디지틀 서명방식 표준(안)에 기반을 둔 통합서명 시스템에 관한 연구

김 승 주† · 김 경 신†† · 원 동 호†††

요 약

정보화 사회의 거의 모든 정보는 **통신망을 통해** 이루어지고, 이에 따라 통신망 상에서의 정보보호가 중요한 과제로 부각되고 있다. 이러한 통신망 상의 **정보보호를 위해 필수**적인 암호학적 도구가 디지틀 서명이며, 세계 여러 나라에서 고유의 디지틀 서명 알고리즘을 **표준화하려는 노력이 경주되어** 왔다.

또한, 1989년 Crypto'89 국제 **학술회의에서** D.Chaum은 단순한 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 확인을 위해서는 반드시 **서명자의 도움을 받게 함으로써**, 서명자에 대한 부당 위협 가능성을 **줄여 주고 개인**의 사생활을 보호할 수 있는 undeniable signatures를 제안하였으며, 지금까지 많은 undeniable형 디지틀 **서명방식들**이 서명의 남용으로부터 서명자나 **수신자를 보호하기 위하여** 제안되었다.

본 논문에서는 기존의 undeniable형 특수 디지틀 서명방식들과 각 디지틀 서명방식 표준(안) - 예를 들어, KCDSA, DSS, GOST 등 - 을 하나로 통합한 **일반화된** undeniable형 디지틀 서명을 제안한다.

A Study on the Integrated Digital Signature System based on Digital Signature Standards

Seung-Joo Kim† · Kyung-Shin Kim†† · Dong-Ho Won†††

ABSTRACT

In the information society, all the information is transferred through the network, so it becomes an issue to protect the data on network. One of the fundamental cryptographic tools to protect the data on network, is digital signatures, and in many countries, cryptographers have been trying to make their own digital signature standard.

Also, at Crypto'89 meeting, D.Chaum suggested an undeniable signature scheme. Undeniable signatures are verified via a protocol between the signer and the verifier, so the cooperation of the signer is necessary. So far, there have been several variants of undeniable signatures to obtain a signature scheme, which can control the abuse of ordinary digital signatures.

※ 이 논문은 1996년도 한국학술진흥재단의 공모과제 연구비에 의하여 연구되었음.

† 준 회 원 : 성균관대학교 전기전자 및 컴퓨터공학부
†† 정 회 원 : 인덕전문대학 방송통신과
††† 종신회원 : 성균관대학교 전기전자 및 컴퓨터공학부

논문접수 : 1997년 12월 15일, 심사완료 : 1998년 2월 10일

1. 서 론

정보화 사회로의 진전으로 컴퓨터 통신망을 통한 다양한 서비스가 요구되고 있다. 이에 따라 메시지의 수신자는 받은 메시지가 전송 도중 내용이 바뀌지 않았는지, 또는 제3자가 송신자를 가장하여 메시지를 보내지 않았는지 등을 확인할 수 있기를 바란다. 이런 목적으로 사용되는 가장 효율적인 도구가 디지틀 서명(digital signatures)이다. 디지틀 서명은 기존의 서류 시스템에서의 인장(도장)이나 서명과 같은 메시지 인증과 사용자 인증의 역할을 정보통신 서비스에서 실현하고자 하는 것이다. 그러므로 디지틀 서명은 도장이나 서명의 특성을 따르게 된다. 일반적으로 서명이나 인감은 개인의 필요성에 의하여 언제든지 발급될 수 있고, 이 서명 또는 인감을 수신한 사람 역시 수신된 서명이나 인감의 정당성을 쉽게 확인할 수 있으며, 서명의 생성자나 인감의 소유자 이외에는 이 서명이나 인감을 발급할 수 없어야 한다. 따라서 디지틀 서명에도 서명자만이 서명을 생성할 수 있는 유일성, 위조가 불가능한 위조 불가능성, 서명의 진위를 쉽게 확인할 수 있는 진위 확인의 용이성, 자신의 서명을 위조된 것이라고 거부하는 것이 불가능한 거부의 불가능성 등의 요구사항을 만족하여야 한다.

1976년 Diffie와 Hellman이 공개키 암호화 방식(public key cryptosystem)의 개념을 소개한 후[1], 1978년 Rivest, Shamir, Adleman이 이 개념을 바탕으로 최초의 디지틀 서명을 개발하였으며[2], 그 후 나름대로 진보된 형태의 많은 디지틀 서명들이 개발되어 왔다.[3,4] 이렇듯 디지틀 서명 알고리즘은 정보보호를 위한 필수적인 조건이며, 세계 각국에서도 고유의 디지틀 서명 알고리즘을 표준화하려는 노력이 경주되어 왔다. 이미 미국이나 러시아 등은 ElGamal형의 국가 표준 서명방식인 DSA(Digital Signature Standard)[5], GOST 등을 채택하였으며[6], 국내에서도 '94년부터 한국전자통신연구소 정보통신 표준연구센터의 지원을 받아 국가 표준화를 목적으로 정보처리 시스템 또는 정보통신망에서 임의의 길이를 갖는 메시지에 대한 확인서 이용 부가형 디지틀 서명의 생성과 검증을 위한 알고리즘 KCDSA(Korean Certificate-based Digital Signature Algorithm)가 발표되었다.[7]

누구나 메시지의 출처와 진위여부를 확인할 수 있는 자체인증기능을 갖는 일반적인 디지틀 서명은 대부분의 응용분야에서는 매우 유용하다. 그러나 개인적으로나 상업적으로 민감한 응용들에서는 이러한 자체 인증은 서명의 사본으로 누구나 서명의 인증이 가능하므로, 필요 이상의 과다한 인증 기능을 제공함으로써 서명의 사본들이 악용될 수 있는 가능성을 높여주게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 서명자나 수신자에 대한 부당 위협 가능성을 줄여 주고 개인의 사생활을 보호할 수 있는 특수 디지틀 서명방식이 보다 바람직한 경우가 존재한다. 이러한 목적에 의해 Crypto'89 회의에서 D.Chaum이 undeniable signatures를 제안한 후, (selectively) convertible undeniable signatures, designated confirmer signatures 등의 많은 undeniable형 디지틀 서명방식들이 서명의 남용을 통제하기 위하여 제안되었다. 국내에서의 undeniable signatures에 대한 연구는 박성준 등에 의해 연구된 entrusted undeniable signatures와 임채훈 등의 directed signatures, 김승주 등의 nominative signatures 등이 있다.

본 논문에서는 이러한 undeniable형 특수 디지틀 서명방식들과 각 디지틀 서명방식 표준(안)들을 하나의 서명방식으로 통합한 방식을 제안한다.[27,28] 이는 시스템의 메모리 비용을 고려할 때 매우 유리할 것이며, 또한 P.Horster의 "Meta-ElGamal 서명방식" 개념을 이용하여 "Meta-Undeniable형 서명방식"으로도 확장될 수 있을 것이다.[18]

본 논문의 구성은 2장에서 대표적인 특수 디지틀 서명방식인 undeniable형 서명방식들에 대하여 살펴보고, 3장에서는 미국, 러시아, 한국 등의 디지틀 서명 표준(안)들에 대하여 살펴본다. 그리고 4장에서는 각 디지틀 서명 표준(안)들을 이용하여 기존의 여러 undeniable형 특수 디지틀 서명방식들을 하나의 서명방식으로 통합한 방식을 제안하고, 5장에서 결론 및 향후 연구 방안을 제시한다.

2. Undeniable형 서명방식

공개키 암호 시스템을 이용한 일반적인 디지틀 서명방식은 공개키가 모든 사용자에게 공개되기 때문에 네트워크에 가입한 사람은 누구든지 메시지의 진위 여부

를 확인할 수 있게 되어 필요 이상의 과다한 인증 기회를 제공하게 되며 이로 인해 개인의 이익 또는 사생활이 노출될 가능성이 있게 된다. 따라서 서명의 사본만으로는 서명의 정당성을 확인할 수 없고 서명의 인증을 위해서는 반드시 서명자의 도움을 받아야 하거나 특정 수신자만이 서명을 확인할 수 있게 하는 방법 등에 의해 개인의 사생활을 보호할 수 있는 특수 디지틀 서명 방식이 보다 바람직한 경우가 존재한다. D.Chaum의 undeniable signatures는 이러한 목적에 의해 제안되었다.

〔정의 1〕 undeniable signatures … 서명자의 도움 없이는 서명문의 진위를 확인할 수 없으며, 서명자는 필요시에 제3자에게 자신이 발행한 디지틀 서명이 정당함을 보일 수 있다[9][10].

기존에 제안된 일반적인 디지틀 서명방식들은 검증 프로토콜에서 단지 서명의 정당성 여부만 확인하는데 비하여 D.Chaum에 의해 제안된 부인 방지 서명은 검증 프로토콜이 서명의 정당성 여부를 판단하는 "확인 프로토콜(confirmation protocol)"과, 확인 프로토콜에서 서명의 정당성 확인이 실패했을 경우 확인하려고 한 서명이 불법적인 침입자에 의해 만들어진 부당한 서명인지, 아니면 정당한 서명에 대하여 서명자가 부인하려는 의도에서 적절하지 않은 응답을 하였는지를 구분하기 위한 "부인 프로토콜(disavowal protocol)"로 나누어져 있다.

J.Boyar 등은 undeniable signatures를 일반적인 서명으로 변환시킬 수 있는 convertible undeniable signatures를 제안하였다.

〔정의 2〕 convertible undeniable signatures … 비밀키의 일부를 노출시킴으로써, 특정한 부인 방지 서명만 선택적으로 혹은 전체 부인 방지 서명을 모두 일반적인 서명으로 변환시킬 수 있는 서명방식이다.[11]

그러나, undeniable signatures나 convertible undeniable signatures는 자신의 서명문을 부인하지 못하게 하는 부인 프로토콜의 성질로 인하여 일종의 거짓말 탐지 기능 문제를 갖고 있어 응용이 제한적인 경우가 있다.[12]

예를 들어, 어느 기관에서 근무하는 공직자가 신문사나 방송국 등의 언론 기관에 비밀 정보를 제공하려 할 때 신원이 밝혀지는 것을 걱정하여 익명을 요구하며 정보를 제공하려고 하는 경우를 생각해 보자. 언론 기관에서는 허위 정보를 보도할 수 없으므로 정보 제공자의 신원을 확인할 필요가 있을 것이고 또한, 언론 기관은 정보 제공자의 요구대로 그의 신원을 밝히지 않겠다는 약속을 할 것이다. 이 경우에도 일반적인 디지틀 서명은 적합하지 않으며 만일 정보 제공자가 undeniable signatures를 사용한다고 가정해 보자.

정보가 기사화 되고 그 출처를 알아내기 위해 해당 기관에서 이를 추적하는 과정에서 이 정보와 관련된 정보를 얻었다고 하자. 그러면 그 해당 기관에서는 의심이 갈 만한 모든 내부 직원에게 부인 프로토콜을 수행하게 함으로써 정보의 출처를 알아낼 수 있을 것이다. 즉, 의심을 받은 사람은 부인 프로토콜을 수행하면 쉽게 자신의 누명을 벗을 수 있고 오히려 이를 거부하는 사람은 자신이 그 정보의 출처임을 시인하는 결과가 될 것이므로 이를 거부할 하등의 이유가 없을 것이다. 따라서 결국 정보 제공자는 신원이 밝혀지게 되므로 이와 같은 응용에서는 undeniable signatures가 적합하지 않음을 알 수 있다. 박성준 등은 이를 해결한 entrusted undeniable signatures를 제안하였다.

〔정의 3〕 entrusted undeniable signatures … 임의의 검증자가 부인 프로토콜을 수행할 수 없게 하고 특정한 자, 예를 들어 분쟁이 발생하였을 때 중재하는 사람 혹은, 재판관만이 부인 프로토콜을 수행할 수 있도록 하되, 디지틀 서명 특성상 확인 프로토콜은 임의의 검증자가 할 수 있는 서명방식이다.[13][14]

또한 undeniable signatures의 경우, 서명자는 자신의 서명에 대한 완전한 통제권을 가지게 됨으로써 서명의 남용으로부터 자신을 보호할 수 있는 장점이 있는 반면, 서명자가 서명 확인/부인 프로토콜을 위한 비밀키를 분실하였다고 주장하거나 서명자의 부재 시에는 서명의 진위를 판정할 수 없다는 단점이 있다. D.Chaum의 designated confirmer signatures는 이러한 단점을 해결하기 위하여 제안되었다.

〔정의 4〕 designated confirmer signatures … 서명자뿐만 아니라 지명된 제3자(designated third party)도 디지틀 서명의 정당성을 증명할 수 있게 함

으로써, undeniable signatures의 "보호 남용(abuse of protection) 문제"를 해결할 수 있는 서명 방식이다.[15][16]

한편 임채훈 등은 수신자가 서명의 사본들이 불법적으로 사용되는 것을 통제할 수 있도록 하는 directed signatures 개념을 소개하였다.

〔정의 5〕 directed (or designated verifier) signatures … 서명자 또는 지명된 수신자(designated verifier)의 도움 없이는 서명문의 진위를 확인할 수 없는 서명방식이다. 이는 "designated third party = receiver"인 designated confirmer signatures의 특별한 경우라고 할 수 있다.[17][18][19]

그러나 directed signatures는 수신자뿐만 아니라 서명자 또한 발행된 서명문을 통제할 수 있으므로, - 수신자가 자신의 서명에 대한 완전한 통제권을 가지지 못함으로써 - 서명자가 지명된 수신자에게 서명한 사실을 부인하기 위해 키를 제3자에게 은밀히 누출시키는 경우 수신자가 자신의 프라이버시에 관련된 서명의 남용을 통제할 수 없다는 약점이 있다.[20] 김승주 등은 undeniable signatures의 쌍대 개념(dual scheme)으로, 발행된 서명이 수신자의 개인적인 이해 관계나 사생활에 밀접한 관련이 있을 경우 수신자의 동의 없이 서명을 확인할 수 없게 하여 특정 수신자에 대한 서명의 남용을 방지할 수 있는 nominative signatures을 제안하였다.

〔정의 6〕 nominative signatures … 지정된 수신자(nominee)만이 서명을 확인할 수 있고 필요시 제3자에게 그 서명이 서명자(nominator)에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있게 함으로써 서명의 남용을 서명자가 아닌 검증자(수신자)가 통제할 수 있는 서명방식이다.[21][22][23]

3. 디지틀 서명 표준(안)

3.1 한국의 KCDSA

디지틀 서명 알고리즘은 정보보호를 위한 필수적 조건이며 "전산망 보급확장과 이용 촉진에 관한 법률의 개정안"에도 전자 문서의 법적 효력을 인정하고 있고, 디지틀 서명이 들어가야 함을 원칙으로 하고 있다. 이러한 때에 '94년부터 국내의 암호학자들과 유관기관의 지원을 받아 국가 표준화를 목적으로 정보처리 시스템 또는 정보통신망에서 임의의 길이를 갖는 메시지에 대한 확인서 이용 부가형 디지틀 서명의 생성과 검증을 위한 알고리즘 KCDSA (Korean Certificate-based Digital Signature Algorithm)가 발표되었다. 본 절에서는 표준안으로 상정된 이 KCDSA를 간략히 기술한다.

시스템 초기화

- 소수 P : $|P|$ = 512 + 256i (단, $0 \le i \le 6$). 안전성을 위하여 (P-1)/2Q이 역시 소수이거나 (P-1)/2이 최소한 Q보다 큰 소수들의 곱으로 구성되는 소수 P를 사용할 것을 권고한다.
- 소수 Q : P-1을 나누는 소수로, $|Q|$ = 128 + 32j (단, $0 \le j \le 4$).
- 기본원 G : 위수(order) Q를 갖는 기본원소, 즉 $G \neq 1$ 이고 $G^Q = 1 \bmod P$인 G.
- 해쉬함수 h : $|Q|$ 비트 길이의 출력을 갖는 충돌저항형 해쉬함수

사용자 초기화

① 서명자는 자신의 비공개 서명키 X ($0 < X < Q$)를 랜덤하게 선택하여 비밀리에 간직한다.

② 서명자는 비공개 서명키 X에 대응하는 공개 검증키 Y를 $Y = G^{X^{-1}} \pmod P$와 같이 계산한다.

서명 생성 과정

① 서명자는 난수값 K를 {1, …, Q-1}에서 랜덤하게 선택한다.

② $W = G^K \pmod P$를 계산한다.

③ 서명의 첫 부분 R = h(W)을 계산한다.

④ 메시지의 해쉬코드 H = h(Z‖M)을 계산한다 (단, Z는 정해진 형식(예를 들면 X.509)에 따라 발부된 서명자 인증 데이터).

⑤ 중간값 $E = R \oplus H \pmod Q$를 계산한다.

⑥ 서명의 두 번째 부분 $S = X(K-E) \pmod Q$를 계산한다.

⑦ 서명 Σ = {R‖S}를 만들어 서명된 메시지 {M‖

Σ}를 출력한다.

단계 1 ~ 단계 2 까지의 과정은 서명할 메시지와 관계가 없으므로 사전에 계산해 둘 수도 있다. 즉 K와 R을 미리 계산해서 보관하고 있다가 서명할 메시지가 들어오면 단계 4부터 실시간 계산을 할 수 있다.

서명 검증 과정

① 서명된 메시지 {M′‖Σ′}로 부터 검증할 메시지 M′, 서명의 첫 부분 R′, 서명의 두 번째 부분 S′를 추출한다. 이 때 0 < R′ < 2^{Q} 이고 0 < S′ < Q임을 확인한다.
② 검증할 메시지의 해쉬코드 값 H′ = h(Z‖M′)을 계산한다.
③ 중간값 E′ = R′+H′ (mod Q)을 계산한다.
④ 서명자의 공개 검증키 Y를 이용하여 W′ = $Y^{S'}G^{E'}$ (mod P)를 계산한다.
⑤ h(W′) = R′이 성립하는지 확인한다.

3.2 미국의 DSS

우선 소수 P, Q의 길이를 살펴보자. Q의 길이는 곧 서명에 사용되는 해쉬함수의 출력길이를 의미한다. 소수 P의 길이는 DSS에서는 512비트부터 1024비트까지 64비트 단위로 증가시킬 수 있게 되어 있고, Q의 길이는 160 또는 256 비트로 고정되어 있다.

사용자 초기화

① 서명자는 자신의 비공개 서명키 X $\in_r Z_Q$를 선택하여 비밀리에 간직한다.
② 서명자는 비공개 서명키 X에 대응하는 공개 검증키 Y를 Y = G^{X} (mod P)와 같이 계산한다.

서명 생성 과정

① 서명자는 난수값 K$\in_r Z_Q^*$를 랜덤하게 선택한다.
② 서명의 첫 부분 R = (G^{K} (mod P)) (mod Q)를 계산한다.
③ 메시지의 해쉬코드 H = h(M)을 계산한다.
④ 서명의 두 번째 부분 S = K^{-1}(RX+H) (mod Q)를 계산한다.
⑤ 서명 Σ = {R‖S}를 만들어 서명된 메시지 {M‖Σ}를 출력한다.

서명 검증 과정

① 서명된 메시지 {M′‖Σ′}로 부터 검증할 메시지 M′, 서명의 첫 부분 R′, 서명의 두 번째 부분 S′를 추출한다.
② 검증할 메시지의 해쉬코드 값 H′ = h(M′)을 계산한다.
③ 서명자의 공개 검증키 Y를 이용하여 W′ = $Y^{S'\cdot R'}G^{S'\cdot H'}$ (mod P)를 계산한다.
④ W′ (mod Q) = R′이 성립하는지 확인한다.

3.3 러시아의 GOST

소수 P의 길이는 GOST에서는 512 혹은 1024비트 두 개로 고정되어 있고, Q의 길이는 160 또는 256 비트로 고정되어 있다.

사용자 초기화

① 서명자는 자신의 비공개 서명키 X $\in_r Z_Q$를 선택하여 비밀리에 간직한다.
② 서명자는 비공개 서명키 X에 대응하는 공개 검증키 Y를 Y = G^{X} (mod P)와 같이 계산한다.

서명 생성 과정

① 서명자는 난수값 K$\in_r Z_Q$를 랜덤하게 선택한다.
② 서명의 첫 부분 R = (G^{K} (mod P)) (mod Q)를 계산한다.
③ 메시지의 해쉬코드 H = h(M)을 계산한다.
④ 서명의 두 번째 부분 S = RX + KH (mod Q)를 계산한다.
⑤ 서명 Σ = {R‖S}를 만들어 서명된 메시지 {M‖Σ}를 출력한다.

서명 검증 과정

① 서명된 메시지 {M′‖Σ′}로 부터 검증할 메시지 M′, 서명의 첫 부분 R′, 서명의 두 번째 부분 S′를 추출한다.
② 검증할 메시지의 해쉬코드 값 H′ = h(M′)을 계산한다.

〈표 1〉 대표적인 디지틀 서명 표준(안)들의 비교
〈Table 1〉 Comparison of digital signature standards

서명 방식	서명 생성	서명 검증
서명키 : $X \in Z_Q$ 검증키 : $Y = G^X \pmod P$		
DSS (미국)	$K \in_r Z_Q$, $H = h(M)$ $R = (G^K \pmod P) \pmod Q$ $S = K^{-1}(RX+H) \pmod Q$	$(Y^{S^{-1}R} G^{S^{-1}H} \pmod P) \pmod Q \doteq R$
GOST (러시아)	$K \in_r Z_Q$, $H = h(M)$ $R = (G^K \pmod P) \pmod Q$ $S = RX + KH \pmod Q$	$(Y^{-RH^{-1}} G^{SH^{-1}} \pmod P) \pmod Q \doteq R$
서명키 : $X \in Z_Q^*$ 검증키 : $Y = G^{X^{-1}} \pmod P$		
KCDSA (한국)	$K \in_r Z_Q$, $H = h(Z \| M)$ $R = h(G^K \pmod P)$ $S = X(K-R \oplus H) \pmod Q$	$h(Y^S G^{R \cdot H} \pmod P) \doteq R$

③ 서명자의 공개 검증키 Y를 이용하여 $W' = Y^{-R'H'^{-1}} G^{S'H'^{-1}} \pmod P$를 계산한다.

④ $W' \pmod Q = R'$이 성립하는지 확인한다.

4. 디지틀 서명 표준(안)에 기반을 둔 통합 서명 시스템

이 장에서는 2장의 여섯 가지 undeniable형 특수 디지틀 서명방식들과 3장의 일반적인 디지틀 서명방식 표준(안)을 하나로 통합할 수 있는 서명방식을 제안한다. 스마트 카드의 한정된 메모리 용량을 고려할 때 이는 매우 바람직할 것이다.

통합된 서명방식에서는 서명자가 서명을 생성할 때 특정한 사람의 공개키를 결부시킴으로써 그 공개키에 대응하는 비밀키(제안된 방법에서는 이산대수(discrete logarithm))의 소유자만이 서명을 인증할 수 있도록 하고 또한 필요가 있을 때에는 제3자에게 그 정당성을 증명할 수 있도록 한다.

즉, 통합 서명방식에서 사용되는 공개키의 종류에 따라 기본원 G를 사용하는 일반적인 디지틀 서명방식, 서명자의 공개키를 사용하는 undeniable signatures와 convertible undeniable signatures, 수신자의 공개키를 사용하는 nominative signatures, 서명자와 재판관의 공유키를 이산대수로 사용하는 entrusted undeniable signatures, 서명자와 제3자의 공유키를 이산대수로 사용하는 designated confirmer signatures, 서명자와 수신자의 공유키를 이산대수로 사용하는 directed signatures 등을 구성할 수 있음을 보인다.

4.1 KCDSA에 기반을 둔 통합 서명 시스템

시스템/사용자 초기화

3.1절의 KCDSA와 같다.

서명 생성 과정

Alice가 Bob에게 메시지 M에 대한 서명을 생성하여 보낸다고 가정한다. 또한 Carol은 제3자이며 재판관은 모든 서명자에게 공개 검증키 Y_{Judge}를 공개한다.

① 서명자는 Alice는 두 개의 난수값 $K_1 = f(K, M) \in_r Z_Q$, $K_2 \in_r Z_Q$를 선택한다.

② $W_1 = G^{K_1 - K_2} \pmod P$, $W_2 = A^{K_1} \pmod P$를 계산한다. 여기에서 Alice는 다음 표 2의 일곱 가지 유형중 하나를 A로 선정한다 (단, f(K, M)는 K를 비밀키로 하는 압축 알고리즘).

③ 서명의 첫 부분 $R = h(W_1 \| W_2)$을 계산한다.

④ 메시지의 해쉬코드 $H = h(Z \| M)$을 계산한다.

⑤ 중간값 $E = R \oplus H \pmod Q$를 계산한다.

⑥ 서명의 두 번째 부분 $S = X_{Alice}(K_2 - E) \pmod Q$를 계산한다.

⑦ 서명 $\Sigma = \{R \| S \| W_1\}$를 만들어 서명된 메시지 $\{M \| \Sigma\}$를 출력한다.

〈표 2〉 A값의 일곱 가지 유형
〈Table 2〉 7 types of A

유형 (type)	A 값
보통의 디지틀 서명	G
undeniable signatures	Y_{Alice}
convertible undeniable signatures	Y_{Alice}
entrusted undeniable signatures	$Y_{Alice}^{Y_{Judge}^{X_{Alice}}}$
designated confirmer signatures	$G^{Y_{Carol}^{X_{Alice}}}$
directed signatures	$G^{Y_{Bob}^{X_{Alice}}}$
nominative signatures	Y_{Bob}

서명의 검증

서명문의 진위를 확인하기 위하여 $E = R \oplus h(Z \| M)$를 구한 후, $R \stackrel{?}{=} h(W_1 \| (Y_{Alice}^{S} G^{E} W_1)^{\log_G A} \pmod P)$을 만족하는지를 검사한다. 즉, 이산대수 $\log_G A$를 알고 있는 사용자는 서명의 정당성을 검증할 수 있다.

확인 프로토콜 (서명의 정당성을 증명)

① 증명자(prover)는 $W_2 = (Y_{Alice}^{S} G^{E} W_1)^{\log_G A} \pmod P$를 계산하여, 확인자(verifier)에게 전송한다.

② 확인자는 $E = h(W_1 \| W_2) \oplus h(Z \| M)$를 계산한다.

③ 증명자는,

$$\log_{Y_{Alice}^{S} G^{E} W_1} W_2 = \log_G A \pmod P$$

를 만족하는 이산대수를 알고 있는지의 여부를 영지식 증명(zero-knowledge) 방법 - 예를 들면 Boyar, Chaum, Damgard 등의 BCD 알고리즘 [7] - 으로 증명한다.

BCD 알고리즘

① 확인자는 두 난수 $a, b \in Z_Q$를 선택하여,

$$ch = (Y_{Alice}^{S} G^{E} W_1)^{a} G^{b} \pmod P$$

를 증명자에게 전송한다.

② 증명자는 난수 $t \in Z_Q$를 선택하여,

$h_1 = ch \cdot G^{t} \pmod P$, $h_2 = h_1^{\log_G A} \pmod P$를 계산, 확인자에게 전송한다.

③ 확인자는 단계 ①의 난수 a, b를 증명자에게 전송한다.

④ 증명자는 확인자로부터 받은 a, b를 이용하여 단계 ①에서 확인자가 적법한 challenge값을 전송했는지를 확인한다. 만일 적법한 값이면 자신의 난수 t를 확인자에게 전송하고 그렇지 않다면 프로토콜을 종료한다.

⑤ 확인자는 증명자로부터 받은 t를 이용하여 $h_1 \stackrel{?}{=} (Y_{Alice}^{S} G^{E} W_1)^{a} G^{b+t} \pmod P$, $h_2 \stackrel{?}{=} W_2{}^{a} A^{b+t} \pmod P$가 성립하는지를 조사한다.

단계 ①~⑤가 정상적으로 수행되면 확인자는 증명자가 $\log_{Y_{Alice}^{S} G^{E} W_1} W_2 = \log_G A \pmod P$를 만족하는 이산대수를 알고 있다는 사실을 확인할 수 있게 된다. 또한 주어진 알고리즘은 영지식 증명 시스템임을 쉽게 증명할 수 있다[7].

방정식 A = G를 사용할 경우, 통신망에 가입한 사람은 누구든지 Alice의 공개키 Y_{Alice}를 이용하여 $R \stackrel{?}{=} h(W_1 \| (Y_{Alice}^{S} G^{E} W_1) \pmod P)$을 만족하는지 검사함으로써 메시지 M에 대한 서명 $\{R \| S \| W_1\}$을 확인할 수 있다 **(보통의 디지틀 서명방식)**. 서명자 Alice의 공개키 Y_{Alice}를 A값으로 선택하는 경우, 대응되는 비밀키 X_{Alice}를 알고 있는 서명자만이 서명의 진위여부를 판별할 수 있으므로 서명자는 서명의 사본들이 남용되는 것을 막을 수 있다 **(undeniable signatures)**. 더욱이 K_1을 K를 비밀키로 하는 해쉬 알고리즘 f(K, M)로 택한 경우에는, K_1을 공개함으로써 이에 대응하는 하나의 메시지 M에 대한 서명만을 보통의 디지틀 서명으로 바꿀 수 있으며, 해쉬 알고리즘 f의 비밀키 K 자체를 공개한다면 임의의 메시지에 대한 서명에 대해서도 누구나 $K_1 = f(K, M)$, $G^{K_1} \stackrel{?}{=} Y_{Alice}^{S} G^{E} W_1 \pmod P$을 계산할 수 있으므로, 이때까지 발행된 모든 undeniable signatures를 보통의 디지틀 서명으로 변환시킬 수 있다 **((selectively) convertible undeniable signatures)**.

한편, $A = Y_{Alice}^{Y_{Judge}^{X_{Alice}}}$를 사용할 경우, $Y_{Judge}^{X_{Alice}}$를 모르는 검증자는 부인 프로토콜을 수행하지 못하나, Diffie-Hellman 공통키, $Y_{Judge}^{X_{Alice}} = Y_{Alice}^{X_{Judge}} \pmod P$

를 알고 있는 제3의 재판관은 다음의 부인 프로토콜을 수행할 수 있게 된다. 이 경우에 확인 프로토콜은 공개키 Y_{Alice}를 A로 랜덤화하기 위하여 공통키, $Y_{Judge}^{X_{Alice}}$를 사용하였다는 사실을 일반적인 영지식 대화형 증명방식을 이용하여 검증자에게 증명한 후 수행하게 한다 **(entrusted undeniable signatures)**.

부인 프로토콜

여기서 안전 파라미터인 k는 공통의 상수로 공개하거나 두 통신 당사자들 사이에 미리 협의되어야 한다. 이때, 증명자가 속일 가능성이 1/k 이므로 이 가능성을 원하는 레벨 이하로 낮추기 위해서는 부인 프로토콜을 필요한 수만큼 반복 시행해야 할 것이다.

① 재판관은 임의의 난수 $b \in Z_Q$와 검증수 $a \in \{0, \cdots, k-1\}$를 선택해서 $ch_1 = (Y_{Alice}{}^{S}G^{E}W_1)^{a}G^{b} \pmod P$와 $ch_2 = W_2^{a/Y_{Alice}^{X_{Alice}}}Y_{Prover}^{b} \pmod P$를 계산하여 (ch_1, ch_2)를 증명자에게 전송한다.

② 증명자는 $ch_1^{X_{Prover}}/\ ch_2$를 계산하여 그 값이 1 이면 본인의 서명이며, 1이 아니면 문헌 [19]의 trial & error 계산을 통하여 a값을 결정한 후, 난수 r을 선택하여 r을 비밀키로 하는 blob(r, a)를 재판관에게 전송한다.

③ 재판관은 자신이 선택한 난수 b를 증명자에게 전송한다.

④ 증명자는 이 b가 $ch_1 = (Y_{Alice}{}^{S}G^{E}W_1)^{a}G^{b}$, $ch_2 = W_2^{a/Y_{Alice}^{X_{Alice}}}Y_{Prover}^{b}$를 만족하는지 조사하여 이를 만족하면 단계 ②에서 사용한 난수 r을 전송한다. 이를 만족하지 않는다는 것은 재판관이 프로토콜을 따르지 않는다는 사실을 의미하므로 프로토콜을 중단한다.

⑤ 재판관은 증명자가 계산한 a값과 자신이 선택한 검증수 a를 비교하여 서명의 정당성을 확인한다.

또한, $A = G^{Y_{Card}^{X_{Card}}}$ 또는 $A = G^{Y_{Bob}^{X_{Bob}}}$를 사용하므로써, Diffie-Hellman 공통키를 알고 있는 서명자와 지명된 제3자(또는 수신자)는 주어진 서명의 진위를 확인할 수 있으며, 필요시에 제3자에게 서명의 정당성을 보일 수 있다 **(designated confirmer signatures (또는 directed signatures))**. 마지막으로, 지정된 수신자 Bob의 공개키 Y_{Bob}을 A값으로 선택하는 경우, Y_{Bob}에 맞는 비밀키 X_{Bob}을 가지고 있는 Bob만이 서명을 확인할 수 있고, 서명이 문제가 되는 경우에 제3자에게 그 서명이 Alice에 의해 자신에게 발행된 정당한 서명임을 증명할 수 있다 **(nominative signatures)**.

4.2 DSS에 기반을 둔 통합 서명 시스템

시스템/사용자 초기화

3.2절의 DSS와 같다.

서명 생성 과정

① 서명자는 Alice는 두 개의 난수값 두 개의 난수값 $K_1 = f(K, M) \in_r Z_Q$, $K_2 \in_r Z_Q^*$를 선택한다.

② $W_1 = G^{K_1 - K_2} \pmod P$, $W_2 = A^{K_1} \pmod P$를 계산한다. 여기에서 Alice는 표 2의 일곱 가지 유형중 하나를 A로 선정한다.

③ 서명의 첫 부분 $R = W_2 \pmod Q$을 계산한다.

④ 메시지의 해쉬코드 $H = h(W_1 \| M)$을 계산한다.

④ 서명의 두 번째 부분 $S = K_2^{-1}(RX_{Alice} + H) \pmod Q$를 계산한다.

⑤ 서명 $\Sigma = \{R \| S \| W_1\}$를 만들어 서명된 메시지 $\{M \| \Sigma\}$를 출력한다.

서명 검증 과정

① $H = h(W_1 \| M)$를 구한다.

② 이산대수 $\log_G A$를 알고 있는 사용자는 $R \stackrel{?}{=} ((Y^{S^{-1}R}G^{S^{-1}H}W_1)^{\log_G A} \pmod P) \pmod Q$을 만족하는지를 검사함으로써, 서명의 정당성을 검사할 수 있다.

확인 프로토콜 (서명의 정당성을 증명)

① 증명자는 $W_2 = (Y^{S^{-1}R}G^{S^{-1}H}W_1)^{\log_G A} \pmod P$를 계산하여, 확인자에게 전송한다.

② 확인자는 $R = W_2 \pmod Q$, $H = h(W_1 \| M)$를 계산한다.

③ 증명자는,

$$\log_{Y^{S^{-1}R}G^{S^{-1}H}W_1} W_2 = \log_G A \pmod P$$

를 만족하는 이산대수를 알고 있는지의 여부를 4.1절의 BCD 알고리즘으로 증명한다.

4.3 GOST에 기반을 둔 통합 서명 시스템

시스템/사용자 초기화

3.3절의 GOST와 같다.

서명 생성 과정

① 서명자는 Alice는 두 개의 난수값 두 개의 난수값 $K_1 = f(K, M) \in_r Z_Q$, $K_2 \in_1 Z_Q$를 선택한다.

② $W_1 = G^{K_1 - K_2} \pmod P$, $W_2 = A^{K_1} \pmod P$를 계산한다. 여기에서 Alice는 표 2의 일곱 가지 유형중 하나를 A로 선정한다.

③ 서명의 첫 부분 $R = W_2 \pmod Q$을 계산한다.

④ 메시지의 해쉬코드 $H = h(W_1 \| M)$을 계산한다.

④ 서명의 두 번째 부분 $S = RX_{Alice} + KH \pmod Q$를 계산한다.

⑤ 서명 $\Sigma = (R \| S \| W_1)$를 만들어 서명된 메시지 $(M \| \Sigma)$를 출력한다.

서명 검증 과정

① $H = h(W_1 \| M)$를 구한다.

② 이산대수 $\log_G A$를 알고 있는 사용자는 $R = ((Y^{-RH} G^{SH} W_1)^{\log_G A} \pmod P) \pmod Q$을 만족하는지를 검사함으로써, 서명의 정당성을 검사할 수 있다.

확인 프로토콜 (서명의 정당성을 증명)

① 증명자는 $W_2 = (Y^{-RH} G^{SH} W_1)^{\log_G A} \pmod P$를 계산하여, 확인자에게 전송한다.

② 확인자는 $R = W_2 \pmod Q$, $H = h(W_1 \| M)$를 계산한다.

③ 증명자는,

$$\log_{Y^{-RH} G^{SH} W_1} W_2 = \log_G A \pmod P$$

를 만족하는 이산대수를 알고 있는지의 여부를 4.1절의 BCD 알고리즘으로 증명한다.

5. 결 론

본 논문에서는 여섯 가지의 undeniable형 디지틀 서명방식들 - 즉, undeniable signatures, convertible undeniable signatures, entrusted undeniable signatures, designated confirmer signatures, directed signatures, nominative signatures - 과 각국의 디지틀 서명방식 표준(안)들을 하나의 서명방식으로 통합한 서명방식을 제안하였다. undeniable형 특수 서명방식들은 사용자가 서명의 남용을 통제할 수 있으므로 개인적으로 민감한 응용들에 매우 유용하다. 특히 제안된 통합 서명 방식은 이러한 여러 가지 특수 서명방식들을 하나로 구현할 수 있으므로, 시스템의 메모리 비용을 고려할 때 매우 유리할 것이며, 또한 P.Horster의 "Meta-ElGamal 서명방식" 개념을 이용하여 "Meta-Undeniable형 서명방식"으로도 확장될 수 있을 것이다.

참 고 문 헌

[1] W.Diffie and M.E.Hellman, "New directions in cryptography," IEEE Transaction on Information Theory, Vol. IT-22 No.6, 1976, pp.644-654.

[2] R.Rivest, A.Shamir and L.Adleman, "A meth-od for obtaining digital signature and publi c-key cryptosystems," Communications of the ACM, Vol.21 No.2, 1978, pp.120-126.

[3] T.ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," IEEE Trans. Inform. Theory, IT-31, 1985, pp.469-472.

[4] C.P.Schnorr, "Efficient signature gene-ration for smart cards," Journal of Cryp-tology, Vol.4 No.3, 1991, pp.161-174.

[5] 임채훈, 이필중, 강신각, 박성준, "확인서 이용 부가형 디지털 서명 방식 표준(안)," 한국통신정보보호학회 종합학술발표회 논문집 Vol.7/No.1, pp.251-264.

[6] NIST, "Digital signature standard," FIPS PUB 186, 1994.

[7] M.Michels, D.Naccache, and H.Petersen,

"GOST 34.10 - A brief overview of Russia's DSA." Computers and Security, 15(8), 1996, pp.725-732.

[8] P.Horster, M.Michels and H.Petersen, "Meta-ElGamal signature schemes," Proc. 2nd ACM conference on Computer and Communications security, 1994, pp.96-107.

[9] D.Chaum and H.Antwerpen, "Undeniable si-gnature," Advances in Cryptology - Crypto '89, Springer-Verlag, 1990, pp.212 -216.

[10] D.Chaum, "Zero-knowledge undeniable sign-atures," Advances in Cryptology - Eurocrypt'90, Springer-Verlag, 1991, pp.458-464.

[11] J.Boyar, D.Chaum and I.Damgard, "Convertible undeniable signature," Advances in Cryptology - Crypto'90, Springer-Verlag, 1991, pp.189-205.

[12] T.Okamoto and K.Ohta, "How to utilize the randomness of zero-knowledge proofs," Adv-ances in Cryptology - Crypto'90, Springer-Verlag, 1991, pp.437-456.

[13] 박성준, 이보영, 원동호, "의뢰 부인방지 서명에 관한 연구," 한국통신학회 논문지 제20권 제6호, 1995, pp.1649-1656.

[14] S.J.Park, K.H.Lee and D.H.Won, "An entrusted undeniable signature," Proc. of JW-ISC'95, 1995.

[15] D.Chaum, "Designated confirmer signatures," Advances in Cryptology - Eurocrypt'94, Springer-Verlag, 1995, pp.86-91.

[16] T.Okamoto, "Designated confirmer signatures and public-key encryption are equivalent," Advances in Cryptology - Crypto '94, Springer-Verlag, 1995, pp.61-74.

[17] C.H.Lim and P.J.Lee, "Modified Maurer-Yacobi's scheme and its applications," Adv-ances in Cryptology - Auscrypt'92, Springer-Verlag, 1993, pp.308-323.

[18] 임채훈, 이필중, "상호 신분 인증 및 디지탈 서명 기법에 관한 연구," 통신정보보호학회 논문지 제2권 제1호, 1992, pp.16-35.

[19] C.H.Lim and P.J.Lee, "Directed signatures and application to threshold cryptosystems," Proc. of 1996 Cambridge Workshop on Security Protocols, 1996.

[20] 김승주, 박성준, 원동호, "수신자 지정 서명방식에 대한 고찰," 한국정보처리응용학회 학술발표회 논문집 제1권 제2호, 1994, pp.530-533.

[21] S.J.Kim, S.J.Park and D.H.Won, "Nominative signatures," Proc. of ICEIC'95, International Conference on Electronics, Informations and Communications, 1995, pp.II-68-II-71.

[22] 김승주, 김경신, 박성준, 원동호, "영지식 수신자 지정 서명방식," 통신정보보호학회 논문지 제6권 제1호, 1996, pp.15-24.

[23] S.J.Kim, S.J.Park and D.H.Won, "Zero-knowledge nominative signatures," Proc. of Pragocrypt'96 International Conference on the Theory and Applications of Cryptology, 1996, pp.380-392.

[24] G. Brassard, D. Chaum and C. Crepeau, "Minimum disclosure proofs of knowledge," Journal of Computer and System Science, Vol. 37 No. 2, pp. 156-189, 1988.

[25] 강신각, 문상재, 박성준, 백재현, 신종태, 원동호, 이경석, 이필중, 임채훈, 장청룡, "부가형 디지틀 서명 표준안에 관한 연구," 한국통신학회 하계종합학술발표회 논문집 (上), 1996, pp.757-760.

[26] 한국통신정보보호학회, "정보보호 표준방식 개발," 한국전자통신연구소 최종연구보고서, 1996.

[27] 김승주, 박성준, 원동호, "수신자 지정 서명방식과 부인 방지 서명방식의 통합 시스템," 한국통신학회 논문지 제21권 제5호, 1996, pp.1266-1273.

[28] 김승주, 이보영, 원동호, "지능형 전자 증명 카드에 적합한 통합 서명 시스템에 관한 연구," 한국통신학회논문지 제22권/제4호, 1997, pp.870 -879.

김 승 주

1994년 성균관대학교 정보공학과 졸업(공학사)
1996년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1996년 3월~현재 성균관대학교 대학원 정보공학과 박사과정

김 경 신

1983년 성균관대학교 전자공학과 졸업(공학사)
1995년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1997년 성균관대학교 대학원 정보공학과졸업(공학박사)
1984년 12월~1991년 2월 삼성전자(주) 컴퓨터부문 선임연구원
1991년 3월~1995년 2월 연암공업전문대학 전산과 부교수
1995년 3월~현재 인덕전문대학 방송통신과 부교수
1998년 3월~현재 인덕전문대학 학술정보처장

원 동 호

1976년 성균관대학교 전자공학과 졸업(공학사)
1978년 성균관대학교 대학원 전자공학과졸업(공학석사)
1988년 성균관대학교 대학원 전자공학과졸업(공학박사)
1978년 4월~1980년 3월 한국전자통신연구소 연구원
1985년 9월~1986년 8월 일본 동경공대 객원연구원
1982년 3월~현재 성균관대학교 공과대학 정보공학과 교수
1995년 3월~1997년 2월 성균관대학교 교학처장
1996년 4월~현재 정보화추진위원회 자문위원
주관심분야 : 암호이론, 정보이론