Approach to Materialize Digital Fingerprinting Scheme using Proxy Certificates

JaeGwi Choi* · Kouichi Sakurai** · JiHwan Park***

1. Introduction

Mobile communication has already been recognized to be an essential means for realizing the information society because of its capabilities of connecting 'anybody', 'anytime', 'anywhere'. The demand for mobile communication service is accelerating and mobile communication industries are growing rapidly all over the world. Moreover, they are expected to provide higher quality of multimedia services for users than today's systems. Thus copyright protection of multimedia contents being provided must be solved along with them.

Digital fingerprinting schemes are an important class of protection techniques of intellectual property. It enables a merchant to trace the buyer of an illegally distributed good by providing each buyer with a slightly different version.

1.1 Motivation

In general, the fingerprinted contents can be made in on-line, because every sold copy is slightly different from the original contents and unique to its buyer. Thus fingerprinting schemes with high complexity are not suited to the real application and, what is more, cannot be implemented in mobile communication. But most of known fingerprinting schemes are based on computationally unspecified black boxes without presenting explicit protocols such as secure multiparty computation or general zero-knowledge proof[1]. These protocols are embodied by difficult problems with much computation such as discrete logarithm problem or graph isomorphic problem. Their complexity is much too high to be materialized even in wire communication. Still less, buyer's memory and computation power is very small in mobile communication. There is an efficient method[2,3] without secure two party computations. But this

* Department of Information Security, Pykyong National Univ. Busan, Korea.
** Faculty of Information Science and Electrical Engineering, Kyushu Univ. Fukuoka, Japan.
*** Division of Electronic and Telecom. Engineering, Pukyung National University
※ The preliminary version was presented in 37th IEEE International Conference on Security Technology and was done while the frist author visited in Kyushu Univ, from Oct.2002 to Aug.2003. The first and third authors were partly supported by grant No.01-2002-000-00589-0 from the Basic Research Program of the Korea Science & Engineering Foundation.
※ 삼가 이 논문을 故 박지환 교수님 영전에 올립니다.

method is also impractical because it uses[4] scheme as a building block for collusion resistance. In [4], their code needed for embedding is so long that the overall system cannot be practical.

To address this problem, we propose a digital fingerprinting scheme for mobile communication using mobile agent who has more computational power than buyer. In our proposal, the mobile agent executes buyer's computations instead of the buyer.

1.2 Our Contribution

Utilization of mobile agents to facilitate electronic commerce operations is an appealing concept, especially when those operations are tedious or very difficult to perform by human users. But, in distributed environment, it is very difficult to assume the trust of mobile agent and the delegation key issuing protocol. The delegation to others can be risky because this means have to carry the buyer's private information to the mobile agent. This exposes the information to attacks because it is copied outside a protected environment. To address this problem, we use proxy certificates, which avoid the need for the mobile agent to have access to the buyer's private information, but still bind the owner to the contents of an order sheet.

The basic primitives of our proposal are homomorphic encryption scheme and proxy certificates. We use homomorphic encryption scheme to remove interactive between a mobile agent and the merchant in a digital fingerprints embedding step and proxy certificates to remove risk about exposure of the buyer's private information.

Our proposal satisfies all properties of anonymous fingerprinting scheme; (1) only the buyer can know the fingerprinted copy, however the buyer delegated his/her power to the mobile agent, and (2) the buyer can perform fingerprinting protocol in safety. In other words, the honest buyer cannot be identified as a traitor even if the mobile agent does dishonest things such as collusion with the merchant, and (3) it is practical and efficient because it reduces amount of the buyer's computations to the minimum.

1.3 Organization

The paper is organized as follows. Section 2, where our methodology, proxy certificates is shown. Then, the proposed proxy certificates-based fingerprinting scheme is described in Section 3. Security and efficiency of the proposed scheme are discussed in Section 4. Finally, we conclude in Section 5.

2. Our Methodology

Security issues related to the usage of mobile agents in performing operations to which their owners have to be bound, such as payments, are of utmost importance if these kinds of agents are to be used in electronic commerce. If this binding is achieved by means of digital signature techniques, this means agents have to

carry the owner's private key to the host where they sign documents. This exposes the key to attacks because it is copied outside protected environments. In our scheme, we used a mechanism, called proxy certificates, that avoids the need for the agent to have access to the user's private key for digitally signing documents, but still binds the owner to the contents of those documents. We briefly review the construction proposed in[5].

[Notation]

- CA: The identity of a certification authority
- $A(X)$: The identity of a mobile agent belonging to X
- PK_X: The public key of X
- SK_X: The private key of X
- $\{M\}$: A message with contents M
- $\{M\}_{SK_X}$: A message with contents M signed by X
- $Cert\{X, PK_X\}_{SK_Y}$: The digital certificates of X issued by Y
- $Cert\{X, PK_{A(X)}, [D]\}_{SK_X}$: The proxy certificates of a mobile agent belonging to X, with additional data D
- Signature verification of $\{M\}_{SK_X}$: Verification is successful iff M equals M_1, $sig\_ver(M, X) = M_1$
- Verification of $Cert\_ver(X, Y) = Z, PK_Z$: Verification is successful iff $sig\_ver(Cert\{X, PK_X\}_{SK_Y}, Y)$ is successful, in which case it has $Z = X$ and $PK_Z = PK_X$

[Issuing Proxy Certificates]

A proxy certificates is issued and signed by the owner of an agent. Obviously, there is an associated key pair that is also generated by the agent's owner.

The certificates contains a validity period, the identity of the agent's owner, and a set of constraints indicating the valid operations that the agent is allowed to perform while using that certificates.

The buyer is bound to the actions performed (i.e., documents signed) by the agent through the owner's identity and signature in the proxy certificates. For this purpose, the identity in the proxy certificates must be the same as the identity in the buyer's signature certificates. Thus a proxy certificates for an agent belonging to buyer B is denoted as $Cert\{B, PK_{A(B)}, [constraints]\}_{SK_B}$.

[Using Proxy Certificates]

When migrating to an external server the agent will carry is proxy certificates, which can be part of the data that composes the agent's specific code. The agent will also carry the buyer's signature certificates, as before. The secret data includes the agent's private signature key, along with the usual secret data, but now excluding the buyer's signature key. i.e., the agent carries, among other elements:

$$\{Cert\{B, PK_B\}_{SK_{CA}}, Cert\{B, PK_{A(B)}, [constrints]\}_{SK_B}, SK_{A(B)}\}$$

When the agent decides to purchase some good of service, it must check the details of the

purchase against the constraints in its proxy certificates, and only proceeds if all of the constraints are satisfied. In order to make a payment and purchase, the agent sends its proxy certificates and the buyer's certificates to the merchant: $\{Cert\{B, PK_B\}_{SK_{CA}}, Cert\{B, PK_{A(B)}, [constrints]\}_{SK_B}\}$. Besides the verification of signatures, discussed below, the merchant should check the constraints in the certificates in order to ensure that the agent is allowed to make the purchase. Even though the agent has already performed this check, the merchant should do it again to prevent possible malfunctions on the agent's behaviors.

[Signature Verification]

The act of verifying a signature made by the agent on some message M represents more than simply binding the agent to the signed data. The buyer has to be bound to the data, as well. Therefore, when verifying a signature, the merchant will first validate the buyer's signature certificates, i.e., performs $Cert\_ver(Cert\{B, PK_B\}_{SK_{CA}}, CA)$ and obtains B and PK_B.

Next, the merchant validates the proxy certificates which $Cert\_ver\{Cert\{B, PK_{A(B)}, [constraints]\}_{SK_B}, B)$ and obtains $A(B)$ and $PK_{A(B)}$. This ensures that the buyer has delegated powers to the agent. Finally, the signature on the data is verified by doing $sig\_ver(M, A(B))$.

3. Our Protocol

3.1 Preliminaries

[Assumptions]

For ease of exposition, we assume that the content being sold is a still image, though in general the protocol is also applicable to audio and video data. We also assume that all of the underlying primitives are secure.

[System Set Up]

Let $p(\leq n bits)$ be a large prime such that $q=(p-1)/2$ is also prime. Let G be a group of order $p-1$ and let g be a generator of G such that computing discrete logarithms to the base g is difficult. That all participants have a pair of a private key and a public key (sk, pk) such that $pk=g^{sk} \pmod p$, all of which have been registered with appropriate certificates authority.

[Notations]

The fingerprinting insertion step can be represented as $Image' = Image \oplus F$, where

- $Image$: Original image to be a vector of "features", $Image=\{ima_1, \cdots, ima_m\}$
- F: Fingerprints as a vector of "fingerprint elements", $F=f_1, \cdots, f_n$ with $m \geq n$
- $Image'$: Fingerprinted image
- $\oplus$: Insertion operation
- $Image \oplus F=\{ima_1 \oplus f_1, \cdots, ima_n \oplus f_n, ima_m\}$
- E/D: Encryption/Decryption scheme with homomorphic property
- $Sign_{sk_X}(M)$: Signature of X on the message M
- $Cert\{pk_X\}_{sk_Y}$: The digital certificates of X issued by Y
- $Cert\{pk_{MA}, [D]\}_{sk_X}$: The proxy certificates of a mobile agent, with additional data D

[Roles of each entity]

The entities of our scheme consist of the fingerprint certificates center (*FC*), a mobile agent, a buyer, and a merchant. The role of each entity is as follows:

Fingerprint Certificates Center (FC)

- He generates random fingerprints in the required manner and issues them to any user (mobile agent) upon request.
- He is in charge of the registration process and has secret database to keep secret user information.
- He has to take part in identification protocol in order to reveal the user's real identity who distributed digital contents illegally when a merchant request.
- He has private sk_{FC} and public key $pk_{FC} = g^{sk_{FC}} \pmod{p}$.
- He is the trusted third party.

Mobile agent

- He carries out fingerprints generation protocol and fingerprints insertion protocol instead of buyers.
- He is able to sign messages about purchasing on behalf of the buyer after execution delegation protocol.
- He has private sk_{MA} and public key $pk_{MA} = g^{sk_{MA}} \pmod{p}$.

Buyer

- She has to register to FC to obtain her own anonymous public key.
- She delegates the power of signing and protocol execution to a mobile agent who will execute protocols instead of herself.
- She issues the proxy certificates to mobile agent.
- She has private key sk_B and public key $pk_B = g^{sk_B} \pmod{p}$.

Merchant

- He is an agent selling digital contents.
- He has database to record anonymous buyers and their information.
- He has to embed the anonymous buyer's information into digital contents without revealing it (decrypting it).

3.2 The Proposed Scheme

The proposed anonymous fingerprinting scheme consists of the following 5 steps.

Step 1. Registration:

A buyer registers to FC as follows:

(1) A buyer chooses secret random sk_{B1} and sk_{B2} in Z_p such as Eq. (1).

$$sk_{B1} \cdot sk_{B2} = sk_B \in Z_p \quad (1)$$

(2) She sends $pk_B^* = g^{sk_B} \pmod{p}$ and encrypting sk_{B2} using *FC*'s public key pk_{FC} such as $E_{pk_{FC}}(sk_{B2})$ to *FC*. pk_B^* is anonymous public key of the buyer. The buyer convinces the *FC* of zero-knowledge of possession of sk_{B1}. The proof given in [6] for showing possession of discrete logarithms may be used here.

(3) The *FC* first decrypts $E_{pk_{FC}}(sk_{B2})$ using his private key sk_{FC} and checks that

$(pk_B^*)^{sk_B} = pk_B \pmod{p}$. If it is verified, FC returns to the buyer certificates $Cert\{pk_B^*\}_{sk_{FC}}$ that states the correctness of pk_B^*.

(4) FC keeps them $(pk_B, Cert\{pk_B^*\}_{sk_{FC}}, pk_B^*)$ secretly in his secure user information DataBase FC_DB.

Step 2. Delegation:

Now, an anonymous buyer and a mobile agent execute delegation step. Here, an anonymous buyer delegates the power of signing (purchase contents) to the mobile agent. After this step, the mobile agent is able to perform the rest of fingerprinting protocol on behalf of the buyer.

We use proxy certificates for secure delegation.

(1) The (anonymous) buyer issues the proxy certificates, $Cert\{pk_{MA}, [text]\}_{sk_B}$ to the agent. The certificates contains her own identity (anonymous identity) and a set of text indicating the valid operations that the agent is allowed to perform while using that certificates and contents to will be purchased.

(2) The buyer sends $Cert\{pk_B^*\}_{sk_{FC}}$ and $Cert\{pk_{MA}, [text]\}_{sk_B}$ to agent.

Step 3. Fingerprints Generation:

This protocol is performed between FC and the mobile agent.

(1) The mobile agent sends the buyer's certificates and proxy certificates to the FC.

(2) FC first verifies the buyer's certificates using his own private key sk_{FC} and then, confirms whether pk_B^* exists in his own DataBase FC_DB or not.

(3) If it exists, FC checks validity of a proxy certificates using the buyer's anonymous public key.

(4) If it holds, FC generates fingerprints F randomly. Note that $F=\{f_1, f_2, \cdots, f_n\}$. Here, we use a specific construction which introduced a spread-spectrum watermarking techniques proposed by Cox et al. [7]. Cox et al. embed a set of independent real numbers $F=\{f_1, f_2, \cdots, f_n\}$ drawn from a zero mean, variance 1, Gaussian distribution into the m largest DCT AC coefficients of an image. Results reported using the largest 1000 AC coefficients show the technique to be remarkably robust against various image processing operations, and after printing and rescanning and multiple-document (collusion) attack. It is pointed out to be highly resistant at collusion attacks[8].

(5) FC encrypts fingerprints F with the buyer's anonymous public key pk_B^* such as Eq. (2). Then, he computes signature $Sing_{sk_{FC}}(Enc\_F \| pk_B^*)$, which certifies the validity of the fingerprint and also ensures that pk_B^* was used to encrypt F as a public key. The FC stores

$F, Enc\_F, Sign\_F, Cert\{pk_{MA}, [text]\}_{sk_m}$ secretly in the buyer's fields of his DataBase FC_DB.

$(pk_B, Cert\{pk_B^*\}_{sk_{FC}}, pk_B^*)$ have already stored in the buyer's fields of FC_DB. Here $\|$ denotes a concatenation and the encryption algorithm is homomorphic.

$$\begin{aligned} Enc\_F &= E_{pk_B^*}(F) \\ Sign\_F &= Sign_{sk_{FC}}(Enc\_F \| pk_B^*) \end{aligned} \quad (2)$$

(6) FC sends $Enc\_F, Sign\_F$ to the mobile agent.

(7) The mobile agent verifies $Sign\_F$ using the FC's public key. If it holds, he obtains the valid fingerprints that encrypted with the buyer's anonymous public key.

Step 4. Fingerprints Insertion:

This is an interactive protocol between a merchant and the mobile agent who must buy digital image instead of the buyer who wants to purchase fingerprinted image.

(1) A mobile agent sends $Cert\{pk_B^*\}_{sk_{FC}}$, $Cert\{pk_{MA}, [text]\}_{sk_m}$, Enc_F, $Sign\_F$ and pk_B^*, pk_{MA}, $Sign\_MA$ such as Eq. (3) to the merchant.

$$Sign\_MA = Sign_{sk_{MA}}(text) \quad (3)$$

(2) A merchant verifies two certificates and $Sign\_MA$. If the verification holds, the next step proceeds.

(3) Let $Image$ denote the original image which the buyer (the mobile agent) wants to purchase. The merchant generates unique W randomly and embeds a unique fingerprint into content $Image$. Let $Image'$ be the fingerprinted image with W. When an unauthorized copy $Image'$ generated from, this unique fingerprint W is used for identifying the original buyer of $Image'$. To embed the second fingerprint F generated by the FC into $Image'$ without decrypting $E_{pk_B^*}(F)$, the merchant encrypts the watermarked content $Image'$ with pk_B^* and finds the permutation σ satisfying $\sigma(E_{pk_B^*}(F)) = E_{pk_B^*}(\sigma(F))$. Because of the homomorphic property of the encryption algorithm E used by the FC, the merchant can compute fingerprinted content $E_{pk_B^*}(Image'')$ by the following process.

$$\begin{aligned} & E_{pk_B^*}(Image'') \\ &= E_{pk_B^*}(Image') \oplus \sigma(E_{pk_B^*}(F)) \\ &= E_{pk_B^*}(Image') \oplus (E_{pk_B^*}(\sigma(F)) \\ &= \{E_{pk_B^*}(ima'_1), \cdots, E_{pk_B^*}(ima'_m)\} \\ &\quad \oplus \{E_{pk_B^*}(f_{\sigma(1)}), \cdots, E_{pk_B^*}(f_{\sigma(n)})\} \\ &= \{E_{pk_B^*}(ima'_1 \oplus f_{\sigma(1)}), \cdots, \\ &\quad E_{pk_B^*}(ima'_n \oplus f_{\sigma(n)}), \cdots, E_{pk_B^*}(ima_m^*)\} \\ &= E_{pk_B^*}(Image \oplus W \oplus \sigma(F)), m \geq n \end{aligned} \quad (4)$$

(4) The merchant transmits $E_{pk_B^*}(Image'')$ to the mobile agent and stores $pk_{MA}, pk_B^*, W, \sigma, Enc\_F, Sign\_F, Sign\_MA$ and two certificates $Cert\{pk_B^*\}_{sk_{FC}}$, $Cert\{pk_{MA}, [text]\}_{sk_m}$ in his DataBase $Merchant\_DB$. $Merchant\_DB$ is a table of records maintained by merchant for

image *Image* containing one entry for each copy of *Image* that he sells.

(5) The mobile agent sends $E_{pk'_B}(Image'')$ to the buyer. The buyer decrypts the encrypted image $E_{pk'_B}(Image'')$ and obtains the fingerprinted image $Image''$.

Note that, the buyer can decrypt the fingerprinted image encrypted with her owns private key sk_{B1}.

In our protocol, the buyer does not know σ, she cannot remove $\sigma(F)$ from $Image''$.

Step 5. Traitor Identification:

When an illegal copy Y of an original image *Image* is discovered,

(1) The merchant extracts the unique watermark U in Y using detection algorithm, and finds W with the highest correlation and obtains the transaction information involving W from the table by computing correlations of extracted watermark W and every watermark stored in *Merchant_DB*. The information consists of $pk_{MA}, pk^*_B, \sigma, Enc\_F, Sign\_F$ $Sign\_MA$ and W. And the merchant sends them with *Image*, Y to an arbiter.

(2) The arbiter verifies $Sign\_F$ with the FC's public key pk_{FC}. If the verification holds, the arbiter performs the next step.

(3) The arbiter sends $pk^*_B, Cert\{pk^*_B\}_{sk_{FC}}$, $Cert\{pk_{MA}, [text]\}_{sk_{B1}}$ to FC. Then the FC sends F back to the arbiter.

(4) The arbiter computes $\sigma(F)$ and checks the existence of $\sigma(F)$ in Y by extracting the fingerprint from Y and estimating its correlations with $\sigma(F)$. If there exists $\sigma(F)$, the buyer is guilty and the buyer's ID is revealed to the merchant.

4. Security and Efficiency

4.1 Security Analysis

We discuss various features of the proposed scheme.

- **Anonymity**: We assume that the Fingerprint Certificates Center does not reveal the buyer's real identity if she is honest. Even if the merchant and the mobile agent know a pseudonym pk^*_B, which is related to pk_B, it is unknown to the merchant and the mobile agent because sk_{B2} is encrypted with FC's public key. Thus buyer's anonymity is provided if the merchant and the mobile agent cannot compute discrete logarithms. Therefore buyers should be able to purchase digital image anonymously in our scheme.
- **Unlinkability**: In our protocol, fingerprinted images sold to a buyer must be encrypted with each different key for unlinkability of digital contents. Also these different keys are transmitted to the merchant. Thus given two digital contents, nobody can decide whether these two images (contents) were purchased by the same buyer or not.
- **Traceability**: Due to the properties of the underlying encryption and digital signature

techniques, we can assume that a malicious buyer cannot change or substitute a fingerprint generated by the fingerprints certificates center. Merchants should insert a fingerprint W and $\sigma(F)$ in the right manner for his own interest. If he does not correctly insert Wor $\sigma(F)$, he would not be able to identify the original buyer of an illegal copy. Further a detecting function in the fingerprint detection must guarantees that the merchant can extract the unique watermark (fingerprint) W that belongs to a traitor. Thus the buyer who has distributed digital contents illegally (traitor) can be traced in our scheme.

- **No Framing**: Since, to forge Y with the special watermark F, the merchant must know either the buyer's private key sk_{BI} or the buyer's unique watermark F. In our proposal, only the buyer knows his private key sk_{BI} and his unique watermark if computing discrete logarithm is hard and used encryption algorithm (underlying primitives) is secure. Because the merchant cannot recreate the buyer's copy with specific watermark, an honest buyer should not be wrongly identified as a traitor in our protocol.
- **No Repudiation**: Since only the buyer can decrypt encrypted fingerprinted contents (Only the buyer knows his own secret key sk_{BI}), the others cannot recreate the buyer's copy. Thus the buyer accused of reselling an unauthorized copy should not be able to claim that the copy was created by the merchant or a security breach of the merchant's system.
- **Collusion Tolerance**: Our scheme has used[7] as a building block. The protocol is secure only as much as the underlying watermarking techniques are secure and robust. We assumed that the underlying watermarking algorithm is secure and this algorithm is pointed out to be highly resistant at collusion attacks[8].

4.2 Efficiency Analysis

In our scheme, the buyer has to execute the registration step and delegation step, and the mobile agent does buyer's computation instead of her.

In previous schemes[2,3,9,10], the buyer has to carry out the registration step, fingerprints generation step, and fingerprints insertion step. There is no comparison between computational cost of fingerprinting step with very high complexity (based on secure multi-party protocols) and that of delegation step. Thus, it is enough to prove that our protocol is more efficient than the other previous schemes from the view of buyers. Our scheme is practicable and efficient scheme from the view of buyers, because it reduces amounts of buyers' computations and memory to minimum.

5. Concluding Remarks

In this paper, we propose proxy certificates-based digital fingerprinting protocol. The complexity of most of known algorithms for anonymous fingerprinting deters their practical implementation, since they rely either on secure multiparty computation or on general zero-

knowledge proofs. In order to address this problem, we introduced concept of mobile agents with proxy certificates, which remove risk about exposure of the buyer's private information and reduce amount of the buyer's computations to the minimum. Thus our approach is suited to the customer-centered commercial transaction and mobile communication that the client (buyer's devices) has a small memory and computation power.

But, our scheme has the drawback that it is insecure if the fingerprint certificates center colludes with the others. A further direction of this study will be to consider the dishonesty of the fingerprint certificates center (TTP).

References

[1] D.Chaum, I.B. Damgard and J.van de Graaf, "Multiparty Computation Ensuring Privacy of Each Party's Input and Correctness of the Result", Crypt'87, LNCS 293, Springer-Verlag, pp.86-119, 1987.

[2] B.Pfitzman and Ahmad-Reza Sadeghi, "Coin-Based Anonymous Fingerprinting", Eurocrypt'99, LNCS 1592, Springer-Verlag, pp. 150-164, 2000.

[3] J.Domingo-Ferrer, "Anonymous Fingerprinting Based on Committed Oblivious Transfer", PKC'99, LNCS 1560, Springer-Verlag, pp43-52, 1999.

[4] D.Boneh and J.Shaw, "Collusion-secure Fingerprinting for Digital Data", Crypt'95, LNCS 963, Springer-Verlag, pp.452-465, 1995.

[5] Artur Romao and Miguel Mira da Silva, "Secure Mobile Agent Digital Signatures with Proxy Certificates", E-Commerce Agents, LNAI 2033, Springer-Verlag, pp.206-220, 2001.

[6] D.Chaum, Evertse, J-H., and Van de Graaf, J., "An Improved Protocol for Demonstrating Possession of Discrete Logarithms and Some Generalizations", Eurocrypt'87, LNCS 304, Springer-Verlag, pp.87-119, 1987.

[7] I.J. Cox, J.Kilian, T.Leighton, and T.Shamnon, "Secure Spread Spectrum Watermarking for Image, Audio and Video", IEEE Transactions on Image Processing, vol.6, no 12, pp.1673-1678, 1997.

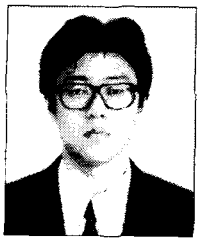
[8] J.Killian, F. Thomson Leighton, Lasely R. Matheson, Talal G. Shannon, Robert E. Tarjan, and Francis Zane, "Resistance of Digital Watermarks to Collusive attacks", Technical Report TR-585-98, Princeton University, Computer Science Department, July. 1998.

[9] B. Pfitzmann and M. Waidner, "Anonymous Fingerprinting", Eurocrypt'97, LNCS. 1233, Springer-Verlag, pp.88-102, 1997.

[10] H.S.Ju. H.J.Kim, D.H.Lee and J.I.Lim, "An Anonymous Buyer-Seller Watermarking Protocol with Anonymity Control", ICISC2002, LNCS 2587, Springer-Verlag, pp.421-432, 2003.

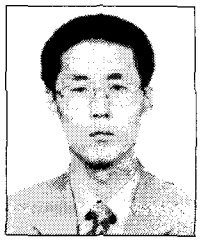
JaeGwi Choi

- She received the B.S. degree in computer science from Pukyong National University and the M.E. degree in computer science education from Pukyong National University in 1998 and 2001, respectively. She was an exchange student in Kyushu University, Japan in 2002~2003. She is currently working toward her Ph.D. degree in information security at Pukyong National University, and studying at the institute of industry science of Tokyo University, Japan as a visiting researcher with the support of KOSEF. Her current research interests are in copyright protection technology and cryptography.



Kouichi Sakurai

• He received the B.S. degree in mathematics from Faculty of Science, Kyushu University and the M.S. degree in applied science from Faculty of Engineering, Kyushu University in 1986 and 1988, respectively. He had been engaged in the research and development on cryptography and information security at Computer & Information Systems Laboratory at Mitsubishi Electric Corporation from 1988 to 1994. He received the Dr. degree in engineering from Faculty of Engineering, Kyushu University in 1993. Since 1994 he has been working for Department of Computer Science of Kyushu University as an associate professor, and now he is a full professor. His current research interests are in cryptography and information security. Dr. Sakurai is a member of the Information Processing Society of Japan, the Mathematical Society of Japan, ACM and the International Association for Cryptologic Research.



JiHwan Park

• He received the B.S degree in electronic engineering from Kyunghee University, Seoul, Korea in 1984 and the M. E. degree and D. E degree from the University of Electro-Communications and Yokoha ma National University, Tokyo and Yokohama, Japan in 1987 and 1990, respectively. He is currently a full professor of the Division of Electronic Computer and Telecom. Eng. PuKyong National University, Busan, Korea. From 1990 to 1996 he was an assistant professor of the department of computer science, National Fisheries University of Pusan, Korea. He was a guest researcher at the institute of industry science, university of Tokyo in 1994~1995. His primary research interests include information theory and its applications, cryptography and its applications, image processing. He is a member of IEEE, Society of Information Theory and its Applications, Korean Institute of Communication Sciences, Korean Institute of Information Security and Cryptology, Korea Information Processing Society and Korean Multimedia Society.