Interval Two-dimensional Hash Chains and Application to a DRM system

Chae Duk Jung[†], Weon Shin[††], Young-Jin Hong[†††], and Kyung-Hyune Rhee[††††]

ABSTRACT

One-way hash chains are important cryptographic primitives and have been used as building blocks of various cryptographic applications. Advantages of one-way hash chains are their simplicity and efficiency for generation based on low-powered processors with short time. However, a drawback of one-way hash chains is their difficulty of control to compute interval values of one-way hash chains. That is, when hash values in one-way hash chain are used as encryption keys, if one hash value is compromised, then the attacker can compute other encryption keys from the compromised hash value. Therefore, direct use of one-way hash chains as encryption keys is limited to many cryptographic applications, such as pay per view system and DRM system. In this paper, we propose a new concept which is called interval hash chain using a hash function. In particular, proposed hash chains are made for only computing interval hash values by using two different one-way hash chains. The proposed scheme can be applied to contents encryption scheme for grading and partially usable contents in DRM system.

Keywords: DRM system, Hash Chains, Multi-Dimensional Hash Chains, Interval Hash Chains

1. INTRODUCTION

One-way hash chains are important cryptographic primitives and have been used as building blocks of various cryptographic applications, for example, extending the lifetime of digital certificates [1], constructing one-time signatures [2,3], electronic payment [4], etc.

One-way hash chains can be generated by low-powered processors within milliseconds using one-way function. In addition, processors can compute a sequence according to starting value. Despite of the computational efficiency of one-way hash chain, it is still challenging to use for encryption algorithm, such as pay per view system and DRM system, since it cannot control to compute interval values of the hash chain.

Digital Rights Management (DRM) is a technology for protecting the copyrights of content providers and enabling only designated user to access contents. In the past years there has been an increasing interest in developing DRM system [5-8]. However, previous DRM systems only consider the rights of copyright holders but ignore the convenience of users.

To satisfy both users and service providers, in terms of the use of content, many DRM systems support the use-count system that counts the number of content use. In [9], the DRM system supports a use-count model which restricts the

※ Corresponding Author : Kyung-Hyune Rhee, Address : (608-737) Daeyeon 3-dong, Nam-gu, Busan, Korea, TEL : +82-51-626-4887, FAX : +82-51-626-4887, E-mail : khrhee@pknu.ac.kr

Receipt date : Oct. 16, 2007, Approval date : Dec. 12, 2007

[†] Department of Information Security, Pukyong National University
(E-mail : jcd0205@pknu.ac.kr)

[††] Department of Information Security, Tongmyong University
(E-mail : shinweon@tu.ac.kr)

[†††] Department of Electrical & Electronic Engineering, Tongmyong University
(E-mail : gryjhong@tu.ac.kr)

[††††] Division of Electronic, Computer and Telecommunications Engineering, Pukyong National University

※ This work was supported by the SKTU Institute of Next Generation Wireless Communications funded by SK telecom (SKTU-07-002)

number of content use. Thus, it cannot support *partial use* such like ten minutes playing among total of two hours length movie. One of the solutions is the accumulated time system [9]. However, it is more difficult to be implemented than the simple use-count one because of the difficulty for time measurement. Furthermore, there are only a few researches on this fields at present.

Our Contribution. In this paper, we present new one-way hash chains, by called the interval hash chains that control for computing the interval values in the hash chain. That is, the system master can control for a user to compute hash values of specific interval in one-way hash chains. In addition, we propose interval two-dimensional hash chains using Multi-Dimensional Hash Chain (MDHC) [4] for grading contents in DRM system. Finally, we propose a new DRM system which achieve the following two goals: 1) partial use of contents and 2) grading contents.

The rest of this paper is organized as follows. The next section describes preliminaries to induce the motivation of the paper. In Section 3, we introduce the notion of interval hash chains and interval two-dimensional hash chains. We apply our hash chains to DRM system in Section 4. Finally, we conclude the paper in Section 5.

2. PRELIMINARIES

2.1 One-way Hash Chain

A one-way hash chain is a sequence of values $(x_n, \cdots, x_0)$ which is generated by applying a hash function multiple times. The value x_n is chosen at random and is called a starting node. All other values are derived from it as follows : $x_i = h(x_{i+1})$, $(0 \leq i \leq n-1)$, where $h: \{0,1\}^* \rightarrow \{0,1\}^l$ is a cryptographic hash function such as SHA-1. The value $x_0 = h^n(x_n)$ is called the root of the one-way hash chain. The Fig. 1 depicts a one-way hash chain of size n:

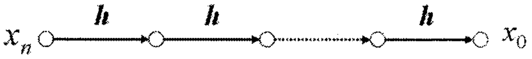

Fig. 1. One-way hash chain.

The chain is generated from x_n to x_0, and exposed from x_0 to x_n.

2.2 Multi-Dimensional Hash Chain [4]

We begin with necessary definitions.

- **Definition 1.** *Two functions* $h_1, h_2: X \rightarrow Y$ *are called commutative* *if* $h_1(h_2(x)) = h_2(h_1(x))$ *for any* $x \in X$.
- **Definition 2.** *A one-way function* $h: X \rightarrow Y$ *is called one-way independent of one-way functions* $h_1, h_2, ..., h_m$ *of the same domain if for any* $x \in X$, *computing* $h^{-1}(x)$ *is intractable even if values* $h_1^{-1}(x), h_2^{-1}(x), ..., h_m^{-1}(x)$ *are known.*

We now introduce Multi-Dimensional Hash Chain (MDHC) in [4] as follow.

- **Definition 3.** *Multi-Dimensional Hash Chain (MDHC). Let* $h_1, h_2, ..., h_m$ *be* m *one-way hash functions that are in pairs commutative and every of them is one-way independent from all others. An* m*-dimensional hash chain of size* $(n_1, n_2, ..., n_m)$ *consists of values* $x_{k_1,k_2,...,k_m}$ *where:*

$$x_{k_1,k_2,...,k_i,...,k_m} = h_i(x_{k_1,k_2,...,k_i+1,...,k_m})$$

for $i = 1, 2, ..., m$ *and* $k_i = 0, 1, ..., n_i$.
The value $X_N = x_{n_1,n_2,...,n_m}$ *is called the starting node, and the value* $X_0 = x_{0,0,...,0}$ *is called the root of the MDHC, which is uniquely determined from* X_N *due to commutativity of the hash functions:*

$$X_0 = h_1^{n_1}(h_2^{n_2}(...(h_m^{n_m}(X_N))...)).$$

As an example, the Fig. 2 shows a two-dimensional hash chain of size (4,2).

MDHC differs from other generalizations of normal hash chain such as hash tree. In particular

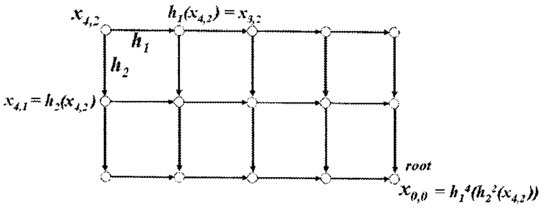

Fig. 2. A two-dimensional hash chain.

such trees are generated from multiple leaf nodes, while a MDHC is generated from a single starting value. However, the main limitation of this construction is the fact that hash functions have to meet the conditions described in the definition of MDHC. The RSA modular exponentiation is known to meet these conditions, but it is not as fast as the traditional hash functions, e.g. SHA-1.

The RSA modular exponentiation functions with appropriately selected exponents could meet MDHC requirements as follow:

- Obviously, these functions are in pairs commutative: $h_i(h_j(x)) = x^{c_i c_j} \bmod M = h_j(h_i(x))$.
- One-wayness of these functions is derived from the RSA assumption [10], which states that the problem of finding the modular root $x = y^{1/c} \bmod M$ in intractable.
- Regarding one-way independence of functions, Shamir [11] showed that if c is not divisor of the product $c_1 c_2 \ldots c_m$ then the modular roots $y^{1/c_1} \bmod M$, $y^{1/c_2} \bmod M$, $\cdots$, $y^{1/c_m} \bmod M$ are insufficient to compute the value of $y^{1/c} \bmod M$.

Therefore, the functions of RSA modular exponentiation can be used to construct multi-dimensional hash chains as one-way hash functions. Note that, for this reason, we use also the functions of RSA modular exponentiation to construct the proposed hash chain.

3. INTERVAL TWO-DIMENSIONAL HASH CHAINS

In this section, first we propose interval hash chains for only computing interval hash values by using two different one-way hash chains. After that, we introduce interval two-dimensional hash chains by combining proposed interval hash chains with two-dimensional hash chains in [4].

3.1 Interval Hash Chains

We now introduce Interval Hash Chains (IHC) as shown in Fig. 3.

Let h be a hash function and x', y_n are random values. A one-way hash chain $(y_n, \ldots, y_0)$ is a collection of values such that each value y_i is a result of a hash function by taking input as the previous value y_{i+1}. A IHC $(x_n, x_{n-1}, \ldots, x_0)$ is generated by the hash chain $(y_n, \ldots, y_0)$ and x' as follow:

$$\begin{aligned} & x_n = h(x' \| h^n(y_n)) = h(x' \| y_0), \\ & x_{n-1} = h(x_n \| h^{n-1}(y_n)) = h(x_n \| y_1), \\ & \ldots, x_0 = h(x_1 \| y_n) \end{aligned}$$

The starting node of the IHC is x_n, and the value $x_0 = h(x_1 \| y_n)$ is called the root of the IHC. To make the matter simply, the one-way hash chain $(y_n, \ldots, y_0)$ is used as a salt of the IHC $(x_n, \ldots, x_0)$.

When a system master wish that a user can only compute hash values (i.e., $(x_j, \ldots, x_i)$) for interval (j, i), the system master assigns a pair (y_{n-i}, x_j) to the user. The user can easily compute interval hash values $(x_j, \ldots, x_i)$ by using received values (y_{n-i}, x_j) and the hash function h as follow: the user computes $(y_{n-i}, \ldots, y_0)$ by using y_{n-i} and then computes $(x_j, \ldots, x_i)$ by using x_j as below Fig. 4.

Hence, even though the user gets $(y_{n-i}, \ldots, y_0)$, the user cannot know any values of $(x_n, \ldots, x_{j-1}, x_{i+1}, \ldots, x_0)$ without knowing $(x_n, \ldots, x_{j+1})$ and $(y_n,$

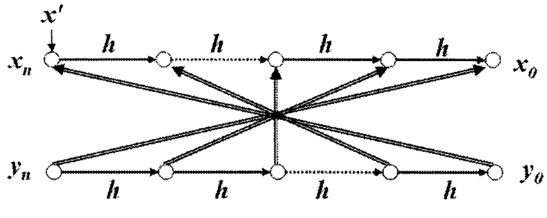

Fig. 3. Interval Hash Chains.

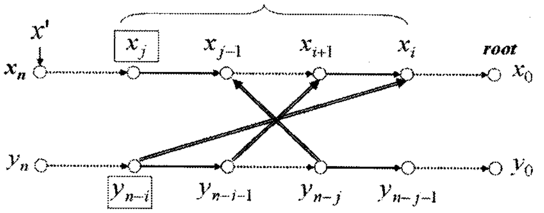

Fig. 4. The example of Interval Hash Chains.

..., y_{n-i+1}). In consequence, the user obtains only interval hash values (x_j,..., x_i) by using the pair (y_{n-i}, x_j) with the hash function h.

3.2 Interval Two-Dimensional Hash Chains

From now, we propose an interval two-dimensional hash chains by combining IHC with two-dimensional hash chain in [4]. Let h, g be two hash functions that are in pairs commutative. That is, $h(g(x)) = g(h(x))$. The interval two-dimensional hash chain consists of two or more levels of IHC. The value of i-th level IHC can be used to compute $(i+1)$-th level IHC. Fig. 5 shows an example of such a structure.

The value $x_n^1 = h(x' \| y_0) = h(x' \| h^n(y_n))$ is called the starting node of 1 level IHC, where x' and y_n are random values. The value $x_0^1 = h(x_1 \| y_n)$ is called the root of 1 level IHC. Generally, the i-th level IHC (x_n^i, ..., x_0^i) is generated by the ($g^{i-1}(y_n)$, ..., $g^{i-1}(y_0)$) and x' as follow:

$$x_n^i = h(x' \| h^n(g^{i-1}(y_n))) = h(x' \| g^{i-1}(y_0)),$$
$$x_{n-1}^i = h(x_n^i \| h^{n-1}(g^{i-1}(y_n))) = h(x_n^i \| g^{i-1}(y_1)),$$
$$..., x_0^i = h(x_1^i \| g^{i-1}(y_n))$$

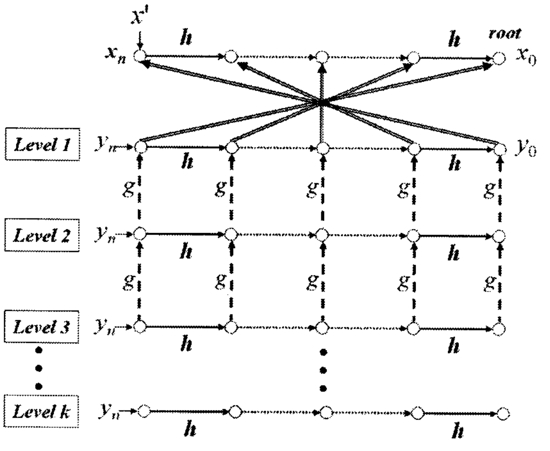

Fig. 5. Interval Two-Dimensional Hash Chain.

For example, a user can compute i-th level interval hash values (x_j^i, ..., x_l^i), $j \geqq i$ by using $(y_{n-j}^i, x_l^i) = (g^{i-1}(y_{n-j}), x_l^i)$. Moreover, the user can also compute same interval hash values of lower level IHC by using the hash function g. That is, the user can compute same interval hash values of IHC from $(i+1)$-th level to k-th level by using

$$(g(y_{n-j}^i), g^2(y_{n-j}^i), ..., g^{k-i-1}(y_{n-j}^i)).$$

In the proposed hash chain, the y_j value is used as salt of x_{n-j} value. Therefore, the $g(y_j)$ can generate different hash chains for same x' value.

4. APPLICATION TO A DRM SYSTEM

In this section, we introduce application of proposed interval two-dimensional hash chains to DRM system. Since our DRM system is based on interval two-dimensional hash chains, it has two advantages in comparison with previous DRM systems: 1) partial use of contents (using the property of interval hash chains) and 2) contents grading (using the property of two-dimensional hash chain).

4.1 Architecture

We describe the architecture of the proposed DRM system. To define architectural model more clearly, we assume are followings:

- The proposed system only considers time-dependent context such as movies and music. Other content types like e-books and applications may not be appropriate to our system.
- All users' devices have their own public/private key pairs, and certificates from the Certificate Authority.

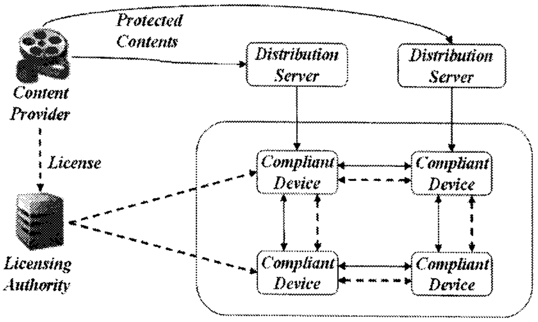

Fig. 6. Proposed DRM system.

Fig. 6 shows the proposed system which consists of Content Provider, Licensing Authority, Distribution Server and Content Manager. The descriptions of system components are as follows:

- Content Provider (CP): CP is responsible for generating Content Encryption Keys (CEKs) by using two different hash chains of IHC technique, and it provides different quality level encryption using corresponding CEKs. Also, it publishes the protected contents to the user's devices (Compliant Devices, CDs) or the distribution server, and then transfers CEKs into the licensing authority so as to make license in a secure manner.
- Licensing Authority (LA): LA is the most important entity in the proposed DRM system. It is responsible for generating license by using interval two-dimensional hash chains technique. After a user legally finishes billing process, LA delivers licenses to users' devices. Also, it maintains the record of user's payment information in its own database.
- Distribution Server (DS): DSs are organizations / companies interested in selling digital content items to consumers. DSs associate usage rules with the content they deliver; This association helps enforcing provider's copyrights, and facilitates a variety of business models.
- Compliant Device (CD): Compliant devices are used to render contents by users.

4.2 DRM System based on Interval Two-Dimensional Hash Chains

In this section, we introduce a new content encryption protocol for DRM system. The proposed protocol is consists of 4-tuple of algorithms given as following steops:

- Key Generation

The CP selects two random values x' and y_n. After that, the CP generates i-th graded interval CEKs as $CEK_1^i, CEK_2^i, ..., CEK_n^i$. The key generation of i-th graded interval CEKs is done as following:

$$\begin{aligned} &CEK_1^i = h(x' \| h^n(g^{i-1}(y_n))), \\ &CEK_2^i = h(CEK_1^i \| h^{n-1}(g^{i-1}(y_n))), \\ &..., CEK_n^i = h(CEK_{n-1}^i \| h(g^{i-1}(y_n))) \end{aligned}$$

- Content Encryption

The CP divides a i-th graded content C_i into interval contents $c_1^i, c_2^i, ..., c_n^i$, such as one minute or five minutes. Each interval contents were encrypted by symmetric encryption algorithm under CEKs, $E_{CEK}()$, such as AES. (note that, $A_j^i = E_{CEK_j^i}(c_j^i)$). Finally, The CP publishes $(A_1^i, ..., A_n^i)$ of encrypted content of C_i to user's devices (CDs) or DSs and delivers (x', y_n) to LA.

- License Issue

The LA generates a license by using received x' and y_n. When a user wants interval (j, k) CEKs of i-th graded contents, the LA generates a license for decrypting $(A_j^i, ..., A_k^i)$ after the user legally finishes billing process. The LA encrypts a set $(y_{n-j}^i, CEK_k^i, ..., CEK_k^l)$ by users' device public key and then the ciphertext is included in the license (where, l is the lowest grade). After that, the LA sends the license to the user.

- Content Decryption

The user's device renders specific interval contents of the same or lower graded contents by using the decrypted $(y_{n-j}^i, CEK_k^i, ..., CEK_k^l)$. When the grade of the extracted CEK is higher than the grade of the protected content, a corresponding

CEK is generated by means of hash chain technique in the section 3.2.

4.3 Evaluations

In this section, we give evaluations for the proposed scheme on viewpoint of convenience.

Since previous DRM systems only consider providing digital data content in a way that protects the copyrights of content providers based on cryptographic techniques, many users are reluctant to use DRM systems. Many users want to enjoy content with as few limitations as possible. In real application, each user has multiple devices for rendering a time-dependent contents such as movie and music. Due to this environment, each user wants to partially use a time-dependent content in user's multiple devices with partial payments of rendered contents. Therefore, a partial use of contents is a fine example of user friendly DRM systems. However, there seems to be no efficient method to support partial use of contents in previous DRM systems [5-8].

The proposed DRM system has two advantages by comparing with previous ones;

- *Partial use of contents*. A user can only compute specific interval (j, k) CEKs of i-th graded content by using the extracted one pair (y^i_{n-j}, CEK^i_k), where $y^i_{n-j} = g^{i-1}(y_{n-j})$. Therefore, the CP can efficiently assign interval CEKs to a user for rendering partial use of contents.
- *Grading contents*. The decrypted $(y^i_{n-j}, CEK^i_k, \ldots, CEK^l_k)$ can be used to render same or lower graded protected content by using interval two-dimensional hash chains technique in the section 3.2.

Furthermore, the proposed DRM system has an advantage from a security point of view in real application. Usually, when an attacker obtains a CEK from an encrypted content, he can render the whole contents, since one content is encrypted under one CEK. However, in our DRM system, even if one of interval CEKs of one content C_i is compromised, the other interval CEKs are still robust against the attack (e.g., the attacker renders only one minute among total of two hours length movie), since one content is divided and then encrypted into many separate ciphertexts under corresponding interval CEKs.

5. CONCLUSION

In this paper, we have proposed interval hash chains, which the system master can control for a user to compute hash values of specific interval in one-way hash chain, and interval two-dimensional hash chains using MDHC [4] for constructing graded contents in a DRM system. In addition, we proposed a new DRM system to enable contents to be rendered partially, and graded by using proposed hash chains. As a result, the users' device can render specific interval contents of the same or lower graded contents than grade of obtained CEKs.

REFERENCES

[1] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," *Advances in Cryptology-CRYPTO '98*, LNCS. 1462, pp. 137-152, 1998.

[2] R.C. Merkle, "A digital signature based on a conventional encryption function," *Advainces in Cryptology-CRYPTO '87*, LNCS. 293, pp. 369-378, 1988.

[3] P, Rohatgi, "A compact and fast hybrid signature scheme for multicast packet," *ACM CCS '99*, pp. 93-100, 1999.

[4] Q.S. Nguyen, "Multi-Dimensional Hash Chains and Application to Micropayment," *WCC 2005*, LNCS. 3969, pp. 218-228, 2006.

[5] A.M. Eskicioglu, J. Town, and E.J. Delp, "Security of Digital Entertainment Content

from Creation to Consumption," *Signal Processing: Image Communication*, Vol.18, No.4, pp. 237-262, 2003.

[6] M. Ripley, C.B.S. Traw, S. Balogh, and M. Reed, "Content Protection in the Digital Home," *Intel Technology Journal*, Vol.6, No.9, pp. 49-56, 2002.

[7] B. C. Popescu, B. Crispo, A. S. Tanenbaum, and F.L.A.J. Kamperman, "A DRM Security Architecture for Home Networks," *The 4th ACM ACM Workshop on Digital Rights Management*, pp. 1-10, 2004.

[8] F.L.A.J. Kamperman, S.A.F.A. van den Heuvel, and M.H. Verberkt, "Digital Rights Management in Home Networks," *IBC 2001*, pp. 70-77, 2001.

[9] Open Mobile Alliance: DRM rights expression language - approved version 2.0 (2006), http://www.openmobilealliance.org.

[10] R. Rivest, A. Shamir, and L.M Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *In Communications of the ACM*, Vol.21, No.2, pp. 120-126, 1978.

[11] A. Sharmir, "On the Generation of Cryptographically Strong Pseudorandom Sequences," *ACM Transactions on Computer Systems (TOCS)*, Vol.1, No.1, pp. 38-44, 1983.

Chae Duk Jung

received the B.S. degree from Dongeui University. Busan. Korea in 2005 and the M.S. degree from Pukyong National University. Busan. Korea in 2007. He is currently in a Ph.D. degree course of the same university of his M.S. degree course. His research interests are in the areas of cryptographic algorithms, information security and PKI.

Shin, Weon

received the M.S. and Ph.D. degrees from Pukyong National University. Busan. Korea in 1996 and 2001, respectively. From March 2002 until January 2005 he worked to develop security softwares and led the development process for security softwares as a senior researcher in AhnLab, Seoul, Korea. He is currently a Assistant Professor in the Department of Information Security, Tongmyong University, Busan, Korea. His research interests are in the areas of software security, reliable P2P computing and security applications.

Hong, Young-Jin

received the B. S. E. E. degree from Seoul National University. Seoul. Korea, in 1978 and the M. S. E. E. and Ph. D.(E. E.), from the State University of New York at Stony Brook in 1982 and 1985, respectively. From January 1986 until May 1986 he was with the Department of Electrical Engineering at the State University of New York ay Stony Brook, as an Assistant Professor. In June 1986 he joined LNR Communications, Inc., Hauppauge, NY, where he was a Research Staff Engineer and working on spread spectrum systems and satellite communications. In 1992 he came back to Korea to join Samsung Advanced Institute of Technology(SAIT), where he had been leading several research projects including CT2, VSAT and TDMA cellular basestations for two years. Since then he has broadened the spectrum of his career path to include not only the area of R&D(CTO of Eastel Systems from 1994 through 1997; CTO of Sungil Telecom in the year of 2004) sector but also the business area(executive managing director of SKC&C from 1997 to 2003). He is currently an Associate Professor in the Department of Electrical and Electronics Engineering, Tongmyong University, Busan, Korea. His research interests are in the areas of smart antenna system, adaptive signal processing and communication systems. Dr. Hong is a member of Korean Institute of Communication Sciences, The institute of Electronics Engineers of Korea. he is also a member of IEEE.

Kyung-Hyune Rhee

received his M.S. and Ph.D. degrees from Korea Advanced Institute of Science and Technology, Daejon Korea in 1985 and 1992, respectively. He worked as a senior researcher in Electronic and Telecommunications Research Institute, Daejon Korea from 1985 to 1993. He also worked as a visiting scholar in the University of Adelaide, Australia, the University of Tokyo, Japan, Kyushu University, Japan, and the University of California, Irvine, U.S.A. He has served as a Chairman of Division of Information and Communication Technology, Colombo Plan Staff College for Technician Education in Manila, the Philippines. He is currently a Professor in the Division of Electronic, Computer and Telecommunication Engineering, and a director of Information and Computer Center of Pukyong National University, Busan Korea. His research interests center on key management, mobile communication security, multimedia security, DRM and cryptographic algorithms, etc.