韓國 컴퓨터情報學會 論文誌
第11卷 第1號, 2006. 3.

2006-11-1-1-5

D-OCSP에서의 그룹키를 이용한 CRL 배포 방법에 관한 연구

이호*, 강현중**, 박준홍***

A Study on CRL Distributing Method based on Group Key Agreement in D-OCSP

Ho Lee*, Hyun-Joong Kang**, Joon-Hong Park***

요 약

E-commerce와 E-business가 급격히 발전함에 따라 인증서의 사용이 증가하고 있다. 인증서 검증은 E-commerce에서 가장 먼저 이루어져야 하며 OCSP Responder는 OCSP를 이용하여 클라이언트에게 CSI를 제공해주게 된다. 인터넷을 기반으로 하는 E-commerce가 급속히 발전함에 따라 많은 클라이언트들이 OCSP Responder에게 CSI요청을 하게 되었으며 OCSP Responder에 대한 로드가 증가하게 되고 과부하 상태에 이르게 될 수 있다. 따라서 이를 해결하기 위하여 D-OCSP가 도입되었으며 CA에 의해 발행되는 CRL은 각 OCSP Responder로 배포되어야 한다. CRL은 폐지된 인증서에 대한 많은 정보를 포함하고 있어 배포 시에 정보 유출의 가능성이 있으므로 무결성뿐만 아니라 기밀성도 유지되어야 한다. 따라서 본 논문에서는 CRL을 무결성과 기밀성을 유지하면서 각 OCSP Responder에게 배포할 수 있는 방법을 제안하고자 한다. 이 방법은 각 OCSP Responder들이 동시에 CSI 서비스를 제공할 수 있도록 해준다.

Abstract

As the E-commerce and E-business are developed actively, using certificate is incremented rapidly. The certificate validation must be confirmed at first in E-commerce and the OCSP Responder can offer CSI to the client using OCSP. With the rapid development of the E-commerce based on the Internet, a lot of clients request CSI to OCSP Responder. So, the load to OCSP Responder is increased and the OCSP Responder may be overloaded. Therefore, for distributing the load to an OCSP Responder, D-OCSP is introduced. As the CRL has a lot of information about revoked certificates and have a high exposure possibility of information in the process of distribution, the confidentiality as well as integrity are required in the process of distribution. So, we propose a CRL distributing method based on group key agreement in D-OCSP. The proposed method can distribute effectively a published CRL to OCSP Responders with confidentiality as well as integrity and offer concurrency that each OCSP Responder can start CSI servicing of new CRL to clients at the same time.

▸ Keyword : CSI(Certificate Status Information), D-OCSP(Distributed OCSP), CRL Distributor, Load Balancer

• 제1저자 : 이 호
• 접수일 : 2005.12.06, 심사완료일 : 2006.02.12

* 한국재활복지대학 컴퓨터정보보안과 부교수, ** 서일대학 인터넷정보전공 부교수,
*** 한국통신공사 연구소 유비쿼터스 사업부 수석연구원

Ⅰ. Introduction

{PKI and CRL.} As the E-commerce and E-business using PKI(Public Key Infrastructure) are developed, the use of certificate is incremented. In a PKI, a trusted third party called CA (Certification Authority) issues a certificate digitally signed by using its private signing key. The certificate is used to bind an user's identity information with the corresponding public key. The certificate's validity period is indicated by an issuing time and an expiration time, both fields also being included in the signed part of the certificate. If the user's private key is compromised or the user's personal information is changed, the users makes a request to the CA for revoking own certificate. The CA has the responsibility of publishing to users that the user's certificate has been invalid. The clients (or OCSP clients) or users check not only the expiration data on the certificate, but also whether the certificate has been revoked or not. The certificate revocation list is increased along with the population growth of certificate user. The CA gathers a list of information about revoked certificates and publishes the CRL(Certificate Revocation Lists) periodically and CRL is the most well-known method. The CRL issued by a CA is stored a CA Directory (or CA Repository). In case of validating user's certificate, the clients or users acquires the CRL stored in CA Directory. And they check whether corresponded certificate is contained in the CRL or not. Therefore, the CSI(Certificate Status Information) of the certificate must be confirmed at first in the E-commerce or E-business. In order to reduce the size of certificate revocation list, a lot of methods have been proposed nowadays. The CRL is a digitally signed list of revoked certificates by CA and is composed of [1,2]

- Version
- Signature Algorithm
- Issuer Name
- This Update
- Next Update
- Revoked Certificates
- Serial Number
- Revocation Date

:

- CRL Entry Extensions
- CRL Extensions
- Signature.

{T-OCSP and D-OCSP.} If the client needs very timely CSI, an online certificate status service like the OCSP(Online Certificate Status Protocol) is more convenient than CRL [3]. As client does not need to download a CRL directly in OCSP, a high communication costs between client and CA Directory is not required. The OCSP Responder(or OCSP Server) acquires the CRL from CA Directory and services a CSI to the clients. In case of validating user's certificate, the client sends an "OCSP Request" to OCSP Responder and the OCSP Responder answers with an "OCSP Response". The OCSP request and response are signed by the sender and are validated by receiver. With the increase of the number of client, the load to an OCSP Responder can centralized in "T-OCSP (Traditional-OCSP)"[4,5]. Therefore, "D-OCSP (Distributed -OCSP)" is introduced for decreasing overload to single OCSP Responder. The D-OCSP can process more CSI requests than T-OCSP in concurrent, because CSI requests from clients are distributed to each OCSP Responder.

{Our Contributions.} CRL has a lot of information about revoked certificates as above. CRL have the integrity by signature of CA's private key but, does not have the confidentiality because of unsigned part of CRL. As CRL have a high exposure possibility of the information in the process of distribution especially, the confidentiality as well as the integrity are required in the process of distribution. Therefore, in this paper, we propose a distributing method based on group key agreement. The method can distribute effectively a published CRL to OCSP Responders with confidentiality as well as integrity in D-OCSP environment. And the method give concurrency that each OCSP Responder can start CSI servicing of new CRL to clients at the same time. This paper is organized as follows. In section 2, we propose a efficient D-OCSP network model and show the necessity of each component and explain the necessity of group session key. In section 3, we apply a group key protocol suitable to proposed network model and propose the method of CRL distribution with confidentiality and concurrent CSI servicing using group session key. In section 4, we analyze the characteristics and efficiency of the proposed model and methods. Finally, in section 5, we bring to a conclusion of this paper.

Ⅱ. A proposal of efficient D-OCSP network model

In this section, we propose a D-OCSP network model and explain the necessity of each component and the application necessity of group session key to the model. (Fig.1) shows the D-OCSP network model and the CRL Distributor and the Load Balancer are needed in the proposed model.

2.1 The necessity of CRL Distributor

In the D-OCSP network model, the required conditions are as follows.

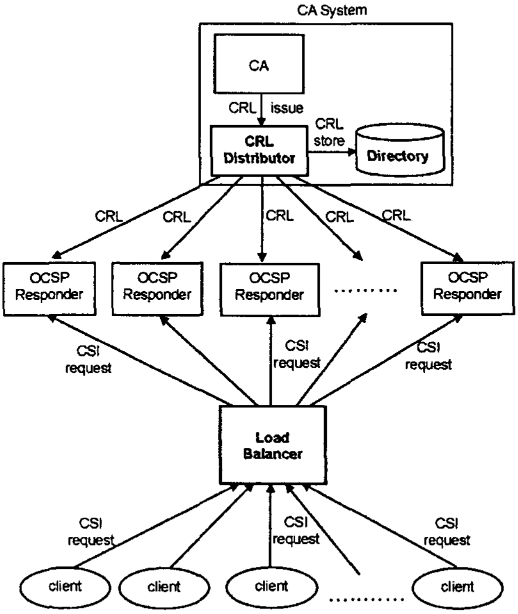

Fig 1. A proposal of efficient D-OCSP network model
그림 1. 효율적인 D-OCSP 네트워크 모델의 제안

As soon as the CRL is issued by CA, the CRL must be sent to each OCSP Responder rapidly. Therefore, the "push method" instead of "pull method" is required [6].

The CA must not have the overload for CRL distribution.

The CRL must be sent to each OCSP Responder concurrently and the each OCSP Responder can start CSI servicing of new CRL concurrently and rapidly.

In the structure of PKI, the addition of new authority for CRL distribution have to be avoided possibly.

To satisfy the above conditions, CRL Distributor having a function of CRL distribution is required in CA system like in [6]. (Fig.1) shows the CRL Distributor subsystem in CA system and the CRL Distributor has the same function with CISProvider of [6]. As soon as the CRL is issued by CA, the CRL Distributor distributes to each OCSP Responder.

2.2 The necessity of Load Balancer

The each OCSP Responder acquires the CRL distributed by CRL Distributor and services CSI to clients. As CSI requests are distributed to each OCSP Responder, D-OCSP network model can prevent the overload of single OCSP Responder in T-OCSP. Also, D-OCSP can process more CSI service than T-OCSP at the same time. However, in case of not offering the "load balancing", some OCSP Responders may have the state of overload in worst case. And the other OCSP Responders may have the state of underloaded or even idle. Thus, the function of load balancing is needed. The separate server having a function of load balancing is needed because OCSP Responders are busy for servicing CSI. The Load Balancer exchanges the control message and data with each OCSP Responder for load balancing of CSI request [7].

2.3 The usage necessity of group session key

Table 1. Computation time comparison of the crypto algorithms [8]

표 1. 암호 알고리즘의 계산 시간 비교

Type	Algorithm	Computational time (msec / operation)
Asymmetric	RSA 1024 signature	4.647
	RSA 1024 verification	0.188
	RSA 2048 signature	29.174
	RSA 2048 verification	0.445
Symmetric	DES (1024 bit)	0.005
	DES (2048 bit)	0.01

{Privacy.} The CRL includes the revocation list of a lot of users in unsigned part and anyone can see the content of CRL. Thus, the information can be exposed easily in CRL distribution [5]. The exposure of information can violate users' privacy and can be abused by an attacker. The confidentiality is more required in CRL than in OCSP having response of good, revoked or unknown(0, 1, 2). Therefore, the confidentiality as well as integrity are required in process of distribution CRL to several OCSP Responder [5].

{Save of computation costs.} ⟨Table 1⟩ shows computation time of each crypto algorithm. In the proposed D-OCSP network model, if each session key(symmetric algorithm like DES) between CRL Distributor and each OCSP Responder is used for encryption of CRL, the number of n session keys are needed in case of n OCSP Responders. The CRL Distributor manages n session key and the encryption computation of n time is needed for CRL's distribution. However, because same CRL is distributed to each OCSP Responder, if the common session key is used, the encryption computation of 1 time only would be needed. Also, the CRL Distributor have only to manage 1 session key.

{Confidentiality of load state information exchanged.} In the proposed network model, the Load Balancer needs a load state information(overload or underload) from each OCSP Responder for load balancing of CSI request. If the load state information is modified by attacker, the load balancing would be failed. Some OCSP Responders can be overloaded or down, other OCSP Responders can be underloaded by wrong load state information. Therefore, the session key is also needed for encryption of load state information between Load Balancer and OCSP Responders. If each session key between Load Balancer and each OCSP Responder is used, the number of n session keys are needed in case of n OCSP Responders and the Load Balancer manages n session key. If the common session key is applied, the management of session key can be simple in Load Balancer and each OCSP Responder.

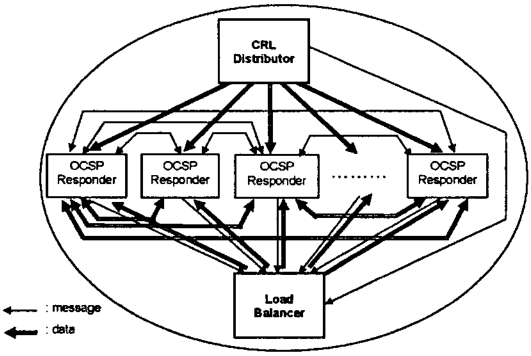

Fig 2. The message and data flow among the components of group model
그림 2. 그룹 모델 구성원간의 메시지와 데이터 흐름

Forwarding of CRL in case of communication problem between CRL Distributor and an OCSP Responder.} If the communication trouble between CRL Distributor and an OCSP Responder is happened, the OCSP Responder can not receive new CRL from CRL Distributor and begin the CSI services of new CRL. The situation can be continued until communication problem is resolved and can influence the efficiency of total system. For preventing the problem, the OCSP Responder can require CRL from near OCSP Responder. The OCSP Responder acquiring encrypted CRL by forwarding can decrypt it using common session key. Thus, group session key is needed among each OCSP Responders.

Therefore, we treat the CRL Distributor, Load Balancer and OCSP Responders as a group and apply "Group Key" to the group. The application group session key decreases the number of managed session key and computation cost for encryption. (Fig. 2) shows a group model composed of the CRL Distributor, Load Balancer and OCSP Responders and the flow of data and message among them.

III. An application of group session key

In this section, we research about group key distribution protocol and apply a group session protocol suitable to the proposed D-OCSP network model.

3.1 Requirements

Table 2. Comparison of group key protocols
표 2. 그룹 키 프로토콜 비교

protocol	round	unicasts	broad-casts	computation cost		forward secrecy	Sig.	Ver.	type
				server	client				
Emmanuel 1	O(n)	n-1	1	high	high	O	1	2	ring
Emmanuel 2	2	n-1	1	high	low	Δ	1	1	Star
Katz-Yung	3		3n	medium	medium	O	2	O(n)	mesh
Nam	3	n-1	n+1	high	low	O	1	1	Star

Note. Sig : Signature Generation, Ver : Signature Verification, Emmanuel 1 means "Provably Group Diffie-Hellman Key Exchange", Emmanuel 2 means "Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices"

The "Group Communication" means the communication among group components using group key in case communication among the group components is frequent. There are the "1-to N" model and "N-to-N" model in group communication. The proposed group model is similar to "1-to N" model. There are the "distribution -type" protocol and "agreement-type" protocol in group key establishment protocol. The manger of a group is needed in "distribution-type" protocol. The group manager selects data and computes the group key. And the group distributes the group key to group components. In "agreement-type" protocol, the all of components participate in the creation of group key. In accordance with it, the distribution-type protocol is mostly used in 1-to-N and the agreement-type protocol is used in N-to-N model. According to passing for computing group session key, they are divided into star type, ring, and mesh type [9,10-14,15-19,7,20]. We suppose that OCSP Responders, CRL Distributor, and Load Balancer are the server. For selecting group session key protocol suitable to proposed D-OCSP network model, the required conditions are as follows.

1. As the proposed D-OCSP network model is belong to mesh type of 1-to N model, group key protocol of star type is suitable.
2. As each OCSP Responder and Load Balancer are always very busy for CSI service, a group session key protocol that almost computation for group session key distribution is processed in server(CRL Distributor) and minimum of computation is processed in client(OCSP Responder and Load Balancer) is suitable.
3. An applied group key protocol must offer authentication, confidentiality, integrity, and forward secrecy.
4. The data exchange in group key protocol is small as soon as possible.
5. The computation costs in group key protocol is small as soon as possible.
6. The communication costs in group key protocol is small as soon as possible.

The several group key protocols have been proposed in [9,10-14,15-19,7,20] now. <Table 2> show the comparison of group key protocols. Nam's group key protocol is suitable to the proposed D-OCSP network model as in <Table 2> [15,16]. Nam's group key protocol proposed in "DH-based Group Key Agreement in a Mobile Environment" written by Junghyun Nam offers the mutual authentication, forward secrecy and group key agreement using signature scheme and needs a two round for group generation [15,16]. Nam's group key protocol offers that the almost computation for group key generation is processed at server and the minimum computation is processed in client

3.2 An application of Nam's group key agreement protocol

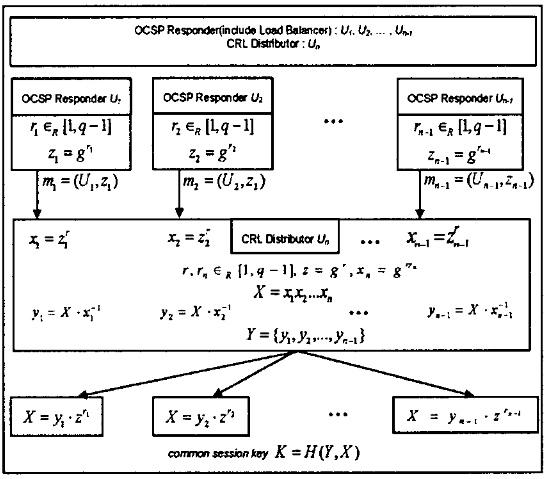

Fig 3. An application of Nam's group key agreement protocol to proposed D-OCSP network model
그림 3. 그룹 키 합의 프로토콜 적용

(Fig. 3) shows an application of the Nam's group key agreement protocol to proposed D-OCSP network model. The generation procedure of group session key performs the following steps:

1. Each OCSP Responder(include Load Balancer) $U_i \neq U_n$ chooses a random $r_i \in Z_q$, computes $z_i = g^{r_i}$, and sends $m_i = (U_i, Z_i)$ to the CRL Distributor U_n.

2. The CRL Distributor U_n chooses random $r, r_n \in Z_q$ and computes $z=g^r$ and $x_n=g^{rr_n}$.

3. The CRL Distributor U_n computes $x=\prod_{i\in[1,n]} x_i$ and the set $Y=y_i|1\leq i\leq n-1$, where x_i and $y_i=X\cdot x_i^{-1}$.

4. The CRL Distributor U_n broadcasts $m_n=(U_n, z, Y)$ to the entire group(each OCSP Responder and Load Balancer).

5. Upon receiving the broadcast, each OCSP Responder(includes Load Balancer) $U_i \neq U_n$ computes $X=y_i \cdot z^{r_i}$.

6. All users in U computes their session key as $K=H(Y,X)$, where H is a one-way hash function modelled as a random oracle in the security proof [15,16].

3.3 A CRL distribution with confidentiality and concurrent CSI servicing using the group session key

(Fig. 4) shows a procedure of CRL distribution with confidentiality and concurrent CSI servicing using the group session key. The detailed procedure using the group session key sk is as follows.

1. When the CRL is issued by CA, the CRL Distributor encrypts CRL using the group session key sk and sends the encrypted CRL, $E_{sk}(CRL)$, to each OCSP Responder.

$$CRL Distributor: E_{sk}(CRL)\rightarrow OCSP Responder$$

2. The CRL Distributor encrypts the "begin of CRL distribution" message and sends to Load Balancer.

$$CRL Distributor: E_{sk}(begin\ of CRL\ distribution)\rightarrow Load Balancer$$

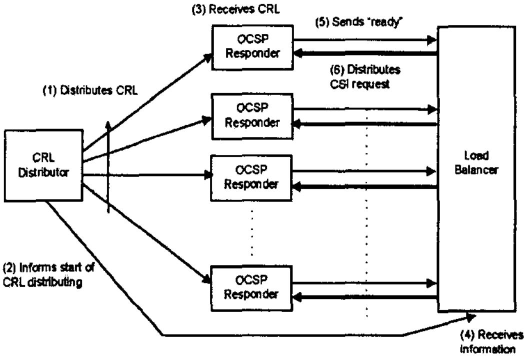

Fig 4. A CRL distribution procedure with confidentiality and concurrent CSI servicing using group session key
그림 4. CRL 분산 절차

3. The each OCSP Responder receives the encrypted CRL, $E_{sk}(CRL)$, and decrypts it using the group session key sk.

$$OCSP Responder: D_{sk}(E_{sk}(CRL)) = CRL$$

4. The Load Balancer receives the encrypted "start of CRL distribution" and decrypts it using the group session key sk. The Load Balancer knows the publishing of new CRL and waits "ready" message from each OCSP Responder.

$$Load Balancer: D_{sk}(E_{sk}(begin\ of CRL\ distribution)) = begin\ of CRL\ distribution$$

5. In case of completing of new CSI servicing preparation by new CRL, the each OCSP Responder sends the encrypted "ready" message to the Load Balancer.

$$OCSP Responder: E_{sk}(ready)\rightarrow Load Balancer$$

6. If the "ready" message is received from each OCSP Responder, the Load Balancer distributes the CSI request to the OCSP Responder.

$$Load Balancer: D_{sk}(E_{sk}(ready)) = ready$$
$$OCSP Responder \Leftarrow CSI request\ Load Balancer$$

7. If the "ready" message is received from an OCSP Responder in limited time, the Load Balancer does not distributes the CSI request to the OCSP Responder until receiving of the message.

Ⅳ. Characteristics

〈Table 3〉 shows a comparison of the proposed D-OCSP model, the general D-OCSP model and the T-OCSP model. The detailed characteristics are as follows:

표 3. 제안 모델과 타 모델의 비교
Table 3. Comparison of the proposed model and the others

	Number of OCSP Responder	Capacity of CSI servicing	Concurrency of CSI Service	Load balancing of CSI request	Integrity of CRL in distribution	confidentiality of CRL in distribution
Proposal	multitude	high	possible	possible	O	O
D-OCSP	multitude	high	difficult	difficult	O	X
T-OCSP	single	low	-	-	O	X

{Proposed D-OCSP network model.}

- The CRL Distributor

- offers the active CRL distribution of push method.
- distributes the CRL to each OCSP Responder concurrently and rapidly.
- does not give the load of CRL distribution to CA.
- Because CRL Distributor is subsystem of CA system, the additional certificate is not required.

- The Load Balancer

- offers the load balancing of CSI request to D-OCSP network model.
- Because the Load Balancer passes only the CSI requests, the Load Balancer does not need the certificate.
- The Load Balancer can be included in like the proxy or gateway server.

{Proposed CRL distribution method using of group session key.}

- The only 1 session key is managed and used among CRL Distributor, OCSP Responders and Load Balancer.
- Because the group session key can be changed periodically, it can reduce the damage of key exposure.
- Because symmetric session key is used, the computation costs for encryption and decryption is small.
- Because the CRL Distributor is idle except at the CRL distribution, the almost computation for generation of group session key is processed in CRL Distributor at idle time.
- Because the OCSP Responder and Load Balancer are busy for CSI service, the minimum of computation for generation of group session key is processed in OCSP Responders and Load Balancer.

{Method of CRL distribution with confidentiality and concurrent CSI servicing.}

- For distributing the CRL to each OCSP Responder, the CRL Distributor computes only one symmetric encryption using group session key.
- Because the CSI requests are distributed to prepared OCSP Responder(having "ready" condition), the concurrency of CSI service can be guaranteed.

V. Conclusion

In this paper, we proposed a method of the CRL distribution with integrity, confidentiality, rapidity and concurrent CSI servicing using group session key in D-OCSP. For this one, we proposed a D-OCSP network model and applied the group key protocol to the model. We presented a method of CRL distribution with confidentiality and concurrent CSI servicing using group session key and showed the characteristics and efficiency of them. The proposed method can be used for designing PKI system effectively.

참고문헌

[1] C. Adams, P. Sylvestor, M. Zolotarev, R. Zuccherato, "Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols", IETF RFC 3029, February, 2001.

[2] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC 2458, January, 1999.

[3] M. Myers, R. Ankney, A. Mappani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IETF RFC 2560, June, 1999.

[4] Dae Hyun Yum, Pil Joong Lee, "A Distributed Online Certificate Status Protocol Based on GQ Signature Scheme", ICCSA 2004, LNCS 3043, pp.471-480, 2004.

[5] Satoshi Koga, Kouichi Sakurai, "A Distributed Online Certificate Status Protocol with a Single Public Key", Public Key Cryptography 2004, LNCS 2947, pp.389-401, 2004.

[6] J.Kwak, K.J.Kim, S.H.Oh, D.H.Won, H.K.Yang, "Real-time Certificate Status Validation Model with CSIProvider", WSEAS Transactions on Communications Vol.1, Issue1, pp.203-210, 2002.

[7] H. Kameda, J. Li, C. Kim, and Y. Zhang, "Optimal Load Balancing in Distributed Computer Systems", Springer Verlag, 1997.

[8] http://www.eskimo.com/~sim/weidai/benchmarks.html.

[9] C. K. Wong, M. Gouda, S. S, Lam, "Secure Group Communications using Key Graphs, Proceedings of ACM SIGCOMM", Vancouver, British Columbia, Sep, 1998.

[10] Emmanuel Bresson, Olivier Chevassut, Abdelilah Essiari, and David Pointcheval, "Mutual Authentication and Group Key Agreement for Low-Power Mobile Devices", The Fifth IEEE International Conference on Mobile and Wireless Communications Networks, 2003.

[11] Emmanuel Bresson, Olivier Chevassut, and David Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange-The Dynamic Case", Asiacrypt 2001, LNCS 2248, pp. 290-309, 2001.

[12] F. Zhu, A. Chan, G. Noubir, "Optimal Tree Structure for Key Management of Simultaneous Join/Leave in Secure Multicast", MILCOM, October, 2003.

[13] G. Noubir, "A Scalable Key Distribution Scheme for Dynamic Multicast Groups", The 6th ACM conference on Computer and Communication Security, Nov, 1999.

[14] I. Chang, R. Engel, D. Kandlur, D. Pndarakis, D.Saha, "Key Management for Secure Internet Multicast using Boolean Function Minimization Techniques", Proceedings of infocom, New York, March, 1999.

〔15〕 Junghyun Nam, Sungduk Kim, Seungjoo Kim, and Dongho Won, "Dynamic Group Key Exchange over High Delay Networks", Proc. of ISPC COMM 2004, International Scientific -Practical Conference on Communication 2004, Springer-Verlag, LNCS, Issyk-Kul Lake, Kyrgyzstan, August 22-29, 2004.

〔16〕 Junghyun Nam, Seokhyang Cho, Seungjoo Kim, and Dongho Won, "Simple and Efficient Group Key Agreement based on Factoring, Proc. of the 2004 International Conference on Computational Science and Its Applications (ICCSA 2004)", LNCS 3043, pp.645-654, May 2004.

〔17〕 Klaus Becker and Uta Wille, "Communication Complexity of Group key Distribution", Proceedings of ACM Conference on Computer and Communications Security, USA, Nov, 1998.

〔18〕 M. Burmester and Y.Desmedt, "A secure and efficient conference key distribution system Advances in Cryptology", Eurocrypt'94, 1994.

〔19〕 Michael Steiner, Gene Tsudik, Michael Waidner, "Diffie-Hellman Key Distribution Extended to Group Communication", CCS, 1996.

〔20〕 Y. Kim, A. Perrig, and G. Tsudik, "Communication -efficient group key agreement. Proc. of International Federation for Information Processing", 16th International Conference on Information Security (IFIP SEC'01), June 2001.

저자소개

이호

1989년 벨기에 VUB 대학원
정보공학과(공학 석사)
2002년 성균관 대학교 대학원
정보공학과(공학 박사)
1982년 ~ 1991년
한국전자통신연구원선임연구원
2005년 12월 현재 :
국립한국재활복지대학
컴퓨터정보보안과 부교수
〈관심분야〉 정보보호,
컴퓨터네트워크

강현중

1980년 성균관대대학교
수학교육(학사)
1986년 연세대학교대학원
전자계산학(이학 석사)
1996년 2월 성균관대학교 대학원
정보공학(공학 박사)
1979년 11월 ~ 1982년 2월
한국과학기술연구소(KIST)
연구원
1982년 3월 ~ 1989년 2월
한화종합금융(주) 전산팀장
2005년 12월 현재 : 서일대학
인터넷정보전공 부교수

박준홍

1978. 3 ~ 1982. 2 경희대학교
공과대학 전자공학과
(공학학사)
1982. 3 ~ 1987. 2 경희대학교
일반대학원 전자공학과
(공학석사)
2000. 3 ~ 현재 : 목원대학교
일반대학원 전자및컴퓨터공학과
(박사과정)
2005년 12월 현재 : 한국통신공사
연구소 수석연구원