디지틀 이동통신 시스템에서 스마트 카드를 이용하는 키분배 프로토콜의 분석 및 개선방안

김승주°, 박성준, 원동호
성균관대학교 정보공학과

Analysis and Improvement of Key Distribution Protocols using Smart Card in Digital Mobile Communication Systems

Seung Joo Kim, Sung Jun Park and Dong Ho Won
Department of information Engineering
Sung Kyun Kwan University
E-mail : sjkim@danjae.skku.ac.kr

요 약

본 논문에서는 기존에 문태욱 등이 제안한 이동통신용 키분배 방식을 살펴보고, 이 세 가지 키분배 프로토콜의 문제점을 제기하며, 이를 해결할 수 있는 개선방안도 제시한다.

1. 서 론

이동통신망은 언제, 어디서, 누구와도 어떤 종류의 통신이 가능토록 하는 것을 목적으로, 인간의 생활 영역이 확대되는데 따라 시간과 공간의 제약을 극복할 수 있는 통신수단으로서 하루가 다르게 발전하고 있다. 이동통신망의 전송 매체는 대기이므로 근본적으로 유선을 이용하는 통신에서 보다 정보보호 측면에서 취약하다. 즉, 정보의 유출이나 정보의 불법 수정 등이 쉽기 때문에 정보 보호의 필요성이 대두된다.

디지틀 이동통신 시스템용 키분배 프로토콜은 Tatebayashi가 처음 제안하였다.[1] 이 프로토콜은 센터가 사용자 인증과 키분배에 직접적으로 관여하여 사용자 터미널의 암호화 연산처리를 분담하는 프로토콜이다. 이 프로토콜에서는 uplink에 RSA 암호방식 중 e = 3을 사용하고, downlink에서 쌍자대치 암호(Vernam cipher를 사용한다. 따라서 매우 빠른 암호화가 수행되지만 비도가 그리 높지 않고, 또한 통신 상대방의 두 가입자인 A와 B가 세번만 통신하게 되면 B는 A의 랜덤수 r_A를 알게 된다. 또한 네트워크 센터는 가입자간의 대화키를 모두 알 수 있기 때문에 모든 가입자의 통신을 쉽게 도청할 수 있다는 단점이 있다.

이러한 문제점을 개선한 키분배 프로토콜이 박춘식 등이 제안한 키분배 프로토콜이다.[2][3] 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.

윤장근 등은 Tatebayashi와 박춘식 등이 제안한 키분배 프로토콜의 장·단점을 상호 보완하기

위하여 RSA 방식을 이용한 키분배 프로토콜을 제안하였다.[4] 이 키분배 프로토콜은 RSA 방식을 이용하기 때문에 박춘식 등이 제안한 키분배 프로토콜보다는 연산처리량이 적지만 같은 비도를 가지며, Tatebayashi가 제안한 키분배 프로토콜보다는 많은 연산처리량을 가지면서 보다 나은 비도를 가진다. 그러나 이 키분배 프로토콜도 상당히 많은 연산처리가 요구되므로 단말기에서 처리해야 하는 연산을 좀 더 줄일 필요가 있다.

문태욱 등은 스마트 카드를 이용하는 보다 효율적인 세 가지의 키분배 프로토콜을 새로이 제안하였다.[5] 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. 프로토콜 III은 Fiat-Shamir의 개인식별 방식과 이 개인식별 방식을 기본으로 새롭게 구성한 키분배 방식을 결합한 것이다.

본 논문에서는, 2장에서 기존에 문태욱 등이 제안한 세 가지 이동통신용 키분배 방식을 살펴보고, 이어 3장에서는 각각의 문제점을 분석하고 이를 극복할 수 있는 개선방안을 제시하고자 한다.

2. 기존의 이동통신 시스템용 키분배 프로토콜

문태욱 등은 스마트 카드를 이용하는 효율적인 세 가지의 키분배 프로토콜을 새로이 제안하였다.[5] 프로토콜 I과 II는 Schnorr의 인증 방식을 이용하고, 프로토콜 III은 Fiat-Shamir의 인증 방식을 이용한다. 그러나 Schnorr의 인증 방식을 그대로 이용하는 데 있어서 세션키의 빈번한 통신 횟수에 따른 랜덤수의 중복 사용으로 인한 비밀키의 노출을 피하기 위해 프로토콜 I과 II에서는 새로운 개인식별 방식을 이용했다.

[5]에 의하면, 세 가지 프로토콜에 대한 안전성은 다음과 같다.

분류 / 프로토콜		사용자 인증	키분배	Replay Attack 방지	상호인증	협잡방지	센터 부정방지
Tatebayashi		O	O	O	×	×	×
Park	I	O	O	O	×	O	×
	II	O	O	O	O	O	O
Yun		O	O	O	×	O	O
Moon	I	O	O	O	×	O	O
	II	O	O	O	×	O	O
	III	O	O	O	×	O	O

표 1. 문태욱 등이 제안하는 프로토콜과 기존의 프로토콜에 대한 안전성의 비교

2.1 Moon I (Okamoto의 키분배 방식을 이용하는 키분배 프로토콜)

< 사전처리 과정 >

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

< 키분배 과정 >

① 센터는 사용자 A의 통신 요청에 의해 랜덤수 R_{C1}을 사용자 A에게 전송한다.
② 사용자 A는

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

단, $R_{AC} = R_{C1} R_A \pmod p \bmod q$
$E_A = h(ID_A||ID_B||t_A)$

를 계산한다.
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,

$$g^{P_A R_{AC}^{-1}} Y_A^{E_A} \pmod p \equiv R_A \pmod p \bmod q$$

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

$$R_{AB} \equiv R_A^{k_B} \cdot SK \pmod p \bmod q$$

를 계산한다. 그 후 자신의 사용자 인증,

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

단, $R_{BC} = R_{C2} R_B \pmod p \bmod q$
$E_B = h(ID_B||ID_A||t_B)$

를 계산한다.
⑥ 사용자 B는 센터에게 $ID_B||ID_A||t_B$, R_{AB}, R_{BC}, P_B를 전송한다.
⑦ 센터는 전송된 R_{BC}를 이용하여,

$$g^{P_B R_{BC}^{-1}} Y_B^{E_B} \pmod p \equiv R_B \pmod p \bmod q$$

를 계산하고, $R_B R_{C2} = R_{BC}$? 에 의해 B의 정당성을 확인하고, 정당한 사용자이면 사용자 A에게 R_{AB}, R_B를 전송한다.
⑧ 사용자 A는

$$\frac{R_{AB}}{R_B^{k_A}} \equiv \frac{R_A^{k_B} \cdot SK}{R_B^{k_A}} \equiv SK \pmod p \bmod q$$

에 의해 세션키를 생성하게 된다.

2.2 Moon II (ElGamal의 변형 키분배 방식을 이용하는 키분배 프로토콜)

< 사전처리 과정 >

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.

2.3 Moon III (Fiat-Shamir의 인증 방식을 이용하는 키분배 프로토콜)

< 파라미터 >

- 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 $SK : Z_n \times Z \rightarrow \{1, \cdots, 2^s-1\}$
- 공개키 v_i, $(i = 1, \cdots, k)$
- 비밀키 $s_i \in Z_n$, $(i = 1, \cdots, k)$이고, $s_i = v_i^{-1/2} \pmod n$

< 키분배 과정 >

① 사용자 A는 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

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

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, 개인식별,

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

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

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

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

⑧ 사용자 A는

$$SK = R_{SK} \prod_{j=1}^{k} S_{Aj}^{2\, e_{ABj}}$$

$$= R_B \prod_{j=1}^{k} V_{Aj}^{e_{ABj}}\ S_{Aj}^{2\, e_{ABj}}\ S_{Bj}^{e_{ABj}}$$

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

를 계산하여 세션키를 생성하게 된다.

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

3. 문제점 및 개선방안

본 장에서는 Moon 방식을 분석하여 문제점을 제기하고 이를 극복할 수 있는 개선방안을 제시하고자 한다.

3.1 Moon I, II의 문제점 및 개선방안

키분배 프로토콜 I, II에 이용되는 변형된 Schnorr의 개인식별 방식은 k의 중복사용에 의해 비밀키가 노출될 위험이 있으며 특히, E 값을 미리 예측할 수 있으므로 프로토콜에 대한 공격을 훨씬 용이하게 한다. 즉, 제3자가 사용자 A의 비밀키를 모르더라도 키분배 프로토콜에 이용되는 개인식별 방식을 통과할 수 있다.

< 문제점 (1) >

① 제3자는 k를 반복하여 사용한 R'_{C1}, E'_A, R'_{AC}, P'_A, R''_{C1}, E''_A, R''_{AC}, P''_A를 얻는다.
② 제3자는

$$(1)\ \left(\frac{P'_A}{R'_{AC}}\right) = k_A + x_A E'_A \pmod q$$

$$(2)\ \left(\frac{P''_A}{R''_{AC}}\right) = k_A + x_A E''_A \pmod q$$

를 이용하여 x_A를 계산할 수 있다.

< 문제점 (2) >

① 제3자는 R'_{C1}, E'_A, R'_{AC}, P'_A를 얻는다.
② 센터는 제3자의 통신 요청에 의해 랜덤수 R_{C1}을 제3자에게 전송한다.
③ 제3자는

$$E_{제3자} = h(ID_A||t_{제3자})$$

를 계산한다.
④ (1) 제3자는 다음을 만족하는 x를 계산한다.

$$E_{제3자} = x \cdot E'_A \pmod q$$

(2) 제3자는 x와 y를 이용하여 $R_{제3자C}$를 계산한다.

㉠ $R_{제3자} = \left(\frac{R'_{AC}}{R'_{C1}}\right)^x \ ((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$

㉡ $R_{제3자C} = R_{C1} \cdot R_{제3자} \ ((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$

⑤ 제3자는

$$P_{제3자} = R_{제3자C} \cdot x \cdot \left(\frac{P'_A}{R'_{AC}}\right) \pmod q$$

를 계산한다.
⑥ 제3자는 센터에게 $ID_A||t_{제3자}$, $R_{제3자C}$, $P_{제3자}$를 전송한다.
⑦ 센터는 전송된 $R_{제3자C}$를 이용하여,

$$g^{P_{제3자} R_{제3자C}^{-1}} Y_A^{E_{제3자}} \pmod p \equiv R_{제3자} \ ((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$$

를 계산하고, $R_{제3자}R_{C1} = R_{제3자C}$? 에 의해 제3자의 정당성을 확인한다.

< 개선방안 >

① 센터는 사용자 A의 통신 요청에 의해 랜덤수 R_{C1}을 사용자 A에게 전송한다.
② 사용자 A는

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

단, $R_{AC} = R_{C1}^{k_A} \ ((\mathrm{mod}\ p)\ \mathrm{mod}\ q)$

$$E_A = h(R_A, ID_A||ID_B||t_A)$$

를 계산한다.
③ 사용자 A는 센터에게 $ID_A||ID_B||t_A$, E_A, P_A, R_A를 전송한다.

여기서 ID_A는 A의 ID, ID_B는 B의 ID, t_A는 time-stamp를 나타낸다.

④ 센터는 전송된 R_A를 이용하여,

$$R_{AC} = R_A^{k_{C1}} \ ((\text{mod } p) \text{ mod } q)$$

를 계산한다. 그 후,

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

를 계산하고, $E_A = h(R_A, ID_A||ID_B||t_A)$? 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

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

를 계산한다. 그 후 자신의 사용자 인증,

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

단, $R_{BC} = R_{C2}^{k_B} \ ((\text{mod } p) \text{ mod } q)$

$$E_B = h(R_B, ID_B||ID_A||t_B)$$

를 계산한다.

⑥ 사용자 B는 센터에게 $ID_B||ID_A||t_B$, E_B, P_B, R_B, R_{AB}를 전송한다.

⑦ 센터는 전송된 R_B를 이용하여,

$$R_{BC} = R_B^{k_C} \ ((\text{mod } p) \text{ mod } q)$$

를 계산한다. 그 후,

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

를 계산하고, $E_B = h(R_B, ID_B||ID_A||t_B)$? 에 의해 B의 정당성을 확인하고, 정당한 사용자이면 사용자 A에게 R_{AB}, R_B를 전송한다.

⑧ 사용자 A는

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

에 의해 세션키를 생성하게 된다.

Remark : 프로토콜 II도 프로토콜 I과 동일하다.

3.2 Moon III의 문제점 및 개선방안

본 절에서는 Fiat-Shamir의 개인식별 방식을 이용하는 프로토콜 III이 센터와의 협잡과 부정방지 등에 대해서 안전하지 못하며, 제3자가 사용자 A와 사용자 B의 비밀키를 모르더라도 A의 공개키를 이용하여 A와 B의 세션키를 계산해 낼 수 있는 문제점이 있음을 지적한다.

< 문제점 >

Fiat-Shamir의 개인식별 방식을 이용하는 프로토콜 III은 ID를 기본으로 하는 인증 방식을 이

용하고 있으므로 망 운영 센터가 사용자에 대한 공개정보를 저장하고 인증시 데이터 베이스와 접속해야 할 필요는 없지만, 등록 과정에서 센터에 사용자의 비밀키가 노출되므로 센터와의 협잡과 부정방지 등에 대해서 안전하지 못하며 특히, 제3자는 사용자 A와 사용자 B의 비밀키를 모르더라도 A의 공개키 V_{Aj} (j = 1, ···, k)를 이용하여 A와 B의 세션키 SK_{AB}를 다음과 같이 계산해 낼 수 있다는 문제점이 있다.

$$SK_{AB} = R_{SK}\prod_{j=1}^{k}(V_{Aj}^{-1})^{e_{ABj}}$$

$$= (R_B\prod_{j=1}^{k}(V_{Aj}S_{Bj})^{e_{ABj}})\ \prod_{j=1}^{k}(V_{Aj}^{-1})^{e_{ABj}}$$

$$= R_B\prod_{j=1}^{k}(V_{Aj}V_{Aj}^{-1}S_{Bj})^{e_{ABj}}$$

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

4. 결 론

통신에서 정보의 개인적 침해나 불법 사용이 큰 문제가 되고 있으며, 특히 무선을 이용하는 이동통신에서의 정보보호의 중요성이 더욱 크게 부각되고 있다. 이동통신에서 공통키 암호시스템을 사용하는 경우에 빈번히 발생하는 세션키의 관리와 사용자에 대한 인증이 필요하기 때문에 키분배와 사용자 인증이 결합된 키분배 프로토콜이 연구되고 있다.

문태욱 등은 스마트 카드를 이용하는 효율적인 세 가지의 이동통신용 키분배 프로토콜을 제안하였다.

본 논문에서는 이 세 가지 키분배 방식을 분석하여 안전성에 문제가 있음을 밝혀내고, 이를 해결할 수 있는 개선방안을 제시하였다.

참 고 문 헌

[1] M. Tatebayashi, N. Matsuzaki. and D. B. Newman, Jr., "Key distribution protocol for digital mobile communication systems", Proc. Crypto'89, pp. 324-333, 1990.

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

[3] C. Park, K. Kurosawa and S. Tsujii, "A key distribution protocol for mobile communication systems", IEICE TRANS. FUNDAMENTALS, Vol. E78-A, No. 1, 1995. 1.

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

[5] 문태욱, 박상우, 이정숙, 조성준, "디지틀 이동통신 시스템에서 스마트 카드를 이용하는 키분배 프로토콜", 통신정보보호학회 논문지 제4권 제2호, pp. 3-16, 1994. 12.

[6] Beller, M.J., Chang, L.F. and Yacobi, Y., "Privacy and Authentication on a Portable Communication System", IEEE GLOBECOM '91 Conference, pp. 1922-1927, 1991.

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