이동통신 시스템을 위한 "역설적인" ID-Based 키분배 방식

최연이*○, 김성덕*, 양형규**, 원동호*

* 성균관대학교 정보공학과

** 강남대학교 전자계산학과

A "Paradoxical" ID-Based Key Distribution Protocol for Mobile Communication Systems

Yeon Yi Choi*, Sung Duk Kim*, Hyung Kyu Yang** and Dong Ho Won*

* Dept. of Information Engineering, Sung Kyun Kwan University

E-mail : yychoi@dosan.skku.ac.kr

** Dept. of Computer Science, Kangnam University

요 약

본 논문에서는 기존에 제안된 이동통신용 키분배 방식의 문제점을 분석하고, Girault가 제안한 자체인증 공개키(Self-certified public keys) 개념을 이용한, 인증자에 기반을 둔(Certification-based) 방식이 아닌 개인식별정보에 기반을 둔(Identity-based) 방식이면서도 사용자가 자신의 비밀키를 선택할 수 있는, 이동 통신망에 적용가능한 "역설적인" ID-based 키분배 방식을 제안한다.

제안한 방식의 안전성은 고차 잉여류 문제(γ^{th}-residuosity problem)와 이산대수(discrete logarithm) 문제에 근거한다.

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.

기존의 이동통신망은 크게 기지국과 가입자 단말로 분류되며, 가입자 단말에서는 전력이 제한되어 있으므로 기존에 통신망에 적용되고 있는 암호방식을 이동통신망에 적용하는 것은 무리가 따른다. 공개키 암호 알고리듬을 이용하는 경우 속도, 전력, 그리고 복잡도 측면에서 단말기에서의 전력 등의 제한을 극복할 수 없다. 이러한 제한을 극복하면서 가입자의 정보보호에 대한 요구를 만족시킬 수 있는 실현 가능하고 효율적인 암호방식 및 인증 방식에 대한 연구가 필요하

다.[1][2][3][6][7][8][9][10]

본 논문에서는, 2장에서 기존에 제안된 이동통신용 키분배 방식의 문제점을 분석하고, 이어 3장에서는 자체인증 공개키(Self-certified public keys) 개념을 이용한, 개인식별정보에 기반을 둔 방식이면서도 센터가 각 사용자의 비밀키를 알 수 없는, 이동통신을 위한 "역설적인" ID-Based 키분배 방식을 제안한다.[4][5][11][12][13][14][15] 제안한 방식은 인증자에 기반을 둔(Certification-based) 방식의 장점(센터가 각 사용자의 비밀키를 알 수 없음)과 개인식별정보에 기반을 둔 (Identity-based) 방식의 장점(인증자가 필요 없음)을 함께 지니고 있으며, 이동 단말기에서의 계산량을 최소화하고, 안전성 유형은 2와 3을 만족한다.

제안한 방식의 안전성은 고차 잉여류 문제(γ^{th}-residuosity problem)와 이산대수(discrete logarithm) 문제에 근거한다.

2. 기존의 이동통신용 키분배 방식

2.1 Tatebayashi 등이 제안한 방식

디지털 이동통신 시스템용 키분배 프로토콜은 Tatebayashi가 처음 제안하였다.[6] 이 프로토콜은 센터가 사용자 인증과 키분배에 직접적으로 관여하여 사용자 터미널의 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 대화키를 모두 알 수 있기 때문에 모든 가입자의 통신 내용을 쉽게 도청할 수 있다는 단점이 있다.

2.2 Park 등이 제안한 방식

Tatebayashi 등의 프로토콜의 문제점을 개선한 키분배 프로토콜이 Park 등이 제안한 키분배 프로토콜이다.[8][9] 이 프로토콜은 이산 대수(discrete logarithm)의 계산이 어렵다는 점에 근거하고 있는 ElGamal의 인증방식을 이용하는 프로토콜로서, Tatebayashi가 제안한 키분배 프로토콜의 문제점을 해결할 수는 있지만 계산량이 매우 많아지는 단점이 있으며, 망 운영 센터가 사용자에 대한 공개정보를 저장하고 인증시 데이터 베이스와 접속해야 한다.

3. 이동통신 시스템을 위한 "역설적인" ID-Based 키분배 방식의 제안

새로 제안하는 자체인증 공개키(Self-certified public keys) 방식에 기반을 둔 "역설적인" ID-Based 키분배 프로토콜은 이동 단말기에서의 계산량을 최소화하고, 개인식별정보에 기반을 둔 (Identity-based) 방식이므로 센터에서의 키관리가 용이하며, 센터가 각 사용자의 비밀키를 알 수 없는 신뢰 유형 2와 3을 만족하는 방식이다.

Remark : 제안하는 ID-Based 키분배 프로토콜은 개인식별정보에 기반을 둔 방식이면서도 사

용자가 자신의 비밀키를 선택할 수 있으므로 "역설적(Paradoxical)"이다.

3.1 등록 과정

이 단계에서는 사용자가 센터에 등록하고, 센터는 사용자의 신분을 확인하여 비밀 정보를 전달한다.

센터는 acceptable triple (n, γ^d, y)를 선택한다. 여기서, $n = p \times q = (2\gamma^d fp' + 1)(2fq' + 1)$, 단, f, p', q'는 서로 다른 소수이고 $\gcd(\gamma, q') = 1$, $\gcd(\gamma, f) = 1$, y는 $(\gamma^d)^{th}$-nonresidue (mod n)이고, b는 order가 f인 Z_n의 원소이다. 센터의 공개키는 (n, γ^d, y, b, f)이고 비밀키는 (p', q')이다.[18][19]

STEP 1. 각 가입자는 랜덤 수 $s(0 < s < f)$를 자신의 비밀키로 선택하여 b^s를 계산하고 b^s와 자신의 identity information ID를 센터에 전송한다.

STEP 2. 센터는 $ID = b^{-s} y^{-i} x^{-\gamma^d} \pmod n$ 를 만족하는 i, x를 계산하여 가입자에게 전송한다. 여기서 i는 $(ID_A\, b^s)^{-1}$ 의 class-index이다.

i와 x를 비밀키로 간주할 필요는 없다. 즉, 유일한 가입자의 비밀키는 s이다. 또한 센터는 가입자의 비밀키 s를 알 수 없다.

3.2 키분배 과정

이 단계는 통신할 때 사용할 대화키를 생성하기 위해, 원하는 통신 상대방과 통신하는 단계이다. A, B 두 사용자간에 세션키를 생성하는 과정을 설명하면 다음과 같다.

STEP 1. 이용자 A는 구간 [0, f-1] 에서 랜덤한 r_A를 선택한 후 다음을 계산한다.

① $K_A = b^{r_A} \bmod n$

② $e_A = h(K_A, t_A)$

단, t_A는 A의 time-stamp를 나타낸다.

③ $z_A = r_A + s_A e_A \bmod f$

STEP 2. 이용자 A는 ID_A, i_A, x_A, z_A, e_A, t_A를 센터에 전송한다.

STEP 3. 센터는 다음에 의해 A의 정당성을 확인하고, 정당한 사용자이면 사용자 B를 호출(call)함과 동시에 K_A를 전송한다.

① $K_A = (ID_A\, y^{i_A} x_A^{\gamma^d})^{e_A} b^{z_A}$

$= b^{r_A} \bmod n$

② $e_A = h(K_A, t_A)$?

STEP 4. 이용자 B는 구간 [0, f-1] 에서 랜덤한 r_B를 선택한 후 다음을 계산한다.

$$① K_B = b^{r_B} \bmod n$$

② $e_B = h(K_B, t_B)$
단, t_B는 B의 time-stamp를 나타낸다.

$$③ z_B = r_B + s_B e_B \bmod f$$

STEP 5. 이용자 B는 ID_B, i_B, x_B, z_B, e_B, t_B를 센터에 전송한다.

STEP 6. 센터는 다음에 의해 B의 정당성을 확인하고, 정당한 사용자이면 사용자 A를 호출(call)함과 동시에 K_B를 전송한다.

$$① K_B = (ID_B\, y^{i_B}\, x_B^{\gamma^d})^{e_B}\, b^{z_B}$$

$$= b^{r_B} \bmod n$$

② $e_B = h(K_B, t_B)$?

STEP 7. 이용자 A는 세션키 K_{AB}를 다음과 같이 계산한다.

$$K_{AB} = K_B^{r_A}$$

$$= b^{r_A r_B} \pmod n$$

이용자 B는 세션키 K_{AB}를 다음과 같이 계산한다.

$$K_{AB} = K_A^{r_B}$$

$$= b^{r_A r_B} \pmod n$$

4. 제안하는 키분배 프로토콜에 대한 안전성 및 효율성 분석

4.1 안전성 및 신뢰 유형

(1) 안전성

제안한 방식의 안전성은 고차 잉여류 문제(γ^{th}-residuosity problem)와 이산대수(discrete logarithm) 문제에 근거한다.

또한, Tatebayashi 등이 제안한 키분배 방식에서는 센터가 사용자의 모든 세션키를 알고 있기 때문에 도청이 가능하다. 그러나 본 논문에서 제안하는 키분배 방식에서는 센터의 역할은 단지 중계기로서의 역할을 할뿐이므로 센터와의 협잡, 센터에 의한 도청 등을 방지할 수 있다. 즉, 키 운영 센터는 사용자의 비밀정보 s를 유도할 수 없으므로 사용자간의 세션키를 구할 수 없다. 따라서 키 운영 센터는 암호화된 트래픽 정보에 대한 불법 도청 및 액세스를 할 수 없다. (표 1. 참조)

(2) 신뢰 유형

각 사용자의 비밀키 (s, i, x)에서 신뢰 센터가 계산하는 i와 x의 비밀성은 제안하는 키분배 방식의 안전성(센터가 알 수 없는 사용자의 비밀키 s에 대한 안전성)과 직접적인 관계가 없기 때문에 실질적으로 공개하여도 무방하다. 그러므로 i와 x를 공개 정보로 사용하여도 된다. 이는 바로 i와 x가 자체인증 공개키 역할을 하는 자체인증 공개키 방식이 된다.

즉, 각 사용자의 비밀키는 자신이 선택한 정보 s이고, 신뢰 센터가 계산한 공개 정보 i와 x는 자체인증이 가능한 공개키가 된다. 제안한 키분배 프로토콜은 인증자를 사용하지 않는다. 이는 물론 i와 x가 인증자 역할을 하게 되나, 특별한 인증 절차를 요구하지 않는다는 의미이다. 즉, 자체인증 공개키 방식이 된다.

물론 신뢰 센터는 사용자 A의 거짓 비밀키 s'를 생성하여 s'에 해당되는 i'와 x'를 생성하여 A로 가장할 수가 있다. 그러나 i와 x를 계산할 수 있는 능력을 보유한 것은 신뢰 센터뿐임으로 한 사용자에 대한 두 개의 공개 정보 i, i', x, x'는 바로 신뢰 센터의 거짓 행위에 대한 증거가 되므로 신뢰유형 3 - 신뢰 센터가 신뢰 유형 2와 마찬가지로 각 사용자의 비밀키를 알 수 없고, 또한 센터는 각 사용자를 흉내낼 수 없다. 여기서 흉내낼 수 없다 함은 실질적으로는 흉내를 낼 수 있으나 센터의 거짓 행위를 알 수 있다는 것이다. - 을 만족한다. (표 1. 참조 [3])

분류 / 프로토콜		사용자 인증	키분배	Replay Attack 방지	상호인증	협잡방지	센터 부정방지	센터의 공개정보 DB
Tatebayashi		O	O	O	×	×	×	×
Park	I	O	O	O	×	O	×	O
	II	O	O	O	O	O	O	O
Yun		O	O	O	×	O	O	O
제안방식		O	O	O	O	O	O	×

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

4.2 효율성

공개키 암호시스템을 이용하여 인증 기능을 수행하는 경우, 통신 상대방의 공개 암호키를 획득하는 방법은 각각의 사용자가 통신 가능성이 있는 모든 통신 상대의 공개키를 저장하는 방법, 비밀 통신에 앞서 상대방과 미리 통신하여 암호화키를 받는 방법, 그리고 키 센터에 상대의 공개키를 조회하는 방법 등이 있다. 이 때, 통신 상대의 암호키 보관 시에 발생하는 어려운 문제를 해결하기 위하여 ID에 의한 방식에 대한 연구가 널리 수행되고 있다.

제안한 키분배 방식은 통신 상대의 ID를 그대로 암호화 키로 사용하는 암호 방식 및 분배 방식으로 암호키 저장측면에서 여로가지로 효율적이다. 즉, 망 운영 센터가 사용자에 대한 공개정보를 저장하고 인증시 데이터 베이스와 접속할 필요가 없다. 더욱이 본 기법은 인증에 필요한 대부분의 계산을 센터가 수행하기 때문에 사용자 측면에서 계산량을 최소화한 개인통신망에 적용 가능한 효율적인 키분배 및 인증 방식이며, Schnorr의 방식에 바탕을 두어 처리속도면에서도 매우 효율적이다.[16][17]

5. 결 론

이동통신망에서의 정보보호는 매우 중요하다.

본 논문에서는 개인식별정보에 기반을 둔 방식이면서도 사용자가 자신의 비밀키를 선택할 수 있는, 이동 통신망에 적용가능한 "역설적인" ID-based 키분배 방식을 제안했다. 제안한 방식은 Girault가 제안한 자체인증 공개키 개념을 개인식별정보에 기반을 둔 방식에 적용한 것이다.

제안한 방식의 안전성은 고차 잉여류 문제(γ^{th}-residuosity problem)와 이산대수(discrete logarithm) 문제에 근거한다.

본 고에서 제안한 방식은 첫째, 센터와의 협잡, 센터에 의한 도청 등을 방지할 수 있으며, 둘째, 신뢰 유형은 2와 3을 만족하며, 셋째, 개인식별정보에 기반을 둔 방식이므로 암호키 저장측면에서 여로가지로 효율적이다. 넷째, 본 기법은 인증에 필요한 대부분의 계산을 센터가 수행하기 때문에 사용자 측면에서 계산량을 최소화한 개인통신망에 적용 가능한 효율적인 키분배 및 인증 방식이며, Schnorr의 방식에 바탕을 두어 처리속도면에서도 매우 효율적이다.

향후에는 좀 더 효율적인 이동통신을 위한 키분배 방식을 제안하고자 한다.

참 고 문 헌

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

[2] 염흥렬, 이만영, 김재공, "이동통신에 적용 가능한 인증 및 세션키 분배 방식과 키 스트림 생성기에 관한 연구", 통신정보보호학회지 제4권 제3호, pp. 5-20, 1994. 9.

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

[4] 박성준, 양형규, 원동호, "자체인증 개인식별정보", 한국통신정보보호학회 종합학술발표회 논문집 제4권 제1호, pp. 9-13, 1994.

[5] 박성준, 원동호, "고차잉여류 문제와 이산대수 문제에 기반을 둔 역설적인 id-based 암호시스템", 통신정보보호학회 논문지 제4권 제2호, pp. 113-118, 1994. 12.

[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] 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.

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

[9] 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.

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

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

[12] M. Girault, "Self-certified public keys", EUROCRYPT'91, pp. 490-497, 1991.

[13] M. Girault and J. C. Pailles, "An identity-based identification scheme providing zero-knowledge authentication and authenticated key exchange", Proc. of ESORICS'90, pp. 173-184, 1990.

[14] S. J. Park and D. H. Won, "A Generalization of Public Key Residue Cryptosystem",

Proceeding of JW-ISC'93, pp. 202-206, 1993.

[15] S. J. Park, Chung Ryong Jang, Kyung Sin Kim and D. H. Won, "A "Paradoxical" identity-based scheme based on the γ^{th}-residuosity problem and discrete logarithm problem", To be published at An International Conference on Numbers and Forms, cryptography and codes, August 21-28, 1994, Khabarovsk, Russia.

[16] Schnorr, "Efficient Identification and Signatures for Smart Cards", EUROCRYPT'89, pp. 686-689, 1989.

[17] Schnorr, "Efficient Identification and Signatures for Smart Cards", CRYPTO'89, pp.239-252, 1989 and J. of Cryptology, Vol.4, No.3, pp. 161-174, 1991.

[18] Y. Zheng, T. Matsumoto,and H. Imai, "Residuosity Prblem and its Applications to Crytpography", Trans. IEICE, vol. E71, No. 8, pp. 759-767, 1988.

[19] Y. Zheng, "A Study on Probabilistic Cryptosystems and Zero-knowledge Protocol", Master thesis, Yokohama National University, 1988.