중재자를 이용한 ID기반 전자서명과 키 업데이팅 전자서명 기법

주 학 수[†] · 김 대 엽[††]

요 약

공개키기반구조에서 공개키 인증서의 효율적 폐지방법은 가장 중요한 연구 분야 중 하나이다. 2001년 Boneh et al.는 RSA 기반 암호시스템에서 사용자의 공개키 인증서를 즉각적으로 폐지할 수 있는 mediated RSA 기법을 제안하였다. 기본 mediated RSA 구조는 SEcurity Mediator (SEM)이라는 중재자를 이용하는 것으로, 사용자가 메시지에 서명 혹은 복호화 연산을 수행하기 위해서는 중재자로부터 토큰을 먼저 얻어야만 한다. 즉, 사용자의 공개키 인증서가 유효하지 않으면 중재자인 SEM은 토큰발행을 중지함으로써 즉각적으로 사용자의 서명 능력 혹은 복호화 능력을 폐지시킬 수 있게 된다. 최근 Libert와 Quisquater는 mediated RSA의 SEM 구조를 이용한 즉각적인 폐지기법이 Boneh-Franklin의 ID 기반 암호기법과 GDH그룹에 기반한 전자서명에도 적용될 수 있다는 것을 보였다. 이 논문에서는 먼저 안전한 ID기반 전자서명(IBS)에 SEM의 구조가 적용된 중재자를 이용한 ID기반 전자서명기법, mIBS를 제안한다. 제안한 기법은 여러 서명값들을 한 번에 검증할 수 있는 배치검증 성질을 유지하게 된다. 또한, Libert와 Quisquater가 제안한 GDH그룹에 기반한 전자서명기법은 개인키의 노출 시 이전 서명값에 대한 위조가 가능하게 되는 순방향 안전성이 보장되지 않는다. 이에, 제안된 mIBS에 기반하여 중재자 기반의 키 업데이팅 전자서명 기법인 mKUS를 설계함으로써 순방향 안전성을 제공하였다.

키워드 : 전자서명, 중재자, 전방향 안전성

Mediated ID based signature scheme and key updating signature scheme

Ju Hak Soo[†] · Kim Dae Youb[††]

ABSTRACT

Revocation is one of the main difficulties faced in implementing Public Key Infrastructures (PKIs). Boneh, Ding and Tsudik first introduced a mediated cryptography for obtaining immediate revocation of RSA keys used in PKIs. Their method is based on the idea that each user's private key can be split into two random shares, one of which is given to the user and the other to an online security mediator (SEM). Thus any signature or decryption must be performed as a cooperation between a user and his/her associated SEM and revocation is achieved by instructing the mediator SEM to stop cooperating the user. Recently, Libert and Quisquater showed that the fast revocation method using a SEcurity Mediator(SEM) in a mRSA can be applied to the Boneh-Franklin identity based encryption and GDH signature schemes. In this paper we propose a mediated identity based signature (mIBS) with batch verification which apply the SEM architecture to an identity based signature. Libert's GDH siganture scheme is not forward secure even though forward security is an important and desirable feature for signature schemes. We propose an efficient key udating mediated signature scheme, mKUS based on mIBS and analyze its security and efficiency.

Key Words : Digital Signature, Mediator, Forward Security

1. 개 요

공개키기반구조에서 공개키 인증서의 효율적 폐지방법은 가장 중요한 연구분야 중 하나이다. 2001년 Boneh et al.는 RSA 기반 암호시스템에서 사용자의 공개키 인증서를 쉽게 폐지할 수 있는 mediated RSA (mRSA) 기법을 제안하였다. 기본 mRSA구조는 온라인 서버인 중재자 SEM (SEcurity Mediator)을 이용하는 것으로, 사용자가 메시지에 서명 혹은 복호화 연산을 수행하기 위해서는 중재자로부터 토큰을 먼저 얻어야만 한다. 즉, 이러한 토큰을 얻을 수 없으면 사용자는 서명 혹은 복호화연산을 수행할 수 없게 된다. 사용자의 공개키 인증서가 유효하지 않으면 중재자인 SEM은 토큰발행을 중지함으로써 즉각적으로 사용자의 서명 능력 혹은 복호화 능력을 폐지시킬 수 있게 된다. 이와 같이 중재자인 SEM의 구조를 이용하는 것은 다음

† 종신회원 : 삼성전자 DM연구소 책임연구원
†† 종신회원 : 삼성종합기술원 CNL. 전문연구원
논문접수 : 2007년 2월 7일, 심사완료 : 2007년 8월 28일

과 같은 이점을 제공한다[1].

○ 서명자의 즉각적인 폐지 : 현재 공개키 기반구조에서 인증서의 검증을 위해 많이 사용되고 있는 인증서 폐지목록(CRLs: Certificate Revocation Lists)을 이용하는 방법과 온라인 상태 검증 프로토콜 등의 방식에서는 유효하지 않은 인증서를 갖고 있는 서명자도 서명문을 생성할 수 있다. 이와 달리, 중재자를 기반한 방식은 서명자의 인증서가 유효하지 않으면 토큰 생성을 중지하여 서명문을 생성할 수 없게 함으로써 서명자의 서명기능이 즉각적으로 폐지된다.

○ 단순화된 전자서명 검증 : 중재자가 전자서명에 사용된 인증서의 유효성을 사전에 체크하기 때문에, 검증자는 온라인 상태 검증 프로토콜(OCSP : Online Certificate Status Protocol) 등을 통해 서명자의 인증서 검증절차를 수행할 필요가 없게 된다.

○ 전자서명의 시점확인기능 : 전자서명의 시점확인기능이란 전자서명을 생성하는데 사용된 개인키와 관련된 공개키 인증서가 서명이 발행되는 시점에 유효할 때만 전자서명이 유효하다는 특성을 말한다. 검증자는 서명자가 생성한 서명을 검증할 때마다 서명자의 인증서가 서명이 생성되는 시점에 유효하였다는 것을 검증해야만 하기 때문에, 현재 존재하는 폐지기법에서 이 성질을 제공하는 것은 복잡하다. 그러나 중재자를 이용하면 검증자는 서명값을 검증하기 위해 단지 서명 자체만을 검증하면 된다.

공개키 기반구조에 비해 ID기반 암호시스템을 이용하면 키 관리문제가 훨씬 쉬어진다. ID기반 암호시스템의 기본 개념은 Shamir가 1984년에 처음 제안한 것으로 공개키 인증서를 이용하는 대신 사용자의 이메일, 전화번호 등을 이용하여 공개키를 생성하는 방법이다. 이는 공개키를 관리하는 공개키 디렉토리를 없애 키 관리를 훨씬 단순하게 하는 이점을 제공한다. 1984년 이후로 현재 많은 ID기반 암호시스템들이 제안되었으며[2,3,4], ID기반 암호시스템에서의 폐지문제는 [5,6]에서 언급되었다. [5]에서 Ding과 Tsudik은 mRSA의 즉각적인 폐지기능 및 ID기반 시스템의 이점을 결합한 ID 기반 mediated RSA(IB-mRSA)를 제안하였다.

2003년 Libert와 Quisquater는 이러한 중재자를 이용하는 구조가 ID기반 암호시스템과 GDH그룹에 기반한 전자서명에도 적용될 수 있음을 보였다[6]. 그러나 ID기반 전자서명에서 사용자의 서명능력(security capability)를 즉각적으로 폐지할 수 있는 방법은 제안되지 않았다.

한편, 전자서명기법에서 순방향 안전성 등 개인키의 노출 위험에 대해 피해를 최소화하기 위한 안전성은 만족해야 할 중요한 성질 중 하나이다. 순방향 안전성의 개념은 Anderson[7]이 처음 제안한 개념으로 현재 사용중인 개인키가 노출 및 공격되더라도 노출되기 이전에 서명된 서명문에 대한 안전성을 보장하는 것을 목적으로 하고 있다. 최근에는 임의의 전자서명 기법을 순방향 안전성을 만족하도록 하는 기법과 순방향 안전성을 만족하도록 특수한 전자서명 기법을 변형한 방법들이 제안되고 있다. 또한, 순방향 안전성의 개념이 확장된 키 업데이팅 암호시스템인 Key insulated 암호시스템[8]과 Intrusion Resilient 암호시스템[9]들이 제안되고 있다. 2002년 Tsudik은 약한 순방향 안전성을 갖는 mRSA기법[10]을 소개하였다. Tsudik의 기법은 서명에 사용자나 SEM의 비밀키 중 하나만 유출되었을 경우에 순방향 안전성을 보장한다는 의미에서 약한 순방향 안전성을 갖는다고 할 수 있다. 또한, Libert와 Quisquater[6]가 제안한 중재자 기반의 GDH 전자서명 기법은 개인키의 노출 시 이전 서명값들에 대한 위조가 가능함으로써 순방향 안전성이 보장되지 않는다.

이 논문에서는 먼저 안전한 ID기반 전자서명(IBS)에 중재자의 구조가 적용된 ID기반 전자서명기법, mIBS를 제안한다. 중재자인 SEM을 이용하는 것은 현재 제시된 ID기반 전자서명의 폐지기법에 비해 단순화된 서명의 검증, 효율적인 ID의 폐지, 서명 능력에 대한 즉각적인 폐지와 같은 이점을 제공한다. 또한, mIBS는 여러 서명값들을 한 번에 검증할 수 있는 배치검증을 가능하게 한다. 그리고, mIBS에 기반하여 순방향 안전성을 제공해 줄 수 있는 키 업데이팅 전자서명기법, mKUS를 제안하고 제안된 기법에 대한 안전성 및 효율성을 분석한다. 키 업데이팅 전자서명 기법에서 사용자의 서명 능력에 대한 폐지 및 제어할 수 있는 방법은 중요하다. 단위시간 i가 짧은 경우, 예를 들어 1분, 1시간에는 이러한 폐지 및 제어능력은 필요 없을 지도 모르지만 단위시간 i가 하루, 한 달, 1년 등 충분히 긴 시간이라면 사용자의 서명능력을 즉각적으로 폐지할 수 있는 방법이 꼭 필요하다. mKUS는 순방향 안전성이 보장되는 mediated GDH 전자서명이며 단위시간 i 동안의 서명능력에 대한 즉각적인 폐지 등 여러 이점을 제공한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 mediated GDH 전자서명기법과 키 업데이팅 전자서명기법 KUS에 대해 설명한다. 3장에서는 IBS에 SEM의 구조를 적용한 mIBS를 제안하고 안전성 및 효율성을 분석한다. 또한, mIBS를 기반으로 설계할 수 있는 mKUS를 제안하고 안전성 및 효율성을 분석한다. 마지막 4장에서 결론과 향후 연구방향에 대해 서술한다.

2. 기존 연구의 고찰

2.1 mGHDS: mediated GDH Signature scheme

mRSA처럼 Libert와 Quisquater[6]가 제안한 mediated GDH 전자서명기법은 사용자의 서명능력에 대한 즉각적인

폐지기능을 제공할 수 있는 단순하고 효율적인 방법이다. 제안된 기법은 사용자의 개인키를 두 개로 분할하여 하나의 분할값은 사용자에게 다른 하나는 중재자인 SEM에게 전달하여 사용자와 SEM이 협력할 때만 자신들의 분할키를 이용하여 메시지에 대한 서명값을 생성할 수 있다. 서명생성 및 검증과정은 Boneh, Lynn와 Ghacham[3]이 제안한 Computational Diffie Hellman문제는 어렵지만 Decisional Diffie Hellman문제는 쉬운 그룹 Gap Diffie Hellman (GDH) 그룹에 기반하고 있으며, 전체 전자서명 과정은 다음과 같다.

○ 키생성 : 신뢰기관 TA는 위수가 q인 그룹 G에 대한 생성자 P를 선택한다. 사용자 U의 키를 생성하기 위해 TA는 랜덤 수 $x_{sem}, x_u \in Z_q^*$를 선택한다. x_{sem}를 SEM에게 x_u를 사용자에게 전달하고 $R=(x_{sem}+x_u)P \in G_1$을 계산한다. 사용자의 공개키 정보는 (q, P, R)이 된다.

○ 서명 : 메시지 m에 서명하기 위해 사용자는 SEM에게 먼저 $h(m) \in G_1$를 전달한다. 그 후 사용자와 SEM은 다음과 같은 연산을 수행한다.

- SEM : 1. 사용자 U가 폐지된 사용자인지 체크한다. 폐지된 사용자라면 프로토콜을 중지한다.
  2. 폐지된 사용자가 아니라면, $S_{sem}=x_{sem}h(m)$을 계산하여 사용자에게 전달한다.
- User : 1. 사용자는 $S_u=x_u h(m)$을 계산한다.
  2. SEM으로부터 S_{sem}을 받아 $S=S_{sem}+S_u$를 계산한다.
  3. S가 메시지 m에 대한 유효한 서명인지 검증해보고 검증이 성립하면 서명쌍 (m, S)을 출력한다.

○ 검증 : 검증자는 $h(m)$을 계산하고 $e(P,S)=e(R, h(m))$이 성립하는지 체킹함으로서 $(P, R, h(m), S)$이 유효한 Diffie Hellman (DH)쌍인지 검증한다.

2.2 KUS : Key Updating Signature scheme

키 업데이팅 전자서명기법[8]은 Dodis, Katz, Xu와 Yung에 의해 처음 제안된 안전성 개념으로 순방향 안전성 개념의 확장이라 할 수 있다. 순방향 안전성의 경우, 공격자가 개인키 노출 이전의 메시지에 대한 서명을 위조할 수 없게 하는 반면, 키 업데이팅 전자서명의 경우, 개인키 노출 이전과 이후의 메시지에 대한 서명을 위조할 수 없게 한다. 키 업데이팅 전자서명 기법에서는 물리적 보안능력이 보장되는 하나의 디바이스를 가정한다. 즉 디바이스에 저장된 데이터는 노출되지 않는다는 것을 가정하고 디바이스의 계산능력은 제한되어 있다는 것을 가정한다. 각 제안된 방식들은 시스템의 생명주기 동안 공격자에 의해 노출 및 공격될 수 있는 안전하지 않은 장소에 저장된 키들이 노출되었을 경우, 그 피해를 최소화할 수 있는 방법들을 제안한다.

사용자는 공개키 pk를 등록하고 pk와 함께 생성된 마스터 개인키 hsk는 물리적으로 보호되는 안전한 디바이스에 저장한다. 그러나, 모든 전자서명 생성은 키의 노출이 일어날 수 있는 안전하지 않은 장소, 사용자의 PC 등에서 수행된다. 전체 시간은 단위 시간 1,2,...,N으로 구분되고 단위시간 i의 시작시점에 사용자는 단위시간 동안 메시지에 대한 서명을 생성하는데 사용할 일시적인 서명 개인키 usk_i를 갱신하기 위해 디바이스와의 통신을 수행하여야 한다.

정의1. 키 업데이팅 전자서명 기법 KUS=(KG, HKU, UKU, Sign, Vrfy)는 다음과 같은 다섯 개의 알고리즘으로 구성된다.

- KG: 랜덤화된 키 생성 알고리즘 KG는 입력으로 안전성 매개변수 k로 하여 (pk, usk_0, hsk)을 출력한다. 여기서 pk는 사용자의 공개키 및 공개키 매개변수를 의미하며, usk_0는 초기단계의 사용자 비밀키, hsk는 디바이스의 마스터키이다. 사용자가 pk, usk_0로 초기화되는 반면 디바이스는 pk, hsk로 초기화된다.
- HKU: $i \geq 1$단계의 시작시점에 디바이스는 i단계의 자신의 키 hsk_i를 얻기 위해 디바이스 키 업데이트 알고리즘 HKU을 i, pk, hsk를 입력으로 수행한다.
- UKU: $i \geq 1$단계의 시작시점에 사용자는 디바이스로부터 hsk_i를 받아 i, pk, hsk_i, usk_{i-1}를 입력으로 하여 UKU를 수행함으로써 i단계의 사용자 비밀키 usk_i를 얻는다. 그리고 나서 이전 비밀키 usk_{i-1}을 삭제한다.
- Sign: 서명자는 현 단계 i, 메시지 $m \in \{0,1\}^*$, 자신의 비밀키 usk_{i-1} 에 랜덤화된 암호알고리즘 Sign을 적용하여 i단계의 서명값 σ를 생성한다.
- Vrfy: i단계에 검증자는 i, pk, σ, m을 입력으로 검증알고리즘 Vrfy를 수행하여 b를 출력한다. b가 1이면 서명이 올바르게 검증되었음을 의미하고 0이면 검증 실패를 의미한다.

일시적인 개인키 usk_i가 저장되는 디바이스는 키 노출에 취약하기 때문에 t(<N)의 단위시간에 해당되는 개인키들이 노출되더라도 그에 따른 피해를 최소화하는 것을 목적으로 하고 있다. 즉 디바이스를 공격한 공격자는 자신이 선택한 t개의 단위시간에 해당되는 개인키들을 얻어낼 수 있지만 나머지 시간에 해당되는 N-t시간동안의 개인키 정보를 알아낼 수 없도록 설계한 방식이라 할 수 있다. 이러한 개념을 (t, N) key insulated라고 정의한다[8]. 또한, 순방향 안전성과 달리 key insulated 기법은 임시 키 usk_i가 갱신될 때 i번째 임시키 usk_i에서 $i+1$번째 임시키 usk_{i+1}로 순차적으로 갱신되는 방식이 아닌 i번째 임시 키 usk_i가 임의의 j번

째 임시 키 usk_j로 랜덤하게 갱신되는 랜덤 갱신방법을 지원한다.

3. 제안방식

3.1 mIBS : mediated Identity Based Signature scheme

ID기반 전자서명, IBS에서 폐지기능을 제공할 수 있는 방법은 ID에 일정기간을 연접하는 방법을 사용할 수 있다. 이는 서명자가 일정기간동안만 자신의 ID를 사용하여 메시지에 서명을 생성할 수 있으며 폐지기능은 키 생성기관(PKG: Private Key Generator)에게 폐지된 ID에 대한 새로운 개인키 발행을 중지하도록 지시함으로써 얻어질 수 있게 한다. 이 방법은 시스템에서 키를 지속적으로 재 발행하도록 PKG가 항상 온라인 상태로 지속되어야 함을 요구한다. [6]에서는 PKG가 항상 온라인 상태에 있을 필요가 없으며, SEM의 구조를 Boneh와 Franklin이 제안한 ID기반 암호, BF-IBE[2]에 적용하는 방법을 제시하였다. 이 절에서는 SEM의 구조를 ID기반 전자서명, IBS에 적용한 mIBS를 제안한다.

제안된 mIBS는 안전성이 증명된 YCK-IBS[4]에 기반하여 설계한다. mIBS는 세 개의 알고리즘 (IBKG, IBSign, IBVrfy)으로 구성되며 각 세부 단계는 다음과 같다. 여기서는 PKG를 신뢰기관의 일반적 표기법인 Trusted Authority (TA) 로 표기하기로 하며 전체적인 구조는 아래 (그림 1)과 같다.

○ mIBKG. TA는 그룹 G의 생성자 P과 난수 $s \in Z_q$를 택한 뒤 $P_{pub}=sP$로 설정한다. 여기서 s는 시스템의 마스터 키가 되며, P_{pub}은 시스템의 공개키가 된다. 또한, 암호학적으로 안전한 해쉬함수 $H_1 : \{0,1\}^* \times G \rightarrow Z_q^*$와 $H_2 : \{0,1\}^* \rightarrow G$를 선택한 뒤 전체 공개키 매개변수로 (P, P_{pub}, H_1, H_2)를 공개한다.

○ mIBExtract. 사용자의 ID가 주어지면, TA는 랜덤한 비밀값 $s_{user} \in_R Z_q^*$을 선택하고 $Q_{ID} = H_2(ID)$, $D_{ID,user} = s_{user} H_2(ID)$ $D_{ID,sem} = (s - s_{user}) H_2(ID)$를 계산한다. TA는 사용자에게는 ID에 대한 개인키로 $D_{ID,user}$를 안전하게 전달하고 $(D_{ID,sem}, ID)$를 SEM에게 전달한다.

○ mIBSign. 메시지 m에 서명하기 위해 사용자는 $r_1 \in Z_q^*$를 선택해 $U_1 = r_1 P$를 계산한 뒤 SEM에게 접속해 (U_1, m, ID)를 전송한다. 그리고 나서 SEM과 사용자는 다음 프로토콜을 수행한다.

- SEM : 1. 사용자 ID가 폐지되었는지를 체크한다. 폐지된 사용자라면 프로토콜을 중지한다.
2. SEM은 $r_2 \in Z_q^*$를 선택해 $U_2 = r_2 P$, $U = U_1 + U_2 = (r_1 + r_2)P$, $h = H_1(m, U)$, $V_{sem} = r_2 Q_{ID} + h D_{ID,sem}$를 계산하여 사용자에게 (U, V_{sem})을 전송한다.

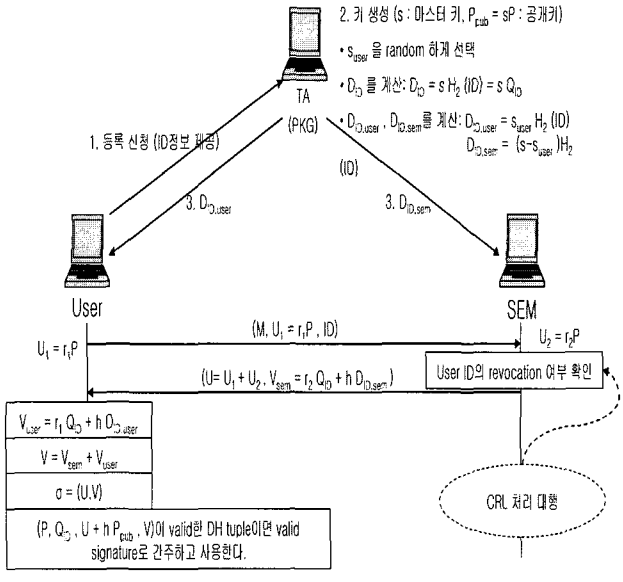
- USER : 1. (U, V_{sem})을 받은 뒤, $h = H_1(m, U)$, $V_{user} = r_1 Q_{ID} + h D_{ID,user}$, $V = V_{sem} + V_{user}$를 계산한다.
2. $(P, Q_{ID}, U + hP_{pub}, V)$가 Diffie Hellman (DH) 쌍이 되는지를 체크하여 메시지 m에 대한 $\sigma = (U, V)$가 유효한 서명값이 되는지를 검증한다. 검증이 성립하면 (M, σ)를 출력한다.

○ IBVrfy. 검증과정은 YCK-IBS[4]의 검증과정과 같다. ID에 대한 메시지 m의 서명 (m, σ)를 검증하기 위해 $h = H_1(m, U)$를 계산한 뒤, $e(P, V) = e(U + hP_{pub}, Q_{ID})$를 체크하여 $(P, Q_{ID}, U + hP_{pub}, V)$이 Diffie Hellman (DH) 쌍이 되는지를 확인한다.

mIBS의 Consistency는 다음 식으로 증명될 수 있다.

$$
\begin{aligned}
&(P, Q_{ID}, U + hP_{pub}, V) \\
&= (P, Q_{ID}, ((r_1 + r_2) + hs)P, (r_1 + r_2)Q_{ID} + h(D_{ID,sem} + D_{ID,user})) \\
&= (P, Q_{ID}, ((r_1 + r_2) + hs)P, ((r_1 + r_2) + hs)Q_{ID})
\end{aligned}
$$

3.2 mIBS의 안전성 및 효율성



(그림 1) mediated Identity based signature scheme (mIBS) 절차

〈표 1〉 mGDHS vs mIBS

			Bilinear Pairing	스칼라 곱	해쉬함수
mGDHS [6]	Sign	USER	2	1	1
		SEM	0	1	0
	Vrfy		2	0	1
mIBS	Sign	USER	2	2	2
		SEM	0	2	2
	Vrfy		2	1	2

3.2.1 효율성

<표 1>에서는 중재자를 이용한 전자서명, mGHS와 중재자를 이용한 ID기반 전자서명, mIBS를 비교한다. ID기반이 아닌 전자서명 mGHS에 비해, 서명알고리즘에서 2번의 스칼라 곱과 2번의 해쉬함수 연산이 추가로 요구되며, 서명 검증에서 가장 많은 연산량이 소요되는 Bilinear Pairing계산[2]은 같으나, 1번의 스칼라 곱과 1번의 해쉬함수 연산이 추가로 요구되었다.

BF-IBE[2]가 IB-mRSA에 비해 덜 효율적이라는 것은 [5]에서 제안되었다. 유사하게 mIBS는 IB-mRSA에 비해 덜 효율적이다. 그러나, 제안된 mIBS는 GDH그룹에 기반함에 따라, RSA를 기반하여 설계할 수 있는 mRSA, IB-mRSA와 달리 다음과 같은 이점을 제공한다. 먼저, YCK-IBS[4]의 배치 검증 특성을 유지함으로써, 같은 사용자 ID로 서명된 여러 서명값들을 검증자가 한 번에 검증할 수 있게 하는 특성을 갖고 있다. 또 다른 장점은 RSA 암호시스템이 아닌 타원곡선 암호시스템을 기반으로 함으로써 개인키의 짧은 길이를 생각할 수 있다.

3.2.2 안전성

Yoon et al.,[4]이 제안한 ID기반 전자서명 YCK-IBS는 임의의 Gap Diffie Hellman (GDH)그룹에서 랜덤오라클 모델 하에 안전하다. SEM과 사용자의 비밀키가 동시에 노출되지 않는 한 mediated GDH 전자서명의 위조불가능성은 threshold 전자서명의 위조 불가능성으로부터 얻어진다. Threshold GDH기법에서 공격자의 서명에 대한 위조는 원 GDH 전자서명의 위조를 수행할 수 있기 때문에, Threshold GDH 전자서명은 GDH 전자서명만큼 안전하다[12]. 이는 사용자가 SEM의 도움 없이는 메시지에 대한 서명을 생성할 수 없다는 것을 증명하게 한다.

IB-mRSA[5]의 경우, 단 하나의 공격자가 단 하나의 공개키/개인키 쌍을 알아내면 모듈러스를 인수분해할 수 있어 다른 사용자의 공개키에 대한 개인키를 알아낼 수 있게 하지만, mIBE는 이에 대한 안전성이 보장된다. 이러한 안전성은 mIBS에서도 성립한다. 공격자가 mIBS 기법을 깨는 유일한 방법은 키생성기관 (PKG)를 제어하는 것이다. mIBS가 IB-mRSA전자서명에 비해 덜 효율적이라 할 수 있지만, 더 안전한 방법이라 할 수 있다.

3.3 mKUS : mediated Key Updating Signature scheme

키 업데이팅 전자서명 기법에서 사용자의 서명 능력에 대한 폐지 및 제어할 수 있는 방법은 중요하다. 단위시간 i가 짧은 경우, 예를 들어 1분, 1시간에는 이러한 폐지 및 제어능력은 필요 없을 지도 모르지만 단위시간 i가 하루, 한달, 1년 등 충분히 긴 시간이라면 사용자의 서명 능력을 즉각적으로 폐지할 수 있는 방법은 필요한 가정이라 볼 수 있다. 제안된 mKUS는 중재자인 SEM 기반 구조를 키 업데이팅 전자서명에 적용한 기법이라 생각할 수 있다.

현재 mRSA 전자서명기법에서 약한 순방향 안전성을 만족하는 기법[10]은 제안되었지만, mGDHS를 약한 순방향 안전성이 보장되도록 하는 기법은 제안되지 않았다. 즉 mKUS는 약한 순방향 안전성이 보장되는 mGDHS이며 단위시간 i 동안의 사용자의 서명능력에 대한 즉각적인 폐지, 배치 검증 등 다양한 이점을 제공한다.

mKUS는 일반적인 KUS[8,14]에 SEM의 구조를 이용하여 설계할 수 있으며, 주된 아이디어는 중재자인 SEM과 사용자가 자신의 부분 키를 개별적으로 갱신한다는 데에 있다. mKUS는 (KG, UpdSEM, UpdUSER, Sign, Vrfy)의 5섯개의 알고리즘으로 구성되며 세부 단계는 아래와 같다.

○ KG. TA는 그룹 G의 생성자 P와 랜덤값 $s, usk \in_R Z_q^*$를 선택하고 $hsk = (s - usk) \bmod q$ 를 계산하고 usk 는 사용자에게, hsk는 SEM에게 전달한다. 사용자의 공개키 $P_{pub} = sP = (usk + hsk)P$를 계산하고 암호학적 해쉬함수 $H_1 : \{0,1\}^* \times G \rightarrow Z_q^*$, $H_2 : \{0,1\}^* \rightarrow G$를 선택한 뒤 공개키 정보 $pk = (P, P_{pub}, H_1, H_2)$를 공개한다.

○ UpdSEM. 입력을 i, pk, hsk로 하여 $hsk_i = hskH_2(i) \in G$를 출력한다.

○ UpdUSER. 입력을 i, pk, usk로 하여 $usk_i = uskH_2(i) \in G$를 출력한다.

○ Sign. 메시지 m에 서명하기 위해 서명자는 $r_{i1} \in Z_q^*$를 선택해 $U_{i1} = r_{i1}P$를 계산한 뒤 SEM에게 접속해 (U_{i1}, m, i)을 전송한다. SEM과 사용자는 다음 프로토콜을 수행한다.

- SEM : 1. 사용자 및 i 정보를 체크한다. 폐지된 사용자라면 프로토콜을 중지한다.
  2. $r_{i2} \in Z_q^*$를 선택해 $U_{i2} = r_{i2}H_2(i)$, $U_i = U_{i1} + U_{i2} = (r_{i1} + r_{i2})P$, $h = H_1(m, U_i)$, $V_{i,sem} = r_{i2}H_2(i) + h \times hsk_i$ 를 계산하여 사용자에게 $(U_i, V_{i,sem})$을 전송한다.

- USER : 1. $(U_i, V_{i,sem})$을 받은 뒤, $h = H_1(m, U_i)$, $V_{i,user} = r_{i1}H_2(i) + h \times usk_i$, $V_i = V_{i,sem} + V_{i,user}$를 계산한다.
  2. $(P, H_2(i), U_i + hP_{pub}, V_i)$가 Diffie Hellman (DH) 쌍 이 되는지를 체크하여 메시지 m에 대한 $\sigma_i = (U_i, V_i)$가 유효한 서명값이 되는지를 검증한다. 검증이 성립하면 (i, m, σ_i)를 출력한다.

○ Vrfy. mIBS 스킴과 유사하게, 메시지 m의 서명 (i,m,σ_i)를 검증하기 위해 $h=H_1(m,U_i)$를 계산한 뒤, $e(P,V_i)=e(U_i+hP_{pub},H_2(i))$를 체크하여 $(P,H_2(i),U_i+hP_{pub},V_i)$이 Diffie Hellman(DH) 쌍이 되는지를 확인한다.

3.4 mIBS와 mKUS의 동치관계

Bellare와 Palacio는 안전한 ID기반 암호기법이 랜덤 갱신방법을 지원하는 (N-1,N) 키 업데이트 암호기법과 동치관계에 있다는 것을 증명하였다[13]. 이와 유사하게 ID기반 전자서명기법과 랜덤 갱신방법을 지원하는 (N-1, N) 전자서명기법은 동치관계가 성립한다는 것도 증명되었다[14]. 이러한 동치결과들은 중재자를 이용하여 설계된 mIBS와 mKUS사이에도 성립한다.

KUS에서 단위시간 i를 mIBS에서의 ID로 생각하면 안전한 mIBS를 쉽게 mKUS로 상호 변환할 수 있다. 단, mKUS를 이용하여 mIBS를 설계할 때 IBSign에서 사용하는 키 $s_{sem}H_2(ID)$, $s_{user}H_2(ID)$를 생성하기 위해 SEM과 USER는 UpdUSER, UpdSEM알고리즘을 이용한다. 즉 IBSign에서 SEM과 USER는 서명을 생성할 때 사용하는 키로 $usk_i = UpdUSER(i,pk,usk), hsk_i = UpdSEM(i,pk,hsk)$를 사용한다.

3.5 mKUS의 안전성 및 효율성

3.5.1 효율성

mKUS는 mIBS와 동일한 연산량이 요구되며 이전 mRSA와 WFS-mRSA의 구조와 비교하면 <표 2>과 같이 정리할 수 있다.

mKUS는 mIBS와 동치성질이 성립하고, mIBS가 YCK-IBS[4]의 배치 검증 특성을 유지함에 따라, mKUS도 임의의 시간에 서명된 서명값들을 한 번에 검증할 수 있는 배치 검증 성질을 갖는 장점이 있다.

3.5.2 안전성

앞 절에서 기술하였듯이 mKUS는 mIBS와 동치관계가 성립함에 따라, mKUS의 안전성은 기본적으로 mIBS의 안전성에 기반한다고 할 수 있다. 여기서는 제안한 mKUS의 순방향 안전성을 기술한다. 공격자는 j 시간에서 사용자의 개인키 정보인 usk_j와 j시간에서 획득한 전자서명값 $(j,m,\sigma_j=(U_j,V_j))$을 갖고 있으며, 새로운 메시지 m'에 대하여 다음과 같은 j시간 이전의 i시간($i<j$)의 서명값 $(i,m',\sigma_i=(U_i,V_i))$을 생성하려고 한다: 공격자는 i시간의 서명값을 위조하여 아래와 같은 서명검증 절차를 통과하여야 한다.

$$
\begin{aligned}
&e(P,V_i)=e(U_i+hP_{pub},H_2(i))\\
&e(P,(r_{i1}+r_{i2})H_2(i)+h(hsk_i+usk_i))\\
&=e(P,((r_{i1}+r_{i2})+hs)H_2(i))\\
&=e(((r_{i1}+r_{i2})+hs)P,H_2(i))\\
&=e(U_i+hP_{pub},H_2(i))
\end{aligned}
$$

위 검증절차를 통과하기 위해서는 공격자는 i시간에 사용된 사용자와 SEM의 개인키 정보인 $usk_i=uskH_2(i)$, $hsk_i=hskH_2(i)$를 자신이 획득한 usk_j, hsk_j를 계산할 수 있어야 한다. 이는 $H_2(j)$($i<j$)로부터 $H_2(i)$를 얻어야하기 때문에 해쉬함수의 안전성에 위배된다. 또한 공격자가 사용자의 개인키 usk를 획득하였다고 가정하면 usk_i를 계산할 수는 있다. 그러나 $j>i$에서 SEM이 사용한 키가 $hsk\times H_2(j)$이고 전송되는 값은 $r_{j2}H_2(j)+h\times hsk\times H_2(j)$이어서, $U_{j2}=r_{j2}H_2(j)$가 공개되더라도, 공격자가 $h\times hsk\times H_2(i)$를 계산하기 위해서는 $h\times hsk\times H_2(j)$의 타원곡선그룹에서의 이산대수문제(Elliptic Curve Discrete Logarithm Problem : ECDLP)를 해결해서 hsk를 획득해야 된다. 동일한 이유에서, hsk 만이 유출되고 usk가 안전한 경우에도 공격자는 단위시간 i의 서명을 생성할 수 없다. 공격자가 사용자와 SEM의 키인 hsk와 usk 둘 다를 획득하게 되면 키생성기관 (PKG)을 제어하는 것과 동일하게 되기 때문에 제안된 기법은 약한 순방향 안전성만을 보장하게 된다.

공격자가 현재 공개키 정보 (P,P_{pub},i)에 대한 메시지 m의 유효한 서명 σ_i를 얻을 수 있다는 것을 가정한다. 이 경우, 현재 단위 시간 $j(i<j\leq T)$에 동일 메시지 m에 대한 서명 σ'을 위조할려고 하는 future dating attack[10]를 생각할 수 있지만 WFS-mRSA[10]에서 고려했던 것처럼 서명생성 시, 현재 단위시간 정보가 삽입되어 계산되기 때문에 Future-Dating Attack에 대하여 안전하다.

〈표 2〉 이전 기법들과의 비교분석

		mRSA[1]	WFS-mRSA[10]	mIBS	mKUS
서명생성	USER	$d_u{}^+ e$	$(d_u\times e^i)+(e\times e^{T-i})$	2 스칼라곱 + 2 pairing	2 스칼라곱. + 2 pairing
	SEM	d_{sem}	$d_{sem}\times e^i$	2 스칼라곱.	2 스칼라곱.
서명 검증		e	$e\times e^{T-i}$	1 스칼라곱. + 2 pairing	1 스칼라곱. + 2 pairing
안전성		-	약한 순방향 안전성	-	약한 순방향 안전성

4. 결 론

우리는 mGDHS에서 약한 순방향 안전성이 보장되는 mKUS기법을 제안하였다. 이 기법은 GDH 전자서명을 기반으로 하기 때문에, 약한 순방향 안전성이 보장되는 mRSA에 비해 연산량이 더 소요된다. 그러나, RSA에서는

제고하지 못하는 배치 검증 기능을 제공함에 따라, 다른 시간 동안 서명된 서명값들을 검증 시에 한 번에 검증할 수 있는 장점을 갖는다. 또한, 기존에 제시된 키 업데이팅 전자서명 기법에서 제공하지 못하는 사용자의 서명능력에 대한 즉각적인 폐지기능을 제공한다. 또한, 우리는 이 논문에서 IBS에 중재자인 SEM의 구조를 적용한 mIBS를 제안하였다. 그리고 나서, KUS와 IBS사이의 동치관계를 이용해 mIBS를 기반으로 하여 mKUS를 제안하였다. 즉 IBS와 KUS사이의 동치관계가 SEM의 구조가 적용된 mIBS와 mKUS사이에도 적용될 수 있음을 보였다. 이러한 SEM의 구조는 침입에 강인한(Intrusion Resilient) 암호시스템[9]에도 적용될 수 있다. 그러나, 기존에 알려졌듯이, KUS보다 침입에 강인한 기법들은 더 높은 안전도를 제공하지만 더 비효율적이라 할 수 있다. 향후, 안전도를 높이면서 효율적인 기법에 대한 연구가 진행되어야 할 것으로 보인다.

참 고 문 헌

[1] D.Boneh, X.Di ng, G. Tsudik, and C.M.W ong. "A method for fast revocation of public key certificates and security capabilities." In 10th USENIX Security Symposium, Washington, D.C. , Aug. 2001.

[2] D. Boneh and M. Franklin. "Identity Based Encryption From the Weil Pairing," In Advances in Cryptology-Proceedings of Crypto '01, volume 2139 of Lecture Notes in Computer Science, pages 213-229. Springer, 2001.

[3] D. Boneh, B. Lynn, and H. Shacham. "Short signatures from the Weil pairing." In Advances in Cryptology-Proceedings of Asiaerypt'01, volume 2248 of Lecture Notes in Computer Science, pages 514-532. Springer, 2001.

[4] H. Yoon, J. H. Cheon, and Y. Kim. "Batch verifications with ID-based signatures." In Information Security and Cryptology - ICISC 2004, pp. 233 - 248, 2005.

[5] X. Ding and G. Tsudik. "Simple Identity-Based Cryptography with Mediated RSA." In Proceedings of CT-RSA '03, Lecture Notes in Computer Science. Springer, 2003.

[6] B. Libert, J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," Symposium on Principles of Distributed Computing-PODC'2003, 2003.

[7] R. Anderson, "Invited lecture at the acm conference on computer and communication security (CCS'97)," 1997.

[8] Yevgeniy Dodis, Jonathan Katz, Shouhuai Xu, and Moti Yung. "Key-insulated public key cryptosystems." In Lars Knudsen, editor, Advances in Cryptology, EUROCRYPT 2002, Lecture Notes in Computer Science. Springer-Verlag, 28 April May 2002.

[9] Gene Itkis and Leonid Reyzin. "Intrusion-resilient signatures, or towards obsoletion of certificate revocation," In Moti Yung, editor, Advances in Cryptology|CRYPTO 2002, Lecture Notes in Computer Science. Springer-Verlag, 18-22 August 2002.

[10] G. Tsudik, "Weak Forward Security in Mediated RSA," Security in Computer Networks Conference (SCN'02), September 2002.

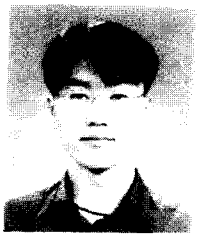
[11] J. Katz and M. Yung. "Threshold Cryptosystems Based on Factoring." In Advances in Cryptology - proceedings of Asiacrypt 2002, Lecture Notes in Computer Science. Springer, 2002.

[12] A. Boldyreva. "Efficient threshold signature, multisignature and blind signature schemes based on the Gap-Diffie-Hellman-group signature scheme." In Proceedings of PKC'03, Lecture Notes in Computer Science. Springer, 2003.

[13] M. Bellare and A. Palacio, "Protecting against key exposure: strong keyinsulated encryption with optimal threshold," Cryptology ePrint archive 2002/064, http://eprint.iacr.org/, 2002.

[14] Dae Hyun Yum and Pil Joong Lee, "Efficient Key Updating Signature Schemes based on IBS," Cryptography and Coding 2003, pp. 167-182, 2003.

[15] Noel McCullagh, "Efficient Batch Verification of Signature Schemes based on Bilinear Maps," Cryptology ePrint archive 2004/088, http://eprint.iacr.org/complete/,2004.9



주 학 수

e-mail : haksoo.ju@samsung.com

1999년 고려대학교 대학원 수학과 (이학석사)

2005년 고려대학교 대학원 수학과 (이학박사)

2001년~2005년 한국정보보호진흥원 연구원

2006년~현 재 삼성전자 DM연구소 책임연구원

관심분야 : DRM, 보안 프로토콜

김 대 엽

e-mail : daeyoub69@paran.com

1997년 고려대학교 대학원 수학과 (이학석사)

2000년 고려대학교 대학원 수학과 (이학박사)

1997년~1999년 (주)텔리맨 위성통신연구소 책임연구원

2000년~2001년 (주)시큐아이닷컴 정보보호연구소 책임연구원

2002년~현 재 삼성종합기술원 CNL. 전문연구원

관심분야 : CAS, DRM, 스마트카드 보안, 보안 프로토콜