위임등록 프로토콜을 이용한 대리서명 기법

박 세 준† · 오 해 석††

요 약

실생활에서 권한의 위임을 통한 대리 서명 기법들이 최근 많이 연구되고 있다. 대리서명은 원서명자가 자신의 서명 권한을 대리 서명자에게 위임하여 대리 서명자가 원서명자를 대신하여 서명을 생성하는 것을 의미하며 기본적으로 원서명자가 위임 정보에 대한 서명을 생성하고 이를 대리 서명자에게 전달하여 대리 서명자가 위임키로서 사용하게 하는 방법을 통하여 이루어진다. 이러한 대리서명 기법을 사용하기 위해서는 몇 가지 보안 사항들이 요구된다. 본 논문에서는 기존의 보안 요구 사항들을 모두 만족하고 원서명자와 대리 서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리 서명자에 대한 위임정보를 검증자에게 등록하는 프로토콜을 제안한다. 제안하는 방법에서는 위임내용에 대해 원서명자가 디지털 서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 대리 서명자에 대한 권한, 기간, 제약사항을 설정한다. 대리 서명자는 위임내용에 대한 고지를 받고 허가된 범위 내에서 대리 서명이 이루어지게 된다. 또한 기존의 대리 서명 기법들과의 비교 분석을 통하여 제안하는 위임 등록 프로토콜에 대한 효율성을 제시한다.

Proxy Signature Scheme based on Proxy-Register Protocol

Se Joon Park† · Hae Suk Oh††

ABSTRACT

Proxy signature schemes based on delegation of warrant are frequently studied in these days. Proxy signatures are signature schemes that an original signer delegates his signing capability to a proxy signer, and the proxy signer creates a signature on behalf of the original signer. Proxy signatures are fundamentally accomplished by the process that original signer creates the signature about the proxy information and transmits to the proxy signer for using by the proxy key. There are several security requirements for using the proxy signature schemes. In this paper we suggest the proxy-register protocol scheme that original signer registers to the verifier about the proxy related information. In our scheme, verifier verifies the signature that original signer creates about the proxy information and sets the warrant of proxy signer, validity period for proxy signature and some limitation. At the same time, all security requirements that were mentioned in previous schemes are satisfied. We also show the advantages of our suggestion by comparing with the previous proxy signature schemes.

키워드 : 위임등록 프로토콜(Proxy-Register Protocol), 대리서명(Proxy Signature), 위조불가능(Unforgeability), 검증성(Verifiability), 신원확인(Identifiability), 부인방지(Undeniability), 오용방지(Prevention of Misuse)

1. 서 론

기업에서는 많은 일로 인해 필요한 서류에 서명을 하지 못하거나 책임자가 부재중일 경우 온라인 상의 문제로 인해 서명을 할 수 없는 상황이 빈번하게 일어나곤 한다. 조직에게 발급된 인증서는 그 조직에 속한 직원들이 사용하고 있는데 이 경우 권한을 위임하기 위해서는 인증서와 비밀키를 직접 직원에게 위임하여 전자 거래에 서명하도록 하는 방법을 사용하고 있다[3, 11]. 직원들에게 인증서가 가지고 있는 모든 권한을 위임하는 것은 보안상 많은 문제점이 있다. 가장 큰 문제점은 조직의 인증서를 직원에게 대여함으로써 발생할 수 있는 인증서와 비밀키의 오남용을 막기가 힘들다는 것이다. 또한 대리 서명 후 직원의 부인 방지를 막을 수가 없고 위임을 받은 직원이 제삼자에게 원서명자의 동의 없이 인증서와 비밀키를 알려 줌으로서 대리 서명 능력을 가지게 할 수 있다. 그리고 비밀키 자체의 노출이 늘어남에 따라 안전성에 심각한 문제를 야기할 수 있다[12, 15].

이러한 문제점을 극복하기 위해 공개키 인증서를 가진 조직이 각 구성원이 위임받을 수 있는 권한에 대해 규정하고 이를 자신의 비밀키로 서명함으로서 인증서를 발급하여 대리 서명을 하는 방법을 사용한다. 대리인은 위임을 받음과 동시에 위임자가 규정한 범위 내에서 제 3자에게 위임자로 인증 받을 수 있다[16, 19].

본 논문에서는 원서명자와 대리 서명자가 기존의 인증서를 발급 받은 환경에서 원서명자가 대리 서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 디지털 서명을 하고 검증자는 이

† 정 회 원 : (주)노스텍 R&D 센터
†† 종신회원 : 경원대학교 IT 부총장
논문접수 : 2003년 9월 1일, 심사완료 : 2004년 1월 5일

에 해당하는 내용을 검증한 후 대리 서명자에 대한 권한, 기간, 제약사항을 설정한다. 이후 대리 서명자는 위임내용에 대해 고지를 받고 허가된 권한과 범위 내에서 위임 서명을 한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 관련 연구들과 문제점들을 알아보고 3장에서는 대리서명의 보안 요구 사항과 기술의 종류에 대해서 알아본다. 4장에서는 제안하는 위임등록 프로토콜을 설계하고 5장에서는 실험환경과 실험데이터를 보여주고 기존의 기법들과 비교분석을 통한 기대효과를 제시하며 마지막으로 6장에서는 결론을 내린다.

2. 기존 대리서명 기법

2.1 Mambo, Usuda, Okamoto's Scheme

MUO 기법에서는 3가지 타입의 위임에 기반하여 대리서명 기술을 구분하였다. 대리 서명 방식에서 원서명자의 서명 권한을 위임하는 형태에 따라서 완전 위임, 부분 위임으로 분류하였고 원서명자에 의해 만들어진 인증서를 사용하여 대리 서명을 실현하는 보증 위임을 제안하였다[3, 15].

완전 위임은 원서명자가 자신의 개인키를 위임자에게 주는 방법으로서 대리 서명자에 의한 서명과 원서명자에 의한 서명이 구분되지 않는다. 부분 위임은 원서명자가 대리서명 비밀키를 자신의 비밀키를 이용하여 생성하는 방법이다. 부분 위임은 대리서명의 암호화에 따라 대리 서명자가 원서명자를 대신하여 서명할 수 있는 대리인 비보호형 대리서명 방식 기법과 정당한 대리 서명자만이 대리서명이 가능한 대리인 보호형 대리 서명방식 기법으로 구분되며 위임 서명키는 원서명자와 위임자 모두에 의해서 생성된다. 보증 위임은 원서명자가 자신과 위임자의 정보와 관련된 권한에 대해서 서명하고 검증자는 이 정보에 기반하여 권한을 검증하는 방법을 말하며 지정한 사람을 대리 서명자로 선언하는 서류에 원서명자가 디지털서명을 통하여 서명한 후 그 서명된 인증서를 이용하여 대리 서명을 실행하는 인증서 기반 대리 서명 방식 기법과 지정한 서명자를 위한 비밀키와 공개키를 생성하고 생성된 공개키에 대하여 원서명자가 인증서를 만들어 지정된 대리 서명자에게 전달하는 소지자 기반 대리 서명 방식 기법으로 구분된다.

이들이 제안한 대리서명 기법은 위임되는 권한에 대한 제약이 없으므로 대리인에 의한 오남용이 가능하다는 점과 원서명자의 동의 없이 제 3자에게 전달하여 대리서명이 가능하고 제 3자가 명백한 위임자인지에 대한 결정을 할 수 없다는 단점이 있다.

2.2 Petersen and Horster's Scheme

PH 기법에서는 자체 보증키를 생성하여 대리 서명을 하는 기법을 제안하였다[7]. 또한 이들은 위임키쌍을 생성하기 위해 기본키 생성 프로토콜과 보안키 생성 프로토콜을 제안하였다. 기본키 생성 프로토콜은 대리인 비보호형 대리 서명 기법으로서 원서명자가 위임키쌍을 생성하여 대리 서명자에게 전달하는 것이며 보안키 생성 프로토콜은 대리인 보호형 대리 서명 기법으로서 원서명자와 대리 서명자가 함께 위임키쌍을 생성하지만 대리 서명자의 개인키를 원서명자가 알 수 없도록 하는 방법이다[6, 8]. 이들이 제안한 대리서명 기법은 대리서명시 위임자에 대한 어떠한 정보도 포함되어 있지 않기 때문에 서명을 수행한 후 추후에 부인할 수 있고 위임자가 위임키를 CA(Certificate Authority)에 자신의 키쌍처럼 등록하여 자신의 목적을 위하여 사용할 수 있으며 원서명자는 위임자의 동의없이 위임자의 ID를 가지고 위임키쌍을 생성하여 CA에 등록하고 자신의 키처럼 사용할 수 있다는 단점이 있다.

2.3 Kim, Park and Won's Scheme

MUO 혹은 PH 기법에서는 원서명자의 정보에 대리 서명자의 신원이나 권한과 같은 어떠한 정보도 포함되어 있지 않기 때문에 권한의 오남용과 같은 문제들이 발생할 수 있다. 이와 같은 문제들을 해결하기 위해 KPW 기법에서는 Schnorr 서명 기법을 이용하고 대리인과 위임되는 권한에 대한 정보를 대리서명에 포함시켜 위임된 권한의 오남용, 제 3자에게로의 서명 권한 전달을 방지하는 방법을 제안하였다[22].

KPW 기법에서는 위임 개인키가 대리인에 의해서만 표현되어질 수 있기 때문에 대리인 보호형 대리서명 기법이다. 이들이 제안한 대리서명 기법은 대리서명 내에 원서명자와 위임자의 역할이 동일하다는 단점이 있다. 그러므로 권한에 대한 내용이 아주 명백하게 표시되어 있어야 하며 그렇지 않은 경우에는 이들의 역할이 바뀔 수 있기 때문에 검증자는 대리서명의 권한에 표시된 내용과 일치하는지에 대해서 체크해야 한다.

2.4 Delos, Quisquater's Scheme

DQ 기법에서는 서명하는 횟수를 제한할 수 있는 ID 기반 서명 기법과 제한된 서명 횟수의 일부분을 대리인이 수행할 수 있는 방법을 제안하였다[20]. ID 기반 인증 모델에서는 각 사용자의 ID에 대응하는 개인키를 생성해주는 신뢰기관의 구축이 필요하기 때문에 ID 기반 서명 기법은 시스템 파라미터와 각 사용자의 개인키를 생성하는 초기화 과정과 이를 이용하여 서명을 생성하고 검증하는 과정으로 구성되어 있다. 이들이 제안한 대리서명 기법은 ID 기반 인증 모델에서의 서명 기법임에도 불구하고 유효성 확인을 위해 원서명자나 신뢰기관이 제공하는 인증서를 사용해야 하며 시스템이 각 사용자의 개인키를 알고 있고 단순한 횟수의 제한을 제외하고는 권한의 사용에 대한 아무런 제약이 없다는 단

점이 있다.

3. 대리서명의 보안 요구사항 및 기술의 분류

3.1 대리서명의 보안 요구 사항

① 검증성 : 검증자는 대리 서명으로부터 위임자의 서명 권한 위임에 대한 동의를 확인할 수 있어야 하며 선택적으로 대리 서명자의 신원을 확인할 수 있어야 한다. 다단계의 위임이 이루어지면 대리 서명자의 신원 확인은 필수 보안 요구 사항이 된다[9, 17].

② 위조 불가능성 : 위임자에 의해 지명된 대리인만이 유효한 서명을 생성할 수 있어야 한다. 또한 위임자나 제 3자는 대리인을 가장하여 유효한 서명을 생성할 수 없어야 한다[4].

③ 신원확인성 : 누구나 대리 서명으로부터 대리 서명자의 신원을 확인할 수 있어야 한다[5].

④ 부인 불가능성 : 대리 서명자는 유효한 대리 서명의 생성 후 서명한 사실에 대한 부인 거부를 할 수 없어야 한다[13, 21].

⑤ 오용 방지 : 위임자가 발급한 위임 인증서는 위임자가 정한 인증서의 사용 범위 내에서 사용되어야 한다. 즉 대리 서명자는 원서명자로부터 위임받은 권한 이외의 목적으로 대리 서명키를 사용할 수 없어야 한다[1, 18].

⑥ 권한의 제약 : 위임된 권한 내에서만 대리 서명키를 사용할 수 있어야 한다.

⑦ 양도 불가 : 위임자가 생성한 대리 서명키는 양도할 수 없어야 한다.

⑧ 적합성 확인 : 검증자는 대리서명의 권한에 표시된 내용에 대한 적합성을 체크해야 한다.

3.2 대리서명 기술의 분류

대리서명 기술은 분류 기준에 따라서 여러 가지로 구분된다. 우선 부인방지 기법에 따라서 strong 대리서명 기법과 weak 대리서명 기법으로 분류할 수 있다[14, 22]. Strong 대리서명 기법은 위임자와 원서명자의 서명을 표현하는 기법으로서 위임자가 대리서명을 수행한 후 부인할 수 없다. 이 기법에서 생성되는 위임키쌍은 다른 목적으로 사용될 수 없다. Weak 대리서명 기법은 원서명자의 서명만을 표현하는 기법으로서 부인방지를 제공하지 못한다. 이러한 단점을 가지고 있는 이유로 분산환경에서는 사용할 수 없다.

원서명자는 특정한 위임자를 명시하지 않고 대리서명의 조건만을 명시하여 일정한 대리 서명자 집합을 만들 수 있다. 이러한 대리서명 위임자 권한의 임명방법에 따라서 designated 대리서명 기법과 non-designated 대리서명 기법으로 구분한다[10]. Designated 대리서명 기법은 원서명자가 위임자를 명시하는 기법으로서 위임자의 신원에 대한 정보가 대리서명키를 포함하는 인증서에 포함되어 있다. Non-designated 대리서명 기법은 원서명자가 위임자를 명시하지 않는 기법으로서 원서명자의 서명 파라미터를 알고 있으면 누구든지 위임키를 생성할 수 있는 방법을 말하며 생성 후 인증서의 정보와 일치하면 원서명자를 대신하여 대리서명을 할 수 있다.

원서명자가 스스로 위임키쌍을 생성하여 대리서명에 사용하는 자체 대리서명 기법은 원서명자와 대리 서명자가 동일인이 된다. 자체 대리서명 기법은 원서명자가 스스로 권한에 대한 정보를 포함한 위임키쌍을 생성하여 자신의 새로운 키쌍으로 사용한다[2]. 이 기법은 키의 갱신 목적으로도 사용될 수 있다.

4. 위임 등록 프로토콜의 설계

공개키기반 구조의 발전과 함께 인터넷뱅킹, 증권거래시스템, 전자결제의 온라인서비스에 인증 기술이 적용되어 디지털 서명을 이용한 로그인과 거래가 보편화되었다. 그러나 원서명자의 부재와 권한위임에 대한 많은 연구가 진행되었으나 현실적인 공개키기반 구조를 반영하지 못하고 있다.

기존의 대리서명 기법에서는 원서명자, 대리 서명자, 검증자의 관계로 구분이 되며 제안된 기법도 언급된 세 부분의 관계를 기초로 하고 있다. 기존의 대리서명 방식은 원서명자와 대리 서명자의 관계를 핵심으로 하여 원서명자가 대리 서명자에게 개인키를 생성해 주거나 혹은 위임내용에 함께 전달하여 처리하는 기법을 핵심으로 하고 있지만 제안한 위임등록 프로토콜은 기존의 원서명자와 대리 서명자의 관계가 아니라 원서명자와 검증자의 관계로 관점을 전환하였으며 이때 보안이 상대적으로 취약한 검증자에게 최우선으로 위임을 등록하기 때문에 효율적인 보안이 설정된다는 아이디어를 제시한다. 또한 현재 공인인증기관이 활성화된 상태에서 추가적인 알고리즘 또는 소프트웨어 없이 대리서명에 대해 안전성을 제공할 수 있다.

제안하는 위임 등록 프로토콜은 PKI 기반의 구성요소를 준용하며 원서명자와 대리 서명자가 기존의 인증서를 발급받은 환경에서 원서명자가 대리 서명자에 대하여 검증자에게 위임정보를 등록하는 프로토콜을 제안한다. 위임내용에 대해 원서명자가 디지털 서명을 하고 검증자는 이에 해당하는 내용을 검증한 후 대리 서명자에 대한 권한, 기간, 제약사항을 설정한다. 이후 대리 서명자는 위임내용에 대해 고지를 받고 허가된 범위 내에서 위임 서명을 할 수 있다.

4.1 구성요소

본 논문에서 제안하는 위임등록 프로토콜을 이용한 대리서명 방식의 구성요소는 다음과 같다. (그림 1)은 제안하는 위임 등록 프로토콜을 이용한 대리서명 방식의 구성요소를

도식화하였다.

① 인증기관(CA : Certificate Authority)

원서명자와 대리 서명자에게 인증서의 발급을 담당한다. 또한 인증서와 관련된 정보를 게시하고 상태정보를 제공한다.

② 원서명자(Original Signer)

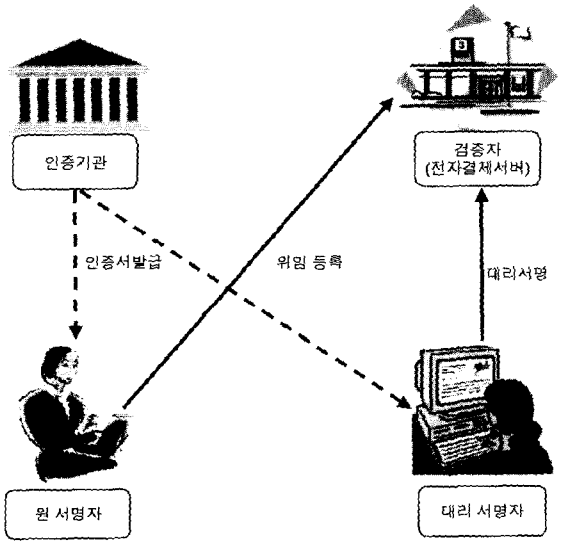
인증서를 발급 받아 온라인서비스를 이용하는 사용자로서 대리 서명자에게 위임권한, 시간, 제약사항을 정의하여 위임할 수 있다.

③ 대리 서명자(Proxy Signer)

원서명자의 권한 중 전부 또는 일부를 위임받아 본인의 인증서를 통해 온라인서비스에 원서명자를 대신하여 디지털 서명을 수행한다.

④ 검증자(Verifier)

검증자는 온라인 서비스의 서버로서 원서명자에게 위임 등록을 제공하고 원서명자가 정의한 권한을 대리 서명자가 위임하여 수행할 수 있게 처리한다.



(그림 1) 대리서명 방식의 구성요소

4.2 위임 등록/해제 시나리오

(그림 2)는 제안하는 위임등록 프로토콜의 시나리오를 나타낸 것이다. 본 논문의 검증자는 온라인서비스를 제공하는 서버이며 원서명자와 대리 서명자는 온라인 서비스의 사용자를 의미한다. 원서명자는 대리 서명자에게 안전한 방법으로 위임권한, 기간, 제약사항을 위임등록 프로토콜을 사용하여 정의할 수 있다.

위임등록 프로토콜의 시나리오는 다음과 같이 구성되어 있다.

① 원서명자는 검증자인 서비스 제공자의 서버에 접속하여 대리 서명자에 대하여 위임 등록을 요청한다. 이때 원서명자가 등록하는 내용은 위임내용, 위임시작시점, 위임종료시점, 위임에 대한 제약사항에 대하여 상세하게 명시한 후 원서명자의 개인키로 서명하여 전송한다.

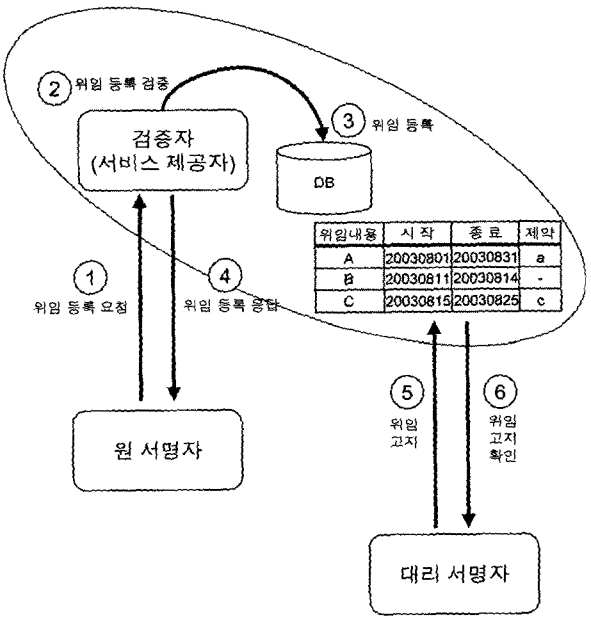
② 검증자는 원서명자로부터 전송받은 위임등록에 대한 검증을 수행한다. 원서명자의 인증서의 유효성과 위임내용의 디지털 서명의 검증 후 결과를 반영한다.

③ 위임정보의 디지털 서명 검증이 정상적으로 이루어졌다면 위임내용, 위임시작시점, 위임종료시점, 제약사항에 대하여 데이터베이스에 등록하여 대리 서명자의 권한을 설정한다.

④ 검증자는 원서명자의 위임 등록 요청에 대하여 검증과 등록 결과를 응답한다.

⑤ 대리 서명자가 검증자의 서비스를 제공받기 위해 로그인을 한 경우 원서명자가 대리 서명자에게 위임한 내용에 대해 고지한다.

⑥ 대리 서명자는 검증자의 서비스를 통해 제공받은 원서명자의 위임내용에 대해 인지하였다는 것을 확인한다.



(그림 2) 위임등록 프로토콜 시나리오

(그림 3)은 제안하는 위임 디지털 서명의 시나리오를 나타낸 것이다. 대리 서명자는 원서명자로 위임받은 권한을 인지한 후, 원서명자를 대신하여 디지털 서명을 수행한다. 이때 검증자는 위임 등록된 위임내용, 위임기간, 제약사항을 확인함으로서 전부 또는 제한적인 위임을 가능하게 한다.

대리 서명자의 디지털 서명과 검증은 다음의 구성과 같다.

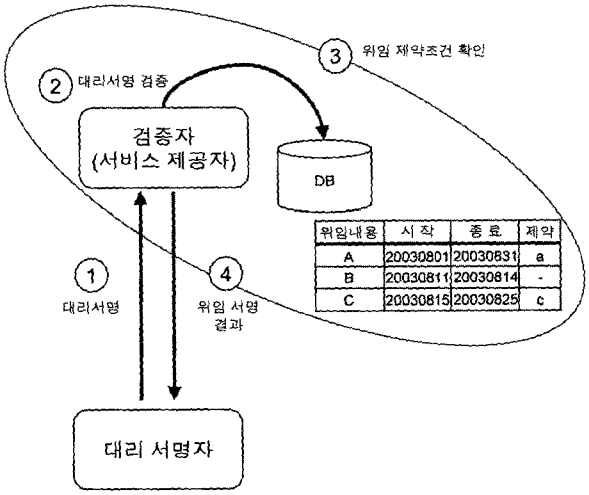
① 대리 서명자는 원서명자를 대신하여 대리 서명자의 개인키로 디지털 서명을 수행한다. 이러한 서비스는 증권거래시스템, 전자결제와 같이 전부 또는 부분적인 권한

을 위임할 수 있는 서비스에 적합하다. 특히 다수의 그룹이 디지털 서명을 수행할 경우를 고려한다.

② 검증자는 대리 서명자의 디지털 서명을 검증한다. 우선적으로 대리 서명자의 인증서를 검증한 후 위임 디지털 서명에 대해 검증을 수행한다.

③ 검증자인 서비스제공자는 대리서명의 검증이 정상적이라도 이미 위임등록 프로토콜을 통해 데이터베이스에 등록된 위임내용, 위임기간, 제약사항에 대해 확인을 한다. 따라서 대리 서명자는 원서명자가 정의한 권한 내에서 디지털 서명을 수행할 수 있다.

④ 대리서명 검증이 정상적이고 위임권한이 확인되면 검증자는 해당하는 결과를 대리 서명자에게 응답한다.



(그림 3) 대리서명 및 검증 시나리오

(그림 4)는 제안하는 위임해제 프로토콜을 나타낸 것이다. 원서명자는 위임기간 내에도 보안상 문제가 발생하거나 기타의 사유로 인해 즉시 해제할 수 있는 기능이 제공되어야 한다. 위임해제 프로토콜은 원서명자의 판단으로 발생하며 검증자에게 위임해제를 통보하도록 제안한다.

① 원서명자는 검증자인 서비스제공자의 서버에 접속하여 대리 서명자에 대하여 위임해제를 요청한다. 해제시점과 해제내용에 대해 명시한 후 원서명자의 개인키로 서명하여 전송한다.

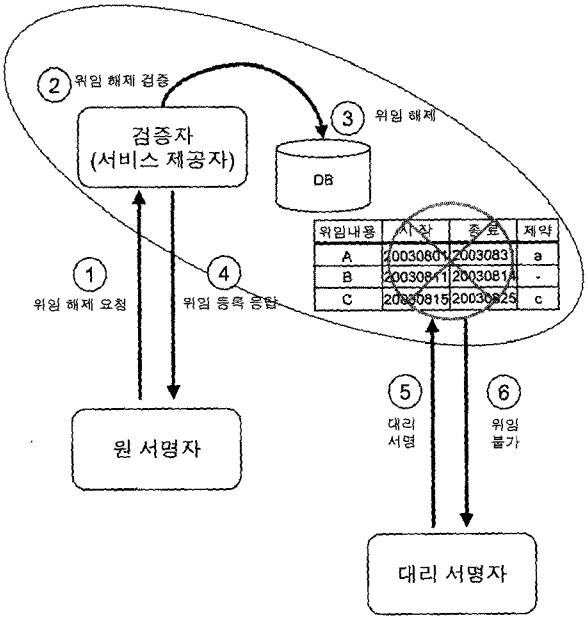
② 검증자는 원서명자로부터 전송받은 위임해제에 대한 검증을 수행한다.

③ 위임해제의 디지털 서명 검증이 정상적으로 이루어졌다면 대리 서명자의 권한을 해제한다.

④ 검증자는 원서명자의 위임해제 요청에 대하여 결과를 응답한다.

⑤ 대리 서명자가 서명을 하게되면 검증자는 원서명자에 의해서 위임이 해제되었다는 것을 확인한다.

⑥ 검증자는 대리 서명자에게 원서명자의 위임해제로 인한 대리서명 불가를 통보한다.



(그림 4) 위임해제 프로토콜 시나리오

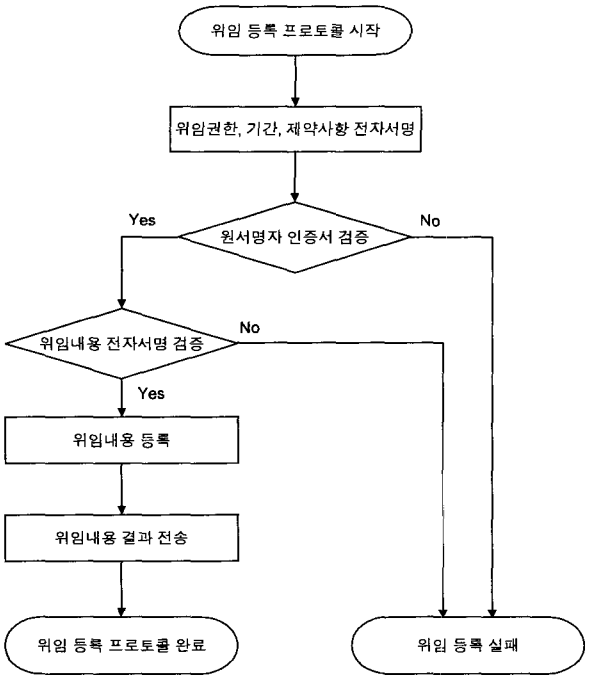
4.3 위임 등록/해제 알고리즘

(그림 5)에 위임 등록 알고리즘을 도식화하였다. 원서명자는 대리 서명자의 위임권한, 위임기간, 제약사항에 대하여 위임 등록을 기술한 후 디지털 서명을 수행한다. 위임내용에 대하여 원서명자의 디지털 서명을 검증하여 상세한 권한을 설정함으로서 이에 대한 권한제어가 가능하다. 검증자는 대리 서명자의 인증서 유효성을 검증한 후 위임내용에 대한 디지털 서명 검증을 수행한다. 원서명자의 위임내용에 대해 디지털 서명을 검증함으로서 보안성과 부인방지 기능을 제공한다. 위임내용에 대해 데이터베이스에 설정한 후 원서명자와 대리 서명자에게 권한 위임을 고지한다. 검증자는 온라인서비스를 제공하는 서버이기 때문에 사용자의 로그인시 내용을 전송한다. 제안한 알고리즘을 적용하면 기존의 인증이 적용된 서비스에 추가적인 시스템이나 새로운 인증서의 발급 없이 경량화된 적용이 가능하다. 또한 보안성과 제한적인 위임을 제공한다.

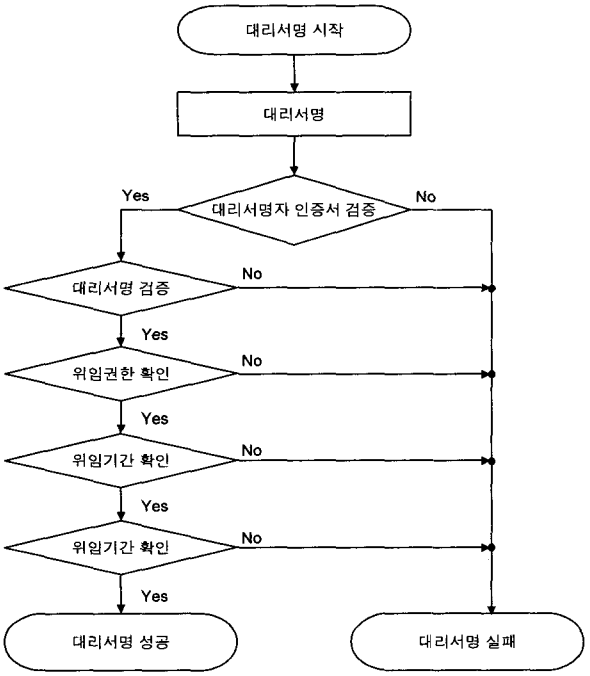
본 논문이 제안한 위임등록 프로토콜은 최종적으로 대리 서명자가 원서명자의 권한을 승계받게 된다. 기존의 대리서명에 대한 연구는 위임권한에 대해 상세화된 설정을 제공하지 않았으나 제안한 방식은 상세한 권한설정 내에서 디지털 서명을 수행한다.

(그림 6)에 대리서명 알고리즘을 명시하였다. 대리 서명자가 본인의 인증서를 이용하여 원서명자의 권한을 승계하여 디지털 서명을 수행한다. 수행된 디지털 서명에 대하여 검증자는 대리 서명자의 인증서의 유효성과 디지털 서명의 데이터를 검증한다. 디지털 서명 검증이 유효하더라도 적합

한 권한내에서 이루어졌는지 검증자는 위임등록 프로토콜에 정의된 내용을 확인한다. 위임내용, 위임기간, 제약사항을 데이터베이스에서 순차적으로 검색한 후 적합할 경우에만 디지털 서명이 유효하다.

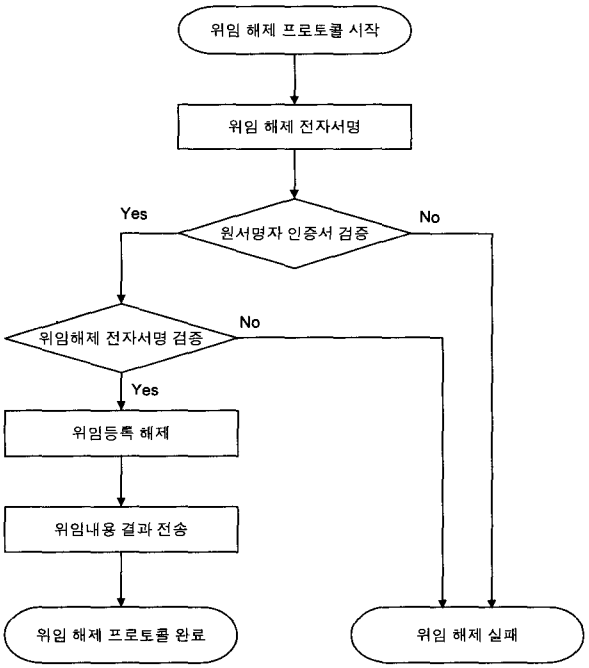


(그림 5) 위임등록 알고리즘



(그림 6) 대리서명 알고리즘

(그림 7)에서는 원서명자의 위임 해제 요청에 따라서 대리 서명자의 권한을 정지시키는 알고리즘을 도식화하였다. 위임해제 프로토콜은 원서명자의 판단에 의하여 이루어지며 해제사실에 대하여 검증자에게 디지털 서명으로 통보를 하면 검증자는 위임해제를 데이터베이스에 반영하여 이후에 발생하는 해당 대리서명을 유효하지 않게 처리한다.



(그림 7) 위임해제 알고리즘

5. 실험 및 평가

5.1 실험 환경

실험환경은 시스템 하드웨어로 펜티엄 IV 1.6GHz, 시스템 메모리 256M SDRAM을 사용하였고 운영체제로 Windows 2000 Server를 사용하였으며 데이터베이스로 MY-SQL 4.0.9를 사용하였다. JAVA 및 JSP 프로그램 언어를 사용하여 개발하였으며 JSP 컴파일러는 Tomcat V4를 이용하였다. 인증모듈은 국내 공인인증기관이 제공하는 클라이언트와 서버 툴킷을 적용하였고 디지털 서명 알고리즘은 RSA 1024bit, 해쉬함수는 SHA-1으로 국제 표준을 준용하였으며 대칭키 알고리즘은 국내 금융기관에서 준용하는 SEED로 구현하였다.

5.2 실험 평가

본 논문에서는 디지털 서명 알고리즘으로 RSA을 구현하였다. RSA 알고리즘에서 서명자 A의 경우는 충분히 큰 소수 p_A, q_A를 선택하여 $n_A = p_A \cdot q_A$를 계산하고 $\varphi(n_A) = (p_A - 1)(q_A - 1)$과 서로소인 e_A를 선택하여 $e_A \cdot d_A \equiv 1 \bmod \varphi(n_A)$를 만족하는 d_A를 구한 후, e_A는 공개키로서 사용하고 d_A는 비밀키로 보관한다. e_A, n_A는 서명검증을 위한 원서명자의 공개정보이고 e_C, n_C는 서명검증을 위한 대

원서명자 A	공개정보 e_A, n_A	검증자 B
P : 위임등록 내용 DN : 대리 서명자의 인증서 DN $Serial$: 대리서명자의 인증서 일련번호 C : 위임내용 T : 위임기간 L : 제약사항 $Cert_A$: 원서명자 A의 인증서 $P = DN \parallel Serial \parallel C \parallel T \parallel L$ $H = h(P)$ $S \equiv H^{d_A} \bmod n_A$	$M, S, Cert_A$ →	$H' = h(P)$ $H \equiv S^{e_A} \bmod n_A$ $H = H'$ 검증 결과가 참이면 → DN, Serial, C, T, L에 대한 내용을 데이터베이스에 삽입 TRUE 검증 결과값 전송 결과가 거짓이면 → FALSE 검증 결과값 전송

(그림 8) 위임등록 프로토콜

대리 서명자 C	공개정보 e_C, n_C	검증자 B
M : 대리 서명 $Cert_C$: 대리 서명자 C의 인증서 $H = h(M)$ $S \equiv H^{d_C} \bmod n_C$	$M, S, Cert_C$ →	$H' = h(M)$ $H \equiv S^{e_C} \bmod n_C$ $H = H'$ 검증 결과가 참이면 → 대리서명 M을 데이터베이스의 DN, Serial, C, T, L의 내용들과 비교 → 결과가 참이면 TRUE 검증 결과값 전송 → 결과가 거짓이면 FALSE 검증 결과값 전송 결과가 거짓이면 → FALSE 검증 결과값 전송

(그림 9) 대리서명 절차

리 서명자의 공개정보이며 d_A는 비밀서명생성 정보이다. 일방향 해쉬함수는 원문 P를 서명할 수 있는 크기로 압축 $H=h(P)$한다. 압축된 서명문 H에 대한 서명 $S \equiv H^{d_A} \bmod n_A$를 계산한다.

(그림 8)은 위임등록 프로토콜을 기술한 내용으로서 위임등록 내용 P는 대리 서명자의 인증서 DN(Distinguish Name), 위임내용 C, 위임기간 T, 위임제약 L의 내용을 가지고 있다. 원서명자 A가 서명한 내용 S에 대해 검증자 B가 검증하여 검증결과가 정상적이면 데이터베이스에 위임정보를 저장한다. 기존의 대리서명 권한의 제약보다 상세한 조건이 가능하며 원서명자가 대리 서명자의 인증서 DN을 지정하였기 때문에 위조가 불가능하다. 그리고 원서명자가 대리 서명자의 DN을 명시하였기 때문에 양도가 불가하며 원서명자가 대리 서명자의 권한에 대해 상세하게 명시하였기 때문에 오용방지가 가능하다. 또한 별도의 대리 서명자의 키쌍 생성을 하지 않기 때문에 효율적인 결과를 나타낸다.

(그림 9)는 대리서명 절차를 기술한 내용으로서 대리 서명자 C는 원서명자와 동일하게 대리서명 M에 대해 본인의 개인키로 디지털 서명을 수행한다. 검증자 B는 검증결과가 정상적이면 데이터베이스에 위임정보를 비교하여 적합한 위임권한인지 검증한다. 대리서명으로부터 대리 서명자의 신원을 인증서를 통해 확인할 수 있기 때문에 검증성이 보장되며 대리 서명자의 인증서는 기존의 발급된 인증서를 적용하기 때문에 신원성이 보장된다. 대리 서명자 C가 수행한 디지털 서명에 대해 제약조건을 비교함으로서 적합성이 확인되며 검증자 B가 대리 서명자 C의 디지털 서명을 보유할 경우 부인방지가 가능하다.

<표 1>은 제안하는 위임등록 프로토콜의 실험데이터를 보여준다. 측정횟수는 측정횟수 10,000번 수행 평균값을 나타내며 명시된 단위는 [ms] : Milliseconds(10^{-3}초), [μs] : Microseconds(10^{-6}초)를 나타낸다. RSA의 암호강도는 공인인증기관에서 적용하고 있는 RSA 1024bit 알고리즘으로 적용하였다.

〈표 1〉 위임등록 프로토콜의 실험데이터

기 능		초당 처리량	1회 처리시간
위임 등록	Sign RSA 1024 bit	58.91 [KB/sec]	16.97 [ms]
	Verify RSA 1024 bit	128.45 [KB/sec]	7.78 [ms]
대리 서명	Sign RSA 1024 bit	33.93 [KB/sec]	29.46 [ms]
	Verify RSA 1024 bit	22.90 [KB/sec]	43.65 [ms]

<표 2>는 제안하는 방식과 기존 방법을 비교 분석한 결과를 보여주고 있다. 대리서명의 보안 요구사항들을 기준으

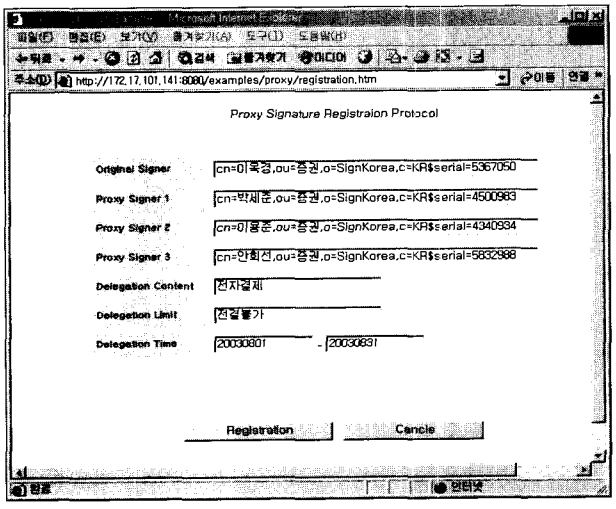
로 MUO(Mambo, Usuda, Okamoto), PH(Petersen, Horster), KPW(Kim, Park, Won), DQ(Delos, Quisquater), SNPS (Strong Nondesignate Proxy Signature)의 기법들과 제안하는 PRP(Proxy-Register Protocol)를 비교 분석하였다.

〈표 2〉 PRP 기법과 기존 기법과의 비교 분석

	MUO	PH	KPW	DQ	SNPS	PRP
검증성	O	O	O	O	O	O
위조불가능성	O	×	O	×	O	O
신원확인성	O	O	O	O	O	O
부인 불가능성	O	×	O	O	O	O
오용방지	×	×	O	×	O	O
권한의 제약	×	×	△	×	△	O
양도불가	×	△	O	△	O	O
적합성 확인	×	×	×	×	O	O
Strong	×	×	O	×	O	O
Non-designate	×	×	×	×	O	O
위임인증서 및 키 생성여부	필요	필요	필요	필요	필요	필요 없음

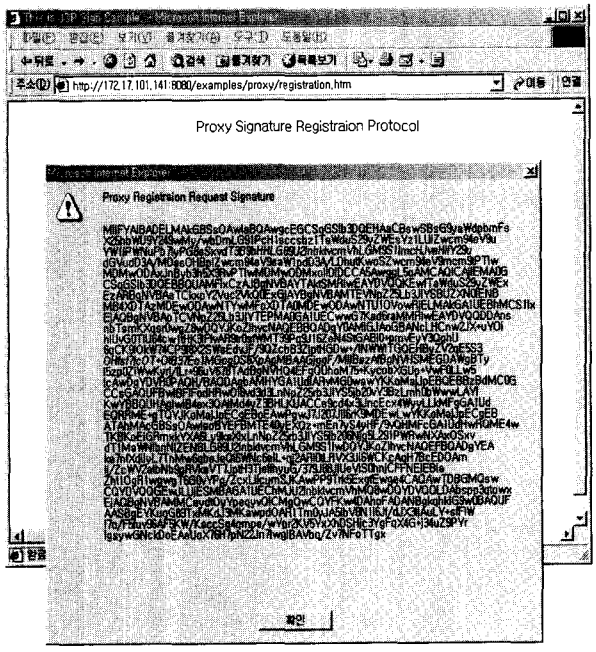
위에서 설계된 개념을 바탕으로 위임등록 프로토콜을 구현하였다. 구현된 부분의 위임등록 과정은 아래그림과 같다.

(그림 10)은 원서명자가 대리 서명자의 집합을 설정해서 등록을 요청하는 과정을 나타내었다. 원서명자가 세명의 대리 서명자를 지정하는 것을 보여주고 있으며 이때 대리 서명자의 유일한 식별을 위해서 인증서의 DN과 함께 Serial 도 지정함으로서 동명이인과 같은 사용자의 충돌을 막을 수 있다. 위임내용과 위임제약을 상세히 명시함으로서 검증자 관점에서 위임내용에 대한 부인방지가 가능하다. 특히 위임기간의 개시와 종료시간을 검증자 측면에서 명시함으로서 기존의 위임기법에 비하여 안전성이 확보된다.



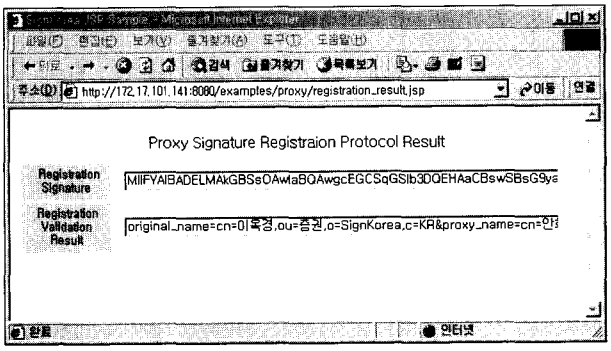
(그림 10) 위임등록 절차(1)

(그림 11)은 원서명자의 개인키로 디지털 서명을 수행하는 과정을 나타내었다. 공인인증기관의 개인키로 위임내용에 대해 디지털 서명을 하고 인증서를 첨부하였기 때문에 원서명자의 신원확인, 부인방지, 무결성이 보장된다.



(그림 11) 위임등록 절차(2)

(그림 12)는 검증자가 원서명자의 위임등록 디지털 서명을 검증한 후 데이터베이스에 등록한 결과를 보여주고 있다. 이후 대리 서명자가 원서명자를 대신하여 디지털 서명을 수행하였을 때 검증자가 보유한 데이터베이스의 위임내용에 대해 정밀한 확인과정을 거치기 때문에 검증자는 대리 서명자의 잠재적인 위험에 대해 보다 안전하다. 또한 원서명자 관점에서는 추가로 대리 서명자에게 신뢰되는 통신으로 위임 서명키를 생성하거나 위임정보에 관한 사항을 전달할 필요가 없다.



(그림 12) 위임등록 절차(3)

6. 결 론

대리서명은 사용자가 자신의 서명 권한을 위임할 필요가

있을 경우 유용하게 사용될 수 있는 기술이다. 그러나 인터넷과 같은 분산환경에서 원서명자나 위임자를 신뢰하기는 매우 어려운 문제이다.

본 논문에서는 기존 대리 서명의 보안 요구사항을 만족하는 위임 등록 프로토콜을 설계하였다. 제안한 기법은 대리서명의 보안 요구사항을 모두 만족하며 기존의 방법보다 강력하다. 또한 기존의 인증서를 사용하기 때문에 위임을 위한 인증서를 따로 생성할 필요가 없으며 이에 따른 위임 키쌍을 생성할 필요가 없으므로 처리 속도가 빠르다. 또한 기존 기법들의 문제점을 해결하였고 위임 등록 프로토콜의 적용은 실제 환경의 보안 요구사항을 분석하여 이루어지며 정의된 요구사항에 맞는 구조를 제공해줄 수 있다. 제안된 기법을 사용하여 전자 상거래에서의 대리서명 기법을 보다 안전하게 제공할 수 있고 이러한 기술은 전자결제와 증권거래시스템과 같은 응용 환경에 적용될 수 있으며 증권에서의 위임에 적용하였을 경우 현재의 HTS(Home Trading System) 프로세스의 변경없이 보다 안전한 방법으로 적용가능하다.

제안한 위임등록 프로토콜은 기존의 공인인증기관 환경의 인증서를 이용하여 추가적인 개선사항 없이 원서명자와 검증자간의 관점에서 적용이 가능하다. 그러나 기존의 위임정보를 모든 대리서명에 첨부하는 방식보다는 효율적이나 위임서명키를 생성하는 메커니즘에 비해 각 검증자에게 별도로 등록해야 하기 때문에 인증 서버에 대한 오버헤드가 나타날 수 있다. 따라서 향후 각 검증자에게 위임 등록정보와 위임해제를 통합하여 전송할 수 있는 제 3의 전송방식이 요구된다.

참 고 문 헌

[1] B. Lee, H. Kim, K. Kim, "Strong Proxy Signature and its Applications," Proc. of SCIS, 2001.

[2] HB. Lee and K. Kim. "Self-Certificate : PKI using Self-Certified Key," Proc. of Conference on Information Security and Crtptology, 2000.

[3] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures : Delegation of the power to sign message," IEICE Trans. Fundamentals, Vol.E79-A, No.9, 1996.

[4] M. Bellare and S. Miner, "A forward-Secure digital signature scheme," Crypto '99, 1999.

[5] S. J. Kim. S. J. Park and D. H. Won, "Nominative signatures," Proc. ICEIC '95, 1995.

[6] M.Abe, T. Okamoto, "Provably secure partially blind signatures," In Advances in Cyyptologt Crypto, 2000.

[7] H. Petersen and P. Horster, "Self-certified keys Concepts and Applications," In Proc. Communications and Multimedia Security '97, 1997.

[8] D. Chaum, "Blind signatures for untraceable payments," Advances in Cryptology : Crypto '82, Prenum Publishing Corporation, 1982.

[9] P. Horster, M. Michels, H. Petersen, "Hidden signature schemes based on the discrete logarithm problem and related concepts," Proc. of Communications and Multimedia Security '95, Chapman & Hall, 1995.

[10] B. Lee, H. Kim and K. kim, "Secure mobile agent using strong non-designated proxy signature," Proc. of ACISP 2001, LNCS 2119, Springer-Verlag, 2001.

[11] L. Yi, G. Bai and G. Xiao, "Proxy multi-signature scheme : A new type of proxy signature scheme," Electronics Letters, Vol.36, No.6, 2000.

[12] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms," IEEE Tran. Information Theory, Vol.31, No.4, 1985.

[13] D. Chaum and H. van Antwerpen, "Undeniable signatures," Advances in Cryptology-CRYPTO '89 Proceedings, Springer -Verlag, 1990.

[14] K. Shum and Victor K. Wei, "A strong proxy signatures scheme with proxy signer privacy protection," Proceedings of the Eleventh IEEE International Workshops on Enabling Technologies : Infrastructure for Collaborative Enterprises, 2002.

[15] M. Mambo, K. Usuda and E. Okamoto, "Proxy signatures for delegating signing operation," Proc. Third ACM Conf. on Computer and Communications Security, 1996.

[16] V. Varadharajan, P. Allen and S. Black, "An analysis of the proxy problem in distributed systems," Proc. 1991 IEEE Computer Society Symposium on Research in Security and Privacy, 1991.

[17] C. Gamage, J. Leiwo and Y. Zheng, "An efficient scheme for secure message transmission using proxy-signcryption," Technical Report 98-01, Peninsula School of Computing & Information Technology, Monash universirt, July, 1998.

[18] H. M. Sun, "On proxy(multi) signature schemes," Proceedings of the 2000 ICS : Workshop on Cryptology and Information Security, 2000.

[19] K. Zhang, "Threshold proxy signature schemes," 1997 Information Security Workshop, 1997.

[20] Byungcheon LEE, Kwangjo Kim, "Strong Proxy Signatures," IEICE Trans. Fundamentals, No.1, 1999.

[21] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology-Crypto 84, 1984.

[22] M. Hwang, I. Lin and E. J. Lu, "A secure nonrepudiable threshold proxy signature scheme with known signers," International Journal of Informatica, 2000.

박 세 준

e-mail : atprince@nostech.co.kr
1996년 숭실대학교 수학과(이학사)
1998년 숭실대학교 대학원 컴퓨터학과 (공학석사)
2001년 숭실대학교 대학원 컴퓨터학과 (공학박사 수료)
2001년~2002년 (주)삼보컴퓨터 통신사업부
2002년~현재 (주)노스텍 R&D 센터
관심분야 : 멀티미디어, 컴퓨터통신, 정보보호, 암호학, 유무선 PKI

오 해 석

e-mail : oh@kyungwon.ac.kr
1975년 서울대학교 응용수학과(이학사)
1981년 서울대학교 계산통계학과(이학석사)
1989년 서울대학교 계산통계학과(이학박사)
1982년~2003년 숭실대학교 정보과학대학 교수
1976년~1982년 태평양화학(주), (주)삼호 전산실
1990년~1991년 일본 동경대학교 객원교수
1997년~1999년 숭실대학교 부총장
2000년~2001년 스탠포드대학교 객원교수
2003년~현재 경원대학교 IT 부총장
관심분야 : 멀티미디어, 데이터베이스, 영상처리, 정보보호, 멀티미디어 암호, 암호학, 유무선 PKI