이동 통신 환경에 적합한 개인식별정보 기반의 디지털 서명 알고리즘에 관한 연구

정영석*, 오수현*, 한종수*, 원동호*

*성균관대학교 정보통신공학부

A Study on ID-based digital signature algorithm for mobile communication environments

Young-Seok Chung*, Soohyun Oh*, Jong-Su Han*, Dongho Won*

*School of Information & communications Engineering, Sungkyunkwan Univ.

요 약

디지털 서명의 정당성을 검증하기 위해서는 서명자 공개키의 유효성을 인증해야 한다. 이 때, PKI 기반의 인증서를 통해 인증을 수행한다면, 무선 인터넷이라는 특성에 따른 보안상의 문제가 있을 뿐만 아니라 비효율적이다. 그런데 별도의 인증서 검증이 필요 없는 개인식별정보 자체를 공개키로 사용한다면 인증서 검증을 위한 무선 인터넷에서 유선 인터넷으로의 접속 없이 서명의 검증이 가능하게 되고, 무선망만을 이용한 통신이 가능하게 된다. 본 논문에서는 이와 같이 이동 통신 환경에 적합하도록 개인식별정보를 공개키로 사용하는 디지털 서명 알고리즘을 제안한다.

I. 서론

디지털 서명을 검증하는데 사용되는 서명자 공개키의 인증에는 PKI(Public Key Infrastructure)에서 사용되는 인증서를 사용하는 인증서 기반 방식과 서명자의 개인식별정보를 이용해서 인증을 수행하는 개인식별정보 기반 방식이 있다. 인증서 기반 방식으로 인증을 수행할 경우 인증서의 상태 검증을 위해 CRL(Certificate Revocation List)이나 OCSP(Online Certificate Status Protocol), SCVP(Simple Certificate Validation Protocol) 등을 사용한다. 반면, 1985년 A. Shamir에 의해 처음 제안된 ID-based 암호 시스템을 이용한 개인식별정보 기반 방식에서는 개인식별정보 자체가 공개키의 역할을 하기 때문에 별도의 인증서 검증을 필요로 하지 않는다.

한편, 대표적인 무선 인터넷 접속 기술인 WAP (Wireless Application Protocol) 기반의 무선 인터넷 환경에서는 WAP 게이트웨이를 통해 유선망과 무선망을 연결한다. 이러한 무선 인터넷 환경에서 인증서를 검증할 경우, 무선망에서 시작해서 WAP 게이트웨이를 거쳐 유선 인터넷에 접속하여 인증서 상태를 검증하게 된다. 즉, 인증서를 검증하기 위해서는 별도로 유선망에 접속해야 한다. 또한, WAP 게이트웨이에서는 WTLS (Wireless Transport Layer Security) 기반의 무선망과 SSL(Secure Sockets Layer)/TLS(Transport Layer Security) 기반의 유선망의 연동을 위해 무선망에서 암호화된 데이터를 복호화 한 후 유선망에 적합하도록 다시 암호화를 하는데(또는 반대의 과정), 이 때 원본 데이터가 누출되는 보안상의 취약점이 발생한다.

따라서 이동 통신 환경에서 보다 효율적이고 안전하게 공개키를 인증하기 위해서는 유선망으로의 접속이 필요 없는 개인식별정보 기반의 인증 방식을 사용하는 것이 바람직하다. 본 논문에서는 사용자간의 통신뿐만 아니라 서명의 생성과 검증 등의 과정도 무선망에서 가능하도록 개인식별정보를 그대로 공개키로 사용하는 디지털 서명 알고리즘을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 제안하는 알고리즘을 이용한 서명 생성과 검증 과정을 설명하고, 3장에서는 알고리즘의 안전성을 분석한다. 마지막으로 4장에서는 결론 및 향후 연구 계획에 대해 언급한다.

II. 제안하는 개인식별정보 기반의 디지털 서명 방식

제안하는 알고리즘에서는 사용자의 개인식별정보를 그대로 공개키로 사용한다. 또한, 각 사용자는 무선 인터넷을 사용하기 위한 이동 통신망에의 가입과 개통을 위해 신뢰성 있는 이동 통신사를 방문하는데, 이 때 이동 통신사는 사용자의 신원을 확인하고, 사용자와 이동 통신사간 1:1 통신에 필요한 통신키를 공유한다. 이동 통신사는 가입자의 신원정보와 함께 통신키를 보관하게 되고, 후에 서명자와 검증자간 통신에 있어 KTC(Key

Transfer Center)의 역할을 하여, 서명 생성과 검증에 필요한 인자를 중계한다.

1. 이동 통신사와 가입자간의 통신키 공유

신뢰성 있는 이동 통신사 T 의 가입자중 서명자를 A, 검증자를 B 라 가정하면, T 는 A 와 B 가 처음 방문했을 때, K_{AT} 와 K_{BT} 를 생성하여 각 가입자와 이를 공유한다. 이 통신키는 A 와 B 의 신원정보와 함께 비밀리에 보관된다. 아래 [그림 1] 이러한 공유 과정을 나타낸다.

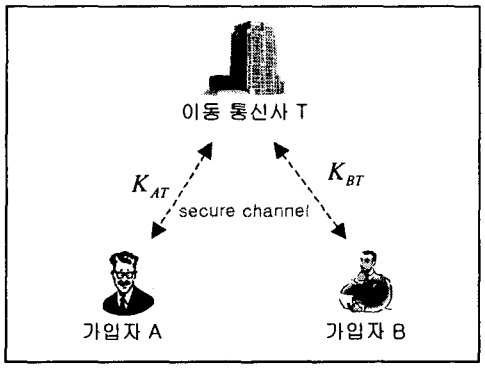

그림 1 통신키 공유 과정

2. 서명자의 비밀키 생성과 비밀키 인자 암호화

서명자 A 는 큰 소수 p 를 선택하고, $q \mid p-1$ 인 소수 q 를 위수로 갖는 원소 g 를 선택한다. 즉, $g^q \equiv 1 \bmod p$ 를 만족하는 g 를 선택하여 p, q 와 함께 공개한다. A 는 개인식별정보인 ID_A 를 공개키로 사용하고, 비밀키 x_A 를 선택한다. 이 때, 고정된 값인 ID_A 와 x_A 가 수학적 연관성을 갖게 하기 위해, $ID_A \equiv g^{x_A} \cdot k \bmod p$ 를 만족하는 비밀키 인자 k 를 계산한다. 그리고 서명의 검증을 원하는 검증자에게 k 를 안전하게 전달하기 위해, 이동 통신사 T 와 공유하고 있는 K_{AT} 로 k 를 암호화하여 T 에게 전송한다. T 는 보관중인 신원정보로 A 를 인증하여 A 가 정당한 사용자임이 확인되면, 전송받은 값을 동일한 키 K_{AT} 로 복호화하여 k 를 복원한다. 그리고, 이 값을 A 의 신원정보와 함께 보관한다. [그림 2]는 서명자의 비밀키 생성과 비밀키 인자 암호화 과정을 나타낸다.

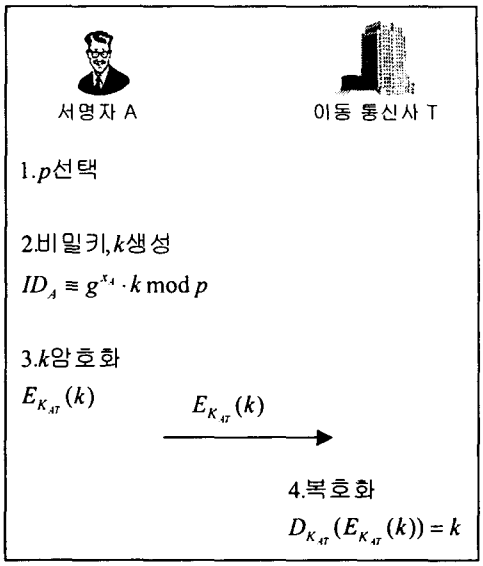

그림 2 비밀키 생성과 비밀키 인자 암호화 과정

3. 서명 생성 및 검증

서명자 A 는 공개 해쉬 알고리즘 $h()$ 을 사용하여, 메시지 M 에 대한 해쉬값 $H = h(M)$ 을 계산한다. 또한, Z_q 상에서 임의의 r 을 선택하여 중간값 $R \equiv g^{r \cdot H^{-1}} \bmod p \bmod q$ 을 계산하고, 서명값 $S \equiv (x_A \cdot H + r \cdot k) \cdot R \bmod p \bmod q$ 을 계산한다. 그리고 나서 A 는 검증자 B 에게 M, R, S 를 전송한다. M, R, S 를 전송 받은 검증자 B 는 T 에게 A 가 생성한 k 를 전송해 줄 것을 요청한다. T 는 B 와 비밀리에 공유중인 K_{BT} 로 k 를 암호화, 즉 $E_{K_{BT}}(k)$ 을 생성하여 B 에게 전송해 준다. B 는 전송받은 $E_{K_{BT}}(k)$ 을 복호화하여 k 를 복원하고, 메시지에 대한 해쉬값 $H = h(M)$ 를 구해, $g^S \equiv (ID_A \cdot k^{-1} \cdot R^k)^{R \cdot H} \bmod p \bmod q$ 인가를 조사하여 서명의 정당성을 확인한다. 검증식은 다음과 같으며, [그림 3]은 이러한 과정을 나타낸다.

$$(ID_A \cdot k^{-1} \cdot R^k)^{R \cdot H}$$

$$\equiv (g^{x_A} \cdot k \cdot k^{-1} \cdot g^{r \cdot H^{-1} \cdot k})^{R \cdot H}$$

$$\equiv g^{x_A \cdot R \cdot H} \cdot g^{r \cdot R}$$

$\equiv g^{(x_A \cdot H + r \cdot k) \cdot R}$

$\equiv g^{S} \bmod p \bmod q$

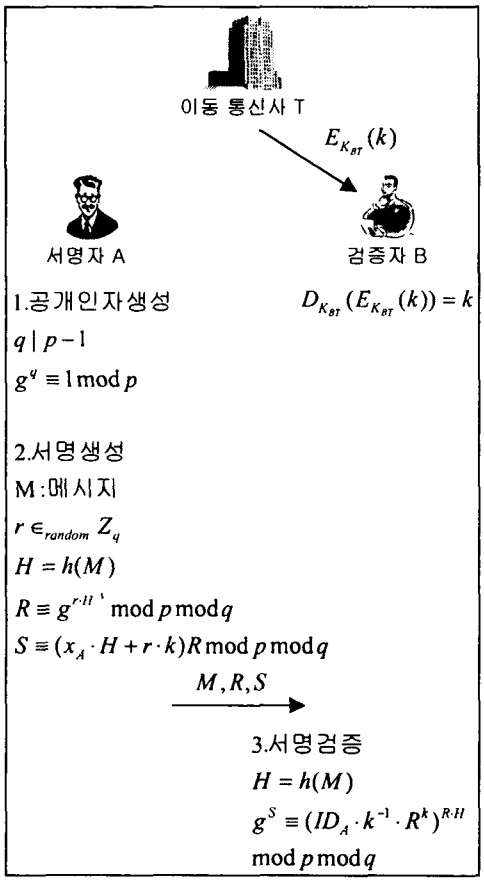

그림 3 서명생성 및 검증 과정

III. 알고리즘의 안전성 분석

제안한 알고리즘을 이용한 디지털 서명은 위조가 불가능하고, 정당한 서명자를 인증할 수 있으며, 서명자는 자신의 서명을 부인할 수 없다. 또한, 서명 내용의 변경이 불가능하고, 하나의 서명을 다른 문서의 서명으로 재사용하는 것이 불가능하다. 제안한 알고리즘이 이와 같은 안전한 서명 알고리즘으로서 갖추어야 할 조건을 만족하는가는 다음과 같다.

1. 위조 불가능

이는 합법적인 서명자만이 디지털 서명을 생성할 수 있어야 한다는 조건이다. 제안한 알고리즘에서 서명자의 비밀키를 모르는 사람은 정당한 서명을 생성할 수 없다.

$$ID_A \equiv g^{x_A} \cdot k \bmod p \quad (1)$$

$$g^S \equiv (ID_A \cdot k^{-1} \cdot R^k)^{R \cdot H} \quad (2)$$

또한, 비밀키 인자인 k 가 공개될 경우 식 (1)에서 k, g, ID_A, p 로부터 비밀키 x_A 를 구하는 것은 이산대수 문제이므로, 비밀키를 계산해 낼 수 없다. 하지만, 이 경우 식 (1)을 만족하는 여러 개의 (x_A', k') 쌍을 생성할 수 있어 제 3자가 정당한 서명을 생성하는 것이 가능하게 된다. 이를 막기 위해 제안한 알고리즘에서 k 는 이동 통신사와 가입자간의 통신키로 암호화되어 전송된다. 검증자는 T 로부터 수신한 k 를 이용하여 서명을 검증하므로, (x_A', k') 로 생성된 서명은 위조되었음을 확인할 수 있다.

또한, 식 (2)에서 공개된 값을 제외하고 서명에 해당하는 R, S 와 k 를 고려할 때, R, S 를 고정하고 k 를 구하는 것, S, k 를 고정하고 R 을 구하는 것, k, R 을 고정하고 S 를 구하는 것 모두 이산대수 문제이므로, 정당한 서명을 임의의 서명으로 위조하는 것은 불가능하다.

2. 서명자 인증

서명자 인증 기능이란 디지털 서명의 서명자를 누구든지 확인할 수 있어야 한다는 조건이다. 제안한 알고리즘에서는 누구에게나 공개되어 있는 개인식별정보 ID_A 를 공개키로 사용하기 때문에, 이를 이용하면 누구든지 서명의 정당성을 검증할 수 있다.

3. 부인 불가능

이는 서명자가 후에 자신이 서명한 사실을 부인할 수 없어야 한다는 조건이다. 제안한 알고리즘에서는 서명자의 비밀키를 알고 있는 사람만이 서명을 생성할 수 있다. 또한, 서명을 검증할 때 서명자의 비밀키와 수학적 연관성이 있는 개인식별정보를 이용하기 때문에 서명자는 부인을 할 수 없게 된다.

4. 변경 불가능

이는 제 3자가 다른 사람의 서명을 자신의 서명으로 변경할 수 없어야 한다는 조건이다.

$$R \equiv g^{r \cdot H^{-1}} \bmod p \bmod q \quad (3)$$

$$S \equiv (x_A \cdot H + r \cdot k) \cdot R \bmod p \bmod q \quad (4)$$

식 (3)에서 g, H, R, p, q 로부터 r 을 구하는 것은 이산대수 문제이므로 불가능하다. 또한, 식 (4)에서 r 을 모르면 x_A 를 구할 수 없다. 따라서, 제 3자는 x_A 대신 자신의 비밀키를 서명에 포함시킬 수 없으므로, A 의 서명을 자신의 서명으로 변경할 수 없게 된다.

5. 재사용 불가능

이는 한 메시지에 대한 서명을 다른 메시지의 서명으로 사용할 수 없어야 한다는 조건이다.

식 (3)에서 보는 바와 같이 서명된 메시지의 해쉬값이 지수승 연산에 사용되었기 때문에, g, R, p, q 로부터 H 를 계산하는 것은 이산대수 문제로 불가능하다. 따라서, 동일한 서명 값을 갖는 서로 다른 메시지를 계산해 낼 수 없기 때문에 서명의 재사용이 불가능하다.

IV. 결론 및 향후 연구 계획

본 논문에서는 이동 통신 환경에서 인증서의 검증 없이 효율적이고 안전하게 서명을 생성하고 검증할 수 있는 디지털 서명 알고리즘을 제안하였다. 기존의 인증서 기반 방식에서는 서명자의 인증서 검증을 위해, 공개키 암호 방식을 이용하여 그 인증서에 대한 디지털 서명을 검증한다. 반면, 제안한 방식에서는 관용 암호 방식을 이용하여 이동 통신사로부터 전송받은 값을 복호화함으로써 서명자의 비밀키 인자값을 검증한다. 따라서, 제안한 방식을 이용하면 보다 효율적으로 서명을 검증할 수 있다. 하지만, 서명의 검증을 위해 이동 통신사와의 통신을 필요로 한다는 단점이 있다. 따라서, 추후 사용자와 이동 통신사간 별도의 통신 없는 개인식별정보 기반의 디지털 서명 알고리즘에 대한 연구가 이루어져야 할 것이다.

참고문헌

[1] Whitfield Diffie and Martin E. Hellman, "New directions in cryptography", IEEE Trans. on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[2] TaherElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms", IEEE Trans. on Information Theory, vol. IT-31, pp. 469-472, 1995.

[3] K. Nyberg and R. A. Rueppel, "Message recovery for signature scheme based on the discrete logarithm problem", Eurocrypt'94 Proceedings, Springer-Verlag, 1995

[4] A. Shamir, "Identity-based cryptosystems and signature schemes", Advanced in Cryptology(Proceedings of Crypto'84), Springer-Verlag, pp.47-53, 1985.

[5] M. Girault, "Self-certified public keys", Advances in Cryptology-Eurocrypt'91, LNCS 547, Springer-Verlag, 1991.

[6] A. Fiat and A. Shamir, "How to prove yourself : Practice solutions to identification and signature problems", CRYPTO'86 Proceedings, Springer-Verlag, pp.186-194, 1987.