4-2 Research Activities on Proxy Cryptosystems and Homomorphic Encryption Schemes

WANG Lihua

In this paper, we introduce our research activities during the past five years and then give a survey about our contributions on designing and developing practical cryptographic protocols including proxy (re)-cryptosystems and homomorphic encryption schemes. Among them, proxy re-encryption and additively homomorphic encryption are significant cryptographic primitives for secure cloud storage and secure data aggregation in wireless sensor networks.

Keywords
Pairing, Proxy cryptosystem, Collusion attack, Homomorphic encryption, Position information authentication

1 Introduction

Public-key encryption schemes use a pair of keys to encrypt and decrypt data. The key for encryption is published, and it is called the public key. The key for decryption is paired with a public key. It is secretly stored by the owner, and called the private key. For example, when sending a message to a user Alice, a plaintext message is encrypted by using Alice's public key before it is sent. It is difficult for users other than Alice to decrypt the ciphertext (encrypted message) by using only public information such as public key; however, Alice can easily decrypt the ciphertext by using her private key to obtain the plaintext. The point here is that Alice's public key must be used to encrypt the data before it is sent to Alice. Otherwise, the information could be disclosed, or decryption may not work. The approach to solve this issue varies depending on infrastructure.

Public Key Infrastructure (PKI)

In traditional public key cryptography (PKC), a public key is simply a string of random characters, and it is not possible to authenticate the owner of the key, Alice, by the key itself. This problem can be solved by using certificates provided by a trusted organization called a Certificate Authority (CA). The CA provides an unforgeable signature and trusted link between the public key and the identity of Alice. Public key infrastructure (PKI) publishes and manages the certificate (chain). In the PKI framework, it is necessary to obtain Alice's certificate before the ciphertext is sent to her to confirm the legitimacy of her certificate. This method is not efficient or practical, especially when the number of users is very large.

Identity-Based Cryptography (IBC)

The aforementioned problem was solved by identity-based cryptography (IBC) that was invented by Shamir[1] in 1984. In this framework, Alice's identity ID (or e-mail address) which is an arbitrary string is used as a public key, and Alice's private key is computed by using a master private key that is provided by a trusted organization called a private key generator (PKG) and her ID. The certificate is provided implicitly, and the public key does not require explicit authentication in this method. The major drawback of identity-based encryption (IBE) is that the PKG is trusted unconditionally. As a result, it makes it possible for the PKG to impersonate arbitrary users or decrypt

arbitrary ciphertext. Therefore, the IBC framework is suitable for a closed organization where the PKG is completely trusted by all users within the group.

Certificate-Based Cryptography (CBC)

In order to integrate the advantages of IBC into PKI, Gentry[2] proposed the concept of certificate-based encryption (CBE). The CBE scheme combines public key encryption scheme between the certifier and user with ID-based encryption scheme. Each user generates their own public key and private key, then requests a certificate from the CA. The CA then creates a certificate using the key generation algorithm of the ID-based encryption scheme. The certificate is implicitly used as a part of the user's decryption key (the decryption key consists of the private key created by the user and the certificate). Although the CA knows the certificate, as they do not possess the user's private key, they cannot decrypt any ciphertext. CBC is a more advanced public key authentication framework that inherits the feature of an implicit certificate from IBC and the "key-escrow-free" feature from PKC.

In the activities of Security Fundamentals Group from FY2006 to FY2010, with an aim to improve the usability for users and security, we designed and evaluated cryptographic protocols that keep up with the progress of the information society and meet the requirements of the real world for each of the aforementioned encryption infrastructure frameworks. This paper outlines our research activities related to the above. In Chapter **2**, we introduce our domestic and international collaboration activities related to efficient pairing-based cryptography, as well as our achievements related to proxy cryptosystems. In Chapter **3**, we introduce our achievements related to homomorphic encryption, as well as the demonstration test of position information authentication that was carried out as a collaboration activity in National Institute of Information and Communications Technology (NICT). Chapter **4** summarizes our contributions to date and future tasks.

2 Research activities on pairing-based cryptosystem

2.1 Workshop for efficient pairing cryptography

Since Boneh and Franklin[3] published the ID-based cryptosystem that uses pairing in 2001, various cryptographic protocols based on the bilinear property of pairing have been proposed and widely discussed. At that time, the computational cost of Weil pairing and Tate pairing was considered to be 10 times and 5 times higher than exponentiation respectively, and due to this large volume of complexity of pairing, in many cases the efficiency of cryptographic protocols will be lowered when it uses pairings. In this research, we conducted joint research with University of Tsukuba and Shanghai Jiao Tong University on efficient cryptographic protocols that maintain properties applicable to the real world, and at the same time use pairing at an appropriate and minimum frequency; and designed an efficient key agreement[4] scheme and proxy cryptosystem.

In FY2008, we received funding from the International Exchange Program/Foreign Researcher Invitation Program, and organized a workshop to build a long-term relationship between the TDT laboratory led by Professor Zhenfu Cao of Shanghai Jiao Tong University and the Security Fundamentals Group of NICT. The workshop offered various lectures on such topics as the current status of pairing technologies, the latest trend of cryptographic researches, cryptography and implementation technologies in application of sensor networks, and authentication technology by Eiji Okamoto (Professor, University of Tsukuba), Zhenfu Cao (Professor, Shanghai Jiao Tong University), Masahiro Mambo (Associate Professor, University of Tsukuba), Tsuyoshi Takagi (Future University-Hakodate), Miao Ying (Associate Professor, University of Tsukuba), and Akihiro Yamamura (NICT), who are specialists in this field. The advocated theory of Professor Zhenfu Cao, "cryptographic technologies are created and developed by the market"

was adopted as the theme of the workshop. In this workshop, Professor Takagi from Future University-Hakodate gave a lecture and introduced that Eta pairing on elliptic curve over GF(3^n) is efficient and it could be adopted for cryptographic systems. However, the problem was that the insolubilities of the discrete logarithm problem on elliptic curve over GF(3^n) had not been verified. This was carried into the joint research[5] on the strength evaluation of cryptographic protocols where security results in a discrete logarithm problem, which was conducted from FY2009 to FY2010.

(http://nictinfo.nict.go.jp/Announce/event/20081024.html Note: the workshop was also held at Shanghai Jiao Tong University in October 2010. http://tdt.sjtu.edu.cn/workshop2010/)

Here we introduce our achievements on more practical cryptosystems by considering what will meet the requirements of the real world, such as a proxy cryptosystem with revocability and a proxy re-encryption scheme that prevents collusion attacks.

2.2 Research on proxy cryptosystems

In 1997, Mambo and Okamoto[6] introduced the concept of proxy cryptosystems (Fig. 1). This is also called proxy decryption. Proxy decryption is a cryptographic scheme that a proxy decryptor decrypts the ciphertext encrypted by user Alice's public key on behalf of Alice. The proxy needs to obtain the proxy decryption right from Alice in advance.

In 1998, Blaze et al.[7] proposed the concept of proxy re-encryption called a PRE system, which is closely related to proxy decryption. In a PRE system, the proxy (proxy re-encryptor) can convert the user Alice's ciphertext to ciphertext for the user Bob without obtaining the information of the plaintext. Therefore, the role of proxy has a very strong connection to untrusted servers in cloud environments.

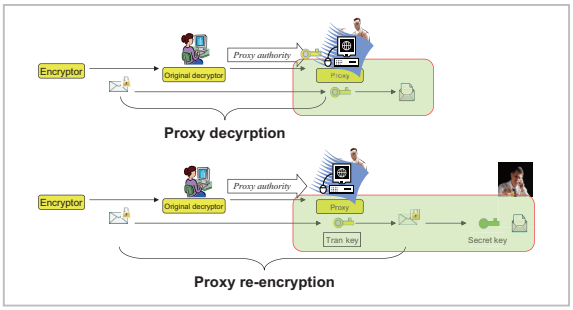

Fig.1 *Proxy decryption & proxy re-encryption*

These two primitives have developed in various ways, and especially since the proposal of pairing-based IBE[3], proxy decryption systems and PRE systems with various features have been proposed for practical uses. Here we introduce a CBE-based proxy decryption system and ID-based PRE system that we have proposed. Both systems employ the bilinear property of pairing.

2.3 The proposed protocols based on pairing

Definition: G_1, G_2 are multiplicative groups, order p is a prime number, and g is the generator of G_1. When the following conditions are satisfied, $\hat{e}$: $G_1 \times G_1 \to G_2$ is an admissible bilinear map.

(1) Bilinear. $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$, for all $a, b \in Z_p^*$.
(2) Non-degenerate. $\hat{e}(g,g) \neq 1_{G_2}$.
(3) Computable. There is an efficient algorithm to compute $\hat{e}(f,h)$ for any $f, h \in G_1$.

Thanks to the bilinear property of $\hat{e}(g^a, g^b) = \hat{e}(g,g)^{ab}$, the proposed cryptographic protocol satisfies the desirable characteristics, and the security of the proposed schemes are based on the assumptions on the following complexity.

Discrete Logarithm Problem:

Given $g, g^a \in G_1$, or $\mu, \mu^a \in G_2$, find $a \in Z_p^*$.

Computational Diffie-Hellman (CDH) Problem:

Given $g, g^a, g^b \in G_1$, find $g^{ab} \in G_1$.

Bilinear Diffie-Hellman (BDH) Problem:

Given $g, g^a, g^b, g^c \in G_1$, find $\hat{e}(g,g)^{abc} \in G_2$.

Decisional Bilinear Diffie-Hellman Assumption (dBDH Assumption):

Given $g, g^a, g^b, g^c \in G_1$ and $\eta \in_R G_2$, dBDH Assumption assumes that it is difficult to separate $\hat{e}(g,g)^{abc}$ from η.

Certificate-based proxy decryption systems with revocability

For the first time in our research, a proxy decryption system (CBPd) was constructed within the CBE framework which is a more advanced infrastructure[8]. The proposed scheme features the advantages of the traditional PKC and IBE, as introduced in **1**. In addition, it has a characteristic called "Revocability" that can retrieve the decryption right which was once delegated by means of publishing common parameters for proxies (proxy decryptors).

[Revocability] means a functionality to revoke the proxy right from the current proxy even during the validity period, and replace the proxy with another one (Fig. 2). For example, a proxy Charlie was delegated a role of the project manager for job project of FY2007 from his manager Alice, and so he is able to decrypt ciphertext related to the job on behalf of Alice until the end of FY2007. However, if Charlie resigns or loses her trust for some reason, Alice needs to revoke the decryption right that was delegated to Charlie.

The proposed scheme features the advantages of the CBE infrastructure, and in this scheme receivers generate their own private keys and do not delegate the private keys to validation centers; therefore, the privacy of the recipients is protected, and at the same time, it provides more usability for the senders, as authentication of PK is not necessary even though e-mails are encrypted by the recipient's ID and PK.

ID-based proxy re-encryption constructions to prevent collusion attack

In the PRE system[7], the proxy (proxy re-encryptor) can convert the user Alice's ciphertext to ciphertext for the user Bob without obtaining the information of the plaintext. Therefore, the role of the proxy has a very strong connection to untrusted servers in cloud environments. This means that when a proxy decryption right is converted to a proxy re-encryption right, the decryption process will be divided into the following two steps: re-encryption process, and decryption process by using the private key of the specified user. The proxy responsible for the re-encryption process can only perform re-encryption, and is unable to decrypt the ciphertext. Thankfully this allows proxy re-encryption to be applied to email forwarding, and secure distributed file storage and therefore it is a very important research theme. For this reason, research on PRE has been drawing a great deal of attention. In this circumstance, a lot of research has been conducted on the ID-based PRE (IB-PRE)[9]-[12]. However, the traditional IB-PRE system requires an assumption that a proxy does not collude with other users and other proxies. This assumption is not realistic in a distributed system environment that is not managed locally, such as the cloud, and therefore it is considered to be an important task to design secure IB-PRE protocol that is protected from collusion attacks.

In 2005, Ateniese et al.[13] presented collusion attacks in the PKI framework for the first time, and defined the security requirements against collusion attacks, including collusion "safeness" and non-transferability (Fig. 3).

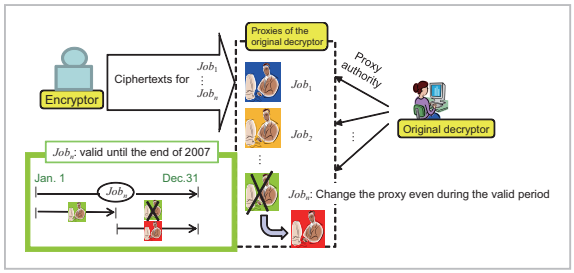

Fig.2 *CBE-based proxy decryption scheme with revocability*

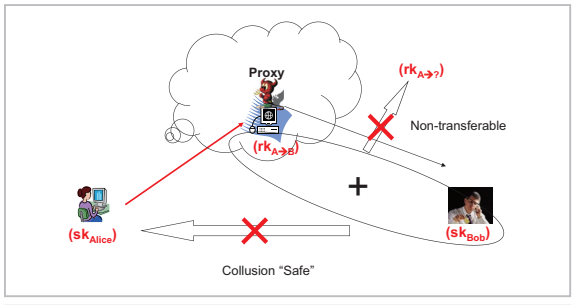

Fig.3 *Collusion "safeness" and non-transferability*

1. Collusion "safeness". Even when the delegatee Bob, i.e., the decryptor who was designated by Alice, colludes with Alice's proxy, Alice's private key will not be disclosed. That is, $rk_{A\to B} + sk_B \nrightarrow sk_A$, where the symbol $rk_{A\to B}$ denotes the re-encryption key for converting Alice's ciphertext to Bob's, and sk_A, sk_B denote Alice's and Bob's private key, respectively.
2. Non-transferability. Even when the delegatee Bob, i.e., the decryptor who was designated by Alice, colludes with Alice's proxy, it is not possible to fake the key for converting Alice's ciphertext to other users' ciphertext except Bob's. That is, $rk_{A\to B} + sk_B \nrightarrow rk_{A\to C}$.

For the first time in the IBE framework, our research proposed IB-PRE constructions that provide security against collusion attacks, such as collusion "safeness" and non-transferability, by using the approach that the key generation center PKG takes part in generating the re-encryption key, in fact generating the re-encryption key seed $\left(\frac{H(id_A)}{H(id_B)}\right)^{u_B}$ [14], which is similar to Matsuo's approach in [11].

As a result, we came to a conclusion that security properties such as collusion "safeness" and non-transferability are reduced IND-CPA (Indistinguishablity under Chosen Plaintext Attack) security versions of an IB-PRE scheme in a single-hop scenario. The proposed scheme is based on a random oracle assumption and is proved IND-CPA/CCA secure under the dBDH assumption.

3 Study on additively homomorphic encryption and its application to position information authentication

3.1 Discrete-logarithm-based additively homomorphic encryption

In homomorphic encryption, when two ciphertexts $Enc(m_1)$, $Enc(m_2)$ are given, it is possible to compute $Enc(m_1 \circ m_2)$ without plaintext or private key, and therefore the cryptographic technique has attracted a lot of interest especially in usage for privacy protection. There are various types of homomorphic encryption schemes depending on which computation type the symbol "$\circ$" denotes, including additively homomorphic encryption[15], multiplicatively homomorphic encryption[16], algebraically homomorphic encryption, and fully homomorphic encryption.

In 1999, Paillier[15] proposed an additively homomorphic encryption based on factoring assumption, which is known as a typical additively homomorphic encryption scheme. This method is constructed from three algorithms.

1. **Key generation:** Let $n=pq$, randomly choose base $g \in B$ where $\gcd(L(g^{\lambda} \bmod n^2), n) = 1$. Therefore, (n, g) denotes the public parameter, and (p, q) (or equivalent $\lambda = lcm(p-1, q-1)$) denotes the secret parameter.
2. **Encryption process:** given plaintext $m<n$, and random number $r<n$, compute ciphertext $c = g^m \cdot r^n \bmod n^2$.
3. **Decryption process:** For any ciphertext $c<n^2$,
   compute plaintext $m = \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n$,
   where the function is given by $L(u) = \frac{u-1}{n}$.

As Paillier's homomorphic encryption scheme satisfies $Enc(m_1 + m_2) = Enc(m_1) \cdot Enc(m_2)$, it is additively homomorphic encryption.

On the other hand, there is no additively homomorphic encryption that is based on discrete logarithm problems. Then in the international conference PKC2006, Chevallier-Mames, Paillier and Pointcheval[17] announced an open problem to "find a discrete logarithm based cryptosystem that would help realize fully additive or fully multiplicative homomorphism". We solved one of the problems, and proposed an additively homomorphic encryption based on ElGamal cryptosystem[18][19]. The original ElGamal cryptosystem is multiplicatively homomorphic. We achieved our target to propose additively homomorphic encryp-

tion, by lifting the message space of ElGamal scheme from M to $g^M{}_0$.

1. **Key generation:** First, choose prime numbers p, p_0 that satisfy the following conditions.
   (1) $p=2q+1$, where q denotes a large prime number,
   (2) $p_0=2t^{\kappa}+1<p$, where t denotes a small prime number, and κ denotes a positive integer.

   Then, choose a generator g of a subgroup of order q of Z_p^* and a generator g_0 of $Z_{p_0}^*$. Thus, system public parameter is given by $params=(p,q,g,p_0,g_0)$, and the plaintext space and the ciphertext space is given by $M=\{0,1,...,p_0-2\}$ and $C=Z_p^*\times Z_p^*$, respectively.

   Next, randomly choose a private key $x\in Z_q$ then compute a public key $y=g^x \bmod p$.
2. **Encryption process:** input a public key y and plaintext $m\in M$, choose a random number $r\in Z_q$, and output ciphertext $(c_1,c_2)=(g^r \bmod p, y^r\cdot(g_0^m \bmod p_0) \bmod p)$.
3. **Decryption process:** input a private key x and ciphertext (c_1,c_2), and compute plaintext $m=L_{g_0}(D_{\times}(x,(c_1,c_2)))$. Here,
   $D_{\times}(x,(c_1,c_2))=c_2/c_1 \bmod p$,
   $L_{g_0}(g_0^m \bmod p_0)=m \bmod (p_0-1)$.

When compared to the aforementioned Basic version, it will be noted that the encryption steps in the proposed scheme are more efficient than Paillier's additively homomorphic encryption scheme, but the decryption steps are more efficient in Paillier's scheme. When comparing both of the Fast versions[15] [19], it will be noted that the proposed scheme is more efficient (Table 1, [19]).

Inner product homomorphic computation based on additively homomorphic scheme

When plaintext satisfies certain conditions, it is possible to realize inner product homomorphic computation by using additively homomorphic scheme.

- Basic rule
  $Enc_{pk}(a)\hat{+}Enc_{pk}(b)=Enc_{pk}(a+b)$.
- Multiple
  $Enc_{pk}(a)\hat{\cdot}\, b=Enc_{pk}(a\cdot b)$.
- "Inner product" of plaintext vector and ciphertext vector is
  $Enc_{pk}(\vec{a})\hat{\cdot}\,\vec{b}=Enc_{pk}(\vec{a}\cdot\vec{b})$.

Table 1 Comparison of complexity

Schemes	Enc	Dec
Paillier-Basic	$[2]exp_{n^2}+[1]mul_{n^2}$ $\approx[128\log p_0]mul_{p_0}$	$[1]exp_{n^2}+[1]mul_n+L_n$ $\approx[64\log p_0]mul_{p_0}$
Paillier-Fast	$[1]exp_{n^2}+[1]mul_{n^2}$ $\approx[64\log p_0]mul_{p_0}$	$[\log\alpha]mul_{n^2}+[1]mul_n+L_n$ $\approx[16\log\alpha]mul_{p_0}$
Our-Basic	$[2]exp_p+[1]exp_{p_0}+[1]mul_p$ $\approx[17\log p_0]mul_{p_0}$	$[1]exp_p+[1]mul_p+L_{g_0}$ $\approx[(8+\log\log p_0)\log p_0]mul_{p_0}$
Our-Fast	$[2]exp_p+[1]exp_{q_0}+[1]mul_p$ $\approx[17\log p_0]mul_{p_0}$	$[\log x]mul_p+[1]mul_p$ $\approx[4\log\alpha]mul_{p_0}$

Therefore,

Given $Enc_{pk}(s_i(0)), Enc_{pk}(s_i(1)), Enc_{pk}(s_i(2)), ...$ and $s_u(0), s_u(1), s_u(2), ...$

Compute
$$\begin{aligned}\tilde{\rho}_{i-u}(\tau)&=\sum_t Enc_{pk}(s_i(t))\hat{\cdot}\, s_u(t+\tau)\\&=\sum_t Enc_{pk}(s_i(t)\cdot s_u(t+\tau))\\&=Enc_{pk}\Big(\sum_t s_i(t)\cdot s_u(t+\tau)\Big)\\&=Enc_{pk}(\rho_{i-u}(\tau))\end{aligned}$$

Then $\rho_{i-u}(\tau)=\mathrm{Dec}_{sk}(\tilde{\rho}_{i-u}(\tau))$, for $\tau=1,2,3,...$

This was useful for a demonstration test of position information authentication.

3.2 Demonstration test of position information authentication based on attentively homomorphic encryption

The pre-project of FY2010, "Demonstration of advanced security technology based on time/position information authentication," aimed to utilize the strength of the fundamental technologies in NICT. In this project, we conducted research and development on a position information authentication system that prevents position information from being fabricated as well as protecting privacy, with the collaboration of the Space-Time Standards Laboratory[20].

Background: Position information is often used in various applications and services, such as for identifying transmission sources or tran-

sit points for physical distribution. However, due to the invariability of position information, the sender of the information is the only resource to rely on, and the authenticity is not very credible. In addition, once the position information has been obtained, it can be used repeatedly, and therefore, it is difficult to detect whether or not multiple information is used to fabricate a position (collusion attack) from interactions over the network. Thus, some ways to authenticate position information are required.

The simple solution is to perform authentication when obtaining position information, for example, by communicating with GPS satellites. However, there are security issues in the existing system, as the user's own position information will be sent to the other party. In addition, it should be possible to detect that the system to obtain position information and the user are located in the same place. It is also necessary to prevent the position information being illegally obtained by the illegal use of the system to obtain position information, with a different position computed and fabricated from the already obtained position information.

In order to solve these issues, it is necessary to utilize not only physically obtained information but also instantaneous information that is generated tentatively. It is also required to establish a trusted third party (TTP) in addition to users and servers, as well as tamper resistance property of devices. Therefore, an infrastructure solution will be required to realize position information authentication. This aims to achieve the following security requirements.

- Detect spoofing of position information
- Detect illegal use and fabrication of position information
- Protect the privacy related to position information

Following this background, this paper applies homomorphic encryption, and proposes two types of protocols, Active Type and Passive Type, which authenticate position information by utilizing the information that can be only generated when a user is in the same location.

Quasi-zenith satellites and LEX signal — Active Type

Quasi-zenith satellites (QZS)[21] are located near the zenith above Japan, and can always receive signals without being affected by buildings or geographical features. For example, as the elevation angle of the current geostationary satellite cannot be set to more than 48 degrees in Tokyo, the signal from the geostationary satellite can be received only in limited locations. On the other hand, as the elevation angle of quasi-zenith satellites can be set to more than 60 degrees, it is possible to receive signal in any location. As the quasi-zenith satellites are always moving, more than three satellites are required to provide 24-hour service. Due to the fact that the quasi-zenith satellites are always moving, from the viewpoint of the receivers who are stationary on the ground, the distance between the satellites and themselves is always changing. LEX signals transmitted from the quasi-zenith satellites use the occupied bandwidth of 42MHz, therefore, distance conversion corresponds to the range resolution of 7.1m. In addition, the orbital speed of the quasi-zenith satellites relative to ground surface is about 2850m/s, therefore, it will take about 2.5ms to cause 7m difference in the distance between the receiver and satellite (Fig. 4).

Assume the positions of three parties, receiver, certificate authority and quasi-zenith satellite, are known. Also assume that the time of all three parties is synchronized. There is a

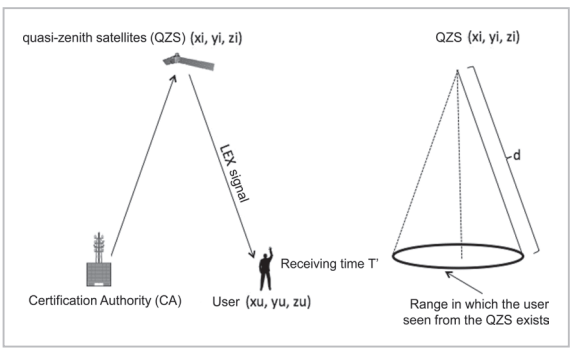

Fig.4 *Active Type position authentication*

time difference from when the quasi-zenith satellite transmits a LEX signal at time T to when the user receives the signal (time received by user, T_0). The distance between the quasi-zenith satellite and user $d=c\cdot|T_0-T|$ can be computed from the time difference $|T_0-T|$. On the other hand, the certificate authority that manages the quasi-zenith satellite knows the location of the satellite (x_i, y_i, z_i) at the time T, therefore, the range of the user's position on the ground surface viewed from the quasi-zenith satellite can be authenticated by (x_i, y_i, z_i) and $d=c\cdot|T_0-T|$, where c denotes the speed of light. Therefore, if the time received by user T_0 is known, the certificate authority will be able to authenticate the range of the user's position (Fig. 5). If T, T_0, (x_i, y_i, z_i) of three different pairs can be obtained, the position of the user can be authenticated from the subspace of the intersection of three circles. The position information authentication scheme that is based on this fact is called Active Type. In reality, the environment to realize this Active Type method is not ready yet, however, a demonstration test of position information authentication has been tried by using radio wave received from broadcasting stations.

Broadcasting station and simultaneous multiple wave receiver — Passive Type

The basic concept of this type is similar to the aforementioned quasi-zenith satellites example. It utilizes the fact that when a microwave transmitted from a broadcasting station is received at two different points, if the distance from the broadcasting station is different in these two received points, a deviation will be generated in the received waveform. Assume there are receiver A and receiver B, and their distance from a broadcasting station is d_A and d_B respectively. Let Wa denote the signal waveform received by receiver A, and Wb denote the one received by receiver B, then input these to a cross correlation function to measure the degree of difference in the locations. Here, there is a time difference between Wa and Wb, according to the difference from the broadcasting station between the receiver A and receiver B, $|d_A-d_B|$. As microwave travels at the same speed as light, the time difference with maximum cross-correlation between Wa and Wb can be computed from $|d_A-d_B|$. On the contrary, when the time difference with maximum cross-correlation between Wa and Wb can be obtained, the range of the receiver B's position from the receiver A's viewpoint can be authenticated. If the time difference between three different parties can be obtained, the position of the receiver can be authenticated from the subspace of the intersection of three circles (Fig. 6)[22]. The position information authentication scheme that is based on this fact is called Passive Type.

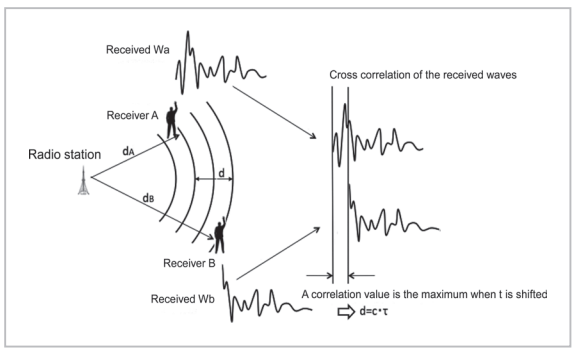

Fig.5 Passive Type position authentication

In the passive type scheme multiple ground waves are received simultaneously. Let V denote the set of transmission sources of ground waves. Each transmission source $(v_i \in V)$ is constantly generating signal sequences $\{s_{i1}, s_{i2}, ...\}$. Each entity of this scheme passively receives these signal sequences. This system is based on an assumption that the time of three entities, certificate authority (CA), trusted third party (TTP), and user, is accurately synchronized. The time difference between receipt times is computed by correlation method.

$$s_i(t) = 0,1,-1,2,0,...$$

$$s_u(t) = 1,-1,2,0,1,...$$

Cross-correlation method: $\rho(\tau) = \int s_i(t)s_u(t-\tau)dt$

$$\rho(0) = \int s_i(t)s_u(t)dt$$

$$= 0\times1+1\times(-1)+(-1)\times2+2\times0+0\times1...$$

$$\rho(1) = \int s_i(t)s_u(t-1)dt$$

$$= 1\times 1 + (-1)\times(-1) + 2\times 2 + 0\times 0 + \ldots$$
$$\vdots$$

The time difference is given by τ_0: $\rho(\tau_0) = \max\{\rho(1), \rho(2), \ldots\}$. In order to compute the time difference while protecting the privacy of the TTP, the signals received by the TTP should be encrypted before being sent to the user. The user computes the inner product between the encrypted sequence received from the TTP and the received plaintext sequence directly from the ground waves. As this ciphertext is based on an inner product homomorphic computation as described in **3.1**, the CA decrypts it as it is in order to obtain $\rho(\tau)$, then τ_0.

Although there are multiple TTPs and their locations are known only to the certificate authority but not to the user, the position information of the TTP is referred to authenticate the user's position information.

The above demonstration test was conducted only by Paillier's additively homomorphic encryption scheme. The remaining tasks include demonstration tests by the proposed discrete logarithm based scheme, efficiency evaluation, and research and development on additively homomorphic encryption technology where the related plaintext space and ciphertext space are equal.

4 Summary

This paper outlined our research activities and achievements on practical encryption protocols by Security Fundamentals Group from FY2006 to FY2010. The above research activities were supported by incentive research/study conducted under NICT special fund, and by the International Exchange Program/Foreign Researcher Invitation Program. We invited specialists in this field to facilitate research exchange. Seminars and workshops were held (Fig. 6), and the achievements were published in international conferences and international journals. The achievements included not only filing a patent application[23], but also publishing to the world the results of the demonstration test through an academic presentation. The projects were rated as "fully achieved" and "surpassed the plan significantly" in the post-project evaluation by the examination

Fig.6 *The 2nd workshop of cooperative research between NICT of Japan and Shanghai Jiao Tong University of China*

committee.

The projects also contributed to the pre-project of FY2010, "Demonstration of advanced security technology based on time/position information authentication," with a collaboration of Space-Time Standards Laboratory and Kashima Space Research Center.

References

1 Shamir, A., "Identity-based cryptosystems and signature schemes," Blakely, G.R., Chaum, D. (eds.), CRYPTO 1984, LNCS, Vol. 196, pp. 47–53, Springer, Heidelberg, 1985.

2 Gentry, C., "Certificate-based encryption and the certificate revocation problem," Biham, E. (ed.), EUROCRPYT 2003, LNCS, Vol. 2656, pp. 272–293, Springer, Heidelberg, 2003.

3 Boneh, D. and Franklin, M., "Identity-based encryption from the Weil pairing," Kilian, J. (ed.), CRYPTO 2001, LNCS, Vol. 2139, pp. 213–229, Springer, Heidelberg, 2001.

4 Wang, S., Cao, Z., Choo, K.R., and Wang, L., "An improved identity-based key agreement protocol and its security proof," Journal of Information Sciences, Vol. 179, pp. 307–318, 2009.

5 Hayashi, T., Shinohara, N., Wang, L., Matsuo, S., Shirase, M., and Takagi, T., "Solving a 676-bit Discrete Logarithm Problem in GF(3^{6n})," PKC2010, LNCS, 6056, Springer-Verlag, Berlin, pp. 351–367, 2010.

6 Mambo, M. and Okamoto, E., "Proxy cryptosystem: delegation of the power to decrypt ciphertexts," IEICE Trans. Fundamentals E80-A(1), pp. 54–63, 1997.

7 Blaze, M., Bleumer, G., and Strauss, M., "Divertible protocols and atomic proxy cryptography," Nyberg, K. (ed.), EUROCRYPT 1998, LNCS, Vol. 1403, pp. 127–144, Springer, Heidelberg, 1998.

8 Wang, L., Shao, J., Cao, Z., Mambo, M., and Yamamura, A., "A certificate-based proxy cryptosystem with revocable proxy decryption power," INDOCRYPT 2007, LNCS 4859, Springer-Verlag, Berlin, pp. 297–311, 2007.

9 Chu, C. and Tzeng, W., "Identity-based proxy re-encryption without random oracles," Garay, J.A., Lenstra, A.K., Mambo, M., Peralta, R. (eds.), ISC 2007, LNCS, Vol. 4779, pp. 189–202, Springer, Heidelberg, 2007.

10 Green, M. and Ateniese, G., "Identity-based proxy re-encryption," Katz, J., Yung, M. (eds.), ACNS 2007, LNCS, Vol. 4521, pp. 288–306, Springer, Heidelberg, 2007.

11 Matsuo, T., "Proxy re-encryption systems for identity-based encryption," Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.), Pairing 2007, LNCS, Vol. 4575, pp. 247–267, Springer, Heidelberg, 2007.

12 Tang, Q., Hartel, P.H., and Jonker, W., "Inter-domain identity-based proxy reencryption," Yung, M., Liu, P., Lin, D. (eds.) INSCRYPT 2008, LNCS, Vol. 5487, pp. 332–347, Springer, Heidelberg , 2008.

13 Ateniese, G., Fu, K., Green, M., and Hohenberger, S., "Improved proxy re-encryption schemes with applications to secure distributed storage," Internet Society (ISOC): NDSS 2005, pp. 29–43, 2005.

14 Wang, L., Wang, L., Mambo, M., and Okamoto, E., "New Identity-Based Proxy Re-Encryption Schemes to Prevent Collusion Attacks," Pairing 2010, Springer-Verlag, Berlin, LNCS 6487, pp. 327–346, 2010.

15 Paillier, P., "Public-key cryptosystems based on composite degree residuosity classes," Stern, J. (ed.), EUROCRYPT 1999, LNCS, Vol. 1592, pp. 223–238, Springer, Heidelberg, 1999.

16 ElGamal, T., "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory (TIT), 31(4), pp. 469–472, 1985.

17 Chevallier-Mames, B., Paillier, P., and Pointcheval, D., "Encoding-free elgamal encryption without random oracles," Yung, M., Dodis, Y., Kiayias, A., Malkin, T.G. (eds.), PKC 2006, LNCS, Vol. 3958, pp. 91–

104, Springer, Heidelberg, 2006.
18 Wang, L., Wang, L., Pan, Y., Zhang, Z., and Yang, Y., "Discrete-log-based additively homomorphic encryption and secure WSN data aggregation," ICICS 2009, Springer-Verlag, Berlin, LNCS 5927, pp. 493–502, 2009.
19 Wang, L., Wang, L., Pan, Y., Zhang, Z., and Yang, Y., "Discrete-log-based additively homomorphic encryption and secure WSN data aggregation," Information Science, to appear, 2011.
20 Wang, L., Tanaka, H., Ichikawa, R., Iwama, T., and Koyama, Y., "A study on position authentication using homomorphic encryption," SCIS2011, 1F1-2, 2011.
21 Japan Aerospace Exploration Agency, "Quasi-Zenith Satellite System User Interface Specifications," http://qzss.jaxa.jp/is-qzss/IS-QZSS_12Draft_J.pdf
22 Takashima, K., Ichikawa, R., Takahashi, F., Otsubo, T., Koyama, Y., Sekido, M., Takiguchi, H., and Hobiger, T., "Fundamental research about the space-time information certification using VLBI correlation technique," The 112th Meeting of the Geodetic Society of Japan, Nov. 4, 2009.
23 Wang, L., "An ID-based 2-functional proxy cryptosystem construction method," Patent application number: PCT/IB2009/006721.

(Accepted June 15, 2011)

WANG Lihua, *Ph.D.*
Expert Researcher, Security Fundamentals Laboratory, Network Security Research Institute
Cryptographic Theory, Information Security