits, and then rewrite the other splits, so that the information is not recognizable. Some scholars have put the research idea of Katti into improving forwarding process of the communication node, and applied the coding idea of multi-path network, which is used for information splitting, that is, it is not visible at the stage of forwarding information in the multi-path, therefore, It can make sure that intercepting information of forward nodes also cannot be decrypted, but there are some defects in this method.

In the process of communication node transmitting information, the attacker destroys multiple communication nodes at the same time, that is, the information of multiple intermediate communication nodes can be intercepted, and the location of the intermediate communication nodes is
regular, therefore, the intercepted information can be decoded. In the wireless communication network, the transmission of information is bidirectional, and the data can be from the sending channel to the receiving channel or from the receiving channel to the sending channel, then the reverse transmission model can be described as:

![G-Network diagram](image)

**Figure 8. Process of reverse transmission**

In Figure 8, the signal sender needs to be defined as a group (G-Provider), the data receiver needs to be defined as a group (G-Receive), the group signature of signal sender is set to $\text{Sig}_{\text{pro}}$, the group signature of signal receiver is set to $\text{Sig}_{\text{rec}}$, the group blind signature of node communication is set to $\text{Sig}_{\text{Mid-store}}$, and the data is sent from Receive to Provider01. In the process of communication, Receive needs to constantly judge the reliability of intermediate nodes. We describe the process from Receive channel to Output channel:

1. Receive randomly selects random number $M$, calculates $V_e = P_e^M \mod N$, and sends $V_e$ to Node06;
2. Receive randomly selects random number $M$, calculates $V_e' = P_e^M \mod N$, and sends $V_e$ to Node07;
3. Receive randomly selects random number $M$, calculates $V_e'' = P_e^M \mod N$, and sends $V_e$ to Node08;
4. Node06 calculates $e'' = H(V_e || \text{port})$ (Port represents the output port), sends $e''$ to Receive;
5. Node07 calculates $e' = H(V_e' || \text{port})$ (Port represents the output port), sends $e'$ to Receive;
6. Node08 calculates $e'' = H(V_e'' || \text{port})$ (Port represents the output port), sends $e''$ to Receive;
7. Receive calculates $aw = (ph - pe).e$ and sends $aw$ to Node06;
8. Receive calculates $aw' = (ph - pe).e'$ and sends $aw'$ to Node07;
9. Receive calculates $aw'' = (ph - pe).e''$ and sends $aw''$ to Node08;
10. Node06 needs to verify whether $q_i(aw, P) = q_i(e, \beta\text{-Receive})$ is established;
11. Node07 needs to verify whether $q_i(aw', P) = q_i(e', \beta\text{-Receive})$ is established;
12. Node08 needs to verify whether $q_i(aw'', P) = q_i(e'', \beta\text{-Receive})$ is established;
13. By argument, Receive decides to send data from Node08.

**5. Discussion**

We take LR98 group-blind signature algorithm as the research object, analyze the reason of algorithm's low efficiency, adopt the new security parameters and combine the signature blind method of Boldyreva, and propose a new group blind method, CL-LR98. The process description and performance analysis of the algorithm are carried out. New group-blind method has excellent characteristics, it has short signature character length, it can be simply realized and it has better encryption performance.

New method is applied to wireless communication network (WSN). A number of communication nodes (AP) and user terminal (UE) are built, which is used as the experimental environment. New group-blind signature method is applied to dynamic refreshing of WSN nodes. The network is divided into Provider, Receive, group network (G-Network) and group-blind signature strategy (Blind-Signature). Based on the proposed group-blind signature algorithm, we do the process description of anonymous communication and reverse communication.
In the process of experiments, new group-blind method has excellent characteristics, it has short signature character length, it can be simply realized and it has better encryption performance. In the node joining part and revocation part of communication process, these excellent characteristics make computation small, make node refresh efficiency high, and it will not cause frequent movement of other communication nodes.

6. Acknowledgements
This work was supported by Hunan Province Colleges and Universities Teaching Reform Research Project "research and practice of application-oriented talents training of computer major in local colleges and Universities Based on the perspective of subject competition" (xiangjiaotong [2017] No.452, 449) , and Xiangnan University Laboratory Open Project "Computer Application and Software Development" (Xiangnan University xiao fa [2018] No.159,12).

7. References
[1] Chellappa R K, Pavlou P A, "Perceived Information Security, Financial Liability and Consumer Trust in Electronic Commerce Transactions[J].", Logistics Information Management, Vol 15 No 5-6, pp: 358-368, 2014.
[2] Engin E, Liu J, Rudolph U, "α2-containing GABAA receptors: A target for the development of novel treatment strategies for CNS disorders[J].", Pharmacology & Therapeutics, Vol 136 No 2, pp: 142-152, 2012.
[3] Pettifor A, Macphail C, Nguyen N, Rosenberg M, "Can money prevent the spread of HIV? A review of cash payments for HIV prevention.[J].", Aids & Behavior, Vol 16 No 7, pp: 1729-1738, 2012.
[4] Cury J, Jové T, Touchon M, Neron B, Rocha EP, "Identification and analysis of integrons and cassette arrays in bacterial genomes[J].", Nucleic Acids Research, Vol 44 No 10, pp: 4539-4550, 2016.
[5] Pritchard G, Vines J, Olivier P, "Your Money's No Good Here:The Elimination of Cash Payment on London Buses[C]", ACM Conference on Human Factors in Computing Systems, Vol 76 No 1, pp: 907-916, 2015.
[6] Chang C H, Yang C W, Hwang T, "Trojan Horse Attack Free Fault-Tolerant QuantumKey Distribution Protocols Using GHZ States[J].", International Journal of Theoretical Physics, Vol 55 No 9, pp:1-12, 2016.
[7] Weinberger J, Saxena P, Akhawe D, Finifter M, Shin R, Song D, "A Systematic Analysis of XSS Sanitization in Web Application Frameworks[C].", European Conference on Research in Computer Security, Vol 6879 No 2, pp: 150-171, 2011.
[8] Umamaheswari S, Mahalakshmi R, "Dynamic Network Event Analysis for Distributed Attack Detection in Wireless Sensor Networks[J].", Sensor Letters, Vol 13 No 1, pp: 64-71,2015.
[9] Nissim N, Moskovitch R, Barad O, Rokach L, Elovici Y, "ALDROID: efficient update of Android anti-virus software using designated active learning methods[J].", Knowledge & Information Systems, Vol 49 No 3, pp: 795-833, 2016.
[10] Huang L H, Zhang X Q, "Preliminary Study on Digital Signature Technology and Application[J].", Advanced Materials Research, Vol 734-737, pp:3158-3162, 2013.
[11] Sun H M, "Reply: Improved group signature scheme based on discrete logarithm problem[J].", Electronics Letters, Vol 35 No 1, pp: 37-38, 2012.
[12] Zuo H, "Cryptanalysis of Quantum Blind Signature Scheme[J].", International Journal of Theoretical Physics, Vol 52 No 1, pp: 322-329, 2013.
[13] Shim K A, "On the security of verifiably encrypted signature schemes in a multi-user setting[J].", Annals of Telecommunications - Annales Des Telecommunications, Vol 69 No 11-12, pp: 585-591, 2014.
[14] Guo zheng H U, Wuhan, "Analysis of Some Attacks against the Schnorr Signature Scheme[J].", Computer Science, Vol 36 No 10, pp: 98-100, 2009.
[15] Tang S, "Simple secret sharing and threshold RSA signature schemes[J].", Journal of Information & Computational Science, Vol 1 No 2, pp: 259-262, 2004.