DOI: 10.3745/KIPSTC.2009.16C.5.575

효율적인 전자문서 관리를 위한 난수 재배열 기반의 키 관리 방법을 이용한 암호화 기법에 관한 연구

김 태 욱[†] · 성 경 상[††] · 김 정 재[†††] · 민 병 묵[††††] · 오 해 석[†††††]

요 약

전자문서의 많은 이점이 있음에도 불구하고 무단 유출, 파괴, 분실, 훼손의 위험이 상존하고 있다. 불법위조, 변조, 멸실로 부터 전자문서를 보호하기 위한 기술들이 절실히 요구되고 있다. 전자문서를 대상으로 하는 다양한 보안 기술들이 개발되어 있으나, 대부분 위·변조 및 부인방지에 치중되어 있다. 본 논문에서는 기존 전자문서 관리시스템에 적용하고 있는 암호화 기술의 문제점을 제시하고, 전자문서 보호를 위한 암호화 알고리즘의 효율적 적용 방안을 통해 문제를 개선하고자 한다. 논문에서 제안하는 난수 재배열 방법을 이용한 키 관리 방안을 적용한 암호화 방식과 기존 전자문서 암호화 시스템과의 비교법에 의한 성능평가를 위해 중요 요소들을 비교 평가 수행하였으며, 안정성과 효율성 두 가지 측면에서 개선된 결과를 얻을 수 있었다.

키워드 : 전자문서, 암호기술, 연산 수행, 키 관리, 난수 재배열

A Study on the Encrypted Scheme Using Key Management Method Based on the Random Number Rearrangement for the Effective E-Document Management

Tae-Wook Kim[†] · Kyung-Sang Sung[††] · Jung-Jae Kim[†††] · Byoung-Muk Min[††††] · Hae-Seok Oh[†††††]

ABSTRACT

With all merits of electronic documents, there exist threats to the security such as illegal outflow, destroying, loss, distortion, etc. The techniques to protect the electronic documents against illegal forgery, alteration, removal are strongly requested. Even though various security technologies have been developed for electronic documents, most of them are emphasized to prevention of forgery or repudiation. This paper presents some problems in cryptography technologies currently used in the existing electronic document systems, and offer efficient methods to adopt cryptography algorithms to improve and secure the electronic document systems. To validate performance of the proposed random rearrangement method comparing with the existing cryptographies, basic elements have been compared, and it has been proved that the proposed method gives better results both in security and efficiency.

Keywords : Electronic Document, Cryptography Technology, Computations Execution, Key Management, Random Number Rearrangement

1. 서 론

인터넷 사용의 보편화와 IT기술의 발달은 조직의 환경을 급격히 변화시켰으며, 전자적인 방법으로의 대체를 통해 새로운 형태의 사무환경을 제공하고 있다. 전자문서 환경은 기업 환경의 변화와 시장의 투명성 증대를 통해 조직의 생산성과 효율성을 확대시키고 국가 경쟁력을 제고시키는 매개체 역할을 수행한다.

그러나 전자문서의 활용에 따른 많은 이점이 있음에도 불구하고 무단 유출, 파괴, 분실·훼손의 위험이 상존하며, 위·변조, 멸실과 같은 보안상의 위협에 노출되어 있다.

이러한 위험으로부터 전자문서 보안성을 확보하기 위하여 암호화 및 불법복제 방지, 권한 기반 접근 제어, 송·수신 데이터의 무결성 확보, 데이터 수신자 확인을 위한 인증 등에 관한 기술 연구가 진행되고 있다[1].

이와 같은 다양한 보안 기술들이 연구·제시되고 있으나,

※ 이 연구는 2009년 경원대학교 지원에 의한 결과임
† 준 회 원 : 경원대학교 전자계산학과 박사과정
†† 정 회 원 : (주)씨에스티 사업개발본부 컨설팅 전략실 선임연구원
††† 정 회 원 : 숭실대학교 컴퓨터공학과 공학박사
†††† 종신회원 : 나노웨어 대표이사
††††† 종신회원 : 대통령 IT 특별보좌관
논문접수 : 2009년 4월 9일
수 정 일 : 1차 2009년 8월 26일
심사완료 : 2009년 8월 26일

대부분 위·변조 및 부인방지에 치중되고 있으며, 전자문서 자체를 보호하기 위한 연구는 미흡한 실정이다. 또한, 전자문서 보호를 위한 암호화 알고리즘의 효율적인 적용 방안 연구를 통해 문제를 개선하고자 하였으나, 복잡한 구조의 암호화 진행 과정에서 발생되는 많은 계산량으로 인해 대용량 문서에 적용하기에 많은 어려움을 가진다. 또한, 사용자마다 지닌 키 정보가 상이하다는 특징 때문에 원본 상태로 보관하게 됨으로써, 외부에 문서 노출 시 심각한 문제를 일으킬 수 있다.

이와 같은 문제를 해결하기 위해 빠른 연산 속도 특성을 지닌 암호화 알고리즘을 적용하고 있으나, 키 관리에 따른 어려움을 극복하지 못하였다. 이러한 키 관리의 어려움을 개선하고자 문서간의 연관성을 기반으로 키를 연속적으로 생성하고 관리하는 일 방향 키 체인 방식이 소개되었다.

그러나 키에 대한 관리가 용이하다는 장점은 가지고 있지만, 키 우선순위에 대한 개념 정립에 문제가 발생됨으로써 접근제어에 관한 권한을 부여받은 사용자의 무분별한 행위에 대해서는 보장받을 수 없다는 문제를 가진다. 또한, 암호화된 전자문서의 중간에 접근하기 위해서는 차례대로 키를 복호화 해야 하며, 초기 키 정보가 유출되거나 손상된 경우에는 암호화된 해당 전자문서에 대해서는 보상받을 수 없다는 문제가 있다. 위와 같은 암호화 방식에는 또 다른 문제점을 지니는데, 전자문서의 마지막 정보를 복호화 할 때에도 차례대로 키를 생성하고 복호화 과정에 따른 시간적 비용에 대해서도 비효율적인 결과를 가져온다. 이와 같은 암호화 방식은 안전성과 효율성의 반비례 관계가 발생하고 있다[2].

따라서 전자문서의 안전한 보호를 위해 빠른 연산 수행속도를 이용하여 암호화 과정을 수행하며, 키 생성에 대한 연관성을 배제하며 키 관리에 따른 어려움을 해결하고 사용자에 의한 무분별한 행위를 방지할 수 있는 키 관리에 따른 안전성과 효율성의 관계를 고려한 모델이 필요하다[5, 6].

본 논문에서는 일반적으로 키 생성을 위해 사용하는 난수 발생기를 이용해 발생되는 난수 정보에 키에 관한 개념을 정립시키고, XOR 연산 기법을 이용하여 키에 관한 규칙성을 부여하고 관리하며, 전자문서 암·복호화에 적용할 수 있는 키 적용 방안에 대하여 제안하였다.

본 논문은 다음과 같은 구성을 통해 전개해 나가고자 한다.

2장에서는 전자문서 암호화 방식으로 이용되는 시스템의 문제점들을 살펴보고, 3장에서는 2장에서 제기된 기존 시스템에서의 문제점을 보완할 수 있는 제안하는 효율적인 키 관리 방안을 이용한 전자문서 암호화에 대한 전체적인 시스템과 각 구성에 따른 모듈별 처리 과정에 대해 기술한다. 4장에서는 기존 전자문서 시스템과 제안하는 개선된 전자문서 시스템의 암호화 방안에 대한 성능 평가를 기술한다. 마지막으로 5장에서는 본 연구의 정리와 4장에서 기술한 시스템 평가 결과를 기반으로 결론을 논하고, 향후 연구 방향에서는 제안하는 기법을 통해 적용 가능 방안에 대해 기술함으로써 개선안의 효과에 대해 기술한다.

2. 관련 연구

본 장에서는 전자문서를 운용함에 따른 시스템의 암호화 운용 방안에 대한 문제를 분석하고 파악함으로써 제안하는 시스템의 기반이 되는 토대를 마련한다.

2.1 슈퍼 암호화 다중 암호화 방식

여러 사용자들이 문서에 대한 접근 권한이 다를 경우 문서의 접근제어 방법을 통해 문서를 공유해야 한다. 암호화 방식을 통한 문서 접근 방법으로 대표적인 모델로 슈퍼 암호화와 다중 암호화 방법이 있다[2].

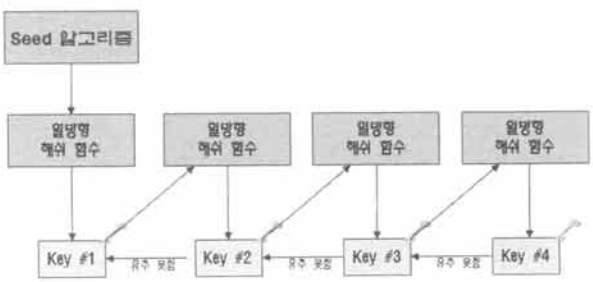
슈퍼 암호화는 많은 사용자가 하나의 문서를 공유할 때 정보의 접근권한 레벨에 따라 여러 번 암호화하는 방법이다. 즉, 가장 중요한 부분을 먼저 하나의 키로 암호화하고 그 다음으로 중요한 부분을 다른 키로 암호화하는 것이다. 정보의 중요도에 따라 여러 번 중복 암호화하는 방법으로 방식은 매우 간단한다. 하지만 각각의 중요도에 따라 다른 키로 암호화되어 있기 때문에 상위 사용자는 모든 하위레벨 키들을 가지고 있어야 하고, 암·복호화 시 많은 계산량이 필요하다는 문제점을 지니고 있다[3, 7].

다중 암호화는 기존 슈퍼 암호화의 문제점을 해결하기 위한 대체방안으로 나온 것이다. 슈퍼 암호화와 가장 큰 차이점이라면 중요도에 따라 각각의 레벨에 맞는 키로 암호화한다는 점이다. 즉, 필요한 부분만을 암호화하여 전달하는 방법이다. 이것은 슈퍼 암호화의 단점 중 하나인 계산량을 현저하게 줄여주지만 상위 사용자는 하위레벨의 모든 키들을 가지고 관리하여야 한다는 단점은 여전히 존재한다[10, 13, 14].

2.2 일방향 키 체인 방식 시스템

일방향 키 체인 방식은 역함수가 존재하지 않는다는 해쉬함수의 특징을 이용하여 키를 생성하고 관리하는 방법으로, 기존에 존재하는 비공개키 암호화 방식에서의 키 관리에 대한 어려움을 극복하기 위해 제안된 방식이다. 이러한 방식은 상위 레벨 키를 가진 사용자는 하위 레벨 키들을 도출해 낼 수 있지만, 그 역은 불가능하다는 뜻이다[9].

(그림 1)과 같이 일방향 해쉬 함수의 성질을 이용하여 키를 만들면 연속적인 체인 형태의 키를 만들어 낼 수 있다[4, 7].



(그림 1) 일방향 키 체인 방식

이러한 방식은 상위 레벨 키를 가진 사용자는 하위 레벨 키들을 도출해 낼 수 있지만, 그 역은 불가능하다는 뜻이다. 다시 말해, 숫자가 낮아질수록 레벨이 높다고 가정할 경우, 만약 키 #2를 가진 사용자는 일방향 함수를 이용한 키 체인을 통해 하위키인 키 #3, 키 #4를 유도해 낼 수 있지만, 그보다 상위키인 키 #1을 알아내는 것은 불가능하다[11-14].

이러한 방법론은 손쉽게 키 관리를 할 수 있는 장점은 가지고 있지만, 키 우선순위에 대한 개념 정립에 문제가 발생됨으로써 접근제어에 관한 권한을 부여받은 사용자의 무분별한 행위에 대해서는 보장받을 수 없다. 또한, 암호화된 전자문서의 중간에 접근하기 위해서는 차례대로 키를 복호화해야 하며, 초기 키 값이 유출되거나 손상된 경우에는 해당 전자문서에 대해서는 보장받을 수 없다는 문제점을 지닌다[13-14].

2.3 등급별 보안을 적용한 암호화 시스템

전자문서 서비스를 제공하는 업체는 사용자와 해당 전자문서를 어떠한 기준에 의하여 여러 그룹으로 나누고, 각각에 대하여 접근 제한 정책을 사용한다. 이와 같이 사용자와 전자문서에 등급을 부여하여 접근을 제한하는 것을 등급별 보안이라 한다[4].

전자문서의 암호화 과정은 등급 정책에 부합하는 등급 키를 랜덤으로 생성하고, (그림 2)와 같이 전자문서 등급에 부합하는 등급 키를 이용하여 암호화한다. 복호화는 사용자가 자신이 소유한 라이선스에서 복호화에 필요한 키를 추출하여 수행한다. 일반적으로 전자문서의 암호화와 복호화에 사용하는 Rijndael 암호 알고리즘을 이용하며 128 비트 키를 생성하여 사용한다. 암호화 과정을 거친 전자문서는 자신의 라이선스에서 등급키를 추출한 후 복호화 과정을 수행한 후 관련 전자문서에 접근하는 과정을 거친다[8, 10].

등급과 범주에 따라서 접근 제한을 두는 방법은 전자문서를 관리하는 입장에 있어서는 매우 편리하게 접근할 수 있다. 사용자의 권한보다 높은 등급의 전자문서에 접근할 수 없게 하고, 해당 등급 이하의 전자문서는 모두 접근하도록 하기 위하여 등급에 따라서 여러 개의 키를 사용하는 방법은 매우 위험할 수도 있다. 즉, 등급에 따라 구분되어지는 접근 권한 여부에 따라 자신 밑에 존재하는 모든 문서에 대해서는 슈퍼 관리자와 같은 권한이 부여되기 때문이다.

또한, 개별 인증이 아니라 등급별 인증 방법을 사용하고, 전자문서 배포 시 사용자 인증절차를 요구하지 않으므로 해당 전자문서나 사용자 등급 조정에 따라 발생되는 문제점에 대해서는 전혀 고려되지 못하고 있다[13-14].

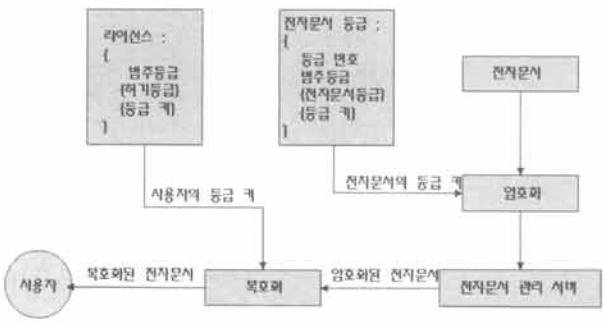
3. 효율적 키 관리 방안을 적용한 제안 시스템 설계

본 장에서는 제안하는 키 관리 방안을 적용하여 안전한 전자문서 암호화 방안을 위해 전체 시스템 구조와 모듈별 기능 그리고 키 관리 프로토콜 설계에 따른 처리 과정에 대해 기술한다.

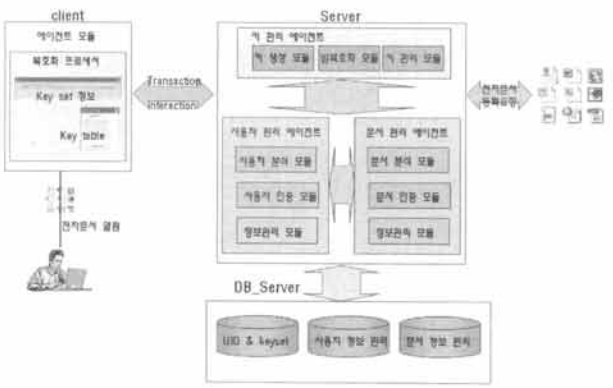
3.1 제안시스템의 전체 구조

개선된 전자문서 암호화 시스템 구축을 위해 난수 재배열 방법 이용하여 규칙성을 부여한 효율적인 키 관리 시스템 설계를 기반으로 하며, 전체 시스템 구조는 (그림 3)과 같다. 서버 측 시스템은 키 관리 에이전트와 사용자 관리 에이전트, 문서 관리 에이전트 그리고 데이터베이스로 구성되며, 클라이언트 측에서는 암호화된 전자문서를 열람하기 위한 복호화 모듈로 구성된다.

제안하는 시스템은 전자문서의 등록 요청이 발생되면 인증된 시스템을 통해 정해진 규정에 따라 전자화 과정을 거치게 된다. 검증 시스템을 통해 전자화 과정을 거치게 된다. 전자화 과정 속에서 문서가 갖는 속성 정보로서 문서의 작성자, 제목, 작성일, 등록일, 주제어, 설명, 보안등급 등 문서를 등록할 때 작성하는 메타데이터가 기록되며, 위와 같은 정보들은 해당 절차에 따라 관리된다. 등록된 전자문서의 분석된 정보를 기반으로 키 관리 에이전트부의 난수 재 정렬 기법을 이용하여 키 생성 모듈을 통해 문서의 암호화 수행에 필요한 키를 생성한다. 생성된 키를 이용하여 암·복호화 모듈에서는 전자문서의 개별 페이지 정보에 대한 암호화를 대칭키 기반의 AES 알고리즘을 이용하여 수행한다[6]. 암호화를 수행한 키의 노출을 막기 위한 방안으로 개별 관리 방법을 이용한다. 전자문서 열람을 원하는 사용자는 정당한 인증과정을 거쳐 등록되며, 사용자 관리 에이전트부의



(그림 2) 전자문서의 암호화와 복호화



(그림 3) 제안하는 시스템 구조

사용자 정보 모듈을 통해 등록된 사용자의 정보는 분석된다. 분석된 사용자 정보는 이름, ID, 주민등록번호, 직업 등의 메타데이터로 정리되며, 위와 같은 정보들은 해당 절차에 따라 관리된다. 키셋 정보 생성을 위해 사용자 인증 모듈에서는 키 관리 에이전트를 호출한다. 분석된 사용자 정보를 기반으로 난수 발생기를 이용하여 난수를 발생시키며, 본 논문에서 제안하는 난수 재정렬을 위해 규칙성 부여 방법을 적용한 키 생성 모듈을 통해 64바이트의 고유한 키셋 정보를 생성하고 관리하는 구조를 지닌다.

3.2 제안 시스템의 구성 및 모듈별 기능

제안하는 시스템 구성은 크게 사용자 정보를 관리하는 사용자 관리 에이전트부와 암호화된 전자문서를 관리하는 문서 관리 에이전트부 그리고 문서의 암호화 수행을 위한 암호키 생성과 사용자를 위한 키셋 정보를 생성하고 관리하는 키 관리 에이전트부로 구성된다. (그림 4)와 같이 키 관리 에이전트부를 중심으로 사용자 관리와 문서관리 에이전트부로 구성되며, 사용자와 문서에 관한 키 생성과 관리 업무를 수행한다. 키 관리 에이전트부의 키 생성 모듈을 통해 사용자를 위한 키셋 정보 생성과 문서 관리를 위한 키 생성에 관한 업무를 수행하며 암·복호화 모듈에서는 생성된 키를 이용하여 전자문서 암호화를 수행한다.

수식 (1)은 사용자를 위한 키셋 정보(***key_setu{}***) 생성을 위해 사용자의 고유 ID(***UID***)와 시스템이 정의한 정보(***UID***)의 XOR 연산(⊕) 수행 과정에 대해 표현한 것이다. 생성된 키셋 정보는, 전자문서의 암·복호화 수행을 위한 키맵(key Map) 역할을 위한 기반을 마련한다.

$$key\_set_u\{\} = UID \oplus ID \tag{1}$$

수식 (2)는 전자문서 암호화 수행을 위한 암호키($_nK\{\}_i$) 생성 과정에 대해 정의한 것으로, 매칭 정보를 위한 페이지별 키 생성을 위해 전자문서 고유 ID 정보(***UID***)와 각 페이지별 정보($_nCID_i$)를 연산 수행하여 키를 생성한다. 생성된 키를 이용하여 AES 암호화 알고리즘을 통해 각 페이지에 대해 암호화를 수행한다.

$$_nK\{\}_i = UID \oplus {}_nCID_i \tag{2}$$

생성된 키($_nK\{\}_i$)를 이용하여 전자문서의 각 페이지(M_{num_i})를 수식 (3)과 같이 암호화(*E*ncryption)를 수행한다. 암호화된 전자문서는 문서 관리 데이터베이스에 저장 관리되며, 암호화된 형태($_nC\{\}_i$)로 보관되므로 문서 유출시 에도 복호화가 불가능하므로 문서의 노출 문제가 개선된다.

$$_nC\{\}_i = E(_nk\{\}_i\ ,\ M_{num\_i}) \tag{3}$$

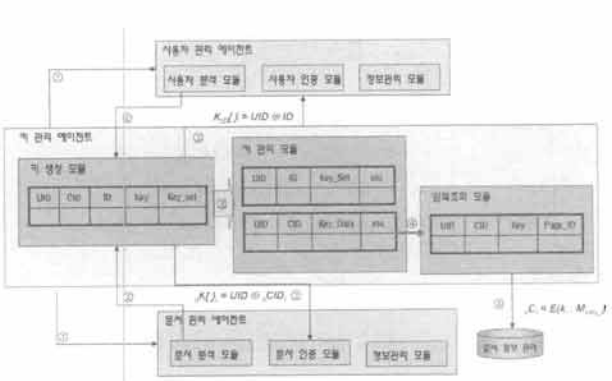
이후, 사용자는 암호화된 전자문서 열람을 위해 수식 (4)와 같은 복호화(*D*ecryption) 과정을 수행한다. 사용자에게 배부된 키셋 정보($key\_set_u\{\}$)를 기반으로 암호화된 전자문서의 암호키를 유추할 수 있는 고유 키테이블($Key\_table_{num\_i}$)과의 연산 과정을 통해 복호화를 수행하여며 열람 가능한 상태로 제공한다.

$$_nM_{num\_i} = D(key\_set_u\{\},\ Key\_table_{num\_i}) \tag{4}$$

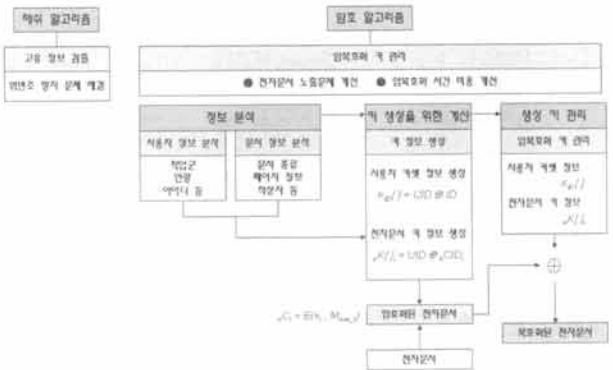
3.3 제안 시스템의 프로세스 흐름도

효율적 전자문서 보호를 위한 방안으로 기존 전자문서 암호화 시스템의 문제를 해결해야 한다. 따라서, 요청된 전자문서의 부분정보 발급을 통해 불필요한 정보유출을 방지하고, 정보유출의 최소화를 위한 암·복호화 키 관리 방안과 안정성과 효율성의 관계를 고려한 모델이 필요하다. 위·변조 방지를 위한 해쉬 정보를 첨부한 전자문서가 개별적으로 관리 가능하다는 특성을 이용하여 부분 정보별로 암호화를 수행할 수 있도록 한다.

본 논문은 (그림 5)에서 보는바와 같이 해쉬 알고리즘을 이용하여 위·변조 및 부인 방지 문제를 해결하는 일반적인 시스템 방식을 기반으로 본 시스템을 구축하였다. 분석된 사용자와 문서 정보를 기반으로 제안하는 키 생성 기법을 이용하여 암복호화를 수행할 수 있는 키셋 정보를 마련한다. 생성된 키셋 정보를 기반으로 각 전자문서 암호화를 수행하며, 사용자에게는 암호화된 전자문서를 복호화할 수 있



(그림 4) 키 관리 에이전트 처리절차



(그림 5) 제안기법의 프로세스 흐름도

는 토대를 마련한다.

이와 같이 제안하는 효율적인 키 관리 방안에 관한 연구를 통해 전자문서 유출 문제를 개선하고 암·복호화 시간 비용과 시스템적 부하를 개선함으로써 전자문서 암호화 시스템에 적용 가능토록 하였다.

4. 제안 시스템의 키 설계 방안

본 장에서는 사용자에게 배부하는 키셋 설계 과정과 전자문서 암호화 수행을 위해 필요한 키 생성과정에 대해 기술한다.

4.1 키셋 생성 과정

사용자가 관리하는 키셋 정보 구성은 사용자의 고유 정보를 기반으로 난수 정보를 64바이트 크기를 생성한다. 제안하는 키셋 정보는 가변적 성격을 가지며, 생성할 수 있는 코드표의 개수는 64!(=1×2×3×...×63×64)만큼 되므로, 중복될 가능성은 매우 희박하다. 즉, 64!개의 사용자 코드표를 생성할 수 있다는 뜻을 내포한다.

(그림 6)은 키셋 정보 생성 과정에 대해 의사코드(pseudo code)화하여 나타낸 것이다.

키셋 생성 과정에서 사용자의 등록 여부를 확인한 후, 등록되어 있지 않으면 user_code를 호출한다. 먼저, 64개의 null을 생성한 후, $A_{(64)}$번째 열까지 사용자 고유 코드 정보와의 연산을 통해 구해진 정보를 기반으로 키셋 정보는 생성된다. 이와 같이 생성된 키셋 정보는 $C_{공개키}(S_{개인키}(key_set))$과 같이 서버의 개인키로 전자서명을 하고, 클라이언트의 공개키로 암호화를 수행한 후, 사용자에게 키셋 정보를 안전하게 전송하는 PKI 기반 구조를 이용한다[5]. 이와 같이 사용자의 ID와 (그림 6)의 복잡한 과정으로 생성된 키셋 정보는 ASCII 코드 구조로서 관리되므로 외부에 노출되더라도 추론이 불가능한 상태로 유지된다. 본 알고리즘은 보안 기능에 치중하였기에 프로세스 시간에는 비 능율적인 면이 있는 것은 사실이다.

```
procedure Array key_set(N)
{
   if user_code != Enroll
     call user_code;
     Array 64byte
     for i := 1 to Code_Key
        if (i == 1)
             temp = user_code XOR A(i)
        else
             temp = temp XOR A(i)
     next

     user_key_set(N) = temp XOR user_code
     return user_key_set(N)
}
```

(그림 6) 키셋 생성 의사코드

4.2 암호키 생성 과정

본 논문에서 제안하는 전자문서의 암호화를 위한 구성요소에는 페이지별 암호화 수행을 위한 키 매칭 정보가 필요하다. 이와 같은 조건을 만족하기 위해 전자문서 수량만큼 키를 생성해야 한다. 이를 위해 전자문서 고유 정보와 난수 발생기를 통해 생성된 키 정보를 연산 수행하여 초기값을 생성하며, 이를 기반으로 각 페이지 정보와의 연산 수행 과정을 통해 각 페이지별 키 정보를 생성한다.

(그림 7)은 암호키 정보 생성 과정에 대해 의사코드화하여 표현한 것이다.

키 생성을 위해 등록된 문서인지 확인한 후, 등록되어 있지 않으면 고유 문서 코드(Doc_code)를 호출한다. 먼저 6개의 null을 생성한 후, 정의된 키셋 테이블을 통해 첫 번째 값부터 $A_{(6)}$번째 열까지 채워나가는데, 첫 번째 값은 분석된 문서에 등록된 *CID* 정보와의 연산 수행을 통해 획득하게 되며, 생성된 이전 값과 *UID* 정보를 XOR 연산 수행함으로써 새로운 값을 얻게 된다. 이와 같은 과정을 반복해 얻은 키값은 문서의 암호화를 위한 정보로서 대칭키 역할을 수행한다.

```
procedure Array Doc_key(N)
{
   if Doc_code != Enroll
     call Doc_code;
     call Random_key;
     Array 64byte
     for i := 1 to 6
        if (i == 1)
             temp = CID XOR A(i)
        else
             temp = UID XOR A(i)
     next

     Doc_key_set(N) = temp XOR Doc_code
     return Doc_key_set(N)
}
```

(그림 7) 암호키 생성 의사코드

5. 성능 평가 및 보안성 비교 분석

본 장에서는 구현한 시스템의 모듈 및 기능별 인터페이스에 대해 기술한다. 또한, 무분별한 난수 정보에 규칙성을 부여하여 생성된 키를 이용하여 전자문서 암호화 수행 결과에 대해 기술하고 기존 시스템과의 성능 비교를 통해 암·복호화의 안전성을 분석하며 성능평가에 대해 논한다.

5.1 구현 환경

제안하는 시스템은 클라이언트와 서버 구조로 구성되며, 서버측에서는 전자문서 관리 시스템을 기반으로 키 관리 시

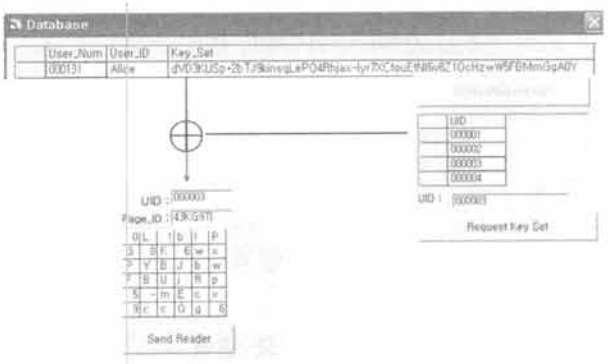
스템과 사용자 관리 시스템을 구축하였다. 서버는 64바이트 크기의 키셋 정보를 정해진 규칙에 의해 생성하며, 분석된 전자문서 정보를 이용하여 암호키를 생성한다. 제안하는 시스템 개발을 위한 환경은 시스템 Intel(R) Pentium(R)-4 CPU 2.66GHz와 2GB RAM, 그리고 MS-Windows XP Professional 운영체제를 사용하였다. Visual Basic 6.0과 .NET을 이용하여 키 정보에 대한 전반적인 내용과 서버 및 클라이언트 인터페이스를 구현하였다. 전자문서의 UID 값과 암호키 그리고 키셋에 대한 정보를 저장하기 위한 데이터베이스는 MS-SQL 2000 프로그램을 이용하였다.

5.2 실험 개요

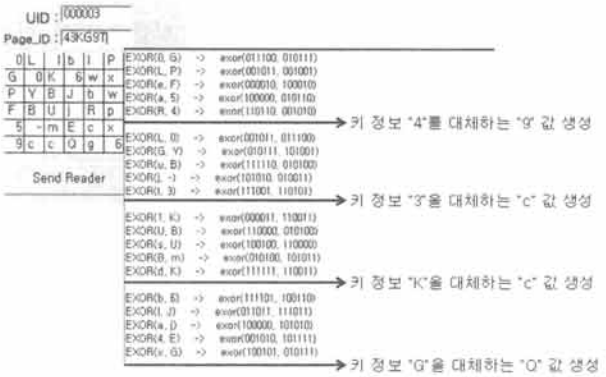
사용자 정보를 기반으로 생성된 키셋 정보는 암호화된 전자문서를 생성하고 복호화하기 위해 사용되는 코드표 역할을 수행하고 64byte 크기의 문자로 구성되어 있으며, 서버와 클라이언트간 상호작용을 한다. 요청자의 키셋 정보를 기반으로 전자문서 암호화 수행에 사용된 키 정보간의 역연산 과정을 거침으로써 생성된 정보는 복호화 수행을 위한 키로 정의되며, 키 테이블 형식을 구성한다.

(그림 8)은 요청자(Alice)의 키셋 정보를 기반으로 복호키 유추를 위한 키테이블 생성과정을 보인것으로 요청자료의 키 정보와 연산 관계를 지니게 된다. 키테이블 정보는 요청할 때마다 키정보(page_ID)를 중심으로 랜덤하게 팩킹(packing)되며 중복되는 경우는 발생되지 않으므로 키 노출에 대한 안전성을 보장하였다.

(그림 9)는 위와 같은 과정을 통해 얻어진 복호키 유추키 테이블의 정당성을 보이기 위한 시뮬레이션 과정으로 XOR 연산 수행에 따른 특징을 따라 복잡도를 높이면서도



(그림 8) 키 테이블 생성과정



(그림 9) 생성된 키 테이블 정보의 시뮬레이션 과정

단순한 과정을 수행함으로써 시간과 시스템적 비용을 개선할 수 있었다.

이와 같이 키 관리에 대한 어려움을 개선하고 암호화된 전자문서를 관리함으로써 문서의 유출 문제를 해결할 수 있게 되었다.

5.3 실험 및 평가

본 논문에서는 제안하는 시스템의 성능 평가를 위해 전자문서 암호화에 따른 중요 항목들에 대해 비교 평가하였으며, 시스템 평가를 통해 제안하는 기법을 적용한 시스템의 성능에 대한 개선된 결과를 확인할 수 있었다.

본 논문에서 제안하는 기법의 평가를 위해 슈퍼 암호화와 다중 암호화, 키 체인 암호화 그리고 등급키를 이용한 암호화 방식을 비교 대상으로 하였다. 이들 암호화 기법들을 본 논문에서 제안하는 모델과 비교하여 암·복호화에 필요한 키 개수, 계산 부하량, 암호화 시 문서 크기 등 대표적인 몇 가지 항목들에 대해 비교하여 <표 1>을 통해 보였다.

본 논문에서 수행한 성능 평가는 등급별 보안[10]에서 평가했던 데이터를 일부 참고하여 작성하였다.

<표 1>에서 보는 바와 같이 슈퍼/다중 암호화 방식은 사용자가 보관해야 하는 키 개수는 암호화 수준에 따라 다수개의 키를 보관하고 등급키 방식은 등급 기준에 따라 보관해야 하는 키 개수가 달라지는 결과를 보였다. 반면에 키 체인 방식과 제안하는 방식에서는 단지 고유 키 정보만을 보유한 상태로 일정하게 유지되는 방식을 취하므로 키에 대한 관리의 복잡성을 피할 수 있다.

그리고 암·복호화 계산량 평가는 중요 레벨 정도에 따라

〈표 1〉 전자문서 암호화에 따른 중요 항목들에 대한 비교 평가

	슈퍼 암호화	다중 암호화	키 체인 암호화	등급키 이용한 암호화	제안하는 방식 적용 암호화
사용자가 보관하는 키 개수 (x: 암호화 필드 수)	x	x	1	등급기준에 따라 달라짐	1
암·복호화에 따른 계산량 (n : 데이터 개수)	1+n(n-1)/2	n	n	$Ke_i = \left(\bigoplus_{i=1}^{n}\right)\left(\bigoplus_{j=1}^{n} K_{ij}\right)$	Ê (Rpub, M)
암호화 시 문서크기 (y:암호화 데이터 필드)	(ay3-by2)/n (단,n>0,a>b)	400y	400y	y	y

기하급수적으로 올라갈 수 있으며, 문서크기에 따른 영향도 미치는 것을 알 수 있다. 다중 암호화와 키 체인 암호화 방식에서는 자신의 레벨에 따른 키로 한 번씩만 암·복호화 하므로 계산량은 현저히 적은 반면, 앞에서 언급했던 것과 같은 노출의 위험성에 처해 있다. 반면에 등급키 기법과 제안하는 기법을 적용한 암호화 방식은 연산 수행의 어려움으로 인하여 계산량은 많은 반면 노출 위험성 문제를 개선할 수 결과를 보인다.

마지막으로, 전자 문서의 암호화 수행 시 발생되는 문서의 크기를 비교한 것으로 슈퍼 암호화는 문서의 크기가 암호화 횟수에 따라 지수적으로 증가하며, 다중 암호화 방식과 체인 암호화 방식은 선형적으로 증가하는 양상을 보인다. 반면에 등급키 방식과 제안하는 방식을 적용한 암호화가 수행된 전자문서의 크기는 동일한 결과를 보인다.

따라서 본 논문에서 제안하는 암호화 기법이 다른 모든 암호화 기법과 비교 평가하여 우수하다는 결과를 보일수는 없지만, 제안하는 기법이 다른 암호화 기법들에서 보이는 장점들을 지니고 있으므로 전자문서의 암호화 수행시 다른 기법들보다 개선된 결과를 보일 수 있었다.

6. 결론 및 향후 연구 과제

전자문서의 중요성이 커지면서 정보유출을 방지하기 위한 방안들이 운영되고 있으며 그 안전성을 보장하고 있지만, 보관단계에서의 관리방안에 대한 많은 어려움을 지닌다. 전자문서 암호화 방식의 무거움으로 인한 직접적인 암호화는 추진하지 못하는 실정이다. 또한 암·복호화 키 관리의 어려움을 이유로 전자문서 보안에 대한 관리적 측면에서 소홀히 대처하고 있으며, 이로 인해 안전성과 효율성의 반비례 관계가 발생하고 있다.

따라서 본 논문에서 제안하는 난수 재배열 방법을 이용한 효율적인 키 관리 기법을 통해 암호화된 전자문서를 관리함으로써 유출 문제에 따른 보안적 측면을 개선할 수 있었으며, 암·복호화 시 발생되는 시간과 시스템적 비용을 개선할 수 있었다. 또한, 클라이언트측은 요청한 정보만을 수신함으로써 불필요한 정보를 처리해야 하는 비용적 측면을 개선할 수 있다. 더불어 서버 측에서 암호화된 문서와 관련된 키 정보의 개별 관리 방안을 통해 노출 문제를 해결함으로써 전자문서의 안전성에 대한 적합성을 검증할 수 있었다.

향후 전자문서에 대한 보안적 측면이 확산되었을 때, 제안하는 키 관리 적용 방안을 기반으로 다양한 응용분야에서 기본 모델로 활용이 가능하다. 또한, 제안 시스템의 로깅 정보를 활용하여 지능형 선호도 계산 알고리즘을 적용함으로써 사용자가 관심 갖고 열람했던 기록 정보들을 활용함으로써 관심 정보 추출을 통한 추천 부분에까지 활용할 수 있는 개선된 전자문서 시스템으로 발전이 가능하다.

참 고 문 헌

[1] 산업자원부, "전자문서의 작성절차 및 방법에 관한 규정," 산자부고시2007-85호, 2007.

[2] 이진호, "ebXML을 이용한 문서 암호화 시스템 설계 및 구현," 한신대학교 대학원 석사학위 논문, 2003.

[3] 윤은준, "다양한 환경을 위한 토큰 기반의 인증된 키 설정 프로토콜," 경북대학교 대학원 석사학위 논문, 2007.

[4] John Linn, "Trust Models and Management in Public Key Infrastructures," Technical Notes and Reports of RSA Laboratories, November, 2000.

[5] 김대중, "전자문서 보관 및 발급 서비스의 안정성 확보를 위한 시스템 설계," 숭실대학교 대학원 박사학위 논문, 2008.

[6] Biham, E. and Keller, N., "Cryptanalysis of reduced variants of Rijndeal," In Proceedings of the Third Advanced Encryption Standard Conference, 2000.

[7] 김희원, "암호학에 관한 연구," 신라대학교 대학원 석사학위 논문, 2005.

[8] 김정재, "멀티미디어 데이터 보호를 위한 대칭키 암호화 시스템에 관한 연구," 숭실대학교 대학원 박사학위 논문, 2005.

[9] Yihl-Chun Hu, M. Jakobsson and A. Perrig, "Efficient Constructions for One-Way Hash Chains," In proceedings of ACNS 2005 LNCS Vol.3531, pp.423-441, 2005.

[10] 김진성, "멀티미디어 컨텐츠에 대한 등급별 보안," 경상대학교 대학원 박사학위 논문, 2007.

[11] 이원우, "EC 환경에서의 XML 보안기술 연구," 순천향대학교 대학원 석사학위논문, 2005.

[12] 박남제 외 4명, "안전한 전자거래를 위한 XML 키 관리 기술," 정보보호학회지,13권 3호, pp.72-82, 2003.

[13] 성경상, "난수 재배열 기반의 키 관리 방안을 이용한 전자문서 암호화에 관한 연구," 경원대학교 대학원 박사학위 논문, 2009.

[14] Grangetto, M., Magli, E. and Olmo, G., "Multimedia Selective Encryption by means of Ranomized Arithmetic Coding," IEEE Transactions om Multimedia 8(5), art. No.1703505, pp.905-917, 2006.

김 태 욱

e-mail : twkm@ku.kyungwon.ac.kr

2004년 호원대학교 컴퓨터공학과(학사)

2007년 경원대학교 전자계산학과(공학석사)

2007~현 재 경원대학교 대학원 전자계산학과 박사과정

관심분야 : 경영정보시스템, 데이터통신, 보안

성 경 상

e-mail : actofgod@paran.com
2001년 호원대학교 전자계산학과(이학사)
2003년 숭실대학교 컴퓨터공학과(공학석사)
2009년 경원대학교 전자계산학과(공학박사)
2009년~현 재 (주)씨에스티 사업개발본부 컨설팅 전략실 선임연구원
관심분야 : 전자거래학, 유비쿼터스, 보안, 정보경영

김 정 재

e-mail : argniss@nate.com
1999년 영동대학교 컴퓨터 공학과(공학사)
2001년 숭실대학교 컴퓨터공학과(공학석사)
2005년 숭실대학교 컴퓨터공학과(공학박사)
관심분야 : DRM, 암호학, RFID

민 병 묵

e-mail : ceo@nanoware21.com
1987년 서울산업대학교 전자계산학과(학사)
1989년 연세대학교 전자계산학과(공학석사)
2007년 숭실대학교 컴퓨터공학과(공학박사)
2008년~현 재 경원대학교 겸임교수
2004년~현 재 나노웨어주식회사 대표이사
관심분야 : 금융정보시스템, 멀티미디어, 보안

오 해 석

e-mail : oh@kyungwon.ac.kr
1975년 서울대학교 계산통계학과(학사)
1981년 서울대학교 계산통계학과(공학석사)
1989년 서울대학교 계산통계학과(공학박사)
2003년~2003년 한국정보처리학회 회장(역임)
1982년~2003년 숭실대학교 컴퓨터학부 교수/부총장(역임)
2003년~2008년 경원대학교 부총장(역임)
2009년~현 재 대통령 IT 특별보좌관
2003년~현 재 경원대학교 IT대학 교수
관심분야 : 멀티미디어, 데이터베이스, 지식경영