2011 年度　財団法人交流協会フェローシップ事業 成果報告書

Certificateless Cryptosystems:

Theory and Practice

国立政治大学資訊科学系
左瑞麟
招聘期間（2011 年 7 月 3 日～8 月 1 日）

2012 年 3 月
財団法人　交流協会

Research Report of the 2011 Fellowship Invited Researcher Sponsored by the Interchange Association (Japan)

Invited Researcher: Raylin Tso (Assistant Professor)

Affiliation: Department of Computer Science,

National Chengchi University

Research Theme: Certificateless Cryptosystems:

Theory and Practice

Research Period: 2011 / 7 / 3 – 2011 / 8 / 1

Accepted Organization: Graduated School of Systems and

Information Engineering, Tsukuba University

Facilitator: Eiji Okamoto

(Full Professor of the Tsukuba University)

The topic of my research for the fellowship is "A research on certificateless cryptosystems and the applications".

Certificateless cryptosystems

In traditional public key cryptography (PKC), the authentication of a user's public key before using the key is necessary. It ensures that the public key has not been tampered with or replaced by a malicious third party. In serving this goal, the general approach is to use Public Key Infrastructure (PKI) in which a trusted authority, called Certification Authority (CA), issues certificates to bind users and their public keys. However, the certificate management in traditional PKI (e.g., certificate revocation, storage, distribution and verification) is generally considered to be costly to use and manage.

Identity-based (ID-based) cryptography, which was first introduced by Shamir [12] in 1984, is introduced to overcome the aforementioned problem. In an ID-based cryptosystem, users can use their unique identifiers (e.g., names or e-mail addresses) as their public keys. These public keys are publicly known and do not need certificates to ensure their authenticity. Thus, the problems associated with certificates can be eliminated. However, this kind of ID-PKC has an inherent key escrow issue, namely the Private Key Generator (PKG) (which generates private keys for users) has all users' private keys. This requires the full trust on the PKG.

Certificateless cryptography was proposed to solve the key escrow problem inherent in ID-based cryptography on one hand and eliminate the use of certificates in the conventional PKI on the other hand. It was first introduced by Al-Riyami and Paterson [1] in 2003. In a certificateless cryptosystem, the third party, which is called KGC, only generates partial private keys for users while users independently generate their own public/secret key pairs. Cryptographic operations in the system are performed successfully only when both the partial key and the secret key are known. This way, the KGC is unable to obtain secret keys of users and the key escrow problem can be overcome in certificateless public key cryptography.

During my stay in Japan, I first gave an invited talk on July 12 about my recent research. The invited talk is about the design of a privacy preserved two-party equality testing protocol. The detail of the invited talk is described below.

Privacy Preserved Two-party Equality Testing Protocol

It is commonly recognized that encryption secures our stored data but seems to make it inert. The encrypted data cannot be manipulated without first decrypting it.

Imagine two entities, say Alice and Bob, each one holds a secret value. If they want to know whether the secret values they hold are equal or not, how can they do it. It is easy and straightforward if privacy is not the main concern. In this case, they just reveal their secret value and then the comparison can be done very easily. However, sometimes we must take privacy protection into consideration.

A better solution is for Alice and Bob to jointly compute some function based on their secret input and without involving other entity. The two parties follow a protocol which specifies their actions in every step. This kind of protocols is usually referred to as secure multi-party computation [9].

Secure multi-party computation was firstly introduced by Yao [14] in 1982. It allows entities that hold different secret data to collaborate and analyze all their data together in such a way that no user learns anything about anyone else's secret data except for whatever is revealed by the output of the analysis.

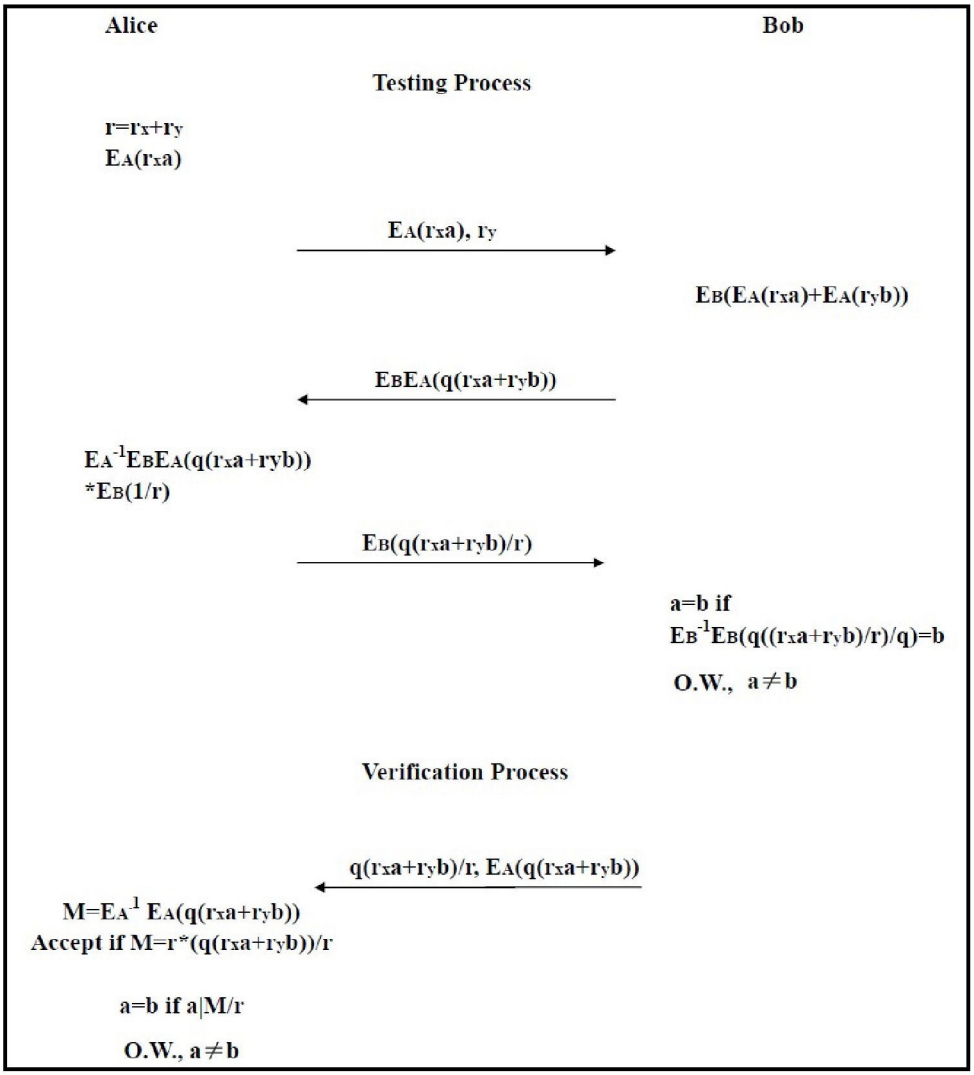
Additionally, two-party equality testing [10] is a special case of secure multiparty computation. It enables two entities to jointly compare the equality of their secret data without revealing the data to the other party. At the end of the testing computation, only the final result is revealed to both the entities. That is, the two entities will only know whether the secret data they holds are equal or not, without knowing the exact value of the other entity's secret data if the values are not equal.

Privacy preserved two-party equality testing is very useful in practical. For example, consider a database that stores encrypted transactions. Without decryption keys, it is typically impossible to issue general queries on that database. However, using two-party equality testing protocols, users will be able to launch very general searches with encrypted queries on that encrypted database.

On the other hand, how to design an efficient and secure two-party equality testing protocol is always a challenging task in the field of cryptography. Some of the existing protocols [5,6,13] need a trusted third party (TTP) to perform interactive operations with the two entities in order to assure that nobody will leak its secret information to the other party. This kind of schemes can be very efficient but the security sometimes relies on the honesty of the TTP. That is, the TTP must be semi-honest who will honestly perform his operation according to the protocol. In addition, users must trust the TTP and assume that the TTP will not collide with any other party. On the other hand, some of the existing protocols [4,5,14] do not need a trusted TTP so the operations of equality testing are performed in the absence of a TTP. However, in these schemes, sometimes, the testing result (i.e., equal or not about the two secret values) is known by only one entity (called informer). The other entity is informed about the testing result by the informer so she must fully trust the informer about the result she received. There is no mean to verify the correctness of

the notification from the informer.

In this talk, we introduce a new two-party equality testing protocol. In our protocol, although the final result is still informed by the informer, we allow the entity being informed to verify the correctness of the final result. In this way, the two entities can make sure whether the secret information they preserved are equivalent or not without revealing it. Our new protocol is described in the following figure.



In the above scheme, *a* is the secret information of Alice and *b* is the secrete information of Bob. In addition, $E_A(x)$ means that the message *x* is encrypted using the public key *A*. To use our new scheme for the comparison of the two secret values, the encryption algorithm must be both additive and multiplicative homomorphic. In addition, it must also be commutative. Homomorphic and commutative encryption is described below.

Homomorphism is a mapping from an algebra system to another similar algebra system (e.g. group, ring or the vector space). The corresponding operations in the

process maintain all the related structure For example, for two natural number *a* and *b*, if function *f(x)* satisfies *f(a+b)=f(a)+f(b)*, then function *f(x)* has homomorphism nature.

Homomorphic encryption can be done by the homomorphic operations between the encrypted ciphertexts. For example, assume two ciphertexts $c_1 = E(m_1)$ and $c_2 = E(m_2)$ where *E*() *is* encryption algorithms having homomorphism property. Do some operations like $c = c_1 \odot c_2$ can obtain $c = E(m)$ where *c* is the new ciphertext and *m is* the corresponding plaintext which is equal to $m_1 \oplus m_2$. Here $\oplus$ may be additive or multiplicative homomorphism.

Additive homomorphism

$c = E(m_1 \oplus m_2) = E(m_1 + m_2)$:

Example:$E(m_1) * E(m_2) = E(m_1 + m_2)$, if $E(m) = km$ or $E(m) = e^m$ for some k or e, we can get $E(m_1) * E(m_2) = E(m_1 + m_2)$.

We can see this method used in [2,8,11]

Multiplicative homomorphism

$c = E(m_1 \otimes m_2) = E(m_1 * m_2)$:

Example: assume e be a pairing operation, $C_1 = g^{m_1} m^{r_1}, C_2 = g^{m_2} m^{r_2}$. $C = e(C_1, C_2) h_1^r$ can is the ciphertext of m=$m_1 * m_2$ 。

Commutative Encryption

Our scheme also makes use of another type of encryption schemes named commutative encryption.

This can be stated as follows:

1. $E_1(E_2(m)) = E_2(E_1(m))$
2. Encryption key E_i and its corresponding decryption key D_i are computable in polynomial time;
3. E_i has the same value range.

Discussion after the talk

As described above, to use our scheme for privacy preserved comparison, we must adopt an encryption algorithm which is not only additive and multiplicative homomorphic but also commutative. There are only few encryption algorithms which satisfy the limitation. So we agree to consider a new scheme which needs only wild-used encryption algorithms such as RSA or ElGamal encryptions. In addition, we also agree to extend the idea into a certificateless setting. In this way, when E is an certificateless cryptosystem instead of a conventional PKI-based encryption algorithm, we can eliminate the use of certificates in the scheme. The work of our research on this topic is started after the discussion and is still undergoing. We have already

solved some critical problems and found out some idea for our construction.

Certificateless aggregate signature

In addition to the discussions on the research of two-party equality testing, we also have discussions on the research of extending an aggregate signature scheme into a certificateless setting. Our discussion is summarized as follows:

Ordered sequential aggregate signature scheme is a signature scheme in which each signer for a group signs an individual document, and guarantees both of the validity of the document and the signing order. Many ordered sequential aggregate signature schemes [3,7] are ID-based scheme and inherit an intrinsic insider problem, called key escrow problem, of the ID-based scheme. We try to propose an ordered sequential aggregate signature scheme with certificateless property which solves the key escrow problem and can be regarded as a hybrid scheme of PKI and ID-based scheme. To the best of our knowledge, certificateless ordered sequential aggregate signature scheme has never been proposed. Since certificateless cryptosystem has the advantages for both of PKI and ID-based scheme, we consider that constructing a certificateless ordered sequential aggregate signature scheme is a meaningful work.

During my stay in Japan, with many times of discussions, finally, the idea comes out. The idea is mainly contributed by Dr. Yanai, a Ph.D. candidate of Prof. Okamoto's team. Our proposed scheme is pairing-based scheme and has the fixed data size for the signature with respect to the number of signers. We also discuss the security of the proposed scheme in the random oracle model.

Conclusion

Sponsored by the Interchange Association (Japan), I had chance to be a fellowship invited researcher and to work with Prof. Okamoto's group in one month. During my staying in Japan, we had discussions about the certificatelss cryptosystems. We discussed on how to design a secure and efficient two-party equality testing protocol in the certificateless setting and also a certificateless aggregate signature scheme. The first one is still in construction. But, we have already solved some critical problem and we expect to have good result in the near future concerning to this part. About the second topic, we had come out a new idea on certificateless aggregate signature scheme. Our new scheme can be proved secure based on the CDH problem. In addition, it is efficient for the communication cost. Finally, I deeply appreciate the Interchange Association (Japan) for giving me this opportunity. The experience of this month will be constructive for my research and for my life.

References

[1]. S. S. Al-Riyami, and K. G. Paterson, "Certificateless public key cryptography", ASIACRYPT 2003, LNCS 2894, pp. 452-473, 2003.

[2]. D. Boneh, E. Goh, and K. Nissim, "Evaluating 2-dnf formulas on ciphertexts", Theory of Cryptography (TCC), pp. 325-341, 2005.

[3]. A. Boldyreva, C. Gentry, A. O'Neill, and D. H. Yum, "Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing", CCS 2007, ACM Press, pp.276-285, 2007.

[4]. A. Beimel, T. Malkin, S. Micali, "The all-or-nothing nature of two-party secure computation", CRYPTO 1999, pp. 80-97, 1999.

[5]. T. Chiang, W. Wang, J. Liau, and -S. Hsu, "Secrecy of two-party secure computation", Data and Applications Security 2005, LNCS 3654, pp. 114-123, 2005.

[6]. W.. Du and Z. Zhan, "A practical approach to solve secure multiparty computation problems", New Security Paradigms Workshop 2002, pp. 127- 135, 2002.

[7]. B. Dou, H. Zhang, C. Xu, and M. Han, "Identity-based sequential aggregate signature from RSA", CG 2009, ACM Press, pp.123-127, 2009.

[8]. T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms". CRYPTO 1985, pp. 10-18, 1985.

[9]. O. Goldreich, S. Micali and A. Wigderson, "How to play any mental game or a completeness theorem for protocols with honest majority", 19th Annual ACM Symposium on Theory of Computing (STOC), pp. 218-229, 1987.

[10]. R. Li and C. K.Wu, "Co-operative private equality test", International Journal of Network Security, vol.1, no. 3, pp. 149-153, 2005.

[11]. P. Paillier, "Public-key cryptosystem based on composite degree residuosity classes", Eurocrypt 1999, Springer-Verlag, pp. 223-238, 1999.

[12]. A. Shamir, "Identity-based cryptosystems and signature schemes", CRYPTO 1984, LNCS 196, pp.47-53, 1987.

[13]. J. Vaidya and C. Clifton, "Leveraging the "multi" in secure multi-party computation", the Workshop on Privacy in the Electronic Society, pp. 53-59, 2003.

[14]. C. Yao, "Protocols for secure computation", 23rd IEEE Symposium on Foundations of Computer Science (FOCS), pp. 160-164, 1982.