효율적인 일방향 상호 인증 키분배 방식

김승주°, 박성준, 원동호

성균관대학교 정보공학과

An Efficient One-Pass Authenticated Key Establishment Schemes

Seung Joo Kim, Sung Jun Park and Dong Ho Won

Department of information Engineering
Sung Kyun Kwan University
E-mail : sjkim@dosan.skku.ac.kr

요 약

Kaisa Nyberg와 Rainer A. Rueppel 등은 [10], [11], [12] 에서 메세지 회복형 DSA를 최초로 제안하였으며, 이를 이용한 일방향 상호 인증 키분배 방식을 제안했다. Nyberg-Rueppel 키분배 방식은 일방향 상호 인증 키분배 방식이면서, 지정된 수신자만이 key token의 출처를 확인할 수 있으며 필요시에 제3자에게 key token의 정당성을 증명할 수 있으므로 메시지의 서명과 암호화를 함께 필요로 하는 응용에 적합하다는 특성을 갖는다.

본 논문에서는 기존의 Nyberg-Rueppel 키분배 방식에 비해 보다 효율적인 키분배 방식을 제안한다.

1. 서 론

컴퓨터 망에서 교환되는 정보의 보호를 위한 가장 기본적인 도구로 관용 암호시스템(conventional cryptosystem)을 이용한 암호화 기법이 가장 널리 사용되고 있다. 이에 필요한 세션키(session key)를 효율적으로 분배하는 것은 중요한 과제의 하나로 많은 연구가 진행되어 왔으며, 특히 최근에는 키분배 과정에서 발생될 수 있는 각종 위협들을 미연에 방지할 수 있도록 키 분배와 신분인증을 결합시킨 방식들이 활발히 연구되고 있다.[1][2][3][4][5][6][7]

인증방식과 키 분배 방식을 결합하는 방법은 크게 키 분배에 의한 인증과 인증에 의한 키 분배로 나눌 수 있다. 먼저 키 분배에 의한 인증이란 통신망의 각 가입자가 자신만의 비밀 정보를 소유하고 있을 때, 임의의 양 가입자는 공통키를 생성할 수 있으며, 양자가 정확한 키를 소유하였을 때 상대방을 인증하는 방법이다. 키 분배 방식으로는 DH 방식, ID 기반의 키 분배 방식 등을 이용할 수 있으며 이러한 인증 방식법은 키 분배 방식의 안전성에 의존한다.[8][9]

인증에 의한 키 분배란 먼저 인증을 행한 후, 인증 과정에서 사용된 데이타를 이용해서 공통키를 생성하는 방법을 말한다. 이 방법의 장점은 이미 안전하다고 입증된 영지식 대화형 증명 방식을 이용하여 안전한 키분배를 할 수 있다는 점인데 이미 제안된 방식으로는 1989년 Bauspieß가 Beth의 ZKIP을 이용하여 키 분배를 행한 것과 FS 방식을 이용한 것이 있다.

한편, Kaisa Nyberg와 Rainer A. Rueppel 등은 [10], [11], [12] 에서 메세지 회복형 DSA를 최

초로 제안하였으며, 이를 이용한 일방향 상호 인증 키분배 방식을 제안했다. Nyberg-Rueppel 키분배 방식은 일방향 상호 인증 키분배 방식이면서, 지정된 수신자만이 key token의 출처를 확인할 수 있고 필요시에 제3자에게 key token의 정당성을 증명할 수 있다는 특징을 갖는다.

본 논문에서는 기존의 Nyberg-Rueppel 키분배 방식에 비해 보다 효율적인 일발향 상호 인증 키분배 방식을 제안한다.

2. 기존의 키분배 방식

2.1 Nyberg-Rueppel 키분배 방식 (I) [10]

K. Nyberg와 R. A. Rueppel 등은 [10], [11], [12] 에서 메세지 회복형 DSA를 최초로 제안하였으며, 이를 기본으로 삼아 일방향 상호 인증 키분배 방식을 제안하였다. Nyberg-Rueppel 키분배 방식은 다음의 특성을 갖는다.

① 일방향으로 사용자의 상호 인증이 가능함과 동시에 공통의 세션키를 안전한 방법으로 공유할 수 있는 일방향 상호 인증 키분배 방식이다.
② 지정된 수신자만이 key token의 출처를 확인할 수 있으며 필요시에 제3자에게 key token의 정당성을 증명할 수 있으므로, 메시지의 서명과 암호화를 함께 필요로 하는 응용에 적합하다.

이 방식을 살펴보면 아래와 같다. (그림 2.1 참조)

[초기화 (Set-up)]

공개키) p : 소수.
q : 소수. 단, q | p-1
α : mod p 상에서 위수가 q인 임의의 수.
k : $k = \alpha^{-s} \pmod p$

비밀키) s : q 보다 작은 임의의 수

[Nyberg-Rueppel 키분배 방식 (I)]

① 사용자 A는 랜덤수 $r \in_R [1, q)$, $R \in_R [1, q)$ 를 선택하여 (e, y)를 구한 후, 사용자 B에게 전송한다.

$$e = \alpha^{R-r} \bmod p$$
$$y = r + s_A e \bmod q$$

② 사용자 A는 세션키 $K = k_B^R \bmod p$ 를 계산한다.
③ (e, y)를 받은 사용자 B는 $K \equiv (\alpha^y k_A^e e)^{-s_B} \bmod p$ 를 계산하여, K를 그들 간의 세션키로 사용한다.

사용자 A		사용자 B
① $s_A \in_R Z_q$ ② $k_A = \alpha^{-s_A} \bmod p$	p, q, α {k_A} {k_B}	① $s_B \in_R Z_q$ ② $k_B = \alpha^{-s_B} \bmod p$
① $r \in_R Z_q$ $R \in_R Z_q$ ② $e = \alpha^{R-r} \bmod p$ $y = r + s_A e \bmod q$		
	(e, y) ------>	
① $K = k_B^R \bmod p$		① $K = (\alpha^y k_A^e e)^{-s_B} \bmod p$

그림 2.1 Nyberg-Rueppel 키분배 방식 (I)

2.2 Nyberg-Rueppel 키분배 방식 (II) [12]

(그림 2.2 참조)

[초기화 (Set-up)]

공개키) p : 소수.
q : 소수. 단, q | p-1
g : mod p 상에서 위수가 q인 임의의 수.
y : $k = g^x \pmod p$

비밀키) x : q 보다 작은 임의의 수

[Nyberg-Rueppel 키분배 방식 (II)]

① 사용자 A는 랜덤수 $k \in_R [1, q)$ 를 선택하여 세션키 $K_{AB} = y_B^k \bmod p$ 를 계산한다.
② 사용자 A는 (r, s)를 구한 후, 사용자 B에게 전송한다.

$r = g^k \bmod p$
$s = k - x_A r' \bmod q$
단, $r' = h(K_{AB}, t)$ 여기서 t는 time-stamp를 나타낸다.

③ (r, s)를 받은 사용자 B는 $K_{AB} = r^{x_B} \bmod p$ 를 계산한 후, 다음에 의해 (r, s)의 정당성을 확인하고, 정당한 key token이면 K_{AB}를 그들 간의 세션키로 사용한다.

$r' = h(K_{AB}, t)$
$r = g^s y_A^{r'} \bmod p$?

사용자 A		사용자 B
① $x_A \in_R Z_q$ ② $y_A = g^{x_A} \bmod p$	p, q, g $\{y_A\}$ $\{y_B\}$	① $x_B \in_R Z_q$ ② $y_B = g^{x_B} \bmod p$
① $k \in_R Z_q$ ② $K_{AB} = y_B^k \bmod p$		
① $r = g^k \bmod p$ $s = k - x_A r' \bmod q$ 단, $r' = h(K_{AB}, t)$		
	(r, s) ---------->	
		① $K_{AB} = r^{x_B} \bmod p$
		① $r' = h(K_{AB}, t)$ ② $r = g^s y_A^{r'} \bmod p$?

그림 2.2 Nyberg-Rueppel 키분배 방식 (II)

3. 제안하는 효율적인 키분배 방식

본 장에서는 기존의 Nyberg-Rueppel 키분배 방식에 비해 보다 효율적인 일방향 상호 인증 키분배 방식을 제안한다. (그림 3.1 참조)

[초기화 (Set-up)]

공개키) p : 소수.
q : 소수. 단, q | p-1
g : mod p 상에서 위수가 q인 임의의 수.
y : $y = g^x \pmod p$

비밀키) x : q 보다 작은 임의의 수

Schnorr에 의하면 p의 길이를 약 512 bits, q의 길이를 약 140 bits 정도로 하는 것이 좋다고 한다.[13][14]

[제안하는 일방향 상호 인증 키분배 방식]

① 사용자 A, B는 $y_{AB} = y_B^{x_A} = y_A^{x_B} \bmod p$ 를 사전 계산한다.

② 사용자 A는 랜덤수 $k \in_R [1, q)$ 를 선택하여 다음을 계산한 후, (r, s)를 사용자 B에게 전송한다.

$$r = g^k \bmod p$$

$K_{AB} = f(y_{AB}, r)$

$s = k - x_A e \bmod q$

단, $e = h(K_{AB}, t)$ 여기서 t는 time-stamp를 나타낸다.

③ (r, s)를 받은 사용자 B는 $K_{AB} = f(y_{AB}, r)$ 를 계산한 후, 다음에 의해 (r, s)의 정당성을 확인하고, 정당한 key token이면 K_{AB}를 그들 간의 세션키로 사용한다.

$$e = h(K_{AB}, t)$$

$$r = g^s y_A^e \bmod p \ ?$$

Remark : f(.)는 y_{AB}에 대한 일방향함수임과 동시에 r을 조작하여 이전의 알고 있던 것과 같은 값을 재발생시키는 것이 불가능한 함수이다. 예를 들면 $f(y_{AB}, r) = (y_{AB} \oplus r) \bmod q$ 역시 안전하게 사용될 수 있을 것이다.

사용자 A		사용자 B
① $x_A \in_R Z_q$ ② $y_A = g^{x_A} \bmod p$	p, q, g $\{y_A\}$ $\{y_B\}$	① $x_B \in_R Z_q$ ② $y_B = g^{x_B} \bmod p$
① $y_{AB} = y_B^{x_A} \bmod p$		① $y_{AB} = y_A^{x_B} \bmod p$
① $k \in_R Z_q$ ② $r = g^k \bmod p$ ③ $K_{AB} = f(y_{AB}, r)$ ④ $s = k - x_A e \bmod q$ 단, $e = h(K_{AB}, t)$		
	(r, s) ⟶	
		① $K_{AB} = f(y_{AB}, r)$ ① $e = h(K_{AB}, t)$ ② $r = g^s y_A^e \bmod p$?

그림 3.1 제안하는 효율적인 키분배 방식

여기서 y_{AB}는 사용자 A와 B만의 공유키로 그 외의 어떤 제3자도 (r, s)로부터 세션키 K_{AB}를 생성할 수 없으며, 사용자 B는 B 자신에게 조차도 사용자 A임을 증명할 수 없다.

또, B는 필요시에 K_{AB}를 공개함으로써, 제3자에게 key token의 정당성을 증명할 수 있으며, 기존의 키분배 방식에 비해 사용자의 계산량이 적어 효율적이다.

4. 결 론

디지틀 통신에 있어서 정보를 보호하기 위한 방법으로서는 관용 암호시스템(conventional cryptosystem)을 이용한 암호화 기법이 가장 널리 사용되고 있다. 암호를 이용하여 정보를 보호하는데 있어서 대두되는 문제는 원하는 통신 상대방과 비밀 통신을 하기 위해 공유해야 하는 세

션키를 생성하는 문제를 들 수 있다.

최근에는 키분배 과정에서 발생될 수 있는 각종 위협들을 미연에 방지할 수 있도록 키 분배와 신분인증을 결합시킨 방식들이 활발히 연구되고 있으며, 특히, Kaisa Nyberg와 Rainer A. Rueppel 등은 [10], [11], [12] 에서 메세지 회복형 DSA를 최초로 제안하였으며, 이를 이용한 일방향 상호 인증 키분배 방식을 제안했다. Nyberg-Rueppel 키분배 방식은 일방향 상호 인증 키분배 방식이면서, 지정된 수신자만이 key token의 출처를 확인할 수 있으며 필요시에 제3자에게 key token의 정당성을 증명할 수 있으므로 메시지의 서명과 암호화를 함께 필요로 하는 응용에 적합하다는 특성을 갖는다.

본 논문에서는 기존의 Nyberg-Rueppel 키분배 방식에 비해 사용자의 계산량이 적은 효율적인 일방향 상호 인증 키분배 방식을 제안하였다. 사용자의 상호 인증이 가능함과 동시에 공통의 세션키를 안전한 방법으로 공유할 수 있는 일방향 상호 인증 키분배 방식은 여러 가지 응용들에서 매우 유용하게 사용될 수 있을 것이다.

참 고 문 헌

[1] J. Brant, I. Damgard, P. Landrock, and T. Pedersen, "Zero-knowledge authentication scheme with secret key exchange", Proc. Crypto'88

[2] C. G. Gunther, "An identity-based key-exchange protocol", Proc. Eurocrypt'89

[3] F. Bauspieß and H. J. Knobloch, "How to keep authenticity alive in a computer network", Proc. Eurocrypt'89

[4] T. Beth, "Efficient Zero-Knowledge Identification Scheme for Smart Cards", Proc. Eurocrypt'88

[5] 이윤호, 양형규, 권창영, 원동호, "ID 기반의 영지식 대화형 프로토콜을 이용한 개인 식별 및 키 분배 프로토콜에 관한 연구", 통신정보보호학회 논문지 Vol. 2. No. 1. 1992. 6.

[6] 임채훈, 이필중, "상호 신분 인증 및 디지탈 서명기법에 관한 연구", 통신정보보호학회 논문지 Vol. 2. No. 1. 1992. 6.

[7] 임채훈, 이필중, "인증 및 키 분배 기능을 결합한 프로토콜의 체계적인 설계방법", 통신정보보호학회 논문지 Vol. 3. No. 1. 1993. 6.

[8] Diffie, Hellman, "New Directions in Cryptography", IEEE Trans. on Information Theory, IT-22, 1976.

[9] A. Shamir, "Identity-based Cryptosystems and Signature Schemes", Crypto'84.

[10] K. Nyberg, R. A. Rueppel, "A New Signature Scheme Based on the DSA Giving Message Recovery", ACM. Conf. on Computer and Communications Security, 1993.

[11] K. Nyberg, R. A. Rueppel, "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Proc. Eurocrypt'94

[12] K. Nyberg, "On One-Pass Authenticated Key Establishment Schemes", SAC'95. 1995. 5.

[13] C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Advances in Cryptology - CRYPTO '89 Proceedings, Berlin: Springer - Verlag, pp. 239-252, 1990.

[14] C. P. Schnorr, "Efficient Signature Generation for Smart Cards", Journal of Cryptology. v.4, n.3, pp. 161-174, 1991.