이동 사용자를 위한 분산 보안 메일 시스템

양 종 필[†] · 서 철[†] · 이 경 현[††]

요 약

본 논문에서는 메일 사용자의 오버헤드를 최소화하고 TTP(Trusted Third Party)의 기밀성을 분산시킨 새로운 Certified E-mail System을 제안한다. 제안 시스템은 전달 메시지의 공정성 및 기밀성 보장을 위하여 전통적인 암호기법과 함께 서버 지원된 서명 기법을 사용함으로써, 메일 사용자의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하는 구조를 가진다. 따라서, 제안 방안은 셀룰러 폰이나 무선 PDA와 같은 컴퓨팅 파워가 취약한 이동 장치를 이용하는 메일 사용자에 적합하다. 또한, 제안된 시스템은 임계 암호시스템에 기반하여 설계되었으므로 이동 공격자에 대하여 강건하며 공모 공격으로부터 안전하다.

Distributed Secure Mail System For Roaming User

Jong Phil Yang[†] · Chul Sur[†] · Kyung Hyune Rhee[††]

ABSTRACT

In this paper, we propose a new certified e-mail system which reduces user's computational overhead and distributes confidentiality of TTP (Trusted Third Party). Based on the traditional cryptographic schemes and server-supported signature scheme for fairness and confidentiality of message, we intend to minimize the computation overhead of mobile device on public key algorithm. Therefore, our proposal becomes to be suitable for mail user who uses mobile devices such as cellular phone and PDA. Moreover, the proposed system is fault-tolerant, secure against mobile adversary and conspiracy attack, since it is based on the threshold cryptography on server-side.

키워드 : 보안 메일(Certified E-mail), 메일 보안(Mail security), 비밀 분산(Secret sharing)

1. 서 론

전자 메일(e-mail)은 현대인의 삶에서 매우 보편적으로 사용되고 있으며, 또한 비즈니스 측면에서도 필수적인 통신 도구가 되고 있다. 우편, 팩스, 전화와 같은 전통적인 통신 도구들에 비하여 e-mail을 통한 통신상의 편리함은 많은 사람들로 하여금 e-mail을 가장 보편적으로 상호 정보를 교환하도록 하였다. 현대 사회의 인프라가 온라인 환경으로 이동함에 따라서 전통적인 면대면(face-to-face)방식에서 고려되지 않던 새로운 문제가 일어나고 있다. 즉, "전자적 정보를 인터넷을 통하여 어떻게 전송하고 교환할 것인가?"에 대한 새로운 연구가 필요한 시점이다. 바꾸어 말하면, 인터넷은 전자적 정보에 대한 안전하고, 공정한 교환(fair-exchange)과 같은 비즈니스 통신 모델에서 요구되는 서비스를 제공하지 못한다. 또한, 전자적 처리에서의 동시성의 결핍으로 인하여 통신 당자들간의 공정성(fairness) 문제를 발생시킨다[1].

공정한 교환 문제에 대한 고전적인 해결책은 교환하고자 하는 아이템의 작은 부분을 점진적으로 교환하는 방식에 기본을 두고 있다. 그러나, 이러한 점진적 교환 방식은 다분히 이론적이며, 높은 컴퓨터 능력과 전송능력을 요구하므로 현실적으로 불가능하다. 공정한 교환 문제의 또 다른 해결 방안으로 certified e-mail 기술에 대한 연구 및 개발이 이루어지고 있다. 이는 기존의 보안 메일 기술인 S/MIME, PGP[2]와는 다른 기술로서, 메일 송·수신자 사이의 공정한 교환을 보장한다. 공정한 교환이란 다음과 같은 상황이 일어나지 않음을 의미한다. 즉, 송신자가 수신자로부터 수신의 증거를 받지 않았지만 수신자가 e-mail을 받거나 또는, 송신자가 수신의 증거를 받았지만 수신자가 e-mail을 받지 못하는 경우이다. 공정성은 전자상거래에서 가장 중요한 특징들 중의 하나이다.

[3 6]에서 제안되었던 certified e-mail 시스템들은 메일 송·수신의 공정한 교환을 위한 서비스와 메일 교환 후 메

※ 이 논문은 2003학년도 두뇌한국21 사업에 의하여 지원되었음.
† 준 회 원 : 부경대학교 대학원 전자계산학과
†† 종신회원 : 부경대학교 전자컴퓨터멀티미디어공학부 교수
논문접수 : 2003년 7월 22일, 심사완료 : 2003년 9월 25일

일 송·수신의 부인 방지, 메일 메시지의 기밀성을 위한 서비스를 제공한다. 하지만, 기 제안된 certified e-mail 시스템들은 셀룰러 폰이나 PDA와 같은 이동 장치를 사용하는 이동 사용자의 계산적인 한계에 대하여 고려해주지 못하고 있으며, 또한 certified e-mail 시스템에서 공정한 교환을 보장하기 위해 사용되는 TTP에 대한 악의적인 공격자들로부터의 훼손 및 공모공격에 대하여 신뢰성과 안전성을 제공해주지 못하고 있다.

본 논문에서 제안하는 새로운 보안 메일 시스템은 N. Asokan과 X. Ding이 제안한 서버 지원된 서명기법[7, 8]을 기반한다. 따라서, 공개키 암호 알고리즘 연산에 따른 사용자의 계산 오버헤드를 최소화함으로써 사용자가 셀룰러 폰이나 PDA와 같은 이동 장치를 통한 보안 메일 전송에 적합한 시스템 구조를 가진다. 또한, TTP로 간주되는 서버 시스템이 사용자를 대신하여 전자서명을 수행하기 때문에 그 서버 시스템은 공격자들의 주요한 공격 목표가 될 수 있다. 따라서, 서버 시스템의 신뢰성과 안전성이 중요한 이슈로 간주될 수 있다. 이를 위해, 제안 시스템은 임계 암호 시스템(threshold cryptosystem)에 기반하여 서버 시스템의 기밀 정보인 비밀키(secret key)를 여러 서버들에게 분산시킴으로써, 악의적인 공격자, 특히 이동 공격자(Mobile Adversary)[5]들로부터 서버 시스템을 보다 강건하게 설계를 하였다.

본 논문은 다음과 같이 구성된다. 2장에서 제안 시스템에 적용된 기술을 소개한 후 3장에서는 새로운 분산 보안 메일 시스템을 제안한다. 또한, 제안 시스템 사용자간의 분쟁 상황 발생시 공정성 보장을 위한 해결방안을 제시하고 분석하겠다. 4장에서는 이동 사용자를 위한 지원방안에 대하여 기술하며 5장에서 제안 시스템의 보안평가를 한 후 6장에서 결론을 맺는다.

2. 적용된 기술

2.1 서버 지원된 서명기법(Server-Supported Signatures Scheme)

제안 방안은 셀룰러 폰, PDA와 같은 낮은 컴퓨팅 파워와 배터리를 소유하고 있는 사용자들이 certified E-mail 전송을 가능하게 하기 위하여, N. Asokan등이 제안한 서버 지원된 서명 기법[7, 8]을 사용하고 있다. 이 방안의 특징은 사용자의 전자 서명에 대한 계산적 부담을 서버가 수행함으로써, 전자 서명문에 대한 송신 부인 방지(non-repudiation of origin)와 수신 부인 방지(non-repudiation of receipt) 서비스를 제공 가능하다. 또한, 위의 서버가 신뢰되는 제 3자의 역할을 수행하면 송·수신자간의 공정한 교환을 보증할 수 있다.

2.2 임계 암호 시스템(Threshold Cryptosystems)

사용자들이 단일 서버로 부터의 보안 서비스를 제공 받는 환경에서는 서비스를 제공하는 서버 시스템의 구성적 측면은 단순해진다. 하지만, 수많은 공격자들의 주요 공격 목표가 될 수 있으며, 그 서버가 침해되었을 경우 전체 서비스가 중단되어야 하는 심각한 상황에 취해질 수 있다. 따라서, 좀 더 강건한 서버 시스템을 구축하기 위한 기술로서 비밀 분산(secret sharing)과 임계 암호 시스템(threshold cryptosystem)에 대한 연구가 활발히 이뤄지고 있다.

(n, t) 임계 암호 시스템, $n \geq 2t+1$[9]는 n 개로 구성된 서버 시스템의 비밀값, 주로 공개키 암호 알고리즘을 위한 비밀키(secret key)를 n 개의 서버로 각각 분산(sharing)시킨다. 즉, n 개의 각 서버들은 자신의 비밀 분배값(share) $s_i (1 \leq i \leq n)$를 소유하게 된다. 그리고, 서버 시스템을 대상으로 암호적 연산이 요구될 시에 요청된 메시지 m를 서명하기 위해서, 최소 $t+1$개의 서버가 자신의 분배값으로 계산한 부분 서명값(partial signature)값 $PS_{s_i}(m) (1 \leq i \leq t+1)$이 모여서 서버 시스템의 비밀키로 서명한 전자 서명문을 생성 가능하다. 따라서, 공격자는 서버 시스템을 침해하기 위해서는 최소한 $t+1$개의 서버를 침해해야 만이 전체 서버 시스템을 가장하여 암호학적 연산을 수행할 수 있다[10, 11].

2.3 Certified E-mail

Certified E-mail은 메일의 공정한 교환을 위하여 신뢰되는 제 3자(TTP : Trusted Third Party)를 사용한다. 최근에 Kenji Imamoto[3], G. Ateniese[4], J. Zhou[5], B. Schneier [6]과 같은 여러 연구자들에 의해서 certified e-mail에 대한 연구가 진행되었으며, TTP의 사용방법에 따라 on-line protocol과 optimistic protocol으로 분류된다.

- On-line protocol : 전달 채널로 TTP를 사용한다. 그러나 프로토콜의 매개체로써 TTP가 계속 관여하게 됨으로써 사용자가 프로토콜을 사용하는 횟수에 비례하여 TTP의 계산량과 통신상의 비용도 증가한다.
- Optimistic protocol : TTP가 단지 예외상황이 발생했을 경우에만 사용이 된다. TTP가 대부분 off-line이므로 TTP에 대한 효율성은 증진된다. 그러나, 송신자가 메일을 보낸 후 송신자와 수신자간에 몇 번의 정보를 교환하는 동안 송신자와 수신자간의 통신이 유지되어야 함으로써, 메일 사용자들에게 상당한 오버헤드가 발생한다.

일반적으로, certified e-mail 시스템이 충족해야할 기본 요구사항은 아래와 같다.

- 공정성(fairness) : 송·수신자 모두 프로토콜 종결 후 자신이 원하는 결과를 얻거나 양쪽 모두 자신이 원하는 결과를 얻지 못해야 한다. 또한, 송·수신자 어느쪽도 자신에게 유리한 결과가 나오도록 프로토콜을 방해하거나 조작할 수 없어야 한다.
- 인증(authentication) : 송·수신자는 정보를 전달하고 있는 상대방이 확실히 의도된 상대방인지를 인증할 수 있어야 한다.
- 기밀성(confidentiality) : 전송되는 정보는 송·수신자 이외의 제 3자가 읽을 수 없어야 한다.
- 무결성(integrity) : 프로토콜 수행도중 전송정보는 공격자에 의하여 변조되어져서는 안된다.
- 송신의 부인방지(non-repudiation of origin) : 프로토콜 종료후 송신자는 자신이 보낸 정보에 대하여 부인할 수 없어야 한다.
- 수신의 부인방지(non-repudiation of receipt) : 프로토콜 종료후 수신자는 자신이 받은 정보에 대하여 부인할 수 없어야 한다.

특히, 공정성은 certified e-mail 프로토콜에서 가장 중요한 요구사항이다. 그러므로, 프로토콜은 공정성을 보장하기 위하여 신뢰되는 제 3자의 훼손 및 어느 한 사용자와 공모하는 악위적인 신뢰된 제 3자에 대하여 강건해야 한다.

3. 분산 보안 메일 시스템 제안

3.1 용어 정리 및 전체 구조

본 논문에서는 아래와 같은 용어를 사용한다.

- S, R : 송신자와 수신자의 식별자
- C : 전송하고자 하는 메시지 M을 설명하기 위한 정보. (예, 메일 제목 등)
- MD_i : Mail Delivery 식별자. 여기서, $1 \le i \le n$.
- NRT : 부인 방지 토큰(non-repudiation token)
- SK : 메시지를 암호화하기 위한 대칭키 암호 알고리즘의 세션키. 메시지 M에 대한 대칭키 암호화를 $[M]_{SK}$로 나타낸다.
- $h_X()$: 개체 X의 일방향 해쉬함수. 개체들은 자신의 해쉬함수를 개인화해야 한다. 예, $h(X, M)$에서 M은 메시지
- K_X : X가 랜덤하게 생성한 비밀값.
- K_X^i : 사용자 X의 $(n-i)$ 번째 서명키. K_X를 기반으로 해서, 사용자 X는 아래와 같은 해쉬 체인을 생성

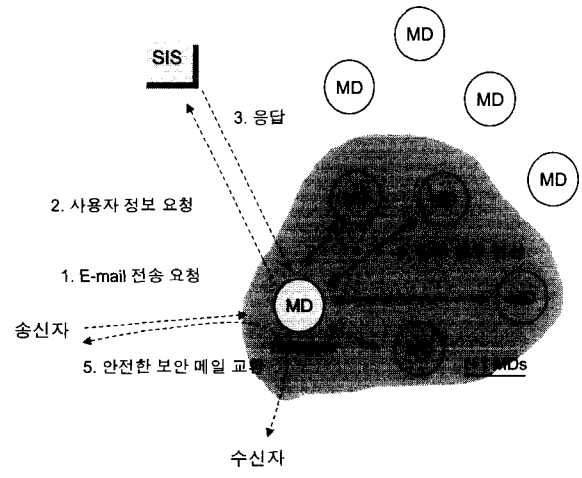
$$K_X^0 = K_X,\ K_X^i = h_X^i(K_X) = h_X(K_X^{i-1})$$

K_X^n을 사용자 X의 루트 서명키라고 하며, 현재 i값을 서명 카운터라고 하며, K_X^i를 X의 현재 서명키라고 한다.

- $H(M)$: 메시지 M에게 일반적인 일방향 해쉬함수 처리를 수행.
- $Sig_X(M)$: 메시지 M에 대한 개체 X의 비밀키를 통한 전자서명.
- $E_X(M)$: 메시지 M에 대한 개체 X의 공개키를 통한 암호화.
- Cre_X : 사용자 X가 SIS(Secure Indexing Server)로부터 수신 받은 신임장(Credential).

$$Cre_X = Sig_{SIS}(X, n, K_X^n, SIS)$$

(그림 1)은 본 논문에서 제안하는 분산 보안 메일 시스템의 전체적인 구조를 보여주고 있다. SIS(Secure Indexing Server)는 각 사용자들에게 보안 메일을 전송하기 위하여 사용되는 신임장(credential)을 발급하는 기관이며, 각 사용자들의 서명 카운터와 현재 서명키를 안전하게 저장하고 있다.



(그림 1) 분산 보안 메일 시스템의 전체 구조

DMD(Distributed Mail Delivery)는 분리된 프로세서에서 각각 실행되는 $n \ge 2t+1$개의 MD(Mail Delivery)들의 집합이다. DMD는 공개키 알고리즘을 위한 키쌍이 존재하며, 이를 DMD의 서비스 공개키/비밀키라고 한다. DMD의 서비스 비밀키는 n개의 MD에게 비밀분산(secret sharing)된다. Certified e-mail을 전송하고자 하는 사용자는 메일을 전송하기 위해서 DMD내의 단일 MD에게 서비스 요청을

한다. 위의 서비스 요청을 수신한 MD는 사용자의 대리자(delegate)가 된다. 대리자는 사용자가 요청한 암호학적 연산을 수행하기 위하여, SIS와 DMD내의 다른 $n-1$개의 MD들과의 협력 작업을 시도한다. 본 논문에서는 다음과 같은 환경을 가정한다.

- SIS와 $MD_h(1 \le h \le n)$ 사이의 통신은 상호 인증된 채널이다.
- 사용자들은 DMD를 신뢰한다. 즉, DMD의 서비스 공개키를 이미 알고 있다.
- 제안되는 분산 보안 메일 시스템에서 사용되는 여러 가지 암호학적 기법은 안전하다고 가정한다.

제안되는 분산 보안 메일 시스템의 전반적인 동작 절차는 아래와 같다.

[Step-1] E-mail 전송 요청 : 메일 송신자는 메일 전송을 위한 암호학적 연산을 위한 요청을 DMD내의 어느 한 MD에게 전송한다.

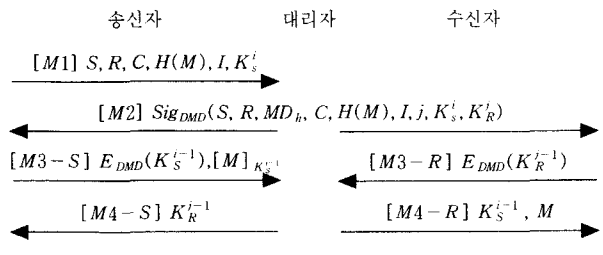
[Step-2] 사용자 정보 요청 : 메일 송신자의 요청을 수신한 MD는 메일 송신자를 위한 대리자가 된다. MD는 메일 송신자가 요청한 암호학적 연산을 위하여 필요한 정보를 SIS에게 요청을 한다.

[Step-3] 응답 : SIS는 메일 송신자에 대한 요청 정보를 응답으로 대리자에게 전송한다.

[Step-4] 임계 암호 연산 : 메일 송신자의 정보를 수신한 대리자는 암호학적 연산을 수행하기 위해서 $n-1$개의 MD에게 서명되어야 할 정보를 전송한다. 대리자는 $t+1$개의 MD로부터 유효한 암호학적 연산 값을 수신한 후에, DMD의 서비스 비밀키를 통한 연산 값을 생성한다.

[Step-5] 안전한 보안 메일 교환 : [Step 4]의 단계가 성공적으로 수행되면, 메일 송신자는 대리자 MD를 통하여 메일 수신자에게 안전하고, 송·수신 부인방지가 가능한 전자 메일을 전송할 수 있다.

3.2 기본 메일 전달 프로토콜



(그림 2) 기본 메일 전달 프로토콜

제안방안에서 사용되는 메일 전달 프로토콜의 시스템 초기화에 대한 가정사항은 다음과 같다. DMD의 서비스 비밀키는 전체 $n \ge 3t+1$개의 $MD_i(1 \le i \le n)$에게 비밀 분산되어서, 각 MD_i는 자신의 비밀 분배값으로 s_i를 소유하고 있다. (그림 2)는 메일 송·수신자와 단일 MD 사이의 기본 메일 전달 프로토콜을 보이고 있다.

[Step-0] 모든 사용자 X는 랜덤하게 생성한 값 K_X를 n번 해쉬한 값 $K_X^n = h_X^n(K_X)$를 SIS에게 제출하고, 신임장(Cre_X)을 발급 받는다. SIS는 모든 사용자 X의 신임장을 디렉토리 서비스(directory service)를 통하여 누구나 사용 가능하도록 만든다.

[Step-1] 송신자는 전송하고자 하는 메일 메시지 M의 해쉬값 $H(M)$를 생성한 후, $S, R, C, H(M), i, K_S^i$를 DMD내의 어느 한 MD_h, $(1 \le h \le n)$에게 전송한다. 즉, 기본 프로토콜의 [M1]을 전송한다.

[Step-2]

- 송신자로부터 [M1]을 수신한 MD_h는 대리자가 되어서, 수신한 현재 서명 키(K_S^i)를 송신자의 신임장 Cre_S내의 루트 서명키를 사용하여 검증한다.

$$h_S^{n-i}(K_S^i) = K_S^n$$

- 대리자는 사용자들의 candidate NRT를 생성하기 위해서, SIS로부터 수신자의 서명 카운터(j)와 현재 서명키(K_R^i)를 요청 및 수신을 한다. 그리고, candidate NRT를 위한 정보를 $S, R, MD_h, C, H(M), i, j, K_S^i, K_R^i$(아래에서는 간단히 α로 표기)와 같이 구성하여, $n-1$개의 $MD_{k \ne h}$, $1 \le k \le n$에게 멀티캐스트함으로써 서명 지원 요청을 한다. 대리자를 포함한 n개의 모든 MD_k, $1 \le k \le n$는 자신의 비밀 분배값인 s_k를 사용하여 부분 서명문(partial signature)인 $PS_{S_k}(\alpha)$를 계산하고, 대리자를 제외한 나머지 $n-1$개의 $MD_{k \ne h}$, $1 \le k \le n$들은 계산된 $PS_{S_k}(\alpha)$를 대리자에게 응답으로 전송한다.
- 대리자는 DMD의 서비스 비밀키의 서명을 생성하기 위해서는 자신의 부분 서명문을 포함한 최소한 $t+1$개의 MD_k로 부터의 올바른 부분 서명문이 필요하다. 따라서, 대리자는 $t+1$개의 부분 서명문를 선택하여 $Sig_{DMD}(\alpha)$를 계산한다. 만약, 계산된 $Sig_{DMD}(\alpha)$ 값이 무효하면 대리자는 또 다른 $t+1$개의 조합을 시도한다. 또 다른 방법으로, 참고문헌[13]에서 사용된 각 부분 서명문에 대한 "proof of correctness"를 사용함으로써, 각각의 수신된

부분 서명문의 유효성을 판단한 후에 전체 서명문 $Sig_{DMD}(\alpha)$를 계산할 수 있으며, 이는 적용되는 임계 암호시스템에 의존한다. 결국, candidate NRT인 $Sig_{DMD}(S, R, MD_h, C, H(M), i, j, K_S^i, K_R^j)$를 생성하여, 메일 송·수신자에게 [M2]를 전송한다.

[Step-3] 메일의 송·수신자는 수신된 [M2], candidate NRT, 에 대해서 각각 아래와 같이 동작한다.

- 메일 송신자

  송신자는 자신이 보낸 메시지에 대하여, DMD가 적절한 전자 서명을 하였는가를 확인한다. 검증이 성공하면, 송신자는 자신의 다음 서명키(K_S^{i-1})를 DMD의 서비스 공개키로 암호화하고, 메일 메시지 M을 다음 서명키로 암호화한 [M3-S]를 대리자에게 전송한다.

- 메일 수신자

  수신자는 [M2]내의 C를 보고, 자신이 대리자가 전달할 메일을 받고 싶을 경우 다음의 절차를 수행하며, 만약 수신을 원하지 않으면 프로토콜 수행을 종료한다. 만약, 수신자가 메일을 받고 싶을 경우에, 수신자는 [M2]에서 DMD의 서명을 검증한다. 위의 검증이 성공적인 경우, 수신자는 자신의 다음 서명키(K_R^{j-1})를 DMD의 서비스 공개키로 암호화한 정보인 [M3-R]을 대리자에게 전송한다.

[Step-4]

- 대리자는 DMD의 공개키로 암호화된 [M3-S]내의 $E_{DMD}(K_S^{i-1})$와 [M3-R]을 복호화하기 위하여, $E_{DMD}(K_S^{i-1})$, $E_{DMD}(K_R^{j-1})$를 DMD내의 다른 $n-1$개의 $MD_{k\neq h}$, $1 \le k \le n$들에게 멀티캐스트하여, DMD의 공개키로 암호화된 암호문을 복호화하기 위한 복호 지원 요청을 한다.
- 대리자를 포함한 n개의 모든 MD_k, $1 \le k \le n$는 자신의 분배값인 s_k를 사용하여 부분 복호문(partial decryption)인 $PD_{s_k}(K_S^{i-1})$, $PD_{s_k}(K_R^{j-1})$을 계산한다. 대리자를 제외한 나머지 $n-1$개의 $MD_{k\neq h}$, $1 \le k \le n$들은 계산된 $PD_{s_k}(K_S^{i-1})$, $PD_{s_k}(K_R^{j-1})$를 대리자에게 응답으로 전송한다. 또한, DMD내의 모든 n개의 MD_k, $1 \le k \le n$들은 각각의 계산된 $PD_{s_k}(K_S^{i-1})$, $PD_{s_k}(K_R^{j-1})$와 대리자 식별자(MD_h)를 분쟁 발생시의 해결을 위하여 SIS에게 전송하고, SIS는 수신한 정보를 분쟁 해결을 위하여 저장한다.
- 대리자는 DMD의 복호문을 생성하기 위해서는 자신의 부분 복호문을 포함한' 최소한 $t+1$개의 MD_k로 부터의 부분 복호문이 필요하다. 따라서, 대리자는 $t+1$개의 부분 복호문을 선택하여 최종적으로 K_S^{i-1}, K_R^{j-1}를 복호한다. 복호된 K_S^{i-1}을 사용하여 [M3-S]내의 $[M]_{K_S^i}$을 복호한다. 대리자는 복호된 K_S^{i-1}, K_R^{j-1}을 SIS에게 전송한다.
- SIS는 최소 $t+1$개의 MD_k, $1 \le k \le n$으로 부터 $PD_{s_k}(K_S^{i-1})$, $PD_{s_k}(K_R^{j-1})$와 대리자 식별자(MD_h)를 수신 받은 후에, 대리자로부터 수신 받은 송·수신자의 다음 서명키와 그 송·수신자의 신임장내의 루트 서명키를 사용하여

$$h_S^{n-i+1}(K_S^{i-1}) = K_S^n,\ h_S(K_S^{i-1}) = K_S^i$$
$$h_R^{n-j+1}(K_R^{j-1}) = K_R^n,\ h_R(K_R^{j-1}) = K_R^j$$

  임을 각각 검증한다.

  - 만약 위의 검증이 실패할 경우, SIS는 대리자에서 "메일 전달 실패"를 알리는 메시지를 전달한다.
  - 만약 위의 검증이 성공적이면, SIS는 송신자의 서명 카운터 i를 $i-1$로, 현재 서명키를 K_S^{i-1}로 대체한다. 또한 수신자의 서명 카운터 j를 $j-1$로, 현재 서명키를 K_R^{j-1}로 대체한다. 그리고, 대리자에게 "메일 전달 계속 진행"을 알리는 메시지를 전달하여, 프로토콜이 계속 수행되도록 지시한다.

[Step-5]

- 대리자가 SIS로부터 "메일 전달 계속 진행"을 나타내는 메시지를 수신할 경우, 대리자는 송신자에게 복호된 수신자의 다음 서명키 K_R^{j-1}인 [M4-S]를 전송한다. 또한, 수신자에게 송신자의 다음 서명키 K_S^{i-1}와 메일 메시지 M로 구성된 [M4-R]을 전송한다.
- 대리자가 SIS로부터 "메일 전달 실패"를 알리는 메시지를 수신할 경우, 프로토콜 진행을 중단한다.

[Step-6] 메일 송·수신자는 최종적으로 수신한 정보를 통하여 다음과 같이 검증 절차를 수행한다.

- 송신자는 "수신 받은 K_R^{j-1}가 candidate NRT내의 K_R^j값의 premiage인가?"를 검증한다. 만약, 위의 검정이 성공적일 경우 송신자는 수신자가 메일 수신에 대한 부인 방지를 못하도록 보장을 하는 NRT를 아래와 같이 얻게 된다.

$$Sig_{DMD}(S, R, MD_h, C, H(M), i, j, K_S^i, K_R^j), K_R^{j-1}$$

  최종적으로 자신의 서명 카운터 i를 $i-1$로 대체함으로써 K_S^i은 이미 사용되었다고 기록한다.

- 수신자 또한 "수신 받은 K_S^{i-1}이 candidate NRT내의 K_S^i 값의 preimage인가?"와 "수신 받은 M이 candidate NRT

내의 $H(M)$의 preimage인가?"를 검증한다. 만약, 이 두 검증이 성공적일 경우 수신자는 송신자가 메일 송신에 대한 부인 방지를 못하도록 보장하는 NRT를 아래와 같이 얻게 되며, 메시지를 정상적으로 수신한다.

$$Sig_{DMD}(S, R, MD_h, C, H(M), i, j, K_S^i, K_R^j), K_S^{i-1}$$

최종적으로 자신의 서명 카운터 j를 $j-1$로 대체함으로써 K_R^j은 이미 사용되었다고 기록한다.

만약, 송·수신자의 최종 검증에서 어느 한쪽이라도 문제가 발생하면, 분쟁이 발생한다. 분쟁 해결에 대한 것은 다음 절에서 언급한다.

제안 방안에서는 RSA 알고리즘을 기반한 임계 암호 시스템[12, 13]을 고려하여 설계되었다. 이산 대수에 기반한 임계 암호 시스템들은 부분 서명값을 생성하기 위해서는 랜덤수를 협상해야하는 부가적인 절차가 필요하기 때문이다[14, 15]. 본 논문의 최종 목적인 이동 사용자들의 계산적 오버헤드를 최소화하기 위하여, RSA 암호 알고리즘을 위한 DMD의 서비스 공개키는 아주 작은 수(예, $e=3$)를 사용할 것을 권한다. 작은 암호화 지수를 사용함으로써 발생되는 보안 취약점의 간단한 해결 방법은 참고문헌[16]에 기술되어져 있다. 위와 같은 작은 e값을 사용함으로써 사용자들은 대리자로부터 수신받은 NRT의 검증과 DMD의 서비스 공개키를 통한 암호화 작업시의 암호학적 연산에 따르는 오버헤드를 최소화 할 수 있다.

3.3 분쟁 해결

제안 방안은 메시지 전송에 대한 공정성 보장뿐만 아니라 인증, 무결성과 송·수신의 부인방지를 제공한다. 본 절에서는 제안되는 기본 메일 전달 프로토콜에서의 부인 또는 분쟁 발생시의 해결 방안에 대해서 분석한다.

[Dispute-1] 송신자가 자신이 전송한 메일에 대한 부인 행위를 할 때의 분쟁 해결

- 수신자는 NRT, $Sig_{DMD}(S, R, MD_h, C, H(M), i, j, K_S^i, K_R^j)$, K_S^{i-1},와 수신한 메시지 M을 중재자에게 제출한다. 중재자는 SIS와 협력하여 아래의 3가지 사항을 검증한다.
  ① "NRT에서 DMD의 서명의 유효한가?"
  ② "SIS내의 송신자의 현재 서명키와 NRT내의 다음 서명키가 동일한가?"
  ③ "수신된 메시지 M을 해쉬처리한 값은 NRT내의 $H(M)$과 동일한가?"
- 위의 어떠한 단계라도 실패하면, 중재자는 송신자의 정당성을 인정한다. 하지만, 위의 모든 검증 단계가 성공하면 송신자는 동일한 현재 서명키를 가지는 다른 NRT를 중재자에게 제시를 해야만, 중재자는 DMD가 공격자로부터 침해되었다고 판단한다. 만약, 송신자가 제시를 하지 못하면, 중재자는 송신자가 부정한 행위를 시도한 것으로 판단한다.

[Dispute-2] 송신자가 수신자의 메시지 수신 영수증을 의미하는 [M4-S]를 수신하지 못할 때

- 기본적으로 대리자($MD_h, 1 \le h \le n$)는 송·수신자로부터 [M3-S]와 [M3-R]을 수신한 상태에서 DMD의 서비스 비밀키를 통한 임계 복호화을 시도한다. 따라서, 임계 복호화를 수행하게 되면, DMD내의 모든 n개의 MD_k, $1 \le k \le n$들은 각각의 계산된 $PD_{s_k}(K_S^{i-1})$, $PD_{s_k}(K_R^{j-1})$와 대리자 식별자(MD_h)를 분쟁 발생시의 해결을 위하여 SIS에게 전송하게 된다. 따라서, 대리자는 임계 복호화 기록이 SIS에 남기 때문에 반드시 복호된 K_S^{i-1}, K_R^{j-1}을 SIS에게 전송해서 프로토콜 계속 진행 여부를 판단 받아야 한다. 따라서, SIS는 송신자에게 전달되지 않은 올바른 K_S^{i-1}값을 소유하게 된다.
- 송신자는 candidate NRT를 중재자에게 전송한다. 중재자는 아래의 사항을 검증한다.
  ① "NRT에서 DMD의 서명이 유효한가?"
  ② "SIS내에서 송신자의 현재 서명키는 candidate NRT내의 현재 서명키의 pre-image인가?"
- 위의 검증이 성공적이면, 중재자는 대리자(MD_h)가 침해되어서, 악의적으로 수신자의 다음 서명키 K_R^{j-1}를 전송하지 않은 것으로 간주한다. 따라서, 중재자는 SIS로부터 수신한 K_R^{j-1}를 송신자에게 전달한다.

[Dispute-3] 수신자가 송신자의 메시지 수신 영수증을 의미하는 [M4-R]를 수신하지 못할 때

- 기본적인 분쟁 해결 방안은 [Dispute-2]의 경우와 유사하다. 수신자가 정당할 경우 중재자는 송신자 또는 침해된 대리자(MD_h)에게 $[MD]_{K_S^{i-1}}$의 제출 요구를 한다.

[Dispute-4] 송신자와 대리자의 공모 또는 수신자와 대리자의 공모를 통한 공정한 교환의 실패

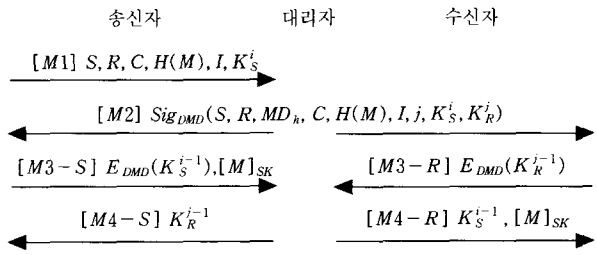
- 제안 프로토콜에서는 최소한 $t+1$개의 MD들이 침해되었을 때, 송·수신 메시지에 대한 위조 및 공모로 인한 공정한 교환 실패를 유도시킬 수 있다.
- 송신자와 대리자 공모 공격의 예
  - 만약 송신자와 대리자가 공모를 하여, 송신자가 [M3-S]에서 암호화된 메시지 $[M]_{K_S^{i-1}}$을 전송하지 않는다.

대리자는 정상적으로 $E_{DMD}(K_S^{i-1})$를 복호화하기 위한 임계 복호화를 수행한다. 대리자는 송신자에게는 [M4-S]를 전송하고, 수신자에게 [M4-R]로서 복호화된 K_S^{i-1}만 전송하거나, [M4-R] 자체를 전송하지 않는다. 이와 같은 경우는 수신자가 메일 메시지 M을 수신 받지 못함으로써 분쟁이 발생된다. 결과적으로, 송신자는 $[M]_{K_S^{i-1}}$을 전송하지 않았음에도 불구하고, 수신자가 성공적으로 메일 메시지를 수신한 증거인 NRT를 소유하게 된다.

- 기본 프로토콜의 [Step-6]의 검증절차에 따라서 수신자는 메일 메시지 수신을 못한것에 대한 분쟁요청을 하게 되며, 이러한 분쟁 발생시 [Dispute-2], [Dispute-3]와 동일하게 처리가 가능하다.

3.4 메일 메시지 기밀성을 위한 방안

기본 메일 전달 프로토콜은 전송하고자 하는 메일에 대한 기밀성을 제공하지 못하고 있다. 따라서, 본 절에서는 메일 메시지에 기밀성을 추가하는 방안에 대해서 살펴본다. 본 논문에서는 이동 장치의 계산량적 오버헤드를 고려하여, 기초적인 DH 키 교환 방법에 의한 메시지 기밀성을 보장하고자 한다. (그림 3)은 기밀성이 강화된 프로토콜을 보여주고 있으며, 기존의 기본 메일 전달 프로토콜에서 변경된 부분에 대해서만 설명하겠다.



(그림 3) 기밀성 강화 프로토콜

[Step-0]

SIS는 큰 소수 p를 선정하고 Z_p 상에서 원시 원소 g를 찾아서 p와 g를 사용자들에게 공개한다. 모든 사용자 X는 DH 키쌍을 생성하기 위하여, 자신의 비밀 정보 $x \in_{RZ_{p-1}}$를 선정하여 공개 정보 $y = g^x \bmod p$를 계산한다. 그리고, 모든 사용자 X는 랜덤하게 생성한 값 K_X를 n번 해쉬한 값 $K_X^n = h_X^n(K_X)$을 계산한다. 모든 사용자 X는 생성한 K_X^n과 y값을 SIS에게 제출하여, 신임장(credential)을 아래와 같이 발급 받는다.

$$Cre_X = Sig_{SIS}(X, n, K_S^n, y, SIS)$$

이번 장에서 사용되는 추가적인 용어은 아래와 같다.

- x_i : 사용자 i의 DH 비밀키
- y_i : 사용자 i의 DH 공개키. 즉, $y_i = g^{x_i} \bmod p$.
- T_i : 사용자 i의 로컬 타임 스탬프값

[Step-1] 송신자는 전송하고자 하는 메시지 M의 해쉬값 $H(M)$를 생성하고, 로컬 시스템의 클럭을 기초로 한 타임스탬프 값(T_S)을 생성하여, 기밀성 강화 프로토콜의 [M1]을 DMD내의 어느 한 MD에게 전송한다.

[Step-3] [M2]를 수신한 메일의 송신자는 자신이 보낸 메시지에 대하여, DMD가 적절한 전자 서명을 하였는가를 확인한다. 검증이 성공하면, 수신자의 신임장내의 DH 공개키($y_R = g^{x_R} \bmod p$), 자신의 DH 비밀키(x_S), T_S 값을 사용하여 메일 메시지 암호화를 위한 세션키(SK)를 아래와 같이 계산한다.

$$SK = H(y_R^{X_S \cdot T_S} \bmod p) = H(g^{X_R \cdot X_S \cdot T_S} \bmod p)$$

송신자는 자신의 다음 서명키 K_S^{i-1}를 DMD의 서비스 공개키로 암호화하고, 메일 메시지 M을 계산된 세션키(SK)로 암호화하여 [M3-S]를 대리자에게 전송한다.

[Step-4] & [Step-5] 대리자는 수신된 [M3-S]에서 세션키(SK)로서 암호화된 메일 메시지를 복호화할 수 없다. SIS로부터 "메일 전달 계속 진행"을 수신했을 때, 대리자는 송신자에게 [M4-S]를 전송하고, 수신자에게는 K_S^{i-1}, $[M]_{SK}$로 구성된 [M4-R]을 전송한다.

[Step-6] 수신자는 "수신 받은 K_S^{i-1}이 candidate NRT내의 K_S^i값의 preimage인가?"를 검사한다. 그리고, 송신자의 신임장내의 DH 공개키($y_S = g^{x_S} \bmod p$), 자신의 DH s비밀키(x^R), T_S값을 사용하여 메일 메시지 암호화를 위한 세션키(SK)를 아래와 같이 계산한다.

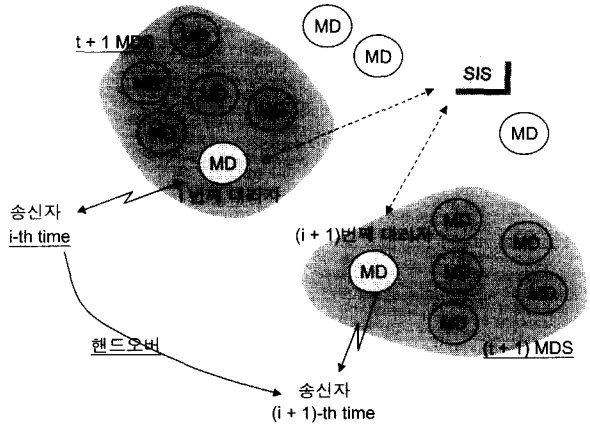
$$SK = H(y_S^{X_R \cdot T_S} \bmod p) = H(g^{X_S \cdot X_R \cdot T_S} \bmod p)$$

계산된 세션키(SK)로서 암호화된 메일 메시지 $[M]_{SK}$를 복호화 한다. 그리고, "M이 candidate NRT내의 $H(M)$의 preimage인가?"를 검증한다. 만약, 이 두 검증이 성공적일 경우 수신자는 송신자가 메일 송신에 대한 부인 방지를 못하도록 보장

하는 NRT를 얻게되고, 메일 메시지를 성상적으로 수신한다.

4. 이동 A사용자를 위한 제안 기법 적용

기존의 셀룰러 폰과 같은 환경에서 제안 논문에서의 MD는 셀영역 내의 기지국에서 그 역할을 수행할 수 있을 것이다. 그리고, 기존의 CDMA와 GSM과 같은 기술에서 보안 프레임워크 및 핸드오버에 따른 사용자 인증 및 전달 메시지 기밀성에 대한 명세서와 표준이 이미 개발된 상태이다. 본 논문은 언급된 하위 계층의 보안 프레임워크를 가정한 환경에서 제안 방안 수행에 필요한 상위 계층의 프로토콜만으로 구성되어 있다. 따라서, 본 논문의 3장에서 소개된 제안 프로토콜은 사용자 장치와 기지국간의 인증 및 핸드오버를 위한 메시지 교환에 대해서는 고려하지 않는다.



(그림 4) 이동 사용자를 위한 지원

(그림 4)는 제안 방안이 이동 사용자들의 보안 메일 전송을 지원하기 위한 간략한 개념도를 보여주고 있다. 이동 사용자는 일반적인 셀룰러 폰, PDA와 같은 낮은 컴퓨팅 파워와 배터리를 소유하고 있는 사용자를 의미한다. 보안 메일을 전송하기를 원하는 이동 사용자는 자신이 현재 위치하는 지역에서 가장 가까운 DMD내의 어느 한 MD에 접속하여 보안 메일 전송을 위한 지원을 요청을 하고, 3장에서 기술한 방식으로 보안 메일 전송을 위한 서비스를 받는다. 이동 사용자가 이전에 접속한 MD의 서비스 영역을 떠나 새로운 지역으로 들어가게 되면, 또 다시 자신이 위치하고 있는 지역의 가장 가까운 DMD내의 어느 한 MD에게 보안 메일 전송을 위한 지원을 요청할 수 있다. 따라서, 보안 메일을 전송하기를 원하는 이동 사용자의 대리자는 대부분이 시간적으로 가까운 지역에 존재하는 다른 MD들로부터의 부분 서명문 또는 부분 복호문의 결과를 수신 받을 것이다. 이는 MD 서버들간의 통신상의 효율성 증대를 기대할 수 있으며, 제안 방안에 대하여 이동 사용자에 대한 시스템 적용은 기지국을 MD 서버의 역할을 하게 함으로써 간편하게 이루어질 수 있다.

5. 제안 시스템의 보안평가

본 논문에서 제안하는 방안은 이동 사용자를 위하여 공정성을 제공하는 certified e-mail 서비스를 수행하기 위하여 최적화되었다. 또한, 제안방안의 전체적인 보안성은 DMD의 서비스 비밀키의 보안과 직결된다. 따라서, DMD는 pro-active secret sharing을 사용하여 각 MD들의 공유값을 주기적으로 갱신함으로써 이동 공격자들로 부터의 DMD를 보다 강건하게 만들 수 있다[17, 18]. 또한, 서비스 거부 공격에 대한 기본적인 해결책은 참고 문헌[13]에서 소개된 방안이 적용 가능하다.

제안 방안은 아래와 같은 2.3절에서 정의한 certified e-mail의 기본요구사항을 제공하며, 3.3절에 기술한 바와 같이 신뢰할 수 있는 분쟁해결 방안을 제공한다. 제안 방안에서 제공 가능한 보안 서비스는 아래와 같다.

- 공정성 : 본 논문에서 사용하는 서버 지원된 서명 기업은 서명 지원을 하는 DMD가 정직할 경우, 메일 송·수신의 공정한 교환은 제공된다.
- 인증 : 송·수신자는 메시지 전송시에 DMD가 서명한 NRT와 신임장을 통해서 상호 인증이 가능하다.
- 기밀성 : 기밀성이 요구되는 메일 메시지는 계산된 세션키를 사용하여 암호화된다. 위의 세션키는 송·수신자의 DH키쌍과 송신자의 타임스탬프을 통하여 계산되며, 이 세션키는 송·수신자만 계산 가능하다.
- 무결성 : 송신자는 메시지의 해쉬값과 수신자의 식별자를 DMD를 통해서 전자서명한다. 만약, 제 3자가 전송내용을 위조한다면 이는 쉽게 발견된다.
- 부인방지 : 메일 교환에 사용되는 NRT를 통해서 프로토콜 종결후 메일 송·수신의 부인 방지가 가능하다.
- 악위적인 단독 MD에 의한 공격 : 단독 MD는 NRT의 위조 또는 전달 메시지의 삭제를 통한 공격은 성공하지 못한다.
- 악위적인 단독 MD와 송신자(또는 수신자)간의 공모에 의한 공격 : 이 공격이 성공하기 위해서는 송신자(또는 수신자)는 최소한 t + 1개의 MD들과 공모해야 한다.
- 빠른 취소(Fast revocation) : 본 장에서 언급하는 취소는 X.509 인증서에 대한 취소가 아니라, 사용자들의 서명 능력에 대한 취소를 의미한다. 만일, 사용자가 자신의 서명키가 누출되었다고 생각하거나, SIS에서 그 사용자의 서

명키가 누출되었다고 판단 되었을 때, 즉시적으로 SIS에서 사용자 관련 신임장를 디렉토리 서비스에서 삭제함으로써 DMD가 앞으로 사용자를 대신하여 서명을 하지 않도록 할 수 있다.

- 좀 더 강한 서명(More secure signature) : DMD가 RSA를 위한 키 생성 및 전자 서명 연산을 수행하기 때문에, 사용자들의 계산량 오버헤드에 대한 부담없이 DMD내의 서버들의 능력에 따라서 좀 더 강한 RSA 키를 사용하는 것이 가능하다.

6. 결 론

본 논문에서는 메일 사용자의 오버헤드를 최소화하고 시스템 전체의 기밀성을 분산시킨 새로운 certified e-mail system을 제안하였다.

제안 시스템은 전달 메시지의 공정성 및 기밀성 보장을 위하여 전통적인 암호기법과 함께 서버 지원된 서명 방안을 사용함으로써, 메일 사용자의 공개키 암호 알고리즘 연산에 따른 오버헤드를 최소화하며, 비밀 분산을 통한 이동 공격자 또는 공모 공격으로 부터 강건한 시스템을 설계하였다. 따라서, 제안 방안은 셀룰러 폰이나 무선 PDA와 같은 이동 장치를 통한 보안 메일 전송에 적합하다.

참 고 문 헌

[1] M. Franklin and M. Reiter, "Fair exchange with a semi-trusted third party," In Proc. ACM Conference on Computer and Communications Security, 1997.

[2] William Stallings, "CRYPTOGRAPHY AND NETWORK SECURITY : Principles and Practice," Second Edition, Prentice-Hall.

[3] Kenji Imamoto, Kouichi Sakurai, "A Certified E-mail System with Receiver's Selective Usage of Delivery Authority," INDOCRYPT 2002, LNCS 2551, 2002.

[4] G. Ateniese, B. D. Medeiros and M. T. Goodrich. "TRICERT : A Distributed Certified E-Mail Scheme," In ISOC 2001 Network and Distributed System Security Symposium (NDSS '01), San Diego, CA, USA, Feb., 2001.

[5] J. Zhou and D. Gollmann, "Certified electronic mail," In Computer Security-ESORICS '96 Proceedings, pp.55-61. Springer Verlag, 1996.

[6] B. Schneier and J. Riordan, "A certified e-mail protocol," 13th Annual Computer Security Applications Conference, pp.100-106, Dec., 1998.

[7] N. Asokan, G. Tsudic, M. Waidner, "Server Supported Signatures," European Symposium on Research in Computer Security, September, 1996.

[8] X. Ding, D. Mazzocchi and G. Tsudik, "Experimenting with Server-Aided Signatures," 2002 Network and Distributed Systems Security Symposium (NDSS '02), February, 2002.

[9] D. Malkhi and M. Reiter, "Byzantine quorum systems," Distributed Computing, 11(4), pp.203-213, 1998.

[10] A. De Santis, Y. Desmedt, Y. Frankel and M. Yung, "How to share a function securely," In Proceedings of the 26th ACM Symposium on the Theory of Computing, Santa Fe, pp.522-533, 1994.

[11] P. Gemmel, "An introduction to threshold cryptography," in CryptoBytes, a technical newsletter of RSA Lab. Vol. 2, No.7, 1997.

[12] R. Gennaro, S. Jarecki, H. Krawczyk and T. Rabin, "Robust and efficient sharing of RSA functions," In Advances in Cryptology-Crypto '96, LNCS 1109, pp.157-172, 1996

[13] Victor Shoup, "Practical threshold signatures," in Proc. Eurocrypt, 2000.

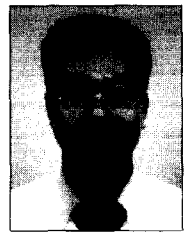
[14] L. Harn, "Group oriented (n, t) digital signature scheme," IEE Proceedings-Computer and Digital Techniques, 141 (5), pp.307-313, September, 1994

[15] M. Cerecedo, T. Matsumoto, H. Imai, "Efficient and secure multiparty generation of digital signatures based on discret logarithms," IEICE Transactions on Fundamentals of Electronics, Information and Communication Engineers, April, 1993.

[16] Alfred, J. Menezes, Paul, C. van Oorshot, Scoot, A. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1997.

[17] A. Herzberg, S. Jarechi, H. Krawczyk and M. Yung "Proactive secret sharing or : How to cope with perpetual leakage," Advances in Cryptology-Crypto '95, the 15th Annual International Cryptology Conference, Proceedings, volumn 963 of LNCS, pp.457-469.

[18] S. Jarecki, "Proactive Secret Sharing and Public Key Cryptosystems," Master thesis, MIT, 1996.



양 종 필

e-mail : bogus@mail1.pknu.ac.kr

1999년 부경대학교 전자계산학과(학사)

2001년 부경대학교 대학원 전자계산학과 (석사)

2002년 부경대학교 대학원 전자계산학과 박사과정

관심분야 : 비밀 분산, 공개키 기반 구조, 인터넷 보안 프로토콜 등

서 철

e-mail : kahlil@mail1.pknu.ac.kr

2000년 부경대학교 전자계산학과(학사)

2001년 부경대학교 대학원 전자계산학과 석사과정

관심분야 : 공개키 기반 구조 응용

이 경 현

e-mail : khrhee@pknu.ac.kr

1978년~1982년 경북대학교 사범대학 수학교육과(이학사)

1983년~1985년 한국과학기술원(KAIST) 응용수학과(이학석사)

1988년~1992년 한국과학기술원(KAIST) 수학과(이학박사)

1985년~1991년 한국전자통신 연구소(ETRI) 연구원

1991년~1993년 한국전자통신 연구소(ETRI) 선임연구원

1993년~1995년 부산수산대학교 전자계산학과 전임강사

1995년~1996년 호주 Adelaide대학 응용수학과 교환교수

1995년~1999년 부경대학교 전자계산학과 조교수

1999년 일본 동경대학 생산기술연구소 객원연구원

1999년~2000년 부경대학교 컴퓨터멀티미디어공학부 부교수

1997년~현재 한국멀티미디어학회 논문편집위원

1997년~현재 한국멀티미디어학회 학술이사, 운영위원

1999년~현재 (주)인트빔 기술고문

1999년~현재 (주)아시아 디자인 기술고문

2000년~현재 한국통신정보보호학회 영남지부 감사

2000년~현재 부경대학교 전자컴퓨터멀티미디어공학부 부교수

관심분야 : 컴퓨터보안, 정보보호론, 네트워크성능 평가, 광대역 통신망, 암호학, 대기체계