通信情報保護學會誌
第3卷 第3號, 1993. 9

Self-Certified 공개키 방식에 관한 고찰

A Study on Self-Certified Public Key Schemes

권창영* · 원동호**

요 약

다른 가입자가 특정 가입자의 공개키를 인증하기 위한 분리된 certificate가 필요하지 않은 공개키 개념인 self-certified 공개키의 개념을 소개한다. Self-certified 공개키 개념은 공개키 방식(public key schemes)에서 저장공간과 계산량을 감소시킬 수 있으며, 비밀키는 가입자 자신이 직접 선택할 수 있으며, 센터에게는 비밀로 할 수 있다. 센터와 가입자가 공개키를 계산하는 전략은 공개키 자체에 certificate를 삽입하여 certificate를 별도로 취하지 않는 것이다.

1. 서 론

1976년 Diffie-Hellman 공개키 방식[1]이 발표된 이래로 많은 공개키 방식이 제안되었는데, 대부분 방식은 해당 가입자만이 아는 가입자의 비밀키 s와 누구든지 아는 공개키 P를 가지고 구성되어진다.

비밀키 s와 공개키 P는 수학적으로 강한 연관성을 가지나 P에서 s를 계산하는 것은 불가능하다. 공개키 P는 비밀성(confidentiality)을 유지하기 위해 보호될 필요는 없다. 그러므로 공개키는 가능한한 공개적으로 만들어져야 한다는 것이다. 그러나 공개키 방식은 이러한 공개성(publicity) 때문에 공개키 디렉토리의 합법적인 공개키(true public key)를 비합법적인 공개키(false public key)로 대치하는 등의 능동적인 공격(active attack)에 부분적으로 공격당할 수 있다.

그러므로, (s, P)에 가입자를 식별하기 위한 가입자의 identification string(또는, identity) I가 추가되어야 하며, P가 가입자 I의 공개키 임을 보증하기 위한 가입자의 공개키 확인자(guarantee, certificate) G가 추가되어야 한다.

공개키 확인자 G의 형태에 따라서 공개키 방식은 분류되며 그들의 공통점은 모든 가입자가 신뢰할 수 있는 센터가 존재해야 한다는 것이다.

"가입자가 센터를 신뢰한다는 것은 과연 무엇을 의미하는가?" 비밀키 방식(secret-key schemes)에서 센터(또는 authority)는 가입자가 설정한 모든 비밀키를 알 수 있으며, 모든 가입자는 센터에게 비밀키를 확인 받아야만 한다. 공개키 방식에서는 비밀키 방식에서의 강력한 조건을 완화시킬 수 있다. 그러므로 센터의 신뢰의 정도를 몇 단계로 나누어서 고려하여 보자.

* 정회원, 대유공업전문대학 사무자동화과 전임강사
** 종신회원, 성균관대학교 정보공학과 교수

신뢰수준 1 : 센터는 가입자의 비밀키를 알거나, 쉽게 계산할 수 있어서 언제라도 임의의 가입자 흉내를 낼 수 있는 수준.

신뢰수준 2 : 센터는 가입자의 비밀키를 알지 못하거나, 쉽게 계산할 수 없다. 그러나, 센터는 비합법적인 공개키 확인자를 만들어서 합법적인 가입자 흉내를 낼 수 있는 수준.

신뢰수준 3 : 센터는 가입자의 비밀키를 알지 못하거나, 쉽게 계산할 수 없으며 센터가 비합법적인 공개키 확인자를 생성하여 합법적인 가입자 흉내를 내려는 센터의 위법행위를 발견할 수 있는 수준.

다음 절에서 확인자 G의 형태에 따른 공개키 방식을 분류하고, 그들의 공통점인 모든 가입자가 신뢰할 수 있는 센터의 신뢰수준을 고려하여 보자.

2. 공개키 방식

전형적인 공개키 방식에서 공개키 디렉토리를 제거하는 데에는 2가지 방법이 있다. 그 중 하나는 certification-based 방식으로 변형하는 것이고, 또 하나는 identity-based 방식으로 변형하는 것이다.

certification-based 방식은 신뢰 센터(trusted center 또는 key authentication center)가 자신의 공개키를 공개하고, 가입자의 identity I와 공개키 P에 대한 서명(signature)를 가입자에게 분배하는 것이다.

Shamir가 최초로 제안한 identity-based 방식은 가입자의 공개키를 가입자의 identity와 관련된 어떤 값으로 대치하는 것이다[2), 3), 4)].

2.1. Certification-based 방식

공개키 확인자 G는 (I, P)에 대한 디지탈 서명 형태(certificate라고 부른다)이며 센터(또는 authority)에 의해서 계산되고 분배된다.

시스템은 (I, s, P, G)로 구성되며 (I, P, G)는 공개된다. 가입자 I를 확인(authenticate)하려면, 공개정보 (I, P, G) 및 모든 가입자가 알고 있는 센터의 공개키를 이용하여 G를 검증할 수 있다.

이 방식의 신뢰수준은 3이며 센터만이 certificate를 생성할 수 있으므로 동일 가입자에 대하여 2개 이상의 다른 certificate가 존재한다는 것은 센터가 cheat되었다는 증거이다. certificate의 검증시 사용하는 추가적인 파라메터를 저장하기 위한 메모리와 전송정보 및 계산량 때문에 certification-based 방식이 비록 신뢰수준 3을 보장하더라도 certification-based 방식이 아닌 다른 방법의 설계가 필요하다.

이 방식은 CCITT Recomendation X.509에서 채택하고 있는 방식이다[5)].

2.2. Identity-based 방식

1984년 Shamir가 소개한 identity-based 방식[2)]은 가입자의 identity I 자체가 공개키 P이며(P=I) 비밀키 s 자체가 공개키 확인자 G이다(G=s). 그러므로 시스템은 (I, s)로 구성된다. 이 방식은 저장하거나, 검증할 certificate가 별도로 없기 때문에 매우 흥미로운 방식이다.

그러나, 이 방식에는 문제점이 있다. 센터가 가입자의 비밀키를 생성하기 때문에 부분적으로 센터는 언제라도 임의의 가입자 흉내(impersonnate)를 낼 수 있다. 즉, identity-based 방식은 신뢰수준이 1이므로 특정 응용시 매우 불만족스럽다.

2.3. Certification-based 방식과 identity-based 방식의 비교

본 절에서는 certification-based 방식과 identity-based 방식의 차이점을 비교하여 보기로 하자.

임의의 공개키 방식은 앞에서 언급한 일반적인 방법으로 certification-based 방식으로 변형되는 데 반하여, 공개키 방식이 identity-based 방식으로 변형되려면 해당 공개키 방식에 적합한 독특한 방법이 필요하다.

certification-based 방식의 신뢰 센터는 각 가입자의 비밀키를 모르지만, identity-based 방식의 신뢰센터는 각 가입자의 비밀키를 직접 생성하므로 각 가입자의 비밀키를 알 수 밖에 없으며, certification-based 방식에서 가입자가 통신 상대방에게 전송하는 전송정보의 크기는 identity-based 방식과 비교하면 크다.

표 1. certification-based 방식과 identity-based 방식의 비교

	공개키 방식의 변형 방법	가입자의 비밀키 생성	전송 정보의 크기
certification-based 방식	일반적인 방법으로 항상 변형 가능	가 입 자	대
identity-based 방식	각 공개키 방식에 적합한 독특한 방법 필요	신뢰 센터	소

3. Self-certified 방식

Self-certified 방식은 certification-based 방식과 identity-based 방식의 중간 형태인 새로운 공개키 방식이다. 공개키 P 자체가 공개키 확인자 G이다 (G=P). 그러므로 시스템은 (I, s, P)로 구성된다. 이 방식은 별도의 certificate를 사용하지 않으므로 certification-based 방식이 아니며, 공개키가 가입자의 identity로 제한되지 않기 때문에 identity-based 방식이 아니다.

결론적으로 self-certified 방식은 가입자가 자신의 비밀키를 선택하고 센터에게는 비밀로 하며, 메모리와 계산량을 감소시킨다.

표 2. 공개키 방식의 비교

	DH	CB	ID	SC
시스템 구성	(s, P)	(I, s, P, G)	(I, s) P=I, G=s	(I, s, P) P=G
공개키(생성)	P 가입자	I, P, G 가입자, 센터	I	I, P 센 터
비밀키(생성)	s 가입자	s 가입자	s 신뢰 센터	s 가입자
G		(I, P)의 디지탈 서명 (센터가 계산)	신뢰 센터	센 터
신뢰수준		3	1	3

단, s : 가입자의 비밀키
P : 가입자의 공개키
I : 가입자의 identification string(또는, identity)
G : 가입자의 공개키 확인자(guarantee, certificate)

4. Self-certified 공개키 방식의 예

RSA 디지탈 서명 방식을 이용하여 제안된 여러 가지 방식[6), 7), 8), 9)]들의 신뢰수준은 2이다. 신뢰수준이 2인 이유는 각 가입자가 센터로부터 합법적인 공개를 지급받은 후에도 다른 공개키를 만들 수 있는 가능성이 있기 때문이다. 즉, 판정관이 센터가 불법행위를 하는지 가입자가 불법행위를 하는지 구별할 수 없기 때문이다.

4.1. Girault의 identity-based 개인식별 프로토콜

두 소수 p=2fp'+1, q=2fq'+1의 곱인 n을 법으로 하는 개인식별 방식으로 변형하자. 단, f, p', q'는 각기 다른 소수이며, f는 200 bits, p'와 q'는 300 bits인 각기 다른 소수이며, 결국 n은 1000 bits의 합성수이다.

e는 p-1과 q-1와 서로소인 공개정보이며 e의 길이는 20 bits에서 70 bits이다. d는 mod lcm(p-1, q-1) 상에서의 e의 승산역원이다.

$$e \cdot d = 1 \pmod{\mathrm{lcm}(p-1,\ q-1)}$$

Z_p 및 Z_q상에서 위수가 f인 원소 α를 정한다. 즉,

mod n 상에서 α의 위수는 f이다. n, f, α, e는 센터의 공개정보이며, p, q, d는 비밀정보이다.

각 가입자는 자신의 비밀키 s_i를 선택하여, α^{-s_i} (mod n)를 계산하여 센터에게 제출하면, 센터는 가입자의 공개키 $P_i=ID^{-d}\cdot\alpha^{-s_i}$ (mod n)을 계산하고 certificate를 생성한다. 각 가입자의 공개키는 가입자의 identity 및 비밀키에 의존적이다. 또한, ID와 P의 관계는 다음과 같다.

$P^e\cdot ID\cdot h^s=1(\text{mod } n)$ 단, $h=\alpha^e$ (mod n)

프로토콜 1 : Girault의 identity-based 개인식별 프로토콜

순서 1-1. 가입자 A는 난수 $r\in_R \{1, 2, \cdots, f-1\}$를 선택한다.

1-2. 가입자 A는 $x=h^r$ (mod n)을 계산한다.

1-3. 가입자 A는 ID_A, P_A, Certificate, x를 가입자 B에게 전송한다.

순서 2-1. 가입자 B는 Certificate를 검증하여 가입자 A의 identification을 확인한다.

2-2. 가입자 B는 난수 $c\in_R \{0, \cdots, e-1\}$를 선택한다.

2-3. 가입자 B는 난수 c를 가입자 A에게 전송한다.

순서 3-1. 가입자 A는 $y=r+S_A\cdot c$ (mod f)를 계산한다.

3-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 4-1. 가입자 B는 $x=h^y\cdot(P^e\cdot ID_A)^c$ (mod n)이 성립하는지 검증한다.

이 방식의 안전성을 생각하기 위하여 "가입자의 비밀키 s를 발견하여 정규 가입자인척 할 수 있는 어려움의 정도는 무엇인가?", "센터의 비밀 정보 d를 발견하여 신뢰 센터인척 할 수 있는 어려움의 정도는 무엇인가?"의 2가지 질문에 대하여 생각하여 보자.

Schnorr 방식[10]같은 non-identity-based 방식에서는 생각할 수 있는 질문이 아니다. 왜냐하면, 대답이 certificate를 생성하는 서명방식에만 의존하기 때문이다. 즉, 서명방식은 개인식별 방식과는 완전히 독립적이기 때문이다. identity-based 방식에서 2개의 질문은 하나가 된다. 왜냐하면, s는 d를 이용하여 ID로 부터 계산되고, d를 발견한다는 것은 s를 발견하는 유일한 방법으로 보이기 때문이다.

Girault의 identity-based 개인식별 프로토콜에서는 위의 2가지 질문이 분리된다. 왜냐하면, 앞에서도 언급했지만, d를 이용하여 s를 계산하는 것이 불가능하기 때문이다. n을 소인수 분해하면, 센터인척 하는 것은 충분하며, mod n 상에서 이산 대수를 계산하면, 가입자인 척 흉내내는 것은 가능하다.

4.2. Girault의 Self-Certified 방식

본 절에서는 신뢰수준이 3인 Girault의 Self-certified 방식[11]를 살펴보겠다.

센터는 시스템 설정을 위하여 RSA의 키(e, d)를 생성하고, 승산군 Z/nZ^*내에서 최대 위수를 갖는 g를 생성한다(단, n=p*q). 센터는 (n, e, g)를 공개하고 (p, q, d)를 비밀로 한다.

가입자 등록 과정에서 가입자는 자신의 비밀키 s (150 비트)를 선택하고, $v=g^{-s}$ (mod n)를 계산하여 v를 센터에게 제시하고, 영지식 대화형 증명 프로토콜을 이용하여 s를 알고 있다는 것을 센터에게 증명한다[12)~15)].

센터는 가입자의 공개키 $P=(g^{-s}-I)^d$ (mod n)을 계산하여 가입자에게 제공한다.

4.2.1. 개인식별 프로토콜

프로토콜 2 : 개인식별 프로토콜

순서 1-1. 가입자 A는 I, P를 가입자 B에게 전송한다.

1-2. 가입자 B는 $v=P^e+1$ (mod n)을 계산한다.

순서 2-1. 가입자 A는 난수 x를 선택한다 (220 비트).

2-2. 가입자 A는 $t=g^x$ (mod n)를 계산한다.

2-3. 가입자 A는 t를 가입자 B에게 전송한다.

순서 3-1. 가입자 B는 난수 c를 선택한다 (30비트).

3-2. 가입자 B는 난수 c를 가입자 A에게 전송한다.

순서 4-1. 가입자 A는 $y=x+s\cdot c$를 계산한다.

4-2. 가입자 A는 y를 가입자 B에게 전송한다.

순서 5-1. 가입자 B는 $t=g^{y}\cdot v^{c} \pmod n$이 성립하는지 검증한다.

위 프로토콜의 완전성은 거의 1이며 s를 알지 못하는 가입자는 $1-2^{-30}$의 확률로 detect된다. 또한, s에 대한 어떤 정보도 노출되지 않는다(minimum-knowledgeness).

위 프로토콜의 특징은 검증할 certificate가 없으며 공개키 자신이 certificate 역할을 한다(self-certified), 또한, 어떠한 가입자도 가입자 A의 공개키에서 가입자 A의 비밀키를 추론할 수 없으며, n의 소인수를 알고있는 센터라도 그 소인수들이 충분히 크면(350 비트), $g^{-s} \pmod n$에서 s를 계산할 수 없다[16].

물론 센터는 아직도 s를 s'로 변경하여 거짓 공개키 P'를 계산할 수 있다. 그러나, 센터만이 $P^{e}+I=g^{-s} \pmod n$을 만족하는 공개키를 생성할 수 있으므로 동일 가입자에 대하여 2개 이상의 다른 합당한 공개키가 존재한다는 것은 그것 자체가 센터가 부정하다는 것을 증명하는 것이다. 그러므로 위 프로토콜은 신뢰수준이 3이다.

4.2.2. 키 분배 프로토콜

프로토콜 3 : 키 분배 프로토콜

순서 1-1. 가입자 A는 I_A, P_A를 가입자 B에게 전송한다. (개인식별시 완료)

1-2. 가입자 B는 $v_A=P_A^{e}+I_A \pmod n$을 계산한다. (개인식별시 완료)

1-3. 가입자 B는 $K_{AB}=v_A^{S_A}=g^{S_AS_B}$를 계산한다.

순서 2-1. 가입자 B는 I_B, P_B를 가입자 B에게 전송한다. (개인식별시 완료)

2-2. 가입자 A는 $v_B=P_B^{e}+I_B \pmod n$을 계산한다. (개인식별시 완료)

2-3. 가입자 A는 $K_{AB}=v_B^{S_B}=g^{S_AS_B}$를 계산한다.

위 프로토콜은 Diffie-Hellman 방식과 밀접한 관계를 갖고 있으나, 가입자 A는 가입자 B와 K_{AB}를 공유했다는 것을 확신할 수 있다.

5. 결 론

1976년 Diffie-Hellman 공개키 방식이 발표된 이래로 많은 공개키 방식들이 제안되었는데, 본 고에서는 공개키 확인자 G의 형태에 따라 기존의 공개키 방식이 분류될 수 있음을 살펴보았으며, 다른 가입자가 특정 가입자의 공개키를 인증하기 위한 분리된 certificate가 필요하지 않은 공개키 개념인 self-certified 공개키의 개념을 소개하였다. 이 방식에서의 센터와 가입자가 공개키를 계산하는 전략은 공개키 자체에 certificate를 삽입하여 certificate를 별도로 취하지 않는다는 것이며, 이 방식은 공개키 방식에서 저장공간과 계산량을 감소시킬 수 있으며, 가입자의 비밀키를 가입자 자신이 직접 선택할 수 있어 센터에게는 비밀로 할 수 있다는 장점이 있다.

또한, 모든 가입자가 신뢰할 수 있는 센터가 존재해야 한다는 공통점에 착안하여 "가입자가 센터를 신뢰한다는 것은 과연 무엇을 의미하는가?"라는 의문에 초점을 맞추어 신뢰 센터의 신뢰 정도를 몇 단계로 나누어서 각 공개키 방식의 신뢰정도를 분석하였다. 신뢰 센터의 신뢰 정도는 향후 보다 면밀히 연구되어야 할 것으로 사료된다.

참 고 문 헌

1. W. Diffie, M. Hellman, "New directions in cryptography", IEEE Transactions on Information theory, Vol. IT-22, pp. 664-654, Nov. 1976.

2. Shamir, "Identity-Based Cryptosystems and Signature Schemes", Crypto'84, pp. 47-53, 1984.

3. Fiat, Shamir, "How to Prove Yourself : Practical Solutions of Identification and Signature Problems", Crypto'86, pp.186-194, 1986.

4. Guillou, Quisquater, "A Practical Zero-Knowledge Protocol Fitted to Security Microprocessor Minimizing Both Transmission and Memory", Eurocrypt'88, pp.233-243, 1988.

5. "The Directory-Authentication Framework", CCITT Recommendation X.509.

6. J.C.Pailles, M.Girault, "CRIPT : A public-key based solution for secure data communication", Proc. of SECURICOM'89, pp.171-185.

7. K.Tanaka, E.Okamoto, "Key distribution system using ID-related information directory suitable for mail systems", Proc. of SECURICOM'90, pp.115-122.

8. M.Girault, J.C.Pailles, "An identity-based identification scheme providing zero-knowledge authentication and authenticated key exchange", Proc. of ESORICS'90, pp.173-184.

9. M.Girault, "An identity-based identification scheme based on discrete logarithms modulo a composite number", EUROCRYPT'90, pp.481-486, 1991.

10. C.P.Schnorr, "Efficient identification and signatures for smart cards", Advancess in Cryptology, Proc. of CRYPTO'89, pp.239-252, 1991.

11. M.Girault, "Self-certified public keys", Advances in Cryptology EUROCRYPT'91, pp.490-497, 1991.

12. 권창영, 양형규, 원동호, "영지식 대화형 증명 방식 및 응용에 관한 연구", 한국통신정보보호학회 학회지, 제2권, 제2호, pp.31-39, 1992.6.

13. 이윤호, 양형규, 권창영, 원동호, "ID 기반의 영지식 대화형 프로토콜을 이용한 개인 식별 및 키 분배 프로토콜에 관한 연구", 한국통신정보보호학회 논문지, 제2권, 제1호, pp.3-15, 1992.6.

14. 원동호, 권창영, 양형규 외, "ZKIP의 round complexity와 응용 프로토콜에 관한 연구", 과학기술처/한국전자통신연구소 92 데이터 보호의 기반기술 연구과제 프로젝트, 최종보고서, 1992.11.

15. 권창영, 이인숙, 원동호, "영지식 대화형 증명 방식 및 응용 프로토콜", 대한전자공학회 학회지(정보기술 특집), 제20권, 제2호, pp.101-114, 1993.2.

16. P.Horster, H.J.Knobloch, "Discrete Logarithm Based Protocols", Advances in cryptology EUROCRYPT'91, pp.399-408, 1991.

□ 著者紹介

원 동 호(종신회원)

1949년생
1976년 성균관대학교 전자공학과 졸업(공학사)
1978년 성균관대학교 대학원 전자공학과 졸업(공학석사)
1988년 성균관대학교 대학원 전자공학과 졸업(공학박사)
1978년~1980년 한국전자통신연구소 연구원
1985년~1986년 일본 동경공대 객원연구원
1982년~현재 성균관대학교 정보공학과 조교수, 부교수, 교수

권 창 영(정회원)

1957년생
1983년 성균관대학교 수학교육과 졸업(이학사)
1991년 성균관대학교 대학원 정보공학과 졸업(공학석사)
1991년~현재 성균관대학교 대학원 정보공학과 박사과정 재학중
1982년~1988년 (주)KOLON 정보 SYSTEM실 팀장
1993년~현재 대유공업전문대학 사무자동화과 전임강사