전자 문서 보관소의 문서 정보 보안에 관한 연구

정회원 나 상 엽*, 이 승 대**

Study on Document Security Mechanism for Digital Document Repository

Sang Yeob Na*, Seung Dae Lee** *Regular Members*

요 약

전통적인 종이 문서 서류의 관리를 위한 노력과 비용은 지속적으로 증가하고 있으며 이러한 종이 문서들은 보관이 용이하지 않으며 기본적으로 보안에 취약한 약점을 가진다. 따라서 최근에는 종이 문서들을 전자화 하여 전자 문서 보관소에 보관하고자하는 연구가 많이 진행되고 있다. 또한 전자 문서 보관소의 경우 최근에는 공인된 기관에서 공인된 제 3자에 의하여 보관되고 제공되는 방법도 제시되고 있다. 전자 문서 보관소의 경우 문서를 전자화하여 보관, 관리하게 되므로 종이 문서를 관리하는 것보다 비용이 적게 소요되는 장점을 가진다. 그러나 이들 전자화된 문서의 보관, 관리를 위한 체계적인 보안 방법이 제시되지 않고 전자 문서 보관소를 소유, 운영하는 기관의 필요에 의하여 보안방법이 제시되고 있어 이들 문서에 대한 체계적인 보안 관리 기법이 필요하다. 본 논문에서는 전자 문서 보관소의 문서 정보 보안을 위한 기본적인 방법들을 연구, 제시하며 이를 통하여 보다 저렴하고 안전한 전자 문서 보안 방법과 보안에 보다 효율적인 전자 문서 보관소의 관리 기법을 제시한다.

Key Words : Digital Document, Security, Document Repository

ABSTRACT

The management and deposit of paper document costs are increased gradually. Specially, it is too expensive to safekeeping paper document in the warehouse. Also paper based document system is exposed in several security problems. Therefore, demands of transformation process from paper document into electronic ones are quietlyneeded. Electronic document repository system is one of the best solutions for solving paper based document system issues.Electronic document repository system can reduce overall costs and provides some advantages in comparison with paper based document system. But, electronic document repository system has no formal methodology for guarantee safeties. Therefore, we suggest a security mechanism for establish electronic document repository system. Suggested security methodology can help for design of more secure electronic document repository system.

Ⅰ. 서 론

최근까지 서류나 문서를 이용하는 방법은 종이에 내용을 수기, 출력 또는 다른 방법으로 표시를 하여 사용하여 왔다. 이러한 종이 문서를 이용하는 방법은 많은 단점을 가지고 있다. 예를 들어 우편물, 팩시밀리를 포함하여 다른 매체를 통해 옮기는 동안에 분실되거나 의도적 또는 비의도적으로 쉽게 변조, 위조될 수 있으며 이를 보관, 관리하기 위한 비용 또한 지속적으로 증가하고 있다. 이러한 일련의 문제를 해결하

※ 이 논문은 2009학년도 남서울대학교 학술연구비 지원에 의하여 연구되었음
* 남서울대학교 컴퓨터학과 (nsy@nsu.ac.kr), ** 남서울대학교 전자공학과(seungdae@nsu.ac.kr)
논문번호 : 10051-1130, 접수일자 : 2010년 11월 30일

고자하는 시도와 정보화 기기들의 발전으로 인하여 종이 문서들이 전자화된 기기에 의하여 종이에 출력되지 않고 전자 기기 내에서 문서로서의 기능을 수행하는 현상도 보편화 되어 가고 있다. 이러한 전자 문서들의 저장, 접근 그리고 효율적인 사용을 위하여 전자 문서 보관소가 필요하게 되었고 전자 문서 보관소는 사용하는 사람들에게 그들의 문서가 적절하게 보관, 이용되고 있다는 것을 보장하여야 한다. 이를 위하여 전자 문서 보관소의 문서 정보 보안에 관한 내용은 다음과 같은 기본 기능을 수행하여야 한다.

전자 문서 보관소는 사용자들이 신뢰할 수 있어야 하고, 필요한 경우 원하는 문서에 연결 할 수 있어야 하며, 문서의 내용에 변화가 발행하는 경우 즉시 탐지가 가능하여야 한다. 일단 전자화된 문서는 문서 보관소에 보관되므로 중앙 관리의 특성상 문서 분실의 가능성은 높지 않으나 다른 사람에 의하여 위, 변조 되거나 허가 되지 않은 비인가 자에게 노출될 수 있는 가능성은 증가한다. 따라서 전자 문서 보관소의 보안 문제는 상당히 중요하다.

본 논문에서는 전자 문서 보관소의 전반적인 보안 문제를 해결하기 위한 보안 관리 체계를 제시하고 전자 문서의 효율적이고 안전한 보관을 위한 새로운 보안 자료 구조를 제시한다. 본 논문에서 제시하는 자료 구조는 원본 문서를 디지털화 하여 이의 보관과 참조에 이용하는 메타-데이터를 함께 저장하도록 한다. 이를 통하여 디지털화된 원본 문서 및 그의 사용에 관련된 보안 자료를 함께 저장, 관리하게 되므로 전자 문서 보관소에 보관되는 문서를 보다 안전하게 보관, 사용할 수 있도록 한다.

본 논문의 구성은 다음과 같다. 2장에서는 전자 문서 보관소의 기본 기능과 문서 보관의 형태에 대하여 설명하고 3장에서는 전자 문서 보관소에 요구되는 보안 기능에 대하여 기술한다. 4장에서는 전자 문서 보관소의 새로운 문서 보안 방법론과 각각의 기술에 대하여 설명하고 마지막 5장에서는 결론과 앞으로의 연구과제에 대하여 기술한다.

Ⅱ. 전자 문서 보관소의 기본 기능과 자료 구조

현재 산업체등에서 사용하는 종이 문서의 사용, 보관에 들어가는 비용은 계속 증가하는 추세이고 최근 산업화와 정보화의 영향으로 종이 문서를 전자 문서로 대치하고 이를 보관, 관리하는 전자 문서 보관소의 필요성은 계속 증가하고 있다. 전자 문서 보관소의 경우 기존의 종이 문서를 대치하기 위하여 안전한 문서 보관, 전자화된 문서의 공인 인증, 그리고 전자 문서의 올바른 문서 전달 등의 기본 기능이 필요하다. 안전한 문서 보관이란 문서의 작성, 관리, 탐색, 백업 그리고 복구 등의 기능을 의미한다. 공인 인증 기능은 전자 문서의 등록, 운반, 기본 인증 등의 기능을 제공하여야 하며 문서 전달은 전자 문서의 분배, 허가된 사용자의 접근, 암호화 그리고 송-수신 확인 등의 기능을 제공하여야 한다.

2.1 전자 문서 보관소의 기본 기능

전자 문서 보관소가 각각의 사용자에게 올바른 문서 보관, 검색, 사용 등의 기능을 제공하기 위한 문서 보관소의 기본 기능으로는 전자 문서의 작성, 문서 전달, 문서의 백업과 복구, 그리고 사용자 로그 보관 등의 기능을 제공하여야 한다.

사용자가 기존의 종이 문서 대신에 전자 문서를 작성하는 경우 사용자가 정의하는 문서의 보안 레벨, 문서의 유효 기간, 문서의 작성 일자, 시간 등의 기본 정보가 문서의 내용과 함께 전자 문서 보관소에 저장되어야 한다.

문서 전달 기능은 문서를 접근하고자 하는 사용자에게 문서를 올바르게 전송하고 전송 여부를 시스템에 보관하는 기능인데 이를 수행하기 위해서는 사용자가 문서를 요청하는 경우 문서 보관소가 문서를 전송하여 주고 전송상의 문제가 발생하지 않은 경우 자동으로 사용자의 수신 정보를 시스템에 저장하여야 한다.

전자 문서 보관소에 보관 되는 전자 문서의 안전한 보관을 문서 백업과 복구는 정기적으로 자동화되어 제공되어야 한다. 이는 시스템 내에 보관되는 문서의 중요도에 따라 다르게 적용될 수 있고 사용자가 문서를 작성하는 단계에서 사용자의 입력 사항을 받아 보관소 시스템에서 정의하여 적용할 수 있어야 한다. 또한 어떠한 이유에 의하여 보관된 문서에 오류가 발생하는 경우 백업 시스템을 이용하여 복구하는 기능이 제공되어야 한다.

위에서 언급한 기능 외에도 모든 사용자나 시스템의 작업이나 상호 작용에 대한 정보는 문서 보관소 시스템에 로그 형태로 저장하여 각 사용자의 작업이나 시스템의 운영 상황을 실시간으로 파악할 수 있는 기능이 제공 되어야 한다.

2.2 전자 문서 보관의 형태

전자 문서 보관소에서 사용하는 전자 문서의 자료 구조는 문서 보관소의 기능을 수행하거나 보관 문서

정보 보안에 중요한 요소이다. 문서 보관소에서 사용하는 문서의 구조는 사용자가 작성한 문서 자체 외에도 문서 보안에 관련된 자료들도 같이 사용할 수 있도록 정형화되고 개방된 구조로 이루어 져야 한다. 이를 위하여 문서가 각각의 사용자에게 전달된 이후에도 문서에 접근 권한을 가진 사용자만이 올바른 방법으로 문서를 사용하는지에 대한 정보도 같이 전달되어야 한다. 전자 문서의 특성상 한 번 사용자에게 전달된 전자 문서는 허가되지 않은 사람도 문서에 접근 할 수 있고 복사되어 다른 사용자에게 제공될 수도 있는 문제가 있다. 따라서 전자 문서 보관소에 저장되거나 각각의 사용자에게 전달되는 전자 문서들은 올바르지 않은 방법으로 사용되지 않도록 일련의 문서 보안 정보를 함께 포함하여 유지 되어야 한다.

Ⅲ. 전자 문서 보관소의 보안 요구 사항

사용자에 의하여 전자 문서 보관소에 전자 문서가 만들어지면 전자 문서 그 자체는 중앙 보관소에 저장되고 백업 시스템에 의하여 보호되므로 보관소 내부에 저장되는 문서들은 유실될 가능성이 미비하다. 그러나 사용자에게 전달되는 전자 문서들은 전자 문서 보관소 시스템 밖으로 유출되고 사용자에 의하여 관리되므로 여러 가지 보안 취약점을 가지게 된다. 전자 문서 보관소 밖으로 유출된 문서에서 야기되는 보안 취약점은 문서의 인증(Authenticity), 무결성(Integrity), 검증(Verification), 그리고 부인-방지(Non-Repudiation) 등이 있다. 이를 해결하기 위하여 문서 보관소 밖으로 전달되는 전자 문서들은 여러 가지 보안 정보들을 가지고 있어야 한다. 위에서 언급된 보안 취약점들의 특징은 다음과 같다.

3.1 전자 문서의 인증(Authenticity)

사용자에게 전달된 전자 문서는 전자 문서 보관소에 보관된 문서와 일치하는 정보를 제공하여야 한다[3]. 이는 전달된 문서가 그의 원본과 상이 하지 않음을 증명하여야 하는데 이는 다른 사용자에 의하여 문서의 내용이 변환되지 않았음을 나타낸다. 전자 문서의 인증은 디지털 서명(Digital Signature)[4]에 의하여 제공될 수 있다. 디지털 서명에는 서명자의 디지털 신원 정보를 포함하게 되는데 이를 통하여 문서의 수신자는 서명된 문서가 전자 문서 보관소에 서명자의 의하여 생성, 저장되고 등록한 이후 문서의 내용이 변경되지 않았음을 인지한다.

3.2 전자 문서의 무결성(Integrity)

전자 문서의 무결성이란 전자 문서의 내용이 허가되지 않은 방법으로 변경되지 않았음을 의미한다. 이는 전자 문서가 사용자에 의하여 생성 될 때 생성자의 원본 문서와 동일하게 전자 문서 보관소에 저장되었음을 나타내거나 전자 문서 보관소로부터 사용자가 전송 받은 문서가 전송되는 도중에 다른 누군가에 의하여 변경되지 않았음을 나타내어야 한다. 전자 문서의 무결성 보장을 위하여 한 방향 해쉬 코드(One Way Hash Code), 메지지 인증 코드(Message Authentication Code : MAC)[5] 또는 순환 중복 코드(Cyclic Redundancy Code : CRC)[6]를 사용 한다.

이러한 기술들은 각각 장단점을 지니고 있는데 한 방향 해쉬 코드의 경우 매우 견고한 무결성을 제공하는 장점을 가지고 있지만 이를 수행하기위한 비용이 많이 드는 단점을 가지고 있고 메시지 인증 코드의 경우 한 방향 해쉬 코드에 비하여 비용은 조금 적게 들지만 상대적으로 견고 하지 못한 단점을 가지고 있다.

따라서 위에서 언급한 기술에 의하여 보안을 적용한 전자 문서는 문서의 무결성을 제공하는 것이고 무결성이 제공되는 전자 문서를 사용하는 사용자는 자신이 전송받은 문서가 위조되거나 변조되지 않고 전자 문서 보관소에 보관되어 있는 원본 문서와 일치한다는 것을 알고 문서를 사용 할 수 있다.

3.3 전자 문서의 검증(Verification)

전자 문서 보관소의 사용자는 자신이 사용하게 되는 문서가 올바른 문서인지 검증하여야 하는데, 이는 단순히 작성자 또는 사용자의 아이디와 비밀 번호 또는 문서 비밀 번호에 의하여 수행 될 수 있다. 그러나 이러한 인증 과정은 단순히 전자 문서 보관소의 사용을 위한 검증은 가능하지만 사용자의 문서 갱신이나 전자 문서 보관소 내에서 수행하는 여러 작업에 대한 검증은 보장할 수 없다.

따라서 전자 문서 보관소는 기존에 존재하는 문서의 갱신이나 삭제 등의 문서의 내용에 변화를 줄 수 있는 작업에 대하여 단순히 사용자의 보관소 시스템 사용 허가를 위한 아이디와 패스워드를 통한 인증을 수행하는 것 이상의 보다 엄격한 사용자의 시스템 내에서의 작업에 대한 검증과 확인을 필요로 한다.

3.4 전자 문서의 부인 방지 (Non-Repudiation)

전자 문서의 부인-방지는 문서의 송신자나 수신자가 각각 자신의 송수신작업에 대한 증명을 의미한다. 이는 전자 문서의 송수신 작업에 있어 송신자나 수신

자가 안전한 방법으로 사용자 인증 이후에 송수신에 참여 하였다는 것을 나타내어야 하며 또한 송수신이 완료된 이후에 참여 여부를 부정 할 수 없게 시스템에서 관리하여야 함을 의미한다[7].

전자 문서 보관소에 보관되는 문서들은 문서의 작성자 또는 전자 문서를 갱신하는 사용자가 자신의 작업에 대하여 서명하여 저장하는 경우 사용자의 저장이나 갱신 행위에 대한 부정을 하지 못하게 관리 하여야 하는데 이는 사용자 인증(User Authentication), 시간 날인(Time Stamping) 그리고 전자 서명(Digital Signature)등의 기법으로 제공 된다.

Ⅳ. 전자 문서 보관소의 보안 방법론

전자 문서 보관소에서 보안을 위한 기본 단계로는 각각의 사용자들이 전자 문서 보관소 시스템을 사용하기를 원하는 단계에서 사용자 아이디와 패스워드를 통한 인증 단계를 거쳐야만 한다. 이를 통하여 기본적인 사용자 인증을 제공할 수 있으며 각각의 사용자가 시스템 내부에서 수행하는 작업의 로그를 기록함으로써 사용자의 수행 작업을 알 수 있을 뿐 아니라 각 사용자가 전자 문서 보관소 시스템에 저장된 문서에 대하여 수행하는 작업도 기록할 수 있게 한다. 본 논문에서 제안하는 전자 문서 보관소의 필수 보안 요소는 다음과 같다.

- 사용자 인증(User Authentication)
- 사용자 로그 파일 저장
- 사용자 인증서(Certificate) 관리
- 사용자 공개키 관리

위에서 제시한 4가지 방법은 전자 문서 보관소의 보안을 제공하기 위한 가장 기본적이고 필수적인 요소들이다. 위의 4가지 보안 방법은 일반적인 시스템에서도 정형화 되어 많이 제공되고 있고 일반화되어 있는 내용이므로 본 논문에서는 위 기술들의 자세한 설명은 생략한다.

본 4장에서는 3장에서 정의한 전자 문서 보관소 보안 요소를 제공하기 위하여 본 논문에서 제안하는 전자 문서 보관소의 보안 기법들에 대하여 설명하고 제안하는 보안 기법들은 다음과 같다.

4.1 전자 문서의 인증(Authenticity)과 부인-방지(Non-Repudiation)를 위한 보안 기법

전자 문서 보관소 시스템은 각각의 사용자에게 인증서를 발급할 수 있는 인증기관 역할을 수행하여야 한다. 이 인증서는 사용자가 시스템에 접근하여 시스템을 사용하고자 하는 경우 사용자 인증에 사용될 수 있으며 또한 사용자가 전자 문서를 생성, 갱신, 삭제 등의 작업을 수행할 때 사용자의 신분 증명을 위한 도구로도 사용될 수 있다. 전자 문서 보관소는 사용자의 인증서를 생성할 때 사용자의 공개키와 비밀키를 생성하여 전자 문서의 인증과 문서 정보의 갱신 등에 사용한다.

또한 사용자의 전자 서명에도 공개키를 사용하게 함으로써 문서의 작성 시 작성된 문서를 사용자가 자신의 비밀키를 이용하여 압축하게 하고 해당 문서를 전송받은 사용자는 이를 공개키로 해독하여 문서가 작성자의 올바른 인증 경로로 작성되었음을 알 수 있게 한다. 또한 이는 전자 서명에도 사용할 수 있는데 작성자가 작성, 갱신한 문서는 각자의 비밀키로 압축을 수행하게 함으로 추후 문서를 사용하는 사람이 해당 문서 갱신자의 공개키를 이용함으로 해당 문서가 비밀키 사용자에 의하여 올바르게 갱신되었음을 판단할 수 있다. 이 경우 문서를 사용자의 비밀키로 압축하게 되면 해당 문서는 상응하는 공개키로 해독이 가능하게 되어 비밀키 소유자는 자신의 작업에 대한 행위의 증거로 사용되므로 이는 전자 서명으로도 사용될 수 있다.

사용자의 작업에 대한 부인-방지를 위하여 전자 문서 보관소에서 제공하는 시간 날인 기법도 사용되어야 한다. 시간 날인은 사용자의 작업에 의하여 문서의 내용이 변경(생성, 갱신 등의 작업)되는 경우 시스템에서 자동적으로 생성하여 문서에 첨부하여야 하는데 이에는 사용자의 아이디, 변경 시간, 시스템에 의하여 생성된 암호키 등의 정보를 포함하여야 한다.

4.2 전자 문서의 무결성(Integrity)과 검증(Verification) 위한 보안 기법

전자 문서 생성 시 같이 보관되는 전자 서명이나 인증서는 해당 전자 문서의 작성자를 증명하고 판단하는데 사용 가능하다. 문서를 전송받아 사용하는 사용자는 문서에 첨부된 전자 서명이나 인증서를 참고하여 문서를 작성하고 갱신한 사람의 인증은 가능하지만 문서 내용의 무결성 증명과 내용의 검증은 제공하지는 못한다. 따라서 문서의 내용이 원본의 문서와 상이하지 않다는 증명(무결성)과 검증은 다른 보안 기법으로 제공하여야 한다.

전자 문서 보관소는 제공하는 문서의 내용에 대한 무결성과 문서 내용의 검증을 위하여 페러티 비트

(Parity Bits), 한 방향 해쉬 코드, 또는 메시지 인증 코드를 문서에 포함하여 제공하여야 한다.

전자 문서 보관소에 문서가 저장, 갱신되거나 저장된 문서가 다른 사용자에게 전송되는 경우 전자 문서 보관소 시스템은 각 문서의 페러티 비트나 순환 중복 코드(Cyclic Redundancy Code)를 생성하여 해당 문서에 첨부하여야 한다. 해당 문서를 전송받은 사용자는 페러티 비트나 순환 중복 코드를 사용하여 문서의 무결성을 체크하여야 한다. 이때 해당 코드로 무결성이 보장되지 아니하면 이 문서는 제 삼자에 의하여 수정되었거나 전송 중에 어떠한 에러가 발생하여 적정하지 않은 문서이므로 사용자는 문서를 재 수신하거나 이상 정보를 전자 문서 보관소로 전송하여야 한다.

또한 문서의 무결성과 검증을 제공하기 위하여 한 방향 해쉬 코드를 사용할 수도 있는데 이 경우 전송받은 문서를 보관소 시스템이 제공하는 해쉬 모듈로 수행하여 동일한 결과를 가지는 경우 문서는 무결성과 문서의 내용에 변환이 없다는 검증 정보로 이용이 가능하다.

메시지 인증 코드 기법은 문서 작성자의 대칭키를 가지고 문서를 압축하여 전송하고 문서의 수신자는 문서 보관 시스템이 제공하는 문서 작성자의 키로 해독하여 문서의 무결성과 검증에 사용하는 방법이다. 문서의 전송 중에 제 삼자가 부정한 방법으로 문서를 획득하여 문서의 내용을 위조하고자 하더라도 시스템이 제공하는 대칭키가 없으면 문서의 위조는 불가능하다.

순환 중복 코드는 두 가지 방법으로 사용이 가능한데 이는 문서 내용을 검증하는 것과 전송되는 문서 전체를 검증하는 방법이다. 문서 내용의 검증은 실제 문서에 대하여서면 순환 중복 코드를 생성하는 방법인데 이는 문서의 내용의 무결성과 검증에 사용가능하다. 다른 방법은 전송되는 문서 전체에 대한 순환 중복 코드를 생성하는 방법인데 이는 실제 문서 이외에 전송되는 전자 서명, 시간 날인 정보, 사용자 인증서 등의 전송되는 모든 정보를 포함한다. 이 방법은 문서의 전송 중에 전체 문서에 위조가 가해지지 않았다는 검증과 무결성 제공에 사용된다.

3.2장에서 설명한 것처럼 한 방향 해쉬 코드와 메시지 인증 코드는 각각의 장단점을 가지고 있으므로 제안하는 전자 문서 보관서는 결합된 방법의 무결성, 검증 방법을 제시하는데 이 방법은 문서의 작성자가 문서 작성 시에 사용자가 문서에 필요한 보안 등급을 정의하게하고 사용자가 필요로 하는 보안 등급이 일정 레벨 이상은 경우 한 방향 해쉬 코드 방식을 사용하게 하고 그렇지 않으면 메시지 인증 코드 방식을 사용하게 한다.

V. 결 론

본 논문에서는 전자 문서 보관소의 전반적인 기능을 정의하고 이의 안전한 수행을 위한 보안방법에 대하여 기술하였다. 전자 문서 보관소는 많은 비용이 발생하는 종이 문서 시스템을 대체할 수 있는 좋은 방법이기는 하지만 아직 그의 기능과 역할이 명확히 정의되지 않았고 사회 정서상 종이 문서를 완벽하게 대체하기에는 아직은 시기상조이다. 하지만 기하급수적으로 증가하는 종이 문서의 관리 비용으로 인하여 앞으로의 요구는 점점 증가할 것이다.

전자 문서 보관소의 경우 문서의 보관이 중앙에서 이루어지므로 문서의 유실에 대한 걱정이나 보관비용의 증가 등의 문제에 대한 해결책은 일부 제시하여 주지만 상호간의 업무 수행에 있어 신뢰를 주기에는 아직 보안 기법이 미약하고 정형화된 방법이 제시되지 아니하였다.

본 논문에서는 이러한 문제를 해결하기 위하여 전자 문서 보관소의 보안을 제공하기위하여 문서의 인증. 무결성, 검증, 그리고 부인-방지를 제공하기 위한 보안 기법을 중점적으로 연구 하였다.

본 논문에서 제안하는 보안 기법으로 전자 문서 보관소의 모든 보안이 완벽하게 제공되지는 않지만 앞으로 전자 문서 보관서의 기능이 보다 정형화되고 이의 활용 방안이 정확하게 정의 된다면 전자 문서 보관소에 관련한 보안 기법에 관한 연구나 문서의 보안에 관련된 새로운 기술도 개발되리라 생각된다.

참 고 문 헌

〔1〕 Jane F. kinkus, Science and Technology Resources on the Internet: Computer Security, *Issues in Science and Technology Librarianship*, No 36, Fall 2002.

〔2〕 Adobe, “A primer on electronic document security”, *Technical White Paper*, Nov 2004.

〔3〕 Charles T. Cullen, Peter B. Hirtle, David Levy, Clifford A. Lynch and Jeff Rothengerg, “Authenticity in Digital Environment”, *Council on Library and Information Resources*, ISBN 1 887334 777, May 2000.

〔4〕 Ralph C. Merkle, “A certified digital signature”,

Proceedings on Advances in cryptology, California, United States, pp. 218 - 238, 1989.
〔5〕 Mihir Bellarea, 1, Joe Kilianb and Phillip Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code", *Journal of Computer and System Sciences*, Vol.61, Issue 3, pp.362-399. December 2000.
〔6〕 Gopalan Sivathanu, Charles P. Wright, and Erez Zadok, "Ensuring data integrity in storage: techniques and applications", *Proceedings of the 2005 ACM workshop on Storage security and survivability*, Fairfax, United States, pp. 26-36, Nov. 2005.
〔7〕 The information security glossary, http://www.your window.to/information-security/gl_nonrepudiation.htm, Nov 2007.
〔8〕 Hans Dobbertin, Lars Knudsen, and Matt Robshaw, "The Cryptanalysis of the AES – A Brief Survey", *Advanced Encryption Standard – AES, 4th International Conference*, AES 2004, LNCS 3373, Bonn, Germany, pp. 1-10, May 2004.
〔9〕 Frank Stajano, "*Security for Ubiquitous Computing*", Wiley, ISBN 0470 84493 0, 2002.
〔10〕 E. Biham and A. Shamir. *Differential Cryptanalysis of the Data Encryption Standard.* Springer-Verlag, New York, 1993.
〔11〕 M Naor and M.Yung, "Universal one-way hash functions and their cryptographic applications", *Annual ACM Symposium on Theory of Computing*, Seattle, pp.33-43, 1989.

나 상 엽 (SangYeob Na) 정회원

1992년 2월 동국대학교 전자계산학과 졸업
1995년 2월 동국대학교 컴퓨터공학과 석사
2000년 2월 동국대학교 컴퓨터공학과 박사
<관심분야> 보안, 전자 문서, 정보 검색

이 승 대 (SeungDae Lee) 정회원

1990년 2월 단국대학교 전자공학과 졸업
1992년 2월 단국대학교 통신공학과 석사
1999년 2월 단국대학교 통신공학과 박사
<관심분야> 전자공학, 통신공학, 주파수 필터