베이지안 네트워크를 활용한 원자력 수출입 위험도 평가 관련조사†

(Proxy Signature, ID-based Partially Blind Signature and Proxy Partially Blind Signature using Bilinear-pairing)

김 현 주 ‡ 여 상 희 § 원 동 호 ¶
(Hyunjue Kim) (Sanghee Yeo) (Dongho Won)

요 약 대리서명은 대리서명자로 하여금 원서명자를 대신해서 서명하도록 하는 암호방식이고, 부분은닉서명은 서명자가 은닉서명을 발행할 때 그가 삽입하기를 원하는 어떠한 정보를 서명에 삽입할 수 있도록 하는 암호방식으로, 부분은닉성과 익명성(또는 불추적성)을 제공하기 때문에 전자상거래에서 전자화폐나 전자투표 등과 같은 사용자의 프라이버시 보호나 보안을 요구하는 응용분야에 중요하게 적용되는 기술이다. 본 논문에서는 bilinear-pairing을 이용한 대리서명 방식과 ID 기반 부분은닉서명 방식을 제안한다. 그리고 두 방식을 결합한 대리부분은닉서명 방식을 제안한다. 제안하는 방식들은 GDH군에서 성립하며 CDHP의 어려움에 기반을 두고 있다. 제안하는 ID 기반 부분은닉서명 방식과 대리부분은닉서명 방식에서 공통정보를 제거하면 두 서명 방식은 각각 ID 기반 은닉서명 방식과 대리은닉서명 방식이 된다.

키워드 : 대리서명 방식, ID 기반 부분은닉서명 방식, 대리부분은닉서명 방식, Gap Diffie-Hellman 문제, Bilinear-pairing

Abstract Proxy signature scheme allow a designated proxy person to sign a message on behalf of the original signer. Partially blind signature scheme allows the signer to insert non-removable common information into his blind signature. Proxy signature and partially blind signature are very important technologies in secure e-commerce. In this paper we propose new proxy signature scheme and ID-based partially blind signature scheme using bilinear pairing. Further combining them, we propose a proxy partially blind signature scheme. The security of our schemes relies on the hardness of Computational Diffie-Hellman Problem. If we removing common information form propose ID-based partially blind signature scheme and proxy partially blind signature scheme, then they become variants of ID-based blind signature scheme and proxy blind signature scheme of Zhangs respectively.

Key words : Proxy signature, ID-based Partially Blind Signature scheme, Proxy Partially Blind Signatur scheme, Gap Diffie-Hellman Problem, Bilinear-pairing

1. 개 요 (임경태 서술 예정)

대리서명 방식은 원서명자가 자신의 부재중에 자신을 대신해서 서명을 할 수 있는 대리 서명자를 지정하여 대신 서명하도록 하는 서명 방식으로 기업의 대표가 과도한 업무나 또는 출장 등과 같은 이유로 제한된 기간 내에 반드시 서명을 해야하는 계약서나 문서에 서명을 못하게될 상황에 대한 해결책으로 유용하게 활용되고 있다. 대리서명 방식은 1996년 M. Mambo, K. Usuda와 E. Okamoto[1]에 의해서 처음 소개되었고, 그 후 많은 사람들에 의해서 연구되었다[2-7].

M. Mambo, K. Usuda와 E. Okamoto는 대리서명 방식을 위임의 형태에 따라서 완전 위임(full delegation), 부분 위임(partial delegation)과 보증 위임(delegation by warrant)으로 분류하였고 S. Kim, S. Park와 D. Won[2]은 부분 위임의 장점과 보증 위임의 장점을 결합한 보증부분위임(partial delegation with warrant)이라는 새로운 개념을 제안하였다. 본 논문에서 제안한 대리서명

† 본 연구는 2004년도 정보통신부 지원 대학 IT 연구센터 육성지원사업(C1090-0403-0005)의 연구비 지원으로 수행하였습니다.
‡ 학생회원 : 성균관대학교 정보통신공학부
hjkim@dosan.skku.ac.kr
§ 비 회 원 : 성균관대학교 정보통신공학부
yeosh72@hanmail.net
¶ 종신회원 : 성균관대학교 정보통신공학부 교수
dhwon@dosan.skku.ac.kr
논문접수 : 2003년 10월 27일
심사완료 : 2004년 09월 02일

Copyright©2004 한국정보과학회 : 개인 목적이나 교육 목적인 경우, 이 저작물의 전체 또는 일부에 대한 복사본 혹은 디지털 사본의 제작을 허가합니다. 이 때, 사본은 상업적 수단으로 사용할 수 없으며 첫 페이지에 본 문구와 출처를 반드시 명시해야 합니다. 이 외의 목적으로 복제, 배포, 출판, 전송 등 모든 유형의 사용행위를 하는 경우에 대하여는 사전에 허가를 얻고 비용을 지불해야 합니다.
정보과학회논문지: 정보통신 제31권 제6호(2004.12)

방식은 보증부분위임방식이다.

2. 베이지안 네트워크 (1~2페이지)

베이지안 네트워크는 ㅌㅌㅌㅌ로서

2.1 베이지안 네트워크의 특징

ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ
ㄹ~~~~~~

2.2 베이지안 네트워크의 유형

ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ
ㄹ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

3. 베이지안 네트워크 활용사례 (1~2페이지)

3.1 일반적인 활용 사례

ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ
ㄹ~~~~~~

3.2 위험도 평가 분야에 대한 활용사례

ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ ㄹ ㅇ
ㄹ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

4. 제안하는 베이지안 네트워크 모델

대리서명 방 하였다. Diffie-Hellman 문제를 정리하면 다음과 같다.

4.1 원자력전용품목 수출 위험도평가 데이터 분석 (월요일이후, 1페이지)

대리서ㅇㄹㅇㄹㅇ.ㅇㄹㅇㄹㅇ

4.2 수출 위험도평가 제안 모델 (월요일 이후, 5페이지)

대리서ㅇㄹㅇㄹㅇ.ㅇㄹㅇㄹㅇ

참 고 문 헌

[1] M. Mambo, K. Usuda and E. Okamoto, "Proxy Signature : Delegation of the Power to Sign Messages," In IEICE Trans. Fundamentals, Vol. E79-A, No. 9, pp. 1338-1353, Sep., 1996.