공인전자문서보관소에서 생성되는 로그의 효율적이고 안전한 보관방법에 대한 연구

강신명* · 문종섭*

요 약

우리나라는 전자거래기본법에 의거해 2005년 3월 세계 최초로 공인전자문서보관소 제도를 채택하였다. 이를 통해 전자문서의 등록·보관·유통을 국가가 공인하는 보관소를 통해 이룰 수 있다. 공인전자문서보관소는 이용기관이나 이용자가 등록하는 문서의 보관도 중요하지만 수행한 이력을 안전하게 보관하는 것도 중요하다. 모든 수행 이력에는 공인된 인증서를 이용하여 전자서명을 하도록 되어있지만 그 관리가 어려운 것이 사실이다.

본 논문에서는 공인전자문서보관소 내에서 생성된 전체 로그를 효율적으로 인증할 수 있게 해시 트리를 적용하여 관리하는 기술에 대한 연구를 서술한다.

An Efficient and Secure Method for Managing Logs of Certified e-Document Authority Using Hash Tree

Shin Myung Kang* · Jong Sub Moon*

ABSTRACT

CeDA (Certified e-Document Authority) was adopted in March 2005. It is possible to register/store/send/receive/transfer/revoke e-documents by using trusted third party, CeDA. It is important to store not only e-documents of users but also logs produced by CeDA. Thus all logs must be electronically signed using certificate of CeDA. But management of electronically signed logs is difficult.

In this paper, the method which can be applicable to authenticate all logs of CeDA using "Hash Tree" is present.

Key words : Certified e-Document Authority, System Management, Log, Hash Tree

접수일 : 2009년 4월 15일; 채택일 : 2009년 4월 18일

* 고려대학교 정보경영공학전문대학원

1. 서 론

공인전자문서보관소(이하 보관소)는 전자거래기본법에 근거, 지식경제부장관의 지정을 받아 국가가 공인하는 기관으로써 전자문서[1]를 보관 또는 증명하거나 그 밖에 전자문서와 관련된 업무를 수행하는 법인을 말한다. 전자문서의 이용을 활성화하기 위하여 전자문서를 안전하게 보관하고 전자문서의 내용 및 송수신 여부 등을 증명해 줄 수 있는 신뢰할 수 있는 제 3의 기관이다[1]. 2007년 2월 1호 사업자가 지정된 이후 2009년 4월 현재 6개의 기관이 지정[2]되어 있다. 이 보관소를 이용하는 이용기관이나 사용자는 보관소가 제공하는 인터페이스를 이용하여 문서를 등록하게 된다.

보관소에 등록되는 문서가 많아지고 전자문서의 유통이 활성화될수록 보관소에서 행한 절차에 대한 이력, 즉 로그는 점차 양이 많아지게 된다. 또한 보관소에서 행해지는 절차들은 법적인 효력을 갖는 전자문서에 관계되므로 생성되는 로그도 더욱 중요하게 되었다. 따라서 저장되고 관리·유통되는 전자문서와 마찬가지로 로그 하나하나에 보관소가 전자서명을 함으로써 무결성을 보장해야 한다[2]. 하지만 로그의 경우에는 폐기되는 경우가 없어야 하기 때문에 전자서명에 사용된 인증서의 유효기간이 끝나게 되면 유효성 검증에 어려움이 생긴다. 이에 대한 대안으로 장기전자서명검증 방법을 사용한다. 하지만 로그와 같은 경우는 크기가 작은 메시지의 개수가 아주 많은 경우가 되므로 RFC 3126이나 RFC 4998을 기반으로 하는 장기전자서명검증 방법을 그대로 따르기에는 무리가 있다. 크기는 작지만 개수가 아주 많은 상황에서는 로그 하나하나에 일일이 장기전자서명 포맷을 유지하기 힘들다. 따라서 이런 문제점을 보완한 모델을 제안하고자 한다. 본 논문에서는 제 2장에서 관련 연구에 대해 서술하고, 제 3장에서 제안 방법에 대해 서술하며, 제 4장에서 제안 방법의 가정 및 결과를 나타내고, 제 5장에서 결론으로 마무리 한다.

1) "전자문서"라 함은 정보처리시스템에 의하여 전자적 형태로 작성, 송신 · 수신 또는 저장된 정보를 말한다.

2) 한국무역정보통신, LG CNS, 삼성 SDS, 한전 KDN, 하나INS, 유포스트뱅크.

2. 관련 연구

2.1 공인전자문서보관소

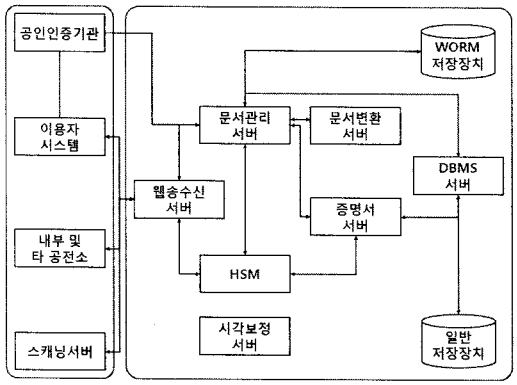
2.1.1 보관소의 기본 업무

종이문서의 경우 사람이 보기에는 편하지만 관리가 힘들다는 단점이 있다. 유통 중에 발생할 수 있는 유실이나 손상에 약하고 많은 양의 종이문서를 보관할 때에는 많은 비용이 소요된다. 또한 종이문서의 경우 분류체계가 제대로 되어있지 않으면 검색이 힘들고 많은 시간이 소요된다. 따라서 IT의 발전에 힘입어 종이문서를 전자문서로 대체하기 위한 시도가 계속되고 있다. 현재는 종이문서의 발급을 위해 인터넷을 이용한 증명서를 발급받는 단계까지 와있다[3].

공인전자문서보관소는 전자문서의 효율성에도 불구하고 전자문서에 대한 신뢰성 부족으로 종이문서를 선호하기 때문에 생기는 문제점들을 해결하기 위해 시작되었다. 보관소의 기본업무로서 전자문서의 보관, 전자문서의 불변경 추정, 전자문서 증명서 발급이 있다. 전자문서의 보관 업무는 전자문서 보관을 대행하는 것을 말하며 보관소에 전자문서를 보관한다는 것은 보관의 법적 효력을 부여받는 것과 같다. 전자문서의 불변경 추정은 보관소에 보관된 전자문서는 보관기간 중 그 내용이 변경되지 않는 것으로 추정되는 것을 나타낸다. 또한 증명서 발급 업무는 보관소에 보관된 전자문서의 보관사실, 보관기간 등에 대한 증명서를 발급하며 증명서에 기재된 사항은 진정한 것으로 추정하는 것을 의미한다.

2.1.2 보관소 시스템 구성

공인전자문서보관소는 이용자 프로그램 및 포털, 문서관리시스템, 문서변환시스템, 증명서관리 서버, 연계 인터페이스, 정보패키지, 위변조방지시스템, HSM, 저장소 등으로 구성되어있다. 이를 간략히 나타낸 구조는 다음 (그림 1)과 같다.



(그림 1) 보관소 시스템 구성

• 증명서버

이용자 혹은 증명서 요청자가 증명서를 요청하거나 문서 등록 등으로 자동으로 증명서가 생성되는 경우 이력에 대한 증명서를 발급한다. 또한 증명서를 폐기하거나 갱신하고 사용자가 요청한 증명서를 검증하며 증명 정책을 관리한다[6].

• 문서관리 서버

사용자에 의해 등록된 문서에 대해 검색을 하거나 열람을 신청하거나 콘텐트를 관리한다. 또한 관리자는 통계를 내거나 사용자를 관리하거나 접근권한 및 정책 등을 관리한다.

• 문서변환 서버

사용자가 등록한 문서가 장기보존을 위한 문서 포맷이 아니면 사용자가 등록 요청한 원본 문서에 대해 장기보존본[3]으로 변환한다.

• HSM

보관소는 보호해야 할 문서가 많기 때문에 전자서명을 수행할 양이 많다. 따라서 전자서명을 빠르게 수행하기 위해 가속기를 사용한다.

• 저장장치

보관소는 전자문서나 전자서명 검증을 위한 부가 검증 데이터를 저장하는 장소가 따로 있다. 이 저장소는 데이터를 한번 쓰면 지울 수 없으며 읽기만 수행되기 때문에 WORM(Write Once Read Many)이라고 불린다.

• 이용자 시스템

이용자 시스템은 이용자가 보관소에 접근하여 서비스를 사용하기 위하여 사용하는 하드웨어 및 소프트웨어를 말한다[4]. 지원하는 기능은 증명서 관련 기능, 패키지 관련 기능[5], 연계인터페이스 관련 기능, 기타 운영 기능으로 나눌 수 있다.

2.1.3 보관소의 로그

공인전자문서보관소에는 여러 가지 종류의 보관해야 할 로그가 있다. 공인전자문서보관소 표준업무준칙[2]에 보면 저장해야 할 로그의 종류가 나와 있다.

또한 보관소는 로그와 관련된 몇 가지 특징이 있다. 첫째, 보관소의 모든 로그는 보호대상이다. 따라서 보관소는 모든 로그에 대해 전자서명을 한다. 둘째, 보관소는 특성상 안전한 저장장소가 있다. 이 저장소는 데이터를 한번 쓰면 지우거나 수정할 수 없고 읽기만 가능한 저장소이다.

2.2 장기전자서명검증

공인전자문서보관소에서 보관하고 관리하는 전자문서와 로그들은 위변조 방지 및 부인방지, 법적

3) 10년, 20년 후에도 특정한 어플리케이션에 종속되지 않고 전자문서의 내용을 확인할 수 있는 포맷을 말한다. 해당 어플리케이션 소스가 공개되어 있어서 개발 회사가 없어지더라도 소스를 통해서 해당 포맷을 이용할 수 있는 포맷을 말한다.

효력 등을 고려하여 기본적으로 전자서명을 적용하여 운용되고 있다. 하지만 보관소가 보관하는 전자문서 및 로그는 일반적으로 단기간 보관이 아닌 장기간에 걸친 보관을 하게 된다.

전자서명이 적용된 전자문서 및 로그를 장기간 보관하게 되는 경우, 일정 시간이 지난 이후에 검증할 때 보관소가 서명한 시점 또는 검증하여 보관하는 시점과 동일한 법적 효력을 보장할 수 있는 방법을 제공해야 한다.

2.2.1 장기전자서명검증의 필요성 및 요구사항

전자서명에 사용된 인증서의 유효기간 내에서 서명검증이 수행되는 경우에는 일반적인 절차에 따라 정상적으로 검증이 수행된다. 하지만 장기간 보관되는 전자서명문서의 경우에는 일반적인 절차에 따라 정상적인 결과를 획득하기 어렵다. 다음과 같은 이유로 장기전자서명검증 방법론이 필요하다.

- 비정상적인 인증서 기반 서명으로 인한 서명의 유효성 분쟁에 대한 대비
- 상대적으로 낮은 비도의 알고리즘으로 인한 서명의 유효성 분쟁에 대한 대비

따라서 전자서명을 장기간 보관하여 향후 검증하는 경우를 대비하고자 한다면, 반드시 전자서명 생성 또는 보관 등 특정 시점에 인증서 상태를 확인할 수 있는 정보를 함께 보관하여야 한다. 또한 필요한 시점에 강한 안전성을 가지는 알고리즘으로 보완해야 한다.

2.2.2 RFC 3126

RFC 3126은 인증서 유효기간이 만료되어 기 수행된 전자서명의 검증을 할 수 없거나, 해당 전자서명에 사용된 암호학적 알고리즘들의 안전성에 문제가 생겨 기존 검증을 신뢰할 수 없는 경우를 대비하여 장기검증에 대한 장기전자서명 포맷을 제시한다[7].

RFC 3126에서의 전자서명 장기검증 메시지는 서명자가 서명을 생성하는 시점 또는 검증자가 서명된 메시지를 검증하는 시점에 생성된다. 즉 전자서명 장기검증 메시지를 생성하는 주체는 서명자도 되며 검증자도 가능한 모델임을 의미한다. 이후 중재자는 생성된 전자서명 장기검증 메시지를 분쟁해결을 위하여 검증하는 역할을 수행한다.

RFC 3126에서는 크게 다음과 같은 메시지 구조를 제안하고 있다.

- ES(Electronic Signature)
- ES-T(ES with Time-Stamp)
- ES-C(ES with Complete Validation Data)
- ES-A(ES with Archive Validation Data)

ES-C는 다음과 같은 확장 형태를 갖는다.

- ES-X long
- ES-X Type1
- ES-X Type2

ES, ES-T, ES-C, ES-X 구조는 인증서 상태확인에 중심을 두고 있으며 ES-A의 경우에는 중첩된 구조를 제시하면서 암호학적 알고리즘의 안전성에 중심을 두고 설계하고 있다.

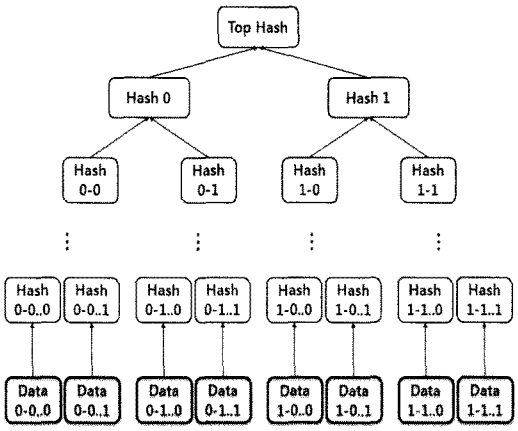
2.2.3 RFC 4998

IETF에서 2004년 RFC 3126을 기반으로 한 보다 고도화된 전자문서에 대한 신뢰할 수 있는 장기보관을 수행하기 위하여 LTANS(Long-term Archive and Notary Service) 워킹그룹(WG)이 형성되었고, 장기보관과 공증 서비스(LTANS)에 대한 본격적인 연구가 시작되었다. RFC 3126과의 가장 큰 차이는 해시 트리(Hash Tree)를 이용하여 여러 문서에 대해 한 번의 시점확인만을 수행해도 각

전자문서에 대한 장기전자서명검증 서비스가 가능하다는 것이다[8].

2.3 해시트리 (Hash Tree)

해시트리(Hash Tree)[4]는 단방향 함수를 이용하여 메시지에 대한 인증 메시지를 생성하기 위한 방법을 구성하기 위하여 발명되었다[9]. 해시트리는 많은 조각으로 나눠져 있는 데이터에 대한 축소 정보를 트리 구조로 가지고 있는 자료구조이다. 해시트리 자료구조의 예를 그림으로 보면 다음 (그림 2)와 같다.



(그림 2) 해시트리 자료구조의 예

해시트리의 종단노드(leaf node)들은 인증하려고 하는 메시지 집합의 원소들이다. 종단노드들의 부모는 종단노드의 해시값이다. 해시트리의 특징은 검증자가 인증된 루트 해시값(Top Hash)을 알고 있으면 모든 종단노드들에 대한 해시를 모르더라도 특정 종단노드를 검증할 수 있다는 것에 있다. 이는 자식노드를 알면 부모노드를 계산할 수 있기에 가능하다.

4) Ralph Merkle에 의해 발명되어 Merkle Tree라고도 한다.

3. 제안 방법

3.1 제안모델의 필요성 및 가정

보관소에서 로그에 대한 장기검증이 필요한 이유는 보관소가 전자문서의 장기보관을 목적으로 하고 보관되는 전자문서와 마찬가지로 로그도 장기적으로 안전하게 보관되어야 하기 때문이다.

제안할 모델이 성립하기 위해서는 몇 가지 가정이 존재한다. 첫째, 로그의 전자서명 주체는 보관소이다. 둘째, 서명 당시 인증서는 유효했었다고 가정한다. 셋째, 전자서명에 대한 인증서에 대한 인증서의 부가 검증데이터들, 즉 인증서 및 인증경로, 폐지목록들(CRL 및 ARL)이 안전하게 보관되어야 한다. 제안 모델에 의해 검증 실패가 발생한 경우에는 개별 로그에 대해 전자서명 검증을 실시해야 하는데 로그 생성 시점의 부가 검증데이터를 모른다면 어떤 로그가 위변조 되었는지 알 수 없다.

3.2 제안모델

공인전자문서보관소에서 생성되는 로그에 대해 해시트리를 적용한다. 로그를 날짜 혹은 시스템 등으로 그룹으로 묶어 해시트리를 적용함으로써 로그에 대한 무결성을 보장하고 RFC 3126 혹은 RFC 4998의 적용으로 발생하는 부하를 줄이는데 목적이 있다.

3.2.1 로그에 대한 해시트리 적용 방법

제안모델에서는 종단노드로 각 로그 메시지를 이용한다. 실제로는 로그의 종류에 따라 로그를 분류하여 부분 해시트리를 적용할 수 있겠지만 여기서는 전체 로그에 대해 해시트리 하나를 구성하는 것으로 한다. 종단 노드의 순서는 로그의 발생 순서로 정렬하는 것으로 구성한다. 또한 종단노드와 그 부모노드를 제외한 노드의 해시 연산에서

입력될 데이터의 연접 순서도 역시 발생 시간으로 정렬한다. RFC 4998을 로그에 대해 적용하기에는 무리가 있는데 RFC 4998의 경우는 이진 정렬을 사용하므로 인증 대상이 많아지면 효율이 떨어지기 때문이다.

보관소의 로그에 대해 여기서 예를 들어 제안하는 해시트리의 깊이는 인증 받을 메시지 부분 노드를 제외한 루트/연/일의 3단계이다. 즉 "일" 해시트리, "연" 해시트리를 부분해시트리로 하여 구성되는 해시트리이다.

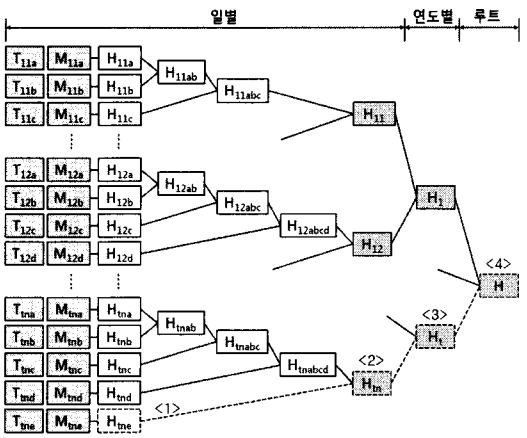
부분 해시트리 중에서 계산이 완료된 부분 해시트리의 경우에는 장기전자서명 포맷을 적용한 후 안전한 저장소에 저장한다. 계산이 완료되지 않더라도 정기적으로 저장해야 할 경우에는 부분 해시트리의 루트 해시값을 안전한 저장소에 저장한다. 해시트리를 항상 안전한 장소에 저장해 놓고 해시를 계산할 수 없는 이유는 보관소에서 사용하는 안전한 저장소가 WORM 장비이기 때문이다.

상위 노드의 값을 로그가 입력될 때마다 계산하지 않으면 시간상의 갭이 생겨 로그에 대한 수정 가능성이 생긴다. 따라서 이전 부분 해시트리의 루트 해시값과 새로 들어온 로그의 해시값을 연접하여 해시를 수행한다. 이를 트리로 나타내면 이진 트리 중 한쪽으로 자라나는 형태의 이진 해시트리가 된다.

로그에 대해 해시트리를 적용하기 위해서는 먼저 모든 로그의 해시값을 얻어야 한다. 하지만 보관소에서는 모든 로그에 대해 전자서명을 수행하므로 전자서명 수행 중에 한번은 꼭 로그에 대한 해시를 계산하게 된다.

(그림 3)은 t년도의 n번째 날짜에 e번째 로그를 추가하는 그림이다. t-1년 까지, n-1일 까지는 부분트리가 계산이 완료되어 있는 상태이다. 이를 실선 형태로 나타냈다.

위의 예에서 M_{tne}로그가 발생한 경우를 생각해 보자. 먼저 로그에 전자서명을 적용하기 위해 해시 연산을 하여 해시값 H_{tne}를 얻은 후 전자서명을



(그림 3) 로그에 대한 해시트리 구성

수행한다①. 생성된 해시값을 일별 해시값의 이전 값 H_{tnabcd}와 연접하여 해시 연산의 입력 데이터를 구성한다. 생성된 입력 데이터를 이용하여 해시 연산을 수행하고 새로운 일별 해시값 H_{tn}을 얻는다②. 일별 해시값이 변경되었기 때문에 연별 해시값을 새로 구해야 한다. 이전 연별 해시값 H_t와 일별 해시값 H_{tn}을 연접하여 입력 데이터를 구성하고 해시 연산을 수행하여 새로운 연별 해시값 H_t를 구한다③. 마찬가지로 연별 해시값 H_t가 변경되었기 때문에 전체 로그의 해시값인 H가 수정되어야 한다. 이전 전체 해시값인 H와 연산된 H_t를 연접하여 입력 데이터를 구성하고 이를 입력으로 해시 연산을 수행하여 새로운 전체 해시값인 H를 구한다④.

4. 가정 및 결과

4.1 단위 연산 정의

다음은 필요한 연산을 정의해본다. 필요한 단위 연산을 간략하게 정의해보면 다음 <표 1>과 같다. 저장소에 읽거나 쓰는데 사용되는 부하와 메시지를 생성하고 분해하는 부하는 생략한다. 또 전자

서명이나 검증에 사용하는 알고리즘은 모두 같다고 가정하고, 사용하는 해시 함수 알고리즘도 동일하다고 가정한다. 또한 네트워크에 접속하여 데이터를 송신하거나 수신하는 경우 연산부하는 없다고 가정한다.

〈표 1〉 필요한 연산 정의

구 분	연산부하
해시 연산	H
암호화	P_E
복호화	P_D
네트워크	N/A

위의 표에서 암호화는 전자서명을 생성하기 위한 암호화를 말하고 복호화는 전자서명을 검증하기 위한 복호화를 말한다.

4.2 단계별 연산부하 정의

각 수행단계에서 어떤 연산이 행해지고 부하는 얼마일지 예상해본다.

- 해시 연산

연산부하는 H로 같다고 가정한다.

- 전자서명

전자서명을 수행하기 위해서는 해시 연산과 암호화 연산이 필요하다. 따라서 연산부하 $S = H+P_E$로 가정한다.

- 전자서명 검증

데이터에 대한 해시 연산과 전자서명에 대한 복호화, 그리고 두 결과의 비교가 필요하다. 따라서 서명검증에 사용되는 연산부하 $V = H+P_D$로 가정한다.

- 시점확인 및 토큰 확보

시점확인을 위해서는 요청, 응답, 확인과정이 필요하다. 요청단계에서는 요청 메시지 생성을 위한 전자서명단계와 송신단계가 필요하고 응답단계에는 수신단계와 응답 메시지에 대한 서명검증단계가 필요하며 확인단계는 토큰 검증을 위해 서명검증단계와 해시값 비교가 필요하다.

요청단계의 연산부하는 S로 가정한다. 응답단계의 연산부하는 V로 가정하고, 확인단계의 연산부하는 V+H로 가정한다.

따라서 전체 연산부하 $T = S+2V+H = 4H+P_E+2P_D$로 가정할 수 있다.

4.3 해시트리 미적용 시스템과의 비교 결과

모든 로그에 장기전자서명검증 포맷을 적용하는 시스템과 로그에 해시트리를 적용한 경우의 차이를 살펴보자. 이를 위해 몇 가지 가정을 한다. 먼저 하루에 생성되는 로그는 n개, 1년은 365일로 가정하여 1년 간의 로그는 $N = 365n$으로 가정한다. 해시트리는 레벨이 L이라고 가정한다. 또한 시점확인용 인증서의 유효기간은 C년으로 한다. 즉 그 해에 생성된 로그 이외에 생성된 지 C년째 되는 장기전자서명 포맷에 대해서도 시점확인을 다시 받아야 한다.

이를 일반화해 보면 장기전자서명 포맷을 적용해야 할 새로운 메시지가 1년에 M_N이고 $Y \geq C$인 Y년이 지났을 때, 첫해에 새로 만들어진 장기전자서명 포맷들이 받은 시점확인 횟수는 $M_N((Y-1)/C+1)$번, 둘째 해에 새로 만들어진 장기전자서명 포맷들이 받은 시점확인 횟수는 $M_N((Y-2)/C+1)$번이 된다. 따라서 Y년 동안 받은 시점확인의 전체 횟수는 다음과 같다.

$$\sum_{i=1}^{Y} M_N\left(\frac{i-1}{C}+1\right) \quad (1)$$

$$= \frac{Y^2+(2C-1)Y}{2C} M_N \quad (Y \geq C)$$

해시 트리를 적용하지 않은 시스템의 경우의 M_N은 다음과 같다.

$$M_N = N = 365n \quad (2)$$

해시트리를 적용한 시스템의 경우 레벨은 L이라고 가정한다. 또한 해시 트리의 각 레벨 당 1년 동안 새로 연산하는 시점확인 개수, 즉 노드의 수를 정의한다. 노드의 레벨이 1일 때 새로 연산하는 시점확인 횟수를 A_1이라고 가정하고 레벨 당 횟수를 $A_1 \le A_2 \le \cdots \le A_L$로 가정하면, 1년간 새로 생성되는 시점확인 횟수는 A로 가정할 수 있다. 즉 $M_N = A$이다.

$$M_N = A = \sum_{l=1}^{L} A_l \quad (3)$$

(그림 3)을 예로 들면 A_1은 1, A_2도 1, A_3은 365가 되고 $M_N = A = 367$이 된다.

위의 가정을 기반으로 Y년 후를 가정해 연산을 추정해보면 다음과 같다. 전체 로그의 개수는 NY로 동일하다.

장기검증을 제외한 연산을 먼저 살펴보면 해시트리를 적용하지 않은 경우는 전자서명만을 수행한다.

$$NSY \quad (4)$$

해시트리를 적용한 경우는 전자서명 외에 각 레벨별로 해시 함수를 수행한다.

$$N(S+(L-1)H)Y \quad (5)$$

장기검증 연산에 대한 연산을 살펴보면 해시트리를 적용하지 않은 경우 식 (1), 식 (2)로부터

$$\frac{Y^2+(2C-1)Y}{2C}NT \quad (6)$$

가 되고 해시트리를 적용한 경우에는 식 (1), 식 (3)으로부터

$$\frac{Y^2+(2C-1)Y}{2C}AT \quad (7)$$

가 된다.

따라서 전체 연산을 보면 해시트리를 적용하지 않은 경우 식 (4), 식 (6)으로부터

$$NSY+\frac{Y^2+(2C-1)Y}{2C}NT \quad (8)$$

가 되며 해시트리를 적용한 경우 식 (5), 식 (7)로부터

$$N(S+(L-1)H)Y+\frac{Y^2+(2C-1)Y}{2C}AT \quad (9)$$

가 된다.

두 경우의 차이(식 (8)-식 (9))를 연도 Y에 대해 풀어보면 2차 방정식이 나온다. 해시트리를 적용하는 이유는 장기검증의 대상을 줄이는 것이므로 1년 간 새롭게 시점확인을 받는 대상이 해시트리를 적용한 경우가 적다. 즉 $N > A$이므로 Y^2의 계수는 0보다 크게 된다. Y^2의 계수가 0보다 클 때 해를 구하면 해시트리를 적용하는 경우 더 효율적이 되기 시작하는 예상연수를 알 수 있다. 0이 아닌 Y의 해가 양수이면 그 만큼의 기간이 지난 후에는 해시트리를 적용한 시스템이 더 효율적이라는 뜻이 된다. Y의 해가 음수이면 해시트리를 적용하면 바로 효율적이 된다고 볼 수 있다. $Y = 0$인 경우를 제외하면 Y의 해는 다음과 같다.

$$Y = \frac{2CN(L-1)}{N-A}\frac{H}{T} - 2C + 1 \ (N \neq A) \quad (10)$$

Y의 해를 살펴보면 N이 A에 비해 충분히 컸을

때, H에 비해 T가 커질수록 Y의 해는 1-2C에 가까워진다. 제 4.2절에서 $T = 4H+P_E+2P_D$로 가정했으므로 전자서명 및 검증연산에 필요한 암·복호화 연산에 비하여 해시 연산이 충분히 빠르면 곧바로 해시트리를 적용한 시스템의 부하가 상대적으로 적어진다.

$$\lim_{N\to\infty}\frac{2CN(L-1)}{N-A}=2C(L-1)\lim_{N\to\infty}\frac{N}{N-A} \quad (11)$$
$$=2C(L-1)$$
$$\lim_{\frac{H}{T}\to 0}(2C(L-1)\frac{H}{T})-2C+1=1-2C \quad (12)$$

식 (11) 식 (12)로부터

$$Y=\frac{2CN(L-1)}{N-A}\frac{H}{T}-2C+1\simeq 1-2C \quad (13)$$
$$(\because N\gg A, T\gg H)$$

위의 결과로 (그림 3)의 예를 적용해 보면 다음과 같다. 즉 시점확인용 인증서의 유효기간 C는 1년이고 해시트리의 레벨은 3이며 레벨 1의 노드는 1일, 레벨 2의 노드는 1년, 루트는 1년에 한번 시점확인을 받는다. 또한 N > A이어야 하므로 하루에 로그는 최소 2개가 생성된다고 가정한다.

$$N=365n(n>1)$$
$$C=1$$
$$L=3$$
$$A=A_1+A_2+A_3=365+1+1=367$$

n값과 H에 대한 T의 비율을 변경시켜 가며 결과를 보면 다음 <표 2>와 같다.

표의 가로축은 하루 당 생성이 예상되는 로그의 개수고 세로축은 해시 연산 H를 1로 봤을 때 H에 대한 T의 비율을 나타낸다. 계산 결과는 해시트리를 적용한 시스템이 적용하지 않은 시스템에 비하여 수행 연산이 적어지기 위해 필요한 예상연수를 나타낸다. 결과를 보면 하루에 로그가 평균 1개만 생성되는 시스템이면 H에 대한 T의 비율이 높아져도 해시트리를 적용한 시스템이 비효율적이다. N>A라는 가정을 어겼기 때문에 Y^2의 계수가 음수가 되어 해가 지날수록 가파르게 효율이 떨어진다. 반면에 하루 생성되는 로그는 어느 수준만 되면 H에 대한 T의 비율이 커질수록 예상연수가 작아진다. 즉 서명 혹은 검증 연산과 비교해서 해시연산이 빠르면 빠를수록 해시트리를 적용한 시스템이 효율적이 될 것이다. n이 1보다 크면서도 결과값이 음수인 것은 첫해부터 해시트리를 적용한 시스템이 효율이 좋은 경우이다.

〈표 2〉 시스템 비교

T \ n	1	2	10	100	10000
2	-366.0	3.02	1.22	1.02	1.00
4	-183.5	1.01	0.11	0.01	0.00
6	-122.7	0.34	-0.26	-0.33	-0.33
8	-92.3	0.01	-0.44	-0.49	-0.50
10	-74.0	-0.20	-0.56	-0.60	-0.60
12	-61.8	-0.33	-0.63	-0.66	-0.67
14	-53.1	-0.43	-0.68	-0.71	-0.71
16	-46.6	-0.50	-0.72	-0.75	-0.75
18	-41.6	-0.55	-0.75	-0.78	-0.78
20	-37.5	-0.60	-0.78	-0.80	-0.80

결과표 <표 2>는 표면 C = 1일 때의 예이므로 (13)에 의해 n과 T가 커질수록 -1로 가까이 가는 것을 알 수 있다.

5. 결 론

보관소에서는 로그를 생성하지 않을 수 없고 또

한 지워서도 안 된다. 문제가 생겼을 때 증거가 될 수 있는 로그를 검증할 수 없다면 문제가 될 수 있다. 따라서 보관소 표준업무준칙을 보면 운영 중에 생기는 여러 로그를 남겨야 하고 또한 관리하여야 하며 그 중요성을 생각하여 비인가자의 접근을 제한하면서 감사관리자는 전자서명을 해야 한다고 나와 있다. 게다가 보관소에 등록된 문서가 많아질수록 로그의 양은 급격히 늘어난다. 이 많은 개수의 로그마다 장기전자서명검증 포맷을 적용하게 된다면 시스템의 부하를 걱정하지 않을 수 없다.

이런 문제점을 해결하기 위하여 해시트리를 이용하여 장기전자서명검증 포맷을 적용할 대상을 줄임으로써 로그의 무결성을 보장하면서도 부하를 줄일 수 있는 방법을 생각해보았다. 이 방법은 부가적으로 로그가 삭제되었는지 전체 로그에 대한 무결성을 검증할 수도 있다.

앞으로 공인전자문서보관소에 대한 연구가 이뤄지고 장기전자서명검증에 대한 연구가 진행 될수록 더 효율적이면서도 안전한 모델이 나올 수 있을 것이다. 또한 해시 알고리즘에 대한 안전성이 침해되었을 때를 대비한 연구도 진행되어야 할 것이다.

참 고 문 헌

[1] 법률 제8461호, "전자거래기본법", 제31조, 2007.

[2] 산업자원부고시 제2006-48호, "전자문서보관 등 표준업무준칙", 제21조, 2006.

[3] 이인수, "인터넷 증명서 발급 시스템의 보안 요구사항 및 안정성에 관한 연구", 고려대학교 대학원, pp. 50-52, 2004.

[4] 한국전자거래진흥원, "이용자 시스템 기술규격", v1.00, KIEC-TS-USER, 2007.

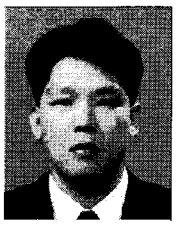
[5] 한국전자거래진흥원, "전자문서 정보패키지 기술규격", v1.10, KIEC-TS-PACKAGE, 2007.

[6] 한국전자거래진흥원, "전자문서 증명서 포맷 및 운용절차 기술규격", v1.10, KIEC-TS-CERTIFICATE, 2007.

[7] D. Pinkas, J. Ross, and N. Pope, "Electronic Signature Formats for long term electronic signatures", RFC3126, September 2001.

[8] T. Gondrom, R. Brandner, and U. Pordesch, "Evidence Record Syntax(ERS)", RFC4998, August 2007.

[9] Ralph Merkle, "Method of providing digital signatures", U.S. Patent 4309569, 1982.



강 신 명

1997년 과학기술원 과학기술대학교 전산학과(공학사)

현재 고려대학교 정보경영공학 전문대학원 석사과정

문 종 섭

1985년 금성통신연구소 연구원

1991년 Illinois Institute of technology 졸업(전산학 박사)

현재 고려대학교 전자 및 정보공학부 교수