通信情報保護學會論文誌
第4卷 第2號, 1994. 12

디지틀 이동통신 시스템에서 스마트 카드를 이용하는 키분배 프로토콜

문 태 욱*, 박 상 우**, 이 정 숙***, 조 성 준***

Key Distribution Protocols using Smart Card in Digital Mobile Communication Systems

Tae-Wook Moon*, Sang-Woo Park**,
Jeong-Sook Yi*** and Sung-Joon Cho***

요 약

본 논문의 저자들은 이전에 디지틀 이동통신 시스템을 위한 키분배 프로토콜을 제안한 바 있다. 그러나 이 프로토콜에서는 사용자 인증에 RSA 방식을 사용하므로 기존의 키분배 프로토콜과 비교하여 여전히 많은 지수승 연산처리가 요구된다. 따라서 본 논문에서는 스마트 카드를 이용하는 보다 효율적인 세 가지의 키분배 프로토콜을 새로이 제안한다. 프로토콜 Ⅰ은 Schnorr의 개인식별 방식을 변형시켜 얻은 개인식별 방식과 Okamoto의 키분배 방식을 결합한 것이고, 프로토콜 Ⅱ는 프로토콜 Ⅰ에서의 개인식별 방식과 ElGamal의 변형 키분배 방식을 결합한 것이다. 이와는 달리, 프로토콜 Ⅲ은 Fiat-Shamir의 개인식별 방식과 이 개인식별 방식을 기본으로 새롭게 구성한 키분배 방식을 결합한 것이다. 끝으로, 지금까지 제안됐던 프로토콜과 본 논문에서 새롭게 제안하는 프로토콜에 대해 안전성과 효율성을 비교했다.

Abstract

Authors of this paper have already proposed a key distribution protocol for digital mobile communication systems which uses RSA scheme as user authentication but the protocol requires many processing operations of exponent multiplication. Therefore, we newly propose three kinds of key distribution protocol based on smart card. Protocol Ⅰ consists of the modified Schnorr identification scheme and Okamoto key distribution

* 주식회사 스탠더드 텔레콤 부설 정보통신 연구소
** 한국전자통신연구소 부호1실
*** 한국항공대학교 대학원 항공통신정보공학과

scheme. Protocol Ⅱ consists of the modified Schnorr identification scheme and the modified ElGamal key distribution scheme. In different from protocol Ⅰ, Ⅱ, protocol Ⅲ consists of Fiat-Shamir identification scheme and a new key distribution scheme based on Fiat-Shamir identification scheme. Finally, newly proposed protocols are compared with existing protocols with respect to secrecy and efficiency.

1. 서 론

통신에서 정보의 개인적 침해나 불법 사용이 큰 문제가 되고 있으며, 특히 무선을 이용하는 이동통신에서의 정보보호의 중요성이 더욱 크게 부각되고 있다. 현재 유럽의 차세대 디지틀 이동통신 시스템인 GSM이나 미국의 CDMA 방식을 제안하고 있는 Qualcomm 사에서는 데이터의 보호를 위해 암호시스템을 도입하고 있다[1,2]. 이동통신에서 사용하려는 암호시스템은 처리속도가 빠르고, 기존의 상용화가 많이 되어 있는 공통키 암호시스템(common key cryptosystem)을 채용하고 있다. 공통키 암호시스템에서는 송·수신자 상호간에 비밀 통신을 위한 공통키(common key)가 필요한데, 이 공통키의 보호가 시스템 전체의 비도와 밀접한 관계가 있다. 공통키 암호시스템의 공통키를 안전하게 분배하기 위한 연구는 비밀키와 공개키가 분리된 공개키 암호시스템(public key cryptosystem)에 의해 매우 급속히 발전하게 되었다. 공개키 암호시스템은 비록 암호화 연산처리가 공통키 암호시스템보다 느리기는 하지만 각각의 사용자가 소유하는 비밀키와 모든 사용자에게 공개하는 공개키로 구성되므로 공통키를 분배할 필요가 없다. 이런 특징을 이용하여 공통키 암호시스템의 공통키를 분배하기 위한 공개키 암호시스템의 키분배 방식이 제안되었다[3]. 이동통신에서 공통키 암호시스템을 사용하는 경우에 빈번히 발생하는 세션키(session key)의 관리와 사용자에 대한 인증이 필요하기 때문에 키분배와 사용자 인증이 결합된 키분배 프로토콜이 연구되고 있다.

본 논문에서는 기존의 이동통신에서의 키분배 프로토콜에 대해 고찰하고, 이 키분배 프로토콜에 대한 문제점을 보완할 수 있는 키분배 프로토콜을 새로이 제안한다. 여기서 사용자 인증시 이용되는 인증 방식은 기존의 프로토콜보다 단말기에서의 연산처리량을 크게 줄일 수 있는 ID를 기본으로 하는 인증 방식이다. 특히, 각 사용자의 키분배에 대한 안전성을 높이기 위하여 센터에서 사용자를 인증할 때 사용자의 비밀정보가 노출되지 않는 인증 방식을 키분배 프로토콜에 적용시키고자 한다. 여러가지 인증 방식 중에서, ID를 기본으로 하는 Schnorr의 개인식별 방식과 Fiat-Shamir의 개인식별 방식이 위에서 고려된 사항을 만족시킬 수 있는 인증 방식이다[4,5]. 그러나, Schnorr의 개인식별 방식은 세션키를 빈번히 발생시키다 보면 사용자의 비밀정보가 노출될 수 있기 때문에 원래의 개인식별 방식을 그대로 프로토콜에 적용하는 데는 안전성 문제가 있으므로, 본 논문에서는 이런 문제점을 보완하여 Schnorr의 개인식별 방식을 변형시킨 새로운 개인식별 방식을 키분배 프로토콜에 이용한다. 또한, Fiat-Shamir의 개인식별 방식에서 사용하는 비밀키와 공개키를 이용하여 구성하는 새로운 키분배 방식을 제안하고 이를 키분배 프로토콜에 이용한다.

본 논문에서는 세가지 키분배 프로토콜을 제안한다. 첫번째 프로토콜은 Schnorr의 개인식별 방식을 변형시킨 새로운 개인식별 방식과 Okamoto의 키분배 프로토콜로 구성하는 프로토콜(이하 프로토콜 Ⅰ이라고 한다)이다. 두번째 프로토콜은 프로토콜 Ⅰ의 개인식별 방식과 Park의 논문에서 제안한 ElGamal의 변형 키분배 방식으로 구성하는 프로토콜(이하 프로토콜 Ⅱ라고 한다)이다. 그리고 세번째 프로토콜은 프로토콜 Ⅰ, Ⅱ와는 구성이 다른, Fiat-Shamir의 개인식별 방식과

Fiat-Shamir의 개인식별 방식을 변형시킨 새로운 키분배 방식을 결합하여 구성하는 프로토콜(이하 프로토콜 Ⅲ이라고 한다)이다. 그리고 본 논문에서는 지금까지 제안됐던 여러가지 키분배 프로토콜과 새로이 제안하는 세가지 키분배 프로토콜을 안전성 및 효율성에 관해 비교 및 검토한다.

2. 지금까지 제안된 이동통신 시스템용 키분배 프로토콜에 대한 고찰

2.1 Tatebayashi와 Park이 제안한 키분배 프로토콜

디지틀 이동통신 시스템용 키분배 프로토콜은 Tatebayashi가 처음 제안하였다[5]. 이 프로토콜은 센터가 사용자 인증과 키분배에 직접적으로 관여하여 사용자 터미날의 암호화 연산처리를 분담하는 프로토콜이다. 이 프로토콜에서는 uplink에 RSA 암호방식 중 $e = 3$을 사용하고, downlink에서 쌍자대치 암호(Vernam cipher)를 사용한다. 따라서 매우 빠른 암호화가 수행되지만 비도가 그리 높지 않고, 또한 통신 상대방의 두 가입자인 A와 B가 세번만 통신하게 되면 B는 A의 랜덤 수 r_A를 알게 된다. 또한 네트워크 센터는 가입자간의 대화 키를 모두 알 수 있기 때문에 모든 가입자의 통신 내용을 쉽게 도청할 수 있다는 단점이 있다.

이러한 문제점은 개선한 키분배 프로토콜이 Park이 제안한 키분배 프로토콜이다[6]. 이 프로토콜은 이산 대수(discrete logarithm)의 계산이 어렵다는 점에 근거하고 있는 ElGamal의 인증 방식을 이용하는 프로토콜로서, Tatebayashi가 제안한 키분배 프로토콜의 문제점을 해결할 수는 있지만 계산량이 매우 많아지는 단점이 있다.

2.2 Yun이 제안한 키분배 프로토콜

Tatebayashi와 Park이 제안한 키분배 프로토콜의 장·단점을 상호 보완하기 위하여 RSA 방식을 이용한 키분배 프로토콜을 Yun과 저자들이 이미 제안한 바 있다[7]. 이 키분배 프로토콜은 RSA 방식을 이용하기 때문에 Park이 제안한 키분배 프로토콜보다는 연산처리량이 적지만 같은 비도를 가지며, Tatebayashi가 제안한 키분배 프로토콜보다는 많은 연산처리량을 가지면서 보다 나은 비도를 가진다. 그러나 Yun이 제안한 키분배 프로토콜도 상당히 많은 연산처리가 요구되므로 단말기에서 처리해야 하는 연산을 좀 더 줄일 필요가 있다.

3. 세가지의 새로운 키분배 프로토콜의 제안

이동통신에 암호시스템을 적용하기 위해서는 몇가지 고려할 사항이 있다. 즉, 연산처리 능력이 극히 제한되어 있는 단말기로서 이상적인 시간내에 세션키를 얻을 수 있어야 하며, 무선을 이용하므로 정보의 노출이나 불법 수정에 대해 안전할 것과 또, 다른 사람이 남의 단말기를 무단 사용하면 그 단말기 소지자의 ID로 요금이 부과되기 때문에 부당한 과금에 대한 대비책도 있어야 한다[9]. 이런 점을 고려하여 차세대 디지틀 이동통신 시스템에서는 단말기와는 별도로 사용자에게 스마트 카드를 발급하여, 스마트 카드내에서 암호화 연산처리를 수행하고, 또한 사용자 개인식별 방식도 수행하도록 하여 단말기와는 별도로 과금할 수 있도록 하고 있다.

따라서 이동통신 시스템에서의 인증 방식으로서는 스마트 카드내에서 연산이 수행되는 인증 방식이 가장 적합한데, 이런 방식에는 Schnorr의 방식과 Fiat-Shamir의 방식이 가장 적합하다.

본 논문에서 제안하는 키분배 프로토콜에 이용하는 키분배 방식으로서는 Okamoto의 방식, Park에 의해 제안된 ElGamal의 변형 키분배 방식, 그리고 Fiat-Shamir의 인증 방식을 변형시킨 키분배 방식을 이용한다. 이 키분배 방식들은 모드 키분배 과정에서 키에 대한 인증을 포함하고

있어 사용자에게 안전성을 제공한다.

디지틀 이동통신 시스템에서의 정보보호는 기존의 전화망(PSTN) 및 미래의 종합정보통신망(ISDN)과의 데이터 호환에 대비하여 인증 및 서명에 사용되는 파라미터에 대한 표준화가 필요하다. 그러나 국내에서는 아직 표준화가 되어 있지 않은 상태이기 때문에 본 논문에서는 미국 NIST의 DSS 파라미터를 기준으로 삼는다[10].

3.1 Schnorr의 개인식별 방식을 이용하는 두가지의 새로운 키분배 프로토콜(프로토콜 Ⅰ, Ⅱ)

이산 대수의 계산이 어렵다는 점을 이용한 Schnorr의 개인식별 방식은 스마트 카드내에서 이용할 수 있는 매우 효율적인 개인식별 방식 및 서명 방식으로서 이미 잘 알려져 있다. 본 논문에서는 이 인증방식에 키분배 방식을 결합하여 새로운 키분배 프로토콜을 구성한다.

3.1.1 프로토콜 Ⅰ, Ⅱ에서 사용하는 파라미터

프로토콜 Ⅰ, Ⅱ에서 사용하는 파라미터는 미국 NIST의 DSS의 파라미터를 기준으로 삼았는데, 키분배 프로토콜에서 사용하는 파라미터는 다음과 같다.

- $2^{511} < p < 2^{512}$인 소수 p
- $q|p-1$이고, $2^{159} < q < 2^{160}$인 소수 q
- $g > 1$이고, $0 < h < p$인 $g \equiv h^{(p-1)/q} \pmod p$
- $0 < x < q$인 비밀키, x
- 공개키, $Y \equiv g^x \pmod p$
- $0 < k < q$인 랜덤수 k
- 일방향 해쉬 함수인 H
- $h, m > 1$이고, $0 < h, m < p$인 임의의 정수 h, m

3.1.2 프로토콜 Ⅰ, Ⅱ에서 이용하는 새로운 개인식별 방식

Schnorr의 개인식별 방식은 k의 중복사용에 의해 비밀키가 노출될 위험이 있기 때문에 이런 위험에 더욱 안전한 인증방식이 필요하다. 또한 원래의 Schnorr의 개인식별 방식을 키분배 프로토콜에 이용할 때 키분배 과정에서 생성되는 랜덤수를 개인식별 방식에 이용하여 보다 효율적인 개인식별 방식을 제안하고자 한다.

키분배 프로토콜에 이용되는 새로운 개인식별 방식은 다음과 같다.

〈초기화〉

사용자 i는 랜덤 수 $k_i \in \{1, \cdots, q^{k_i} - 1\}$를 선택하여 $R_i \equiv g^{k_i} \pmod p$를 계산한다.

〈세션키 처리 과정〉

① 사용자 B에게서 전송된 R_B를 이용하여 사용자 A는 랜덤수 $k_A \in \{1, \cdots, q^k - 1\}$을 선택한 후, $R_{AB} \equiv R_B^{k_A} \ ((\bmod p) \bmod q)$를 계산한다.

② 사용자 A는 $P \equiv R_{AB}(k_A + x_A E) \pmod q$를 계산한다. 단, $E = H(ID_A||ID_B)$이다.

③ 사용자 A는 B에게 $ID_A||ID_B$, P, R_A를 전송한다.

〈확인 과정〉

사용자 B는 $R_{AB} \equiv R_A^{k_B} \ ((\bmod p) \bmod q)$를 계산하고, $PR_{AB}{}^{-1}$를 계산한 후, $V \equiv g^{PR_{AB}{}^{-1}} Y^E \equiv R_A \pmod p \overset{?}{=} R_A$를 계산하여 A가 정당한 사용자임을 확인한다.

위와 같은 개인식별 방식을 키분배에 이용함으로서 확인 과정에서 비록 같은 k_A를 반복하여 사용하더라도 랜덤수 R_{AB}에 의해 비밀키 x_A의 노출을 막을 수 있다.

3.1.3 Okamoto의 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅰ)

3.1.2에서 제안한 인증 방식을 이용하여 다음과 같은 키분배 프로토콜을 제안한다.

〈사전처리 과정〉

각각의 사용자 i는 랜덤 수 $k_i \in \{1, \cdots, q^k - 1\}$를 선택하여 $R_i = g^{k_i}((\mathrm{mod}\ p)\mathrm{mod}\ q)$를 계산한다.

〈키분배 과정〉

① 센터는 사용자 A의 통신 요청에 의해 랜덤 수 R_{C1}을 사용자 A에게 전송한다.

② 사용자 A는

$$P_A \equiv R_{AC}(k_A + x_A E_A)(\mathrm{mod}\ q)$$

를 계산한다. 단, $R_{AC} = R_{C1}R_A((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$, $E_A = h(ID_A||ID_B||t_A)$이다.

③ 사용자 A는 센터에게 $ID_A||ID_B||t_A$, R_{AC}, P_A를 전송한다.
여기서 ID_A는 A의 ID, ID_B는 B의 ID, t_A는 time-stamp를 나타낸다.

④ 센터는 전송된 R_{AC}를 이용하여,

$$g^{P_A R_{AC}^{-1}} Y_A^{E_A}(\mathrm{mod}\ p) \equiv R_A((\mathrm{mod}\ p)\mathrm{mod}\ q)$$

를 계산하고, $R_A R_{C1} = R_{AC}$에 의해 A의 정당성을 확인하고, 정당한 사용자이면 사용자 B를 호출(call)함과 동시에 $ID_A||ID_B||t_A$, R_A, R_{C2}를 전송한다.

⑤ 사용자 B는 세션키, SK와 R_A를 이용하여

$$R_{AB} \equiv R_A^{k_B} \cdot SK((\mathrm{mod}\ p)\mathrm{mod}\ q)$$

를 계산한다. 그 후 자신의 사용자 인증,

$$P_B \equiv R_{BC}(k_B + x_B E_B)(\mathrm{mod}\ q)$$

를 계산한다. 단, $R_{BC} \equiv R_{C2}R_B((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$, $E_B = h(ID_B||ID_A||t_B)$이다.

⑥ 사용자 B는 센터에게 $ID_B||ID_A||t_B$, R_{AB}, R_{BC}, P_B를 전송한다.

⑦ 센터는 전송된 R_{BC}를 이용하여,

$$g^{P_B R_{BC}^{-1}} Y_B^{E_B}(\mathrm{mod}\ p) \equiv R_B((\mathrm{mod}\ p)\mathrm{mod}\ q)$$

에 의해 B의 정당성을 확인하고, 정당한 사용자이면 사용자 A에게 R_{AB}, R_B를 전송한다.

⑧ 사용자 A는

$$\frac{R_{AB}}{R_B^{k_A}} \equiv \frac{R_A^{k_B} \cdot SK}{R_B^{k_A}} \equiv SK((\mathrm{mod}\ p)\mathrm{mod}\ q)$$

에 의해 세션키를 생성하게 된다.

3.1.4 ElGamal의 변형 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅱ)

프로토콜 Ⅰ의 키분배 방식 대신 Park이 제안한 ElGamal의 변형 키분배 방식을 이용하는 키분배 프로토콜을 제안한다. 이 프로토콜 Ⅱ는 Okamoto의 방식과 연산처리는 비슷하지만, 만약 각 사용자가 상호 인증(mutual authentication)이 필요할 경우에는 Okamoto의 방식보다 더 효율적으로 대체할 수 있는 장점이 있다. ElGamal의 변형 키분배 방식은 Okamoto의 방식에서와 마찬가지로 키에 대한 인증이 포함되어 있다. 프로토콜 Ⅱ에서 사전처리 과정은 프로토콜 Ⅰ과 같으며, 프로토콜 Ⅱ에서 사용한 파라미터 또한 프로토콜 Ⅰ과 같다.

〈키분배 과정〉

① ~ ③은 프로토콜 Ⅰ과 동일하다.

④ 사용자 인증은 프로토콜 Ⅰ과 동일하며, A의 정당성이 확인되면 사용자 B를 호출(call)함과 동시에 $ID_A||ID_B||t_A$, R_A, R_{C2}를 전송한다.

⑤ 사용자 B는 R_{C2}를 이용하여 프로토콜 Ⅰ과 같은 방법으로 사용자 인증을 계산하고, 키분배를 하기 위하여

$$R_{AB} = R_A^{k_B} \oplus SK$$

를 계산한다.

⑥ 사용자 B는 센터에게 $ID_B||ID_A||t_B$, R_{AB}, R_{BC}, P_B, R_B를 전송한다.

⑦ 인증 과정은 프로토콜 Ⅰ과 동일하고, 사용자 A에게 R_{AB}, R_B를 전송한다.

⑧ 사용자 A는

$$SK = R_B^{k_A} \oplus R_{AB}$$

에 의해 세션키를 생성하게 된다.

3.2 Fiat-Shamir의 인증 방식과 새롭게 제안하는 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅲ)

프로토콜 Ⅰ, Ⅱ에서는 키분배 방식에서 요구하는 사전처리가 매우 큰 지수승 연산이기 때문에 연산처리횟수가 매우 커져서 실질적인 통신을 수행하는 데 큰 문제가 있다.

Fiat-Shamir의 인증 방식은 ID를 기본으로 하며, 연산처리의 수행이 RSA 방식이나 Schnorr의 인증 방식에 비해 매우 빠른, 고속 인증 방식이다. 그러나 키분배 프로토콜에 Fiat-Shamir의 인증 방식을 이용하는데 알맞는 키분배 방식이 없기 때문에 각 사용자의 비밀키와 공개키로 구성되는 키분배 방식을 이용하는 새로운 키분배 프로토콜을 제안한다.

3.2.1 프로토콜 Ⅲ에서 사용하는 파라미터

프로토콜 Ⅲ에서 사용하는 파라미터는 기본적으로 Fiat-Shamir의 인증 방식에서 사용된 파라미터와 동일하다.

- 큰 두개의 소수 p, q
- $2^{511} < n < 2^{512}$인 양의 정수, $n = pq$
- 의사 랜덤 함수 $f : Z_n \times Z \rightarrow \{1,\cdots,2^k-1\}$
- 세션키 $SK : Z_n \times Z \rightarrow \{1,\cdots,2^k-1\}$
- 공개키 $v_i, (i = 1,\cdots,k)$
- 비밀키 $s_i \in Z_n, (i = 1,\cdots,k)$이고, $s_i \equiv v_i^{-1/2} \pmod n$

3.2.2 키분배 프로토콜 Ⅲ

Fiat-Shamir의 개인식별 방식을 사용자 인증 방식으로 하고, Fiat-Shamir의 개인식별 방식을 변형시킨 키분배 방식을 결합시켜서 다음과 같은 키분배 프로토콜을 구성한다.

① 랜덤수 R_A를 생성하여 $f(R_A^2 \pmod n, ID_A||ID_B||t_A) = e_{A1}, e_{A2}, \cdots, e_{Ak} = E_A$를 계산하고, 개인식별,

$$P_A = R_A \prod_{j=1}^{k} S_{Aj}^{e_{Aj}}$$

을 계산한다.

② 사용자 A는 $ID_A||ID_B||t_A$, E_A, P_A를 센터에게 전송한다.

③ 센터는

$$f(P_A^2 \prod_{j=1}^{k} v_{Aj}^{e_{Aj}}, ID_A||ID_B||t_A) \stackrel{?}{=} E_A$$

를 확인하여 A가 정당한 사용자인가를 확인하고, 사용자 B에게 E_A를 전송한다.

④ 사용자 B는 R_B를 생성하여 $f(R_B^2 \pmod n, ID_B||ID_A||t_B) = e_{B1}, e_{B2}, \cdots, e_{Bk} = E_B$를 계산하고, 개인 식별

$$P_B = R_B \prod_{j=1}^{k} S_{Bj}^{e_{Bj}}$$

을 계산한다.

⑤ B는 랜덤수 E_A를 이용하여 $E_{AB} = E_A E_B = e_{AB1}, e_{AB2}, \cdots, e_{ABk}$를 계산하고,

$$R_{SK} = R_B \prod_{j=1}^{k} (v_{Aj} S_{Bj})^{e_{ABj}}$$

를 계산한다. 사용자 B는 세션키,

$$SK = R_B \prod_{j=1}^{k} S_{Bj}^{e_{ABj}}$$

를 생성한다.

⑥ 사용자 B는 $ID_B||ID_A||t_B$, P_B, P_{SK}, E_B, E_{AB}를 센터에게 전송한다.

⑦ 센터는

$$f(P_B^2 \prod_{j=1}^{k} v_{Bj}^{r_{Bj}},\ ID_B||ID_A||t_B) \stackrel{?}{=} E_B$$

를 확인하여 B가 정당한 사용자인가를 확인하고, 사용자 A에게 R_{SK}, E_{AB}를 A에게 전송한다.

⑧ 사용자 A는

$$\begin{aligned} SK &= R_{SK} \prod_{j=1}^{k} S_{Aj}^{2r_{ABj}} \\ &= R_B \prod_{j=1}^{k} v_{Aj}^{r_{ABj}} S_{Aj}^{2r_{ABj}} S_{Bj}^{r_{ABj}} \\ &= R_B \prod_{j=1}^{k} S_{Bj}^{r_{ABj}} \end{aligned}$$

를 계산하여 세션키를 생성하게 된다.

⑨ 위와 같은 각 사용자 인증은 t회, 키분배 방식은 S회 반복한다.

4. 제안하는 세가지 키분배 프로토콜에 대한 안전성 및 효율성 분석

4.1 안전성

Schnorr의 개인식별 방식을 이용하는 키분배 프로토콜 Ⅰ, Ⅱ는 이산대수의 계산이 어렵다는 데에 근거한 Okamoto의 키분배 방식과 ElGamal의 변형 키분배 방식을 이용하기 때문에 세션키 R_{AB}는 안전하다고 볼 수 있다.

Fiat-Shamir의 개인식별 방식을 이용하는 프로토콜 Ⅲ은 평방 잉여 제곱근 분해의 어려움에 근거하는 키분배 프로토콜이다. 이 프로토콜에서 사용되는 키분배 방식은 송신자 자신의 비밀키와 수신자의 공개키를 이용하기 때문에 자신의 비밀키가 공개키에 의해 노출되지만 않는다면 키분배 방식은 안전하다.

여기서 제안하는 모든 프로토콜은 replay attack에 대해서는 time-stamp를 이용하여 공격에 대비했으며, 특히 센터에 사용자의 비밀정보가 노출되지 않는 Schnorr의 방식과 Fiat-Shamir의 방식을 이용했기 때문에 센터와의 협잡과 센터의 부정방지 등에 대해서는 기존의 프로토콜에 비해 매우 안전하다. 표 1은 본 논문에서 제안하는 프로토콜과 기존의 프로토콜에 대해서 여러가지 공격에 대한 안전성을 비교한 것이다.

표 1. 본 논문에서 제안하는 세가지 프로토콜과 기존의 프로토콜에 대한 안전성의 비교

분류 / 프로토콜		사용자 인증	키분배	Replay Attack 방지	상호 인증	협잡 방지	센터 부정방지
Tatebayashi		○	○	○	×	×	×
Park	Ⅰ	○	○	○	×	○	×
	Ⅱ	○	○	○	○	○	○
Yun		○	○	○	×	○	○
제안방식	Ⅰ	○	○	○	×	○	○
	Ⅱ	○	○	○	×	○	○
	Ⅲ	○	○	○	×	○	○

4.2 효율성

연산처리량을 비교하기 위하여 각각의 키분배 프로토콜에서 사용하는 파라미터로서, 이전에 제안했던 RSA 방식에서는 n = 512로, Schnorr의 개인식별 방식과 새롭게 제안하는 개인식별 방식에서는 각각 t = 72, p = 512, q = 160으로, 또한 Fiat-Shamir의 방식에서는 k = 9, t = 8, n = 512로 구성한다. 프로토콜에서의 사용자 인증 방식의 연산처리에 관한 비교를 표 2에 나타내었다.

표 2. 사용자 인증에 이용되는 인증 방식의 연산처리 비교
(Exp(·)는 지수승 계산, M(·)는 곱셈 계산)

분류 / 방식	Trusted Center	연산수			총계	
		전처리	인증	확인		
RSA	불필요	—	Exp(1)	M(2)	Exp(2)+M(2)	M(752)
Schnorr	필요	Exp(1)	M(1)	Exp(2)	Exp(3)+M(1)	M(721)
제안한 방식	필요	Exp(2)	M(2)	Exp(2)+M(1)	Exp(4)+M(3)	M(963)
Fiat-Shamir	필요	--	M(45)	M(45)	M(90)	M(90)

여기서 Schnorr의 방식과 제안하는 방식에서의 Exp(1)은 대략 M(240) 정도의 곱셈 연산에 해당하고, RSA 방식의 Exp(1)는 약 M(750) 정도의 곱셈 연산에 해당한다[11]. 표 2는 Fiat-Shmair의 방식이 RSA 방식이나, Schnorr 방식, 제안하는 방식보다 연산처리가 매우 빠름을 나타낸다. 그러나 스마트 카드의 연산처리 속도를 향상시키거나, 보다 효율적인 사전처리 과정을 통해 RSA 방식이나, Schnorr의 방식, 제안하는 방식의 연산처리 속도를 증가시킬 수 있다. 표 2를 보면 본 논문에서 제안하는 Schnorr의 방식을 변형시킨 개인식별 방식은 원래의 Schnorr의 방식과 비교해 볼 때 센터가 전송하는 랜덤수 R_G에 의해 연산처리에 있어서 지수승이 1회 증가하므로 원래의 방식보다 효율이 나빠짐을 알 수 있다. 그러나 본 논문에서 제안하는 키분배 프로토콜에서는 센터가 전송하는 랜덤수 R_G의 지수승 연산이 전체 프로토콜의 비도에 큰 영향을 주지 못하므로, 센터는 사전처리 과정에서의 연산처리가 생략된 자연 발생적인 512비트의 랜덤수를 발생하여 전송하므로써, 원래의 Schnorr의 방식에 비해 계산적인 큰 차이가 없이 사용자 인증의 효율을 높일 수 있다. 또한 이 Schnorr의 방식을 변형시킨 개인식별 방식을 디지틀 서명으로 사용할 때, 키분배가 되지 않은 상태에서는 R_B가 수신된 후에 실질적으로 서명이 시작되므로 Schnorr의 방식과는 달리 사전처리 과정 후의 연산처리가 지연된다. 그러나 디지틀 서명을 세션키가 분배되는 통신로에서 사용하려는 경우, 세션키가 분배된 후의 서명 과정에서 새로 제안하는 개인식별 방식의 ① ~ ②가 생략되기 때문에 연산처리량은 Schnorr의 방식보다 적어진다. 따라서 호접속시 세션키를 분배하는 디지틀 이동통신에서 디지틀 서명을 수행할 때는 새로 제안하는 개인식별 방식을 서명으

로 이용하게 되면 사전처리 과정을 생략할 수 있으므로 연산처리량면에서 매우 효율적이다.

새로 제안하는 프로토콜과 기존에 제안한 Yun 프로토콜을 연산처리량면에서 비교하면 표 3과 같다. 같은 비도에서 비교하기 위해 RSA 방식을 이용하는 키분배 프로토콜(Yun 프로토콜)에서는 $e = 3$, $n = 512$로, Schnorr의 방식을 이용하는 프로토콜(프로토콜 Ⅰ, Ⅱ)에서는 각각 $t = 72$, $p = 512$, $q = 160$으로, Fiat-Shmair의 방식을 이용하는 프로토콜(프로토콜 Ⅲ)에서는 $k = 9$, $t = 8$, $n = 512$로 정했다.

표 3. 새로 제안하는 프로토콜에서의 연산처리량의 비교
(Exp(·)는 지수승 계산, M(·)는 곱셈 계산)

		연산수			
		키분배	인증	총계	
Yun		Exp(4)+M(2)	Exp(6)+M(4)	Exp(10)+M(6)	M(3216)
제안하는 프로토콜	Ⅰ	Exp(4)+M(2)	Exp(4)+M(6)	Exp(8)+M(8)	M(1928)
	Ⅱ	Exp(4)	Exp(4)+M(6)	Exp(8)+M(6)	M(1926)
	Ⅲ	M(128)	M(90)	M(218)	M(218)

프로토콜 Ⅲ은 Fiat-Shmair의 방식을 이용하기 때문에 프로토콜 Ⅰ, Ⅱ보다 수행 속도가 매우 빠르다. 그러나 같은 비도를 갖기 위해서는 키분배를 할 때, 매우 많은 데이터량이 필요하다.

스마트 카드내에 저장되는 비밀정보와 공개정보의 데이터량과, 프로토콜을 수행하는 데 필요한 데이터량을 비교하면 표 4와 같다. 이 표에 나타낸 모든 키분배 프로토콜에는 $(ID_i||ID_j||t_i)$가 똑같이 추가되므로 실질적인 데이터량이 그 만큼 증가하지만 비교에서는 제외했다.

표 4. 새로 제안하는 프로토콜을 수행하는 데 필요한 데이터량의 비교 (단위 : 비트(bits))

		데이터량			
		비밀정보	공개정보	인증 및 키분배	총계
Yun		512	512	1024	2048
제안하는 프로토콜	Ⅰ	160	1696	480	2336
	Ⅱ	160	1696	480	2336
	Ⅲ	36864	1512	232	38608

5. 결 론

본 논문에서는 이동통신 시스템을 위한 세가지 키분배 프로토콜을 제안했다. 이 프로토콜들은 ID를 기본으로 하는 인증 방식을 이용하고 있는데, 프로토콜 Ⅰ과 Ⅱ는 Schnorr의 인증 방식을 이용하고, 프로토콜 Ⅲ은 Fiat-Shamir의 인증 방식을 이용한다. 그러나 Schnorr의 인증 방식을 그대로 이용하는 데 있어서 세션키의 빈번한 통신횟수에 따른 랜덤수의 중복 사용으로 인한 비밀키의 노출을 피하기 위해 프로토콜 Ⅰ과 Ⅱ에서는 새로운 개인식별 방식을 이용한다. 프로토콜 Ⅰ과 Ⅱ는 단말기에서 인증에 필요한 연산처리량이 매우 적기 때문에 이동통신 시스템과 같이 단말기 크기에 제한이 있는 시스템에 적합하다. 그러나 프로토콜 Ⅰ과 Ⅱ는 키분배 과정에서 계산량이 그래도 많다. 따라서 보다 효율적인 키분배를 위하여 Fiat-Shamir의 인증 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅲ)도 제안했다.

제안한 프로토콜과 RSA 방식을 기본으로 하는 키분배 프로토콜을 종합적으로 비교하면 표 5와 같다. 이 표에서 프로토콜 Ⅰ과 Ⅱ는 이동국 단말기에서 인증시 필요한 연산처리량이 RSA 방식을 기본으로 하는 Yun 프로토콜과 비교하면 적지만, 프로토콜 Ⅲ과 비교하면 상당히 많다. 연산처리량면에서 비교하면, 프로토콜 Ⅲ이 가장 적어 매우 효율적이다. 그러나 프로토콜 Ⅲ은 프로토콜에서 수행되는 데이터량이 다른 프로토콜에 비해 많다. 또, 센터와 단말기에서의 연산처리의 분담면에서 살펴보면 프로토콜 Ⅰ과 Ⅱ는 인증에 필요한 대부분의 계산을 센터가 수행하기 때문에 다른 프로토콜에 비해 이동국 단말기의 처리 부담이 매우 적다.

따라서 연산처리 속도가 빠른 스마트 카드일 경우에는 프로토콜 Ⅰ과 Ⅱ가 더 효율적이고, 데이터의 저장 능력이 큰 스마트 카드일 경우에는 프로토콜 Ⅲ이 더 효율적이라고 할 수 있겠다.

표 5. 프로토콜의 장·단점 비교

비교 / 방식	연산처리량	데이터량	센터와 단말기의 연산처리 분담
Yun 프로토콜	가장 크다	Ⅲ에 비해 매우 적다	단말기와 센터에서의 처리량이 같다
프로토콜 Ⅰ과 Ⅱ	Yun 프로토콜에 비해 적으나, 프로토콜 Ⅲ에 비해 매우 크다		단말기의 연산을 센터에서 대부분 처리
프로토콜 Ⅲ	가장 적다	가장 크다	단말기와 센터에서의 처리량이 같다

참 고 문 헌

[1] *GSM Recommendation*, GSM 03.20, Jan. 1991.

[2] EIA/TIA Standards, *Common Cryptographic Algorithm*

[3] W. Diffie and M. E. Hellman, "New directions in cryptography,", IEEE Trans. on Information Theory, vol. IT-22, pp. 644-654, 1978.

[4] C. P. Schnorr, "Efficient identification and signature for smart cards," Proc. Eurocrypt '89, pp. 161-174, 1989.

[5] A. Fiat and A. Shamir, "How to prove yourself : Practical solution to identification and signature problem," Proc. Crypto '86, pp. 186-194, 1986.

[6] M. Tatebayashi, N. Matsuzaki, and D. B. Newman, Jr., "Key distribution

protocol for digital mobile communication systems," Proc. Crypto '89, pp. 324-333, 1990.

[7] C. Park, K. Kurozaya, "A secure and effective key distribution protocol in communication systems," Proc. ISEC' 92-39, 1992.

[8] 윤장근, 문태욱, 조성준, "이동통신 시스템을 위한 키분배 방식에 관한 연구," 통신정보합동 학술대회 논문집 제3권, pp. 357-360, 1993.

[9] R. Akiyama, S. Sasaki, "Authentication and encryption in a mobile communication system," Proc. 43rd IEEE VT Conference, pp. 927-930, 1993.

[10] *Specification for a Digital Signature Standard*, NIST, FIPS XX, Draft, Aug. 1991.

[11] E. Fujisaki, T. Okamoto, "On comparision of digital signature scheme," Proc. SCIS '92, pp. 1A, 1992.

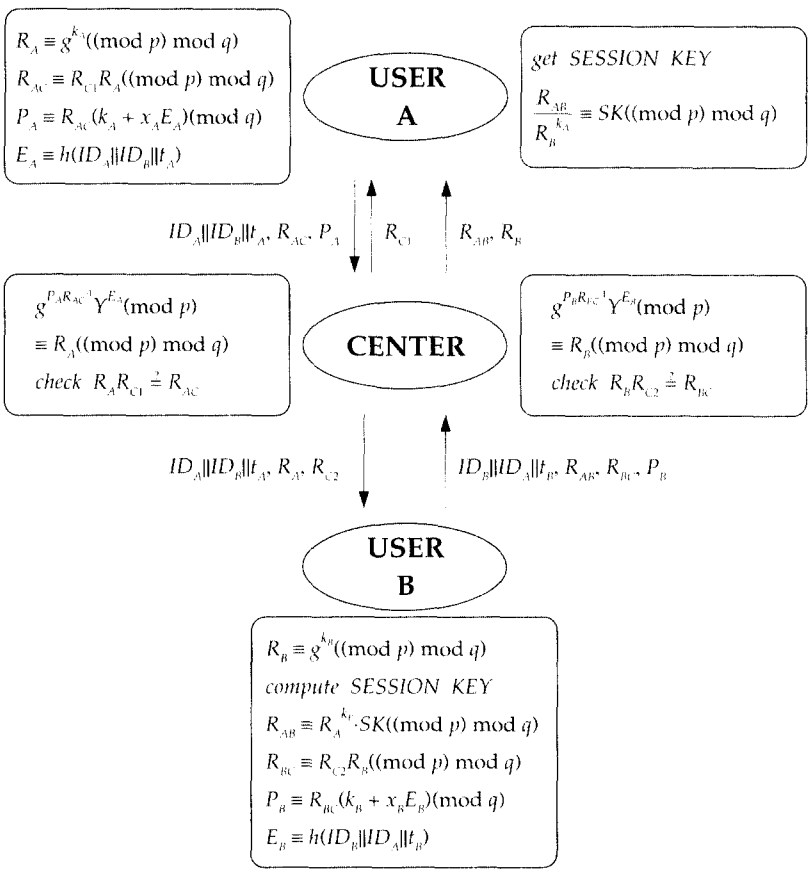


그림 1. Okamoto의 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 I)

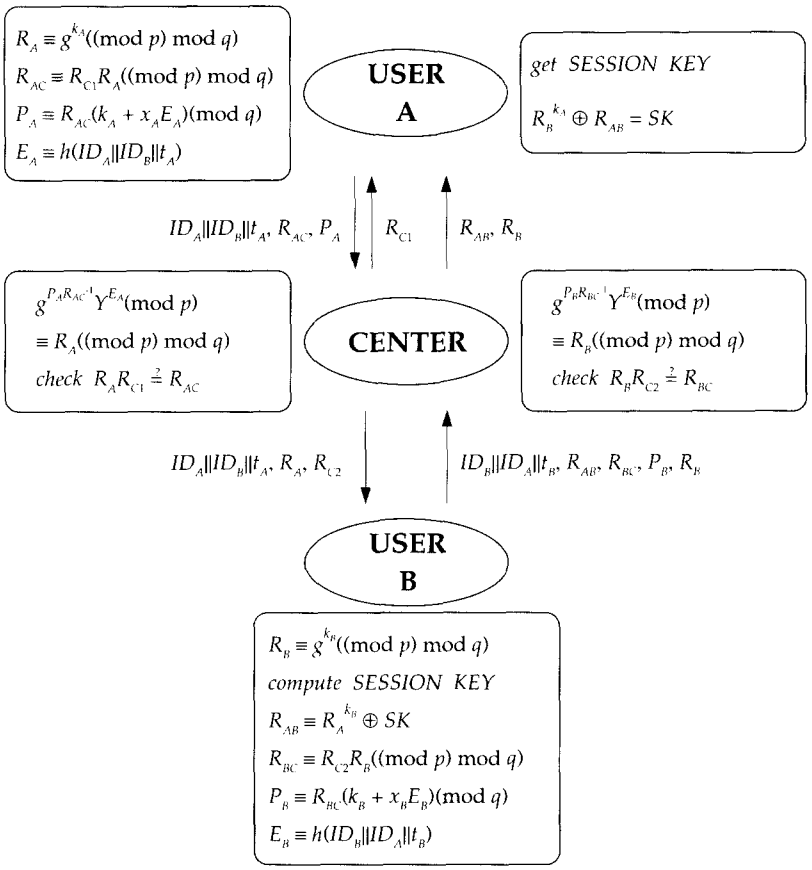


그림 2. ElGamal의 변형 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅱ)

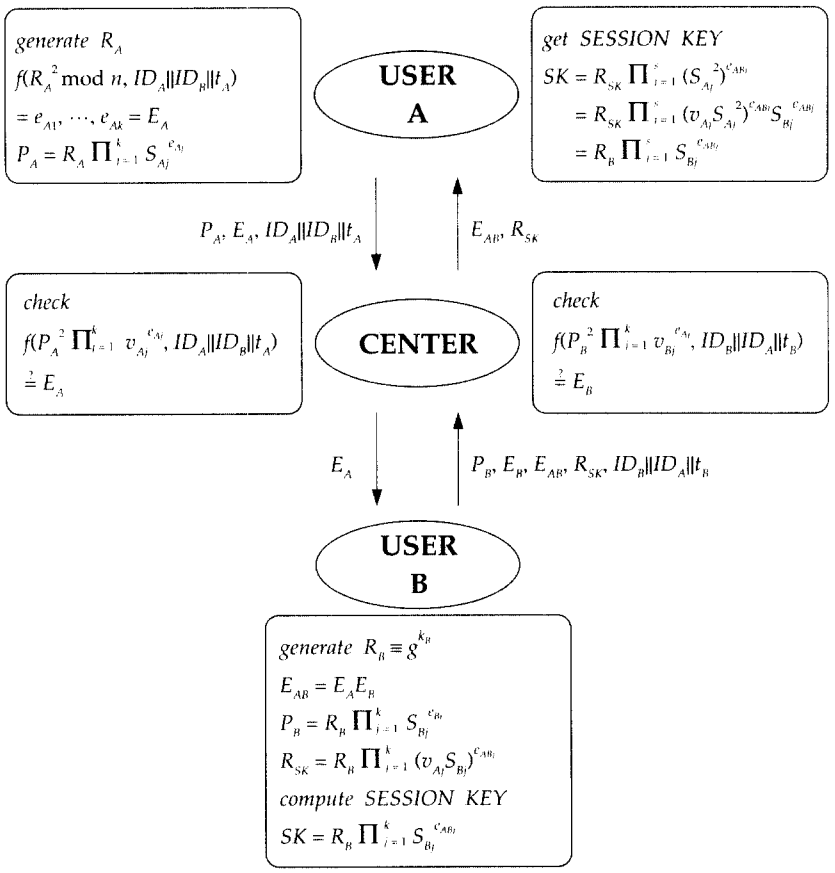
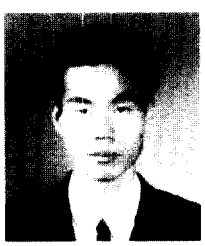


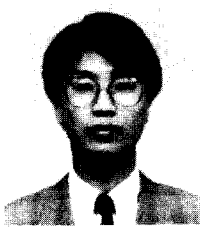
그림 3. Fiat-Shamir의 인증 방식과 새로운 키분배 방식을 이용하는 키분배 프로토콜(프로토콜 Ⅲ)

□ 著者紹介



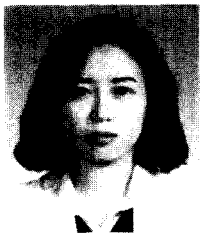
문 태 욱 (정 회 원)

1992년 2월 : 한국항공대학교 항공통신정보공학과 졸업(공학사)
1994년 8월 : 한국항공대학교 대학원 항공통신정보공학과 졸업(공학석사)
1994년 9월 ~ 현재 : 주식회사 스탠더드 텔레콤 부설 정보통신 연구소 연구원



박 상 우 (정 회 원)

1989년 2월 : 고려대학교 사범대학 수학교육과 졸업(이학사)
1991년 8월 : 고려대학교 대학원 수학과 졸업(이학석사 : 응용수학 및 확률론)
1991년 9월 ~ 현재 : 한국전자통신연구소 연구원



이 정 숙 (학생회원)

1991년 2월 : 한국항공대학교 항공통신정보공학과 졸업(공학사)
1993년 9월 ~ 현재 : 한국항공대학교 대학원 항공통신정보공학과 석사과정

조 성 준 (정 회 원)

1969년 2월 : 한국항공대학 항공통신공학과 졸업(공학사)
1975년 2월 : 한양대학교 대학원 졸업(공학석사)
1981년 3월 : 오사카대학 대학원 졸업(공학박사)
1972년 8월 ~ 현재 : 한국항공대학교 항공통신정보공학과 교수