안전성이 증명된 의뢰 undeniable signature

박성준°, 김성덕, 원동호
성균관대학교 정보공학과

A Provable Entrusted undeniable signature

Sung Jun Park, Sung Duk Kim and Dong Ho Won
Department of information Engineering
Sung Kyun Kwan University

요 약

대화형 영지식 증명시스템을 사용하여 D. Chaum의 undinable signature에 대한 거짓말 탐지기 기능 문제를 해결한 안전성이 증명된 의뢰 undeniable signature 방식을 제안한다.
제안한 방식의 안전성은 영지식 대화형 증명시스템과 고차 잉여류 문제에 기반을 두고 있다.

1. 서론

고도의 정보처리 및 정보통신을 기반으로 하는 정보화사회에서는 컴퓨터 통신망에 대한 다양한 보안서비스들에 대한 요구가 절실히 요구되고 있다. 이 중에서도 가장 중요한 것 중의 하나는 인증 기술이다. 특히 메세지 및 사용자 에 대한 인증을 동시에 해결할 수 있는 디지틀 서명 기술은 각종 보안 서비스에서 필수 불가결한 도구로 사용된다. 특히 누구나 메세지의 출처와 메세지의 진위여부를 확인할 수 있는 자체 인증기능을 갖는 디지틀 서명은 대부분의 응용분야에서는 매우 유용하다.

그러나 개인적으로나 상업적으로 민감한 응용들에서는 이러한 자체인증은 필요 이상의 과다한 인증 기능(서명의 사본으로 누구나 인증 가능)을 제공함으로서 서명의 사본들이 악용될 수 있는 가능성을 높여주게 된다. 따라서 단순한 서명의 사본만으로는 이를 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 서명자나 수신자의 부당한 위협가능성을 줄여주고 프라이버시를 높여줄 수 있는 서명방식이 보다 바람직한 경우가 있다.[LL]

이러한 특수한 서명방식중 하나가 D.Chaum에 의해 제안된 undeniable signature이다. D. Chaum에 의해 제안된 undeniable signature은 서명자의 도움없이는 서명문을 확인할 수 없는 특징을 가지고 있으며,서명문의 진위를 확인해주는 confirmation protocol과 자신의 서명문을 부인하지 못하게 하는 disavowal protocol로 구성된다.[C][CH]

그러나 undeniable signature은 자신의 서명문을 부인하지 못하게 하는 disavowal protocol로 인하여 일종의 거짓말 탐지기 기능을 제공해주게 된다. 이와 같은 문제를 해결하기 위하여 T. Okamoto 등이 제안한 것이 non-transitive digital signature이다. 그러나 *non-transitive digital signature*은 서명이 문제가 되었을 때 분쟁 해결의 기능이 없다는 점에서 디지를 서명이라고 볼 수 없다.[OO]

한편 임채훈 등은 지정된 수신자만이 서명을 인증할 수 있고 필요시 제3자에게 그 서명이 자신에게 발행된 유효한 서명임을 증명할 수 있게 함으로서 자신에게 발행된 서명의 남용을 통제할 수 있는 수신자 지정 서명방식을 제안하였다.[LL]

또한 박성준 등은 영지식 대화형 증명시스템(ZKIPS : *Zero-Knowledge Interactive Prorf System*)을 이용하여 undeniable signature의 특성을 유지하면서 거짓말 탐지기 기능 문제를 해결해주는 의뢰 undeniable signature 를 제안하였다. 그러나 제안한 의뢰 undeniable signature의 안전성은 안전성이 증명안된 RSA 암호시스템을 이용하여 구성하였다.[PW2]

본 논문에서는 고차잉여류 문제를 사용하여 의뢰 undeniable signature의 안전성을 이론적으로 증명할 수 있는 안전성이 증명된 의뢰 undeniable signature 를 제안한다.

2. 의뢰 undeniable signature

본 장에서는 영지식 대화형 증명시스템을 이용하여 거짓말 탐지기 기능 문제를 해결하는 의뢰 undeniable signature 방식을 설명한다.[PW2]

Undeniable signature 방식에서 거짓말 탐지기 기능 문제가 발생하는 것은 결국 검증을 원하는 임의의 검증자가 disavowal protocol을 수행할 수 있다는 데서 기인한다. 따라서 거짓말 탐지기 기능 문제를 해결하기 위해서는 임의의 검증자가 disavowal protocol을 수행하지 못하고 특정한 자(예를 들어 분쟁이 일어났을 때 해결해주는 사람, 재판관 등)만이 disavowal protocol을 수행할 수 있도록 만드는 것이다. 또한 디지를 서명의 특성상 confirmation protocol은 임의의 검증자에게 수행할 수 있도록 해야 한다.

Entrusted undeniable signature의 구성 방법은 먼저 undeniable signature의 disavowal protocol에서 사용되는 서명자의 공개키 g^x를 $(g^x)^r$로 랜덤화 함으로서 r를 모르는 검증자는 disavowal protocol를 수행하지 못하게 한것이다.

그러나 confirmation protocol은 먼저 g^x를 랜덤화한 g^{rx}를 영지식 대화형 증명시스템을 이용하여 검증자에게 증명한 후 수행하게 함으로서 임의의 검증자에게 가능하도록 하고 분쟁 해결(서명문의 서명자를 확인)을 위해 랜덤 변수 r를 commitment scheme을 사용,후에 부정을 못하도록 한것이다.

- 시스템 구성도
  - Undeniable signature 시스템
  - 재판관
    . Disavowal protocol을 수행함
    . RSA 시스템 사용
      공개키 : (e,n)
      비밀키 : (d,p,q)
- CS(Commitment Scheme)
  $CS(r)=r^e \bmod n$
- 서명문 : $< CS(r), (g^{rx}, m^{rx}) >$
- Confirmation protocol
  전체 과정은 그림 1과 같다.

서 명 자		검 증 자
random r	CS(r) , g^{rx} ---------->	
	< CS(r) , g^{rx} > 에 대한 ZKIP	
	confirm protocol < g^{rx}, m^{rx} >	
	서명문 <CS(r), (g^{rx}, m^{rx})> ---------->	

그림 1. Confirmation protocol

- < CS(r) , g^{rx} > 에 대한 영지식 대화형 증명시스템
그림 2의 과정을 t회 반복한다.(여기서 서명자의 속임수를 인지할 수 있는 확률은 2^{-t}이다.)

서 명 자		검 증 자
랜덤 수 l $v_1=l^e$ modn $v_2=g^{rlx}$ modP	v_1 , v_2 ---------->	
	b <----------	랜덤 비트 b
b=0 : R=l b=1 : R=rl	R ---------->	b=0 v_1, v_2 확인 b=1 $R^e=v_1r^e$ mod n $v_2=(g^x)^R$ mod P

그림 2. < CS(r) , g^{rx} > 에 대한
영지식 대화형 증명시스템

- < g^{rx}, m^{rx}> 에 대한 confirmation protocol
비밀키 x를 사용하는 대신에 rx를 사용한다는 것을 제외하고는 D. Chaum의 프로토콜과 같으며 절차는 그림 3과 같다.

서명자		검증자
	$m^a g^b$ <----------	랜덤 수 a,b
랜덤 수 q	$m^a g^{b+q}$, $(m^a g^{b+q})^{rx}$ ---------->	
	a,b <----------	
	q ---------->	

그림 3. $< g^{rx}, m^{rx} >$ 에 대한 confirmation protocol

○ 서명문 $<CS(r), (g^{rx}, m^{rx})>$ 에 대한 재판관의 disavowal protocol

- $< CS(r), g^{rx} >$ 에서 r를 계산한다.

  $r=(CS(r))^d \bmod n$

- $< g^{rx}, m^{rx} >$ 에 대한 disavowal protocol

  그림 4의 과정을 t회 반복한다.

- $z \neq m^{rx}$

서명자		재판관
	$m^a g^A$, $z^a g^{rxa}$ <----------	랜덤 수 $s \varepsilon \{0,\ldots,k\}$, a
s를 계산하여 commit 한다	blob(1,s) <----------	
	a <----------	
	1 ---------->	

그림 4. $< g^{rx}, m^{rx} >$ 에 대한 disavowal protocol

3. 안전성이 증명된 의뢰 undeniable signature

본 장에서는 고차잉여류 문제를 사용하여 안전성을 이론적으로 증명할 수 있는 의뢰 undeniable signature 방식을 설명한다.

기존에 제안한 의뢰 undeniable signature 방식는 재판관이 사용하는 commitment scheme 으로 안전성을 증명할 수 없는 RSA 방식을 사용하였다. 새로이 제안하는 시스템은 재판관이 사용하는 commitment scheme으로 안전성을 이론적으로 증명할 수 있는 γ^{th}-residuosity 문제를 사용한다.[PW1][PJKW]

- ㅇ 시스템 구성도
  - Undeniable signature 시스템
  - 재판관
    . Disavowal protocol을 수행함
    . γ^{th}-residuosity 문제 사용
      공개키 : Acceptable한 triple (n,γ,y)
      비밀키 : n의 소인수
- ㅇ CS(Commitment Scheme)
  $CS(r)=y^r \bmod n$
- ㅇ 서명문 : $\langle CS(r),(g^{rx},m^{rx})\rangle$
- ㅇ Confirmation protocol
  전체 과정은 2장의 그림 1과 같다.

  - $\langle CS(r), g^{rx}\rangle$ 에 대한 영지식 대화형 증명시스템
    그림 5의 과정을 t회 반복한다.
    (여기서 서명자의 속임수를 인지할 수 있는 확률은 2^{-t}이다.)

서 명 자		검 증 자
랜덤 수 l $v_1=y^l \bmod n$ $v_2=g^{(r+1)x} \bmod P$	v_1, v_2 ---------->	
	b <----------	랜덤 비트 b
b=0: R=l b=1: R=r+l	R ---------->	b=0 v_1, v_2 확인 b=1 $R^e=v_1y^r \bmod n$ $v_2=(g^x)^R \bmod P$

그림 5. $\langle CS(r), g^{rx}\rangle$ 에 대한
영지식 대화형 증명시스템

4. 결론

본 논문에서는 D. Chaum의 undeniable signature 방식의 거짓말 탐지기 기능 문제를 영지식 대화형 증명시스템을 이용하여 해결한 의뢰 undeniable signature 방식에서 고차 잉여류 문제를 이용하여 안전성을 이론적으로 증명한 안전성이 증명된 의뢰 undeniable signature 방식을 제안하였다.

향후에는 위의 시스템을 좀 더 효율적으로 구성하는 방법과 영지식 대화형 증명시스템(계산량이 많고,많은 interaction을 필요로 하는 단점)을 사용하지 않는 의뢰 undeniable signature 방식을 연구하고자 한다.

5. 참고문헌

[BCD] J. Boyar, D. Chaum, and I. Damgard, "Convertible undeniable signature", Proc. Crypto'90.

[C] D. Chaum, " Zero-knowledge undeniable signature", Proc. Eurocrypt'90.

[CH] D. Chaum and H. Antwerpen, "Undeniable signature", Proc. Crypto'89.

[KPW] 김승주, 박성준, 원동호, "수신자지정서명방식에 관한 고찰", 한국정보처리응용학회 학술발표회, 1994.10.8.

[LL] 임채훈, 이필중, "상호 신분 인증 및 디지틀 서명기법에 관한 연구", 통신정보보호학회논문집 제2권 제1호, 1992.

[OO] T. Okamoto and K. Ohta, "How to utilize the randomness of zero-knowledge proofs", Proc. Crypto'90.

[PLW] 박성준, 이보영, 원동호, "의뢰 Undeniable Signature", 한국통신학회 학술발표회, 1994년.7.

[PW1] S. J. Park and D. H. Won, "A Generalization of Public Key Residue Cryptosystem", Proceeding of JW-ISC'93, pp.202-206, 1993.

[PW2] S. J. Park and D. H. Won, "An Entrusted Undeniable Signature", Submitted to JW-ISC'95, Japan, 1995.1.

[PJKW] S. J. Park, Chung Ryong Jang, Kyung Sin Kim, and D. H. Won, "A "Paradoxical" identity-based scheme based on the γ^{th}-residuosity problem and discrete logarithm problem", To be published at An International Conference on Numbers and Forms, cryptography and codes, August 21-28, 1994, Khabarovsk, Russia.

[ZMH] Y. Zheng, T. Matsumoto, and H. Imai, "Residuosity Prblem and its Applications to Crytpography", Trans. IEICE, vol.E71, No.8, pp.759-767, 1988.

[Z] Y. Zheng, "A Study on Probabilistic Cryptosystems and Zero-knowledge Protocol", Master thesis, Yokohama National University, 1988.