情報保護學會論文誌
第11券 第6號, 2001. 12

타원곡선 암호를 이용한 효율적인 인증서 폐지 메커니즘

윤 이 중*, 한 재 우*, 한 대 완*, 류 재 철**

An Efficient Certificate Revocation Mechanism Using Elliptic Curve Crypto-system

I-Jung Lee*, Jae-Woo Han*, Dae-Wan Han*, Jae-Cheol Ryou**

요 약

각종 인터넷 보안기술의 기반기술로 작용하는 PKI 기술의 중요성이 강조되고 있는 가운데, PKI의 효율적인 운용을 위해서는 네트워크의 비효율적인 이용, 인증서 폐지 이유 발생 시점과 실제 인증서 폐지 시점의 시간차 발생 등의 문제를 갖고 있는 CRL을 이용하는 기존의 인증서 폐지 메커니즘의 개선이 필요하다. 본 논문에서는 타원곡선 암호체계에서 mECC 기술과 Weil pairing을 이용하여 새로운 방식의 인증서 폐지 메커니즘을 제안한다. 제안하는 인증서 폐지 메커니즘은 PKI 시스템 운용에 있어서 전반적으로 성능 향상을 가져올 수 있을 것으로 기대되며, 특히 무선 PKI와 같이 빠른 속도와 효율적인 리소스 활용을 요구하는 환경에 적합하다.

ABSTRACT

CRLs are the most common way to handle certificate revocation. But, They have several problems. Since the validity period of certificates is long and the number of users is immense, CRLs can grow extremely long. Therefore, a great amount of data needs to be transmitted. Moreove, CRLs cannot provide immediate revocation. In this paper, we propose a new certificate revocation mechanism using mECC and Weil pairing in elliptic curve crypto-system. Our certificate revocation mechanism simplifies the process of certificate revocation and provides the immediate revocation.

keyword : *Certificate revocation, CRL, mECC, Weil pairing*

Ⅰ. 서 론

인터넷의 급격한 발전과 함께 이에 대한 역효과로 인터넷을 통한 각종 보안사고 및 위협이 증대하고 있다. 이에 따라 각종 보안사고 및 위협으로부터 정보 시스템을 보호하기 위한 인터넷 보안기술의 중요성이 높아지고 있다.

다양한 인터넷 보안기술 가운데에서도 특히 PKI 기술은 여러 가지 인터넷 보안기술의 운용에 기반기술로 작용한다는 점에서 그 중요성이 더욱 강조되고 있다. PKI 기술을 구성하는 요소 기술은 크게 다음과 같은 6가지로 구분할 수 있다.

- 인증서 및 CRL 프로파일
- 인증경로 검증 기술
- 인증서 폐지 메커니즘

* 한국전자통신연구원 부설 국가보안기술연구소(yej@etri.re.kr)
** 충남대학교 공과대학 정보통신공학부

- 운영 프로토콜
- 관리 프로토콜
- 인증업무준칙

그런데, 이와 같은 PKI 요소 기술 가운데 인증서 폐지 메커니즘과 관련된 부분은 많은 문제점이 지적되고 있다. 기존 인증서 폐지 메커니즘은 X.509 v2 CRL을 이용한 방법이 대부분인데, CRL의 크기가 매우 커서 네트워크 자원을 비효율적으로 이용할 수밖에 없으며, 인증서 폐지 이유가 발생한 시점과 실제로 인증서가 폐지되는 시점과의 시간차가 발생하여 PKI 운용시 분쟁이 발생할 수 있기 때문이다. 더군다나 최근 들어 무선인터넷이 급격하게 발전하고 있는 가운데, 무선인터넷에서도 유선인터넷과 동일한 수준의 보안 서비스를 제공하기 위해서는 무선 PKI 기술의 적용이 필수인데, 기존 CRL을 이용한 인증서 폐지 메커니즘은 무선환경에서의 이용이 거의 불가능하다고 할 수 있다. 이는 무선인터넷이 대역폭이나 라운드 트립 등에서 유선인터넷에서 비해 제한적이며, 무선 단말기 역시 CPU와 메모리 성능, 자원 활용 등에 있어서 유선환경에 비해 제한적인 가운데, 유선환경에서도 많은 부담이 되는 CRL은 사용이 곤란하기 때문이다.

이와 같은 CRL의 문제점이 지적되고 있는 가운데, 이를 개선하기 위해 CRS, CRT, OCSP 등 다른 방식의 인증서 폐지 메커니즘들이 제안된 바 있다. 그러나 이러한 방식들의 대부분은 CRL에 기반하여 설계되었으며, CRL에 비해 크게 성능이 개선되었다고 하기는 힘든 것이 사실이다.

D. Boneh 등은 이러한 문제점들을 해결하기 위하여 mRSA 기술을 이용한 새로운 인증서 폐지 메커니즘을 제안하였다.[1] 그러나, RSA 암호체계를 기반으로 한 Boneh의 제안은 타원곡선 암호체계에서는 적용될 수 없는 한계가 있었다. 이에 본 논문에서는 타원곡선 암호체계에서 운영할 수 있는 효율적인 인증서 폐지 메커니즘을 제안하고자 한다.

본 논문의 2장에서는 CRL, CRS, CRT, OCSP, Short-lived 인증서 등 기존의 인증서 폐지 메커니즘들에 대해서 살펴본다. 3장에서는 본 논문에서 제안하는 새로운 인증서 폐지 메커니즘을 설명하고, 기존 메커니즘과 비교한다. 끝으로 4장에서는 결론을 맺는다.

II. 여러 가지 인증서 폐지 메커니즘

2.1 인증서 폐지 메커니즘 개요

PKI 운영에 있어서 인증서의 폐지는 필수적으로 발생한다. 이에 따라 인증서 폐지 방법, 폐지된 인증서 목록의 배포 등 인증서 폐지와 관련된 사항을 효율적으로 처리할 수 있는 인증서 폐지 메커니즘의 역할은 매우 중요하다.

CA 입장에서는 인증서 폐지 서비스를 신뢰할 수 있는 방법으로 제공해야만 한다. 예를 들어, 불법적인 사용자가 CA로 위장하여 유효한 인증서가 폐지된 것으로 거짓 정보를 유포하는 것이 가능하다면 PKI 전체를 신뢰할 수 없다. 또한 사용자 입장에서는 인증서 폐지가 언제 발생했으며, 인증서 폐지에 대한 정보를 언제, 어떤 방법으로 획득하느냐가 매우 중요하다. 즉, 인증서 폐지 사실을 모르고 이미 폐지된 인증서를 유효한 인증서로 인식하여 사용함으로써 손해를 입는 문제가 발생할 수 있다.

이와 같은 인증서 폐지가 발생하는 이유는 일반적으로 다음과 같은 4가지로 구분할 수 있다.

- 키 손상 : 인증서 소유주나 CA의 비밀키가 손상되었거나, 손상된 것으로 의심되는 경우이다. 비밀키 도난 또는 누출, 비밀키 저장장치의 손상 등이 이 경우에 해당된다.
- 인증서 정보의 변경 : 인증서 소유주 관련 정보나 그 밖의 정보가 더 이상 유효하지 않은 경우이다.
- 대체 : 인증서가 다른 인증서로 대체된 경우이다.
- 운영 중단 : 인증서가 더 이상 본래 목적으로 사용되지 않는 경우이다.

이 밖에도 다음과 같은 경우에는 인증서 폐지가 수행되어야 한다. 일반적으로 앞서 살펴본 4가지 경우에는 이유 발생 즉시 인증서가 폐지되어야 하나, 다음의 경우에는 이유 발생 즉시 인증서가 폐지될 필요는 없는 것으로 받아들여지고 있다.

- 알고리즘 손상 : CA에서 인증서를 발급하는데 사용된 알고리즘의 결함이 발견된 경우, 또는 보다 발전된 알고리즘이 개발되어 현재 사용되는 알고리즘을 대체하는 경우에 해당된다.
- 상위 인증서의 폐지 : 인증경로에서 상위에 위치

하는 인증서가 폐지된 경우이다.

- 보안토큰의 손실/손상 및 패스워드 또는 PIN의 손실 : 인증서 소유주의 비밀키 및 비밀키 보호에 사용되는 패스워드 또는 PIN을 저장하는 보안토큰을 잃어버리거나 보안토큰이 고장 등의 이유로 손상된 경우, 또는 외부로부터의 불법적인 접근에 의해서 비밀키, 패스워드/PIN 등이 외부로 유출된 경우이다.
- 키 용도의 변경 : CA로부터 인증 받은 키가 더 이상 인증된 용도로 사용되지 않는 경우이다.
- 보안정책의 변경 : CA가 더 이상 본래의 보안정책에 따라 인증 서비스를 제공하지 않는 경우이다. CA가 인증 서비스의 제공을 중지하는 경우가 이에 해당된다.

이와 같이 인증서 폐지는 다양한 이유에 의해서 발생하며, 인증서 폐지 메커니즘 또한 여러 가지 방법으로 제공될 수 있다. 대표적인 인증서 폐지 메커니즘으로는 다음과 같은 것들이 있으며, 본 장에서는 이들 인증서 폐지 메커니즘에 대해서 살펴보고자 한다.

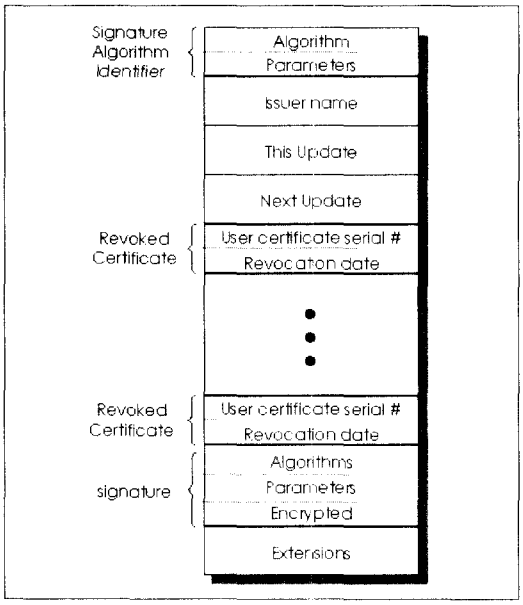
- 인증서폐지목록(CRL)
- 인증서폐지시스템(CRS)
- 인증서폐지트리(CRT)
- 온라인 인증서 상태 확인 프로토콜(OCSP)
- Short-lived 인증서

2.2 인증서폐지목록(CRL)

X.509 CRL(Certificate Revocation List)은 X.509 인증서와 함께 1998년에 ITU-T에 의해서 제안되었으며, 1993년에 X.509 v2 CRL로 개정되어 지금까지 사실상 표준으로 사용되고 있다. CRL은 폐지된 인증서들의 일련번호를 저장하며, 24시간이나 1달 등 정기적인 주기로 발행된다.

X.509 v2 CRL의 포맷은 [그림 1]과 같다.[2] 즉, CRL의 내용은 폐지된 인증서의 일련번호, 취소 날짜, CRL의 발행일 및 다음 발행일 등이며, 인증서의 취소 이유 등이 추가적으로 포함될 수 있다.

이러한 형식으로 생성된 CRL은 CA에 의해서 전자서명 되어진다. 이 때, CRL을 발행하는 CA와 인증서를 발행하는 CA가 반드시 동일할 필요는 없으나, 인증서를 발행한 CA에서 CRL도 발행하는



[그림 1] X.509 v2 CRL

것이 일반적이다. 앞에서 설명하였듯이 CRL은 주기적으로 발행되어 디렉토리에 저장되며, 인증서 사용자는 디렉토리에서 CRL을 획득하여 최신의 CRL인지 여부를 확인하고, 전자서명 검증을 통해 유효한 CRL인지를 확인해야 한다. CRL에 대한 유효성 검사가 완료되면, CRL 내에 자신이 이용하려는 인증서가 포함되었는지 확인한다. 확인 결과, 인증서의 일련번호가 CRL 내에 포함되어 있으면, 그 인증서는 유효하지 않은 인증서로 간주한다.

이와 같이 CRL은 개념 자체가 어렵지 않고, 사용이 편리하기 때문에 현재까지 가장 널리 이용되는 인증서 폐지 메커니즘이다. 그러나 인증서의 유효기간이 1년 이상으로 긴 경우가 일반적이고, 인증서 소유주의 수는 계속해서 증가하기 때문에 CRL의 크기가 매우 커질 수밖에 없다는 단점을 갖고 있다. CRL은 네트워크를 통해서 사용자에게 배포되어야 하는데, CRL의 크기가 매우 커질 경우 이는 매우 부담되는 일이다. 또한 인증서 폐지 이유가 발생한 시점과 CRL이 생성되어 배포되는 시점 사이에 시간차가 발생하기 때문에 사용자가 폐지된 인증서를 이용하는 경우가 발생할 수 있다.

CRL의 기본 개념은 변경하지 않은 채, 이와 같은 CRL의 단점을 개선하기 위해서 제안된 메커니즘으로 delta-CRL이 있다. delta-CRL의 기본 개념은 이전에 발행된 CRL과 비교하여 상태가 변경된 인증

서의 정보만을 제공하는 것이다.[3] 즉, 가장 최근의 인증서 상태정보가 필요한 사용자는 만약 이전에 발행된 CRL을 저장하고 있다면, 가장 최근의 CRL을 다운로드 받는 대신 가장 최근의 delta-CRL을 다운로드 받는다. delta-CRL을 다운로드 받은 사용자는 저장되어 있는 CRL과 비교하여 인증서의 상태정보를 파악할 수 있다. 즉, 폐지 여부를 확인하려는 인증서가 CRL과 delta-CRL 모두에 포함되어 있지 않다면 유효한 인증서이다.

delta-CRL은 CRL과 비교하여 변경된 사항만 저장함으로써 CRL에 비해 크기가 매우 작은 것이 특징이며, 따라서 저장소로부터 다운로드 받는 속도를 향상시킬 수 있다.

그러나 delta-CRL을 이용한다 하더라도, 다운로드 받아야 하는 데이터의 크기는 대폭 줄어들지만, 다운로드 받는 횟수는 줄어들지 않는다. 즉, delta-CRL은 delta-CRL 발행 바로 전에 발행된 CRL에 대해 변경된 사항을 반영하는 것이 일반적이기 때문에, 사용자 시스템에 저장되어 있는 CRL이 너무 오래된 것일 경우에는 올바른 인증서 상태정보를 알 수 없다. 따라서 대개의 경우, 사용자는 delta-CRL과 CRL을 교대로 다운로드 받아야 한다. 따라서 delta-CRL을 사용하여 평균적으로 성능이 개선된다 하더라도, 여전히 CRL이 갖고 있는 문제점은 존재하게 된다.

2.3 인증서 폐지 시스템(CRS)

CRS(Certificate Revocation System)는 1995년에 소개된 개념이다. CRS 사용자는 CRL과는 달리 폐지된 모든 인증서의 목록을 다운로드 받지 않는다. 즉, 인증서의 유효성을 확인하려는 사용자는 그 인증서의 상태를 묻는 메시지를 전송하고, 그에 대한 응답으로 해당되는 인증서에 대한 짧은 응답을 받는다. CRS에 대해서 보다 자세하게 살펴보면 다음과 같다.

CRS에서 시스템은 다음과 같이 설정된다. CA는 i의 간격을 갖는 CRS의 사용기간 n을 설정한다.(예를 들어 CRS의 사용기간이 1년이고, 1일을 주기로 CRS가 갱신된다면, n=365, i=1로 설정한다.) CRS는 X.509 인증서를 이용하는데, X.509 인증서가 CRS에 적용되기 위해서는 추가적인 확장필드가 필요하다. 확장필드는 2개의 100비트 필드인데, 하나는 Y(yes)로 명명되며, 다른 하나는 N(no)로 명명된다. 이 2개의 값은 CA의 전자서명으로 유효성이 보장된다. CA는 2개의 100비트 난수 Y_0와 N_0을 생성한 뒤, 이 값을 안전하게 보관한다. 그리고 CA는 다음과 같은 계산을 수행한다. 즉, Y를 얻기 위해서는 n번의 해쉬(H) 연산이 필요하며, N을 얻기 위해서는 1번은 해쉬 연산이 필요하다.

- $Y=Y_n=H_n(Y_0)$
- $N=H(N_0)$

또 CRS에서 가장 최신의 정보를 유지할 수 있도록 하기 위해서 CA는 다음 정보를 디렉토리에 저장한다.

- L : 유효기간이 만료되지 않은 모든 인증서의 일련번호를 저장하고 있는 목록이다. L은 항상 최신의 정보를 유지할 수 있도록 지속적으로 업데이트 되어야 하며, 타임스탬프와 CA의 전자서명이 첨부되어야 한다.
- V : 모든 인증서에 대해서 계산된 100비트 값이며, 계산방법은 다음과 같다.
  - i 내에서 새로운 인증서가 발급된 경우, 또는 인증서가 유효기간이 만료되지 않았거나 폐지되지 않은 경우: $V=Y_{n-i}=H^{n-i}(Y_0)$
  - i 내에서 인증서가 폐지된 경우: $V=N_0$

이 때, 폐지된 인증서에 대해서는 폐지된 시간이나 폐지된 이유와 같은 추가적인 정보에 대한 전자서명이 함께 제공된다. 이렇게 해서 저장소에는 모든 인증서의 일련번호와 각각의 인증서에 대한 V 값이 함께 저장되게 된다.

인증서의 폐지 여부를 확인하기 위해서 사용자는 먼저 목록 L을 저장소에서 가져와서 전자서명 검증을 통해 L의 유효성을 확인한다. L이 유효한 것으로 확인되면, 사용자는 폐지 여부를 확인하려는 인증서의 일련번호가 L에 포함되어 있는지 확인한다. 만약 포함되어 있다면, 다음과 같은 계산을 계속해서 수행한다.

- $H^i(V)$를 계산하여 Y와 같은지 확인한다. 만약 같다면, 인증서는 i 내에서 유효한 것이다
- 만약 동일하지 않다면, H(V)를 계산하여 H(V)가 N과 같은지 확인한다. 만약 같다면, 폐지된 인증서이다.

위의 2가지 경우에 모두 해당하지 않는 경우는, 데이터 전송 상에서 문제가 발생하였거나, 서비스 거부 공격이 일어나는 경우 등이다.

이와 같은 CRS를 이용할 경우에 얻을 수 있는 장점은 다음과 같다.

- 크기가 큰 목록 L은 오프라인으로 제공된다.
- 해쉬 함수가 사용되고, Y와 N의 크기가 100비트로 비교적 작기 때문에 V를 검증하는 절차가 비교적 간단하며, 따라서 V의 검증은 온라인에서 수행 가능하다.

그러나 CRS는 인증서 상태정보를 파악하는 절차가 CRL과 비교하여 복잡한 편이며, Y_0와 N_0가 노출될 경우, 안전성이 전혀 보장될 수 없다는 단점을 가지고 있어 널리 사용되고 못하고 있는 실정이다.

2.4 인증서 폐지 트리(CRT)

1998년에 소개된 CRT(Certificate Revocation Tree)는 해쉬트리를 이용한 개념이다.[4] CRT의 동작 원리에 대해서 살펴보면 다음과 같다.

CRT 시스템은 다음과 같이 초기화된다.

- low < i < high 결정, 이 때 i는 인증서의 일련번호이다. 즉 일련번호가 i인 인증서는 C_i이다.
- 폐지된 인증서 C_j와 C_k는 (j,k)로 표현된다. 이 때, C_j와 C_k 사이에는 또 다른 폐지된 인증서가 없어야 한다.
- N은 폐지된 인증서의 개수이며, 폐지된 인증서 정보는 $L_0, \cdots, L_N$와 같이 표기되며, 각각의 정보는 폐지 이유 및 폐지일을 포함하고 있다.
- 모든 $L_n(0 \le n \le N)$은 해쉬함수 H에 의해서 생성되는 해쉬트리를 구성하는 이진트리의 leaf node로 사용된다.(이때, 트리는 높이가 $\log_2(N+1)$인 complete tree이며, N+1은 2의 제곱수이다.)

노드 $N_{i,j}$는 left ancestor인 $N_{i-1,l}$와 right ancestor인 $N_{i-1,r}$을 이용해서 다음과 같이 계산에 의해 생성된다.

$$N_{i,j}=H(N_{i-1,l} \,||\, N_{i-1,r})$$

트리를 구성하기 위해서 트리의 root인 $N_{k,0}$에 이를 때까지 계산을 반복한다. 이 때 $k=\log_2(N+1)$이다. 계산이 완료되면 트리의 root는 CRT의 발행일 및 만기일 등의 정보와 함께 CA에 의해서 전자서명된다. 그리고 해쉬트리와 이에 대한 전자서명은 사용자가 다운로드 받을 수 있도록 디렉토리를 통해서 배포된다.

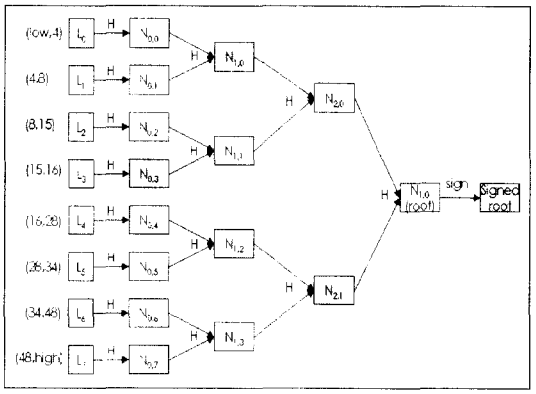
인증서의 상태정보를 알기 위해서 사용자는 폐지여부를 알고자 하는 인증서의 일련번호가 포함된 요청 메시지를 디렉토리로 전송한다. 이에 대한 응답은 다음과 같은 메시지로 구성된다.

- 문의된 일련번호를 포함하고 있는 자료구조 L_i
- i가 짝수일 경우에는 $N_{0,i+1}$, i가 홀수일 경우에는 $N_{0,i-1}$
- root를 계산하는데 필요한 노드를 나타내는 최소한의 해쉬값
- root
- 전자서명

이와 같은 응답 메시지를 수신한 사용자는 위에서 설명된 방법과 같은 방법으로 해쉬값을 계산하여 그 결과가 root와 동일한지 확인한다. 만약 동일한 경우라면 L_i에 대해서 CRT는 유효하며, 인증서의 상태정보를 결정할 수 있다. 그렇지 않은 경우는 CRT를 신뢰할 수 없다.

[그림 2]는 CRT가 사용되는 예를 보여준다. N=7이며, 폐지된 인증서의 일련번호는 4, 8, 15, 16, 28, 34, 48이다. 예를 들어 일련번호가 14인 인증서의 상태정보를 확인하기 위해서는 L_2, $N_{0,3}$, $N_{1,0}$, $N_{2,1}$, root의 전자서명 등이 필요하다.

해쉬함수가 사용되며, 데이터의 양이 트리의 leaf



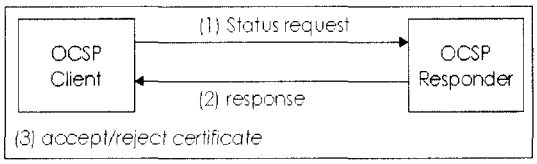
[그림 2] CRT의 사용 예

수의 logarithm으로 증가한다는 점에서 CRT는 속도가 매우 빠른 효율적인 인증서 폐지 메커니즘이라고 할 수 있다.

또한 각 노드의 값이 미리 계산되며, root에 대한 전자서명 또한 오프라인으로 계산되어 네트워크에 대한 부담을 줄일 수 있다는 것도 CRT의 장점이다. 그러나 오프라인으로 동작한다는 점은 최신의 정보를 얻는데 문제가 있다.

2.5 온라인 인증서 상태 확인 프로토콜

OCSP(Online Certificate Status Protocol)는 CRL을 대체 또는 지원하기 위한 수단으로 IETF에서 개발중인 인증서 폐지 메커니즘으로, 가장 최신의 인증서 상태정보를 적절한 시간에 제공하면서, CRL에서 제공하지 않는 추가적인 정보를 제공하는데 적합하도록 설계되었다.[5] OCSP의 기본 동작은 [그림 3]과 같다.



[그림 3] OCSP의 동작

① 사용자는 인증서의 상태를 묻는 status request를 생성하여 OCSP 서버에게 전송한다.
② OCSP 서버 또는 OCSP responder는 사용자가 문의한 인증서의 상태를 기록한 정보인 response를 생성하여 사용자에게 전송한다.
③ 사용자는 서버로부터 response를 받기 전까지는 인증서를 유효한 것으로 인정하지 않으며, OCSP로부터 response를 받은 후에 인증서의 상태를 확인하고 인증서를 신뢰하여 사용할 것인지, 그렇지 않을 것인지를 결정한다.

이와 같이 OCSP는 CRL을 이용할 경우 사용자가 수행되어야 할 절차들을 OCSP 서버가 대신 수행하고, 그 결과만을 사용자에게 알려주는 구조이다. 구조가 비교적 간단하고 response의 크기가 작아 네트워크의 효율도 높다고 할 수 있지만, 보안과 관련하여 다음과 같은 사항들이 고려되어야 한다.

- OCSP 서비스가 효율적으로 제공되기 위해서는 반드시 사용자와 OCSP 서버 간의 네트워크가 설정되어 있어야 한다. 만약 그렇지 못한 경우에 사용자는 OCSP 서비스를 제공받지 못하고, CRL 메커니즘을 사용할 수 밖에 없다.
- OCSP 서버는 서비스 부인 공격(Denial of Service Attack)에 취약해지기가 쉽다. 이는 OCSP 서버에 인증서 상태정보에 대한 문의가 집중되기 때문이다. 더군다나, response 메시지를 생성하기 위해서 소요되는 전자서명 연산 시간은 OCSP 서버를 이런 공격에 더욱 취약하게 한다. 또한 에러 메시지를 전송하는 response 메시지는 전자서명이 첨부되지 않는데, 이로 인해 외부의 공격자는 쉽게 거짓 response 메시지를 생성할 수 있다.
- 미리 생성된 response 메시지를 사용할 경우, 재전송 공격의 위험이 있다. 즉, 공격자는 이전에 전송되었던 response 메시지를 가로채 보관하고 있다가, OCSP 서버로 위장한 상태에서 보관하고 있던 메시지를 전송함으로써 사용자에게 피해를 주는 공격이 가능하다.
- OCSP 서비스가 HTTP를 통해서 제공될 경우, HTTP 캐쉬 메커니즘에 의해서 이전 데이터들이 전송되는 경우가 발생할 수 있다.

2.6 Short-lived 인증서

WAP PKI에서 사용자 인증서의 경우는 기존 X.509 인증서를 그대로 사용하고 있다. 따라서 기존 유선 PKI에서 많이 사용되는 CRL이나 OCSP 등을 이용한 인증서 상태 확인이 가능하다.

그러나 무선환경에서 인증서 폐지 메커니즘은 성능, 네트워크 대역폭 등의 요소를 고려할 때, 유선환경에서의 인증서 폐지 메커니즘과는 다른 방법으로 수행되어야 한다. 즉, CRL은 이미 유선환경에서도 비효율적인 것으로 받아들여지고 있으며, 무선환경에서 CRL의 이용은 거의 불가능한 것으로 인식되고 있다. 또한 CRL의 비효율성을 극복하기 위한 방법 가운데 하나인 OCSP 역시 라운드 트립을 증가시키고, 검증 절차가 비교적 복잡하여 무선 환경에서는 이용하기가 곤란하다. 이와 같은 이유로 인해 WAP PKI에서는 인증서 상태 확인을 위해 Short-lived 인증서라는 개념을 제안하고 있다.[6]

서버 인증을 중심으로 설명하면, 서버나 게이트웨이는 장기 인증기간(long-term credentials period)

동안 CA로부터 1번 인증을 받는다. 이 기간은 대개 1년 정도 되며, 이 기간 동안에는 동일한 공개키쌍이 사용된다. 한편, CA는 서버나 게이트웨이에 대해 유효기간이 48시간 정도로 짧은 인증서를 장기 인증기간 동안 24시간을 주기로 발행한다. 서버나 게이트웨이는 짧은 주기로 발급되는 Short-lived 인증서를 해당 기간 동안 사용자와 보안통신을 하는데 이용한다.

만약, CA가 비밀키 손상 등의 이유로 서버나 게이트웨이의 인증서를 폐지해야 하는 경우가 발생한다면, CA는 새로운 인증서의 발행을 중지하는 것으로 인증서 폐지를 대신한다. 즉, 새로운 인증서의 발행이 중지되면 서버나 게이트웨이는 사용자에게 유효한 인증서를 제시할 수 없으며, 따라서 보안 통신도 불가능하다.

Short-lived 인증서를 이용하는데 있어서 가장 중요한 요소는 이전 인증서와 현재 인증서의 유효기간 사이에는 반드시 겹쳐지는 부분이 존재해야 하며, 무선 단말기에 충분히 정확한 시간을 획득할 수 있는 기능이 구현되어야 한다는 점이다. 그러나 이 방법은 공격자가 서버에게 계속해서 인증서를 요구하는 형태의 새로운 서비스 거부 공격에 노출될 위험이 크다는 단점이 있다.

2.7 기존 인증서 폐지 메커니즘의 분석

지금까지 살펴본 인증서 폐지 메커니즘들을 비교해보면 〈표 1〉과 같다. 이들은 각기 장단점을 갖고 있어 어떤 하나의 메커니즘이 가장 효율적이라고 말하기는 매우 곤란하다.

또한 이러한 인증서 폐지 메커니즘을 적용하고 있는 PKI 응용 프로그램의 현황을 살펴보면 〈표 2〉와 같다.

〈표 1〉과 〈표 2〉에서 알 수 있듯이 현재 제공되고 있는 인증서 상태 확인 메커니즘들은 성능 면에서 압도적으로 효율적인 것은 없는 상태이며, 대부분의 인증서 사용시스템에서 여러 가지 인증서 폐지 메커니즘을 동시에 지원하고 있는 상태이다.

Ⅲ. 효율적인 인증서 폐지 메커니즘 제안

앞서 서론에서 언급하였듯이 D.Boneh 등은 mRSA 기술을 이용하여 새로운 인증서 폐지 메커니즘을 제안하였다.[1] 그러나, mRSA는 구조적으로 이산대수

〈표 2〉 인증서 폐지 메커니즘의 비교

구분	장점	단점
CRL	■ 어플리케이션에서 인증서 상태 확인 ■ 현재 사실상 표준으로 사용 가능한 시스템이 가장 많음	■ 매우 큰 사이즈를 필요로 함 ■ 많은 네트워크 자원 소요 ■ 캐쉬 필요
CRT	■ 인증서 상태정보의 크기가 CDP/CRL보다 작고, OCSP보다는 큼 ■ 모든 response 메시지에 대해서 전자서명을 수행할 필요 없음 ■ 안전성이 높은 ■ 구축비용이 작음	■ 트리 구축 및 인증서 상태정보 배포에 많은 시간 소요
OCSP	■ 어플리케이션에서 인증서 상태 확인 ■ 항상 최신의 인증서 상태 정보 획득 가능 ■ response 메시지의 크기가 작음	■ response 생성때마다 매번 전자서명 필요 ■ 외부로부터의 공격 위협이 큼
Short-lived 인증서	■ 구현이 간단함 ■ 빠른 속도로 인증서 상태 정보 확인 가능	■ 외부로부터의 공격 위협이 큼

〈표 3〉 인증서 폐지 메커니즘 사용 현황

	CRL	OCSP	CRT	Short-lived
IE	지원	지원	지원	-
Navigator	지원	지원	-	-
IIS	-	지원	지원	-
Suit Spot	지원	지원	지원	-
Apache	지원	지원	지원	-
Exchange	-	지원	지원	-

의 어려움에 기반하는 타원곡선 암호체계에는 적용할 수 없는 한계를 지니고 있다.

이에 본 장에서는 타원곡선 암호체계에서 운영 가능한 효율적인 인증서 폐지 메커니즘을 제안하고자 한다. 제안 메커니즘은 mECC(Mediated ECC) 기술을 사용하여 암호문의 복호화와 전자서명을 생성한다. 암호문을 복호화할 때는 임의의 타원곡선에서 가능하지만, 전자서명을 생성하기 위해서는 초특이 타원곡선(Supersingular elliptic curve)상에서 정의되는 Weil pairing의 성질을 이용하여야 한다. 따라서, 본 제안의 메커니즘을 설명하기에 앞서 Weil pairing을 이용한 타원곡선 상에서의 서명 생성 및 검증법을 설명하기로 한다.

3.1 Weil pairing을 이용한 서명 생성 및 검증

Weil pairing은 초특이타원곡선상에서 정의되는 쌍선형형식을 말한다. Weil pairing의 내용과 암호학에 응용되는 성질에 관한 자세한 내용은 참고문헌 [7]의 부록을 참고하기 바란다.

E가 유한체 GF(q)상에서의 초특이타원곡선이고, 점 P는 E의 위수가 큰 기점이라고 하자. 타원곡선 암호체계에서 사용자(U)의 공개키(EK)와 비밀키는 다음과 같이 정의된다.

$$EK : aP \qquad DK=a$$

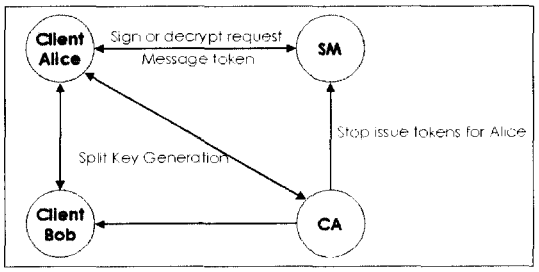
위와 같은 타원곡선 암호체계에서 전자서명은 다음과 같은 간단한 절차를 거쳐 생성할 수 있다.

① 사용자 U는 서명을 생성하려고 하는 메시지 m의 해쉬값 h(m)=Q를 구한다.
② m의 전자서명 s는 aQ의 x 좌표가 된다.
생성된 전자서명 s는 사용자의 공개키 aP와 Weil pairing을 이용하여 e(aP,Q)=e(P,aQ)가 성립하는지를 확인하면 된다.

3.2 시스템 구성

본 절에서는 본 논문에서 제안하는 인증서 폐지 메커니즘의 내용에 대해서 살펴본다. 이 메커니즘을 구성하는 요소는 [그림 4]와 같다.

SM은 온라인에서 동작하는 신뢰할 수 있는 서버이다. Alice는 전자서명이나 복호화를 위해서 전자서명 또는 복호화 요청 메시지(sign or decrypt request)를 SM 서버에게 전송한다. 전자서명 또는 복호화 요청을 접수한 SM 서버는 적절한 사용자 인증 과정을 거친 뒤, 메시지 토큰을 Alice에게 전송한다. 이 토큰 없이는 Alice는 전자서명이나 복호화를 수행할 수 없다.



[그림 4] 시스템 구성

Alice의 인증서를 폐지하기 위해서는 CA와 같이 폐지 권한을 가진 기관에서 SM에게 Alice의 인증서 폐지 사실을 통보하기만 하면 된다. 폐지 통보를 받은 SM 서버는 CA에 대한 적절한 인증 과정을 거친 뒤, 이를 접수한다. 이 후에는 Alice로부터 전자서명이나 복호화 요청이 있어도 SM서버에서 더 이상 토큰을 발급하지 않음으로써 간단히 인증서 폐지가 이루어진다. 각 구성요소에 대해서 좀 더 자세히 살펴보면 다음과 같다.

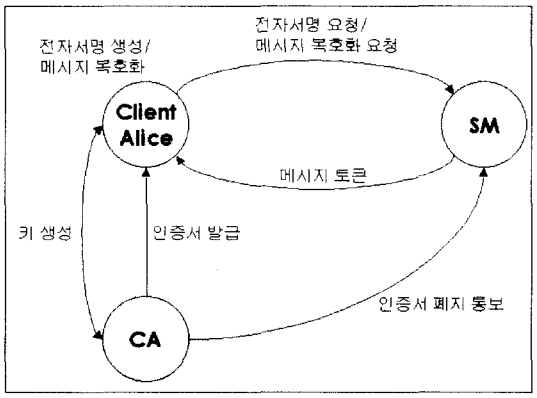
- CA : 하나의 CA는 비교적 적은 수의 SM 서버를 관리하며, 사용자가 어떤 SM 서버로부터 서비스를 받을 것인지를 오프라인으로 맺어준다. 또한 CA는 생성한 비밀키를 분할하여 SM 서버와 사용자에게 전송한다.
- 사용자 : 사용자는 초기에 CA로부터 부분적인 비밀키의 정보를 받은 후, 복호화 및 전자서명시 SM 서버로부터 서비스를 받아 처리한다.
- SM 서버 : SM 서버는 대규모 사용자를 대상으로 서비스를 제공한다. 따라서 물리적 보안 등에서 우수한 기능을 제공해야 한다. 또한 사용자의 전자서명이나 복호화 요청을 처리할 수 있는 데몬 프로세스가 동작해야 한다. 사용자로부터 전자서명이나 복호화 요청이 접수되면, SM 서버는 자신의 폐지목록을 검색하여 사용자가 폐지목록에 등록되어 있는 사용자이면 서비스 거부 메시지를 사용자에게 전송한다. 그렇지 않을 경우에는 부분 전자서명인 메시지 토큰을 사용자에게 전송한다. 분리된 비밀키의 한 부분을 SM 서버에 저장할 수도 있고, CA에 저장하면서 필요할 때만다 CA로부터 전송 받아 사용할 수도 있다.

3.3 시스템 동작

본 절에서는 제안된 인증서 폐지 시스템의 동작과정에 대해서 살펴본다. 시스템의 동작절차를 간략하게 살펴보면 [그림 5]와 같다. 이에 대해서 보다 자세하게 살펴보면 다음과 같다.

3.3.1 키 생성 및 인증서 발급

본 시스템에서의 키 생성은 mRSA와 마찬가지로 CA에 의해서 생성되게 된다. CA가 키를 생성하는 과정을 자세히 살펴보면 다음과 같다.



〔그림 5〕 시스템의 동작절차

① [1, q]에 있는 정수 a_S, a_U를 선택한 후, $a=a_S \cdot a_U$를 계산하여 비밀키를 생성한다.
② $b=a^{-1}$를 구하고, $b=b_S+b_U$가 되도록 b_S와 b_U를 생성한다.
③ (a_S, b_S)는 SM에게 안전한 방법을 통해서 전송하고 (a_U, b_U)는 사용자에게 역시 안전한 방법을 통해서 전송한다.

지금까지 살펴본 바와 같은 방법을 통해서 키 생성 및 분배가 이루어지고 나면, 사용자는 전자서명, 암호화 및 복호화 등의 기능을 이용할 수 있다.

3.3.2 데이터 암호화 및 복호화

mECC에서의 암호화는 ECC에서와 동일하다. 즉, 임의의 난수 k를 생성한 후, 다음과 같은 방법으로 평문 M의 암호문 C를 생성한다.

$$C=(kP,\ M+k(aP))$$

반면 복호화는 다음과 같은 방법으로 진행한다.
① 사용자는 kP를 SM에게 전송한다.
② 메시지를 수신한 SM은 사용자의 인증서가 유효한지 검증하고 유효한 경우, $(a_S(kP), a_Sb_S(kP))$를 계산한 후 사용자에게 전송한다.
③ SM으로부터 메시지를 수신한 사용자는 수신한 메시지와 자신이 가지고 있는 정보를 이용하여 $b_Ua_U a_S(kP)+a_Ua_Sb_S(kP)$의 값이 kP인지를 검증하여 올바른 SM으로부터 온 메시지인지 확인한다.
④ ③의 확인 결과 맞으면 $M=(M+k(aP))-a_Ua_S(kP)$의 식으로부터 평문을 얻는다.

3.3.3 전자서명 생성 및 검증

mECC에서의 전자서명은 앞서 언급하였듯이 Weil pairing의 성질을 이용하여 생성하게 된다.

① 사용자는 전자서명을 첨부하려는 메시지의 해쉬값을 x 좌표로 가지는 타원 곡선 위의 점 Q를 SM에게 전송한다.
② 메시지를 수신한 SM은 사용자의 인증서가 유효한 지를 검증하고 유효한 경우, $(a_SQ,\ a_Sb_SQ)$를 계산한 후 사용자에게 전송한다.
③ 사용자는 $b_Ua_U(a_SQ)+a_U(a_Sb_SQ)$의 값이 Q인지를 확인하고, 맞으면 전자서명 $aQ=a_Ua_S(Q)$를 생성한다.

위와 같이 생성한 전자서명의 검증은 앞서 1절에서 설명한 것과 동일한 방법으로 수행한다.

3.3.4 인증서 폐지

사용자의 인증서에 대한 폐지 사유가 발생한 경우에 CA는 이 사실을 SM 서버에게 통보한다. 인증서 폐지 사실을 수신한 SM 서버는 인증서 폐지 사실을 알리는 메시지에 첨부된 CA의 전자서명을 검증한 후, 전자서명이 유효하면 사용자의 인증서를 폐지한다. 이는 SM 서버에서 관리하는 인증서가 폐지 목록에 해당되는 사용자를 추가하는 것이다.

사용자로부터 전자서명이나 데이터 복호화 요청 메시지를 SM 서버가 수신하면, SM 서버는 요청한 사용자가 자신이 관리하는 목록에 포함되어 있는지를 확인한다. 확인 결과, 목록에 포함되어 있는 경우에는 사용자에게 서비스 거부 메시지를 전송한다.

3.3.5 mECC의 특징

앞에서 설명한 바와 같이 mECC는 일반적인 ECC를 약간 수정한 형태이며, ECC에 비해 몇 가지 중요한 특징을 지니는데, 이를 살펴보면 다음과 같다.

- CA에 의한 키 생성 : ECC를 사용할 경우에는 일반적으로 키쌍은 키를 사용하게 될 사용자에 의해서 생성된다. 그러나 mECC를 사용하는 경우에는 CA가 모든 사용자의 키쌍을 생성한다. 즉, CA는 모든 사용자의 비밀키를 알게된다. 이와 같은 키 생성 방법은 자연스럽게 키 위탁이 이루어진다는 점에서 소규모의 조직에서는 바람직한 방법일 수 있다. 예를 들어 어떤 회사에서

한 사원이 회사정보를 자신의 공개키로 암호화하여 관리하고 있었다면, 이 사원이 회사를 그만두었을 때, RSA를 사용한 경우에는 사원의 비밀키 정보를 쉽게 알 수 없기 때문에 회사정보를 복호화하여 그 내용을 보는 절차가 복잡해질 수 있다. 그러나 mECC를 사용할 경우에는 CA에서 모든 사원의 비밀키를 알고 있으므로 쉽게 회사정보를 볼 수 있다.

- 즉각적인 인증서 폐지 : 인증서 폐지 사유가 발생하고, 인증서 소유주에 의한 인증서 폐지 신청 후, 실제로 인증서 폐지가 전체 PKI에 반영되는 과정에서 발생하는 시간차의 문제는 mECC를 이용할 경우에는 쉽게 해결이 가능하다. 즉, 사용자 인증서의 폐지는 사용자의 SM에게 사용자 인증서 폐지 사실을 알리는 것만으로 간단하게 이루어진다. 사용자 인증서 폐지 사실을 통보 받은 SM은 사용자의 전자서명이나 복호화 요청이 있어도 비밀키의 다른 한 부분을 제공하지 않음으로써, 사용자가 전자서명이나 복호화 기능을 이용하지 못하도록 한다.
- 투명성 : mECC는 상대방의 공개키를 이용해서 데이터를 암호화 하거나, 전자서명을 검증하는 사용자에게는 ECC와 완벽하게 동일하게 보여진다. 또한 mECC에서 사용되는 인증서와 ECC에서 사용되는 인증서 사이에도 차이점은 전혀 없다.
- CA의 업무 : mECC를 이용한다 하더라도, 기본적인 CA의 업무에 커다란 변화는 없다. 즉, 최초에 공개키쌍을 생성하는 부분과 분리된 비밀키를 인증서와 함께 배포해야 된다는 점을 제외하면, CA는 여전히 오프라인 상태에서 동작하며, 사용자 및 SM과의 통신도 오프라인으로 이루어진다.

3.4 시스템의 안전성

본절에서는 제안된 인증서 폐지 메커니즘의 안전성을 분석한다.

공개키 암호 시스템에서 가장 쉽게 생각할 수 있는 공격은 사용자에게 보내지는 암호문을 공격자가 복호화 하거나 사용자의 서명을 공격자가 위조하는 것이다. 본 시스템의 경우에는 SM 서버로부터 사용자에게 전송되는 메시지 토큰을 공격자가 가로챈 뒤, 이를 이용하여 암호문을 복호화 하거나, 서명을 위조하는 경우가 이에 해당한다. 그러나 메시지 토큰은 그 자체로는 아무 의미 없는 데이터이며, 비밀키의 다른 한부분을 알기 전에는 데이터의 복호화나 전자서명의 생성이 불가능하다.

다음으로, 사용자가 자신의 인증서가 폐지된 이후에도 계속해서 전자서명을 생성하여 사용함으로써 전체 PKI 사용자에게 혼란을 주는 공격이 가능하다. 이와 같은 위협 또한 제안된 시스템을 통해 충분히 방어가 가능한데, 이는 일단 SM 서버에 폐지된 인증서로 등록된 이후에는 SM 서버가 사용자의 전자서명 또는 복호화 요청에 대해 메시지 토큰을 발행하지 않기 때문이다.

또한 제안된 시스템은 사용자나 SM 서버 가운데 한쪽의 부분 비밀키가 노출되는 경우에도 다른 한쪽의 부분 비밀키 마저 노출되지 않는 한 비밀키 전체가 노출되지는 않는다는 장점이 있다.

3.5 기존 인증서 폐지 메커니즘과의 비교

기존의 인증서 폐지 메커니즘에서는 암호화 및 전자서명의 검증을 하는 사용자들이 매번 인증서 폐지 목록과 같은 정보를 다운로드 받아야 했다. 본 논문에서 제안한 인증서 폐지 메커니즘은 복호화와 전자서명을 하는 사용자가 SM 서버와 작은 정보만을 1회 주고 받음으로써, 네트워크 자원의 이용 면에서 볼 때 기존의 인증서 폐지 메커니즘에 비해서 매우 효율적이다.

또한 인증서 폐지 사유가 발생한 즉시 이 사실이 SM 서버에게 통보되어 인증서 폐지가 수행될 수 있다는 점도 기존 인증서 폐지 메커니즘에 비해서 개선된 점이며, OCSP와 비교할 때, SM 서버로부터 사용자로 전송되는 메시지에 특별한 암호 메커니즘이 적용될 필요가 없다는 점에서도 효율적이다.

그리고 CA 또는 SM 서버나 사용자가 저장하고 있는 부분 비밀키가 노출된다 하더라도 다른 한부분이 노출되기 전에는 비밀키 전체가 노출되지 않으므로 비밀키 관리 면에서의 안전성도 향상되었다.

Ⅳ. 결 론

본 논문에서는 타원곡선암호체계에서 CRL을 비롯한 기존의 인증서 폐지 메커니즘이 갖고 있는 단점을 개선한 인증서 폐지 메커니즘을 제안하였다.

제안한 인증서 폐지 메커니즘은 Weil pairing과

mECC 기술을 이용하여 사용자의 비밀키를 사용자와 CA 또는 SM 서버가 분리해서 보관하도록 하고, 이를 인증서 폐지에 이용하였다.

제안한 메커니즘은 인증서 상태정보 확인을 위해 사용자가 주고 받아야 하는 정보의 크기를 최소화 시킴으로써 효율성을 향상 시켰으며, 인증서 폐지 요청이 발생한 즉시 이를 적용할 수 있다는 장점을 갖고 있다.

기존의 대표적인 인증서 폐지 메커니즘인 CRL의 비효율성은 계속해서 지적되고 있는 사항이다. 특히, 무선인터넷의 발전과 함께 많은 연구가 진행되고 있는 무선 PKI 분야에서의 CRL의 사용은 무선인터넷이 갖고 있는 특성상 거의 불가능하다고 할 수 있다. 이러한 가운데 본 논문에서 제안한 인증서 폐지 메커니즘은 인증서 상태정보 확인에 필요한 데이터의 크기가 작고 속도가 빠를 뿐 아니라, 기존의 타원곡선암호체계를 기반으로 하는 PKI 환경을 변형시키지 않고 그대로 적용할 수 있기 때문에, PKI 시스템의 전반적인 성능 향상을 가져올 수 있을 것으로 기대된다.

참 고 문 헌

[1] D. Boneh, X. Ding, G. Tsudik, C. M. Wong, "A Method for Fast Revocation of Public Key Certificates and Security Capabilities", Proceeding of 10th USENIX Security Symposium, 2001.

[2] R. Housley, W. Ford, W. Polk, D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", IETF RFC2459, 1999. 6.

[3] David A. Cooper, "A more Efficient Use of Delta-CRLs", Proceedings of the 2000 IEEE Symposium on Security and Privacy, 2000. 5.

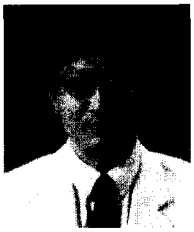
[4] P. Kocher, On certificate revocation and validation, Proceeding Of Financial Cryptography, 1998.

[5] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP", IETF RFC2560, 1999. 6.

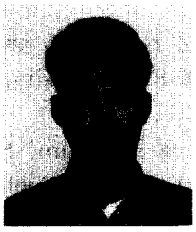
[6] "WAP Certificate and CRL Profiles", WAP Forum Specification, 2000. 3.

[7] D. Boneh, M. Franklin, "Identity-Based Encryption from the Weil Pairing", Full version available at http://crypto.stanford.edu/ibe.

〈著者紹介〉



윤 이 중 (E-Joong Yoon) 정회원
1990년 2월 : 인하대학교 전산과 석사
1997년 2월~현재 : 충남대학교 컴퓨터과학과 박사과정
1990년 2월~2001년 2월 : 한국전자통신연구원 정보보호시스템연구부장
2001년 2월~현재 : 국가보안기술연구소 기반기술연구부장
〈관심분야〉 정보보호, PKI, 컴퓨터네트워크, 데이터베이스



한 재 우(Jaewoo Han) 정회원
1991.2 : 서강대학교 수학과(학사)
1993.2 : 한국과학기술원 수학과(석사)
1999.8 : 한국과학기술원 수학과(박사)
1999.7~1999.12 : 한국전자통신연구원 선임연구원
2000.1~현재 : 국가보안기술연구소 선임연구원
〈관심분야〉 공개키 암호, 매듭이론

한 대 완(Daewan Han) 정회원
1995.2 : 서울대학교 수학과(학사)
1997.2 : 서울대학교 수학과(석사)
1998.2~2001.1 : 공군기상전대 수치예보개발장교
2001.3~현재 : 국가보안기술연구소 연구원
〈관심분야〉 공개키 암호, 해쉬 함수

류 재 철(Jae-Cheol Ryou) 정회원
1985.2 한양대학교 산업공학과 졸업
1988.5 Iowa State Univ. 전산학 석사
1990.12 Northwestern Univ. 전산학 박사
1991.2~현재 :충남대학교 정보통신공학부 부교수
〈관심분야〉 인터넷 보안, PKI, 스마트카드 보안