위탁 방식을 이용한 무선 통신 상의 키 분배 및 키 복구 시스템

주 미 리[†] · 원 동 호[††]

요 약

무선 통신은 환경적인 특성 때문에 안전성과 효율성이라는 상반된 목적을 만족시킬 수 있는 암호 시스템을 요구한다. 본 논문에서는 이를 만족시킬 수 있도록 위탁 방식을 이용하여 무선 통신상의 효율적인 키 분배 및 키 복구 시스템을 제안하였다. 제안하는 시스템은 암호의 역기능을 방지하기 위하여 요구되는 키 복구 기능을 추가하였으며, 키 복구 정보에 대한 유효성 검사가 가능하다. 또한 전송되는 정보가 적어 효율적이다. 본 논문에서 제안한 키 복구 방식은 송수신자 양쪽에서 동일한 방법을 사용하므로 다양한 응용 분야에 적용될 수 있다.

Key Exchange and Key Recovery System in Wireless Communications using Key Escrow

Mi-Ri Joo[†] · Dong-Ho Won[††]

ABSTRACT

Wireless communications require the cryptography system which satisfies a opposite purpose as safety and efficiency. In this paper we proposed the efficient key distribution system satisfying in wireless communication using escrow in order to satisfy the requirements. We supplemented the key recovery function to prevent side effects of cryptography and it is possible to check verification. Also, transmitted information is a little so that the system is efficient. The proposed key recovery method can be applicable to various application fields.

키워드 : 무선 통신(wireless communications), 인증(authentication), 키 분배(Key exchange), 키 복구(Key recovery)

1. 서 론

현대 사회는 컴퓨터와 통신 기술의 발전에 따라 정보화 사회로의 급속한 진전이 이루어지고 있으며 유선을 이용한 데이터 전송, 처리가 급속한 발전을 이루었다. 유선 통신에 이어 무선 통신 기술이 개발됨으로써, 이동성과 휴대성이라는 편리함을 제공하게 되었다. 그러나 무선 통신의 전송 매체는 대기이므로 근본적으로 정보보호 측면에서 취약하여 유선을 이용하는 통신에 비해 정보의 유출, 불법 수정 등이 용이하다.

유무선 통신 환경에서 기밀성 및 인증 기능을 제공하기 위하여 다양한 암호 방식이 사용되고 있다. 암호 방식은 크게 관용 암호 방식과 공개키 암호 방식으로 나뉘어진다. 관용 암호 방식은 고속의 계산 속도를 가진 반면 키 분배의 어려움을 가지고 있으며, 공개키 암호 방식은 공개키 디렉토리를 이용하므로 키 분배가 필요하지 않으나 계산량이 많기 때문에 속도, 전력, 복잡도 면에서 많은 제한이 따른다[1].

단말기의 계산 능력이 제한되어 있는 무선 통신 환경에서는 안전성과 효율성이라는 상반된 목적을 만족시키기 위해서 공개키 암호 방식을 사용하여 키를 분배하고 분배된 키를 이용하여 관용 암호 방식을 사용하는 다양한 암호 시스템이 제안되었다.

그러나, 키를 소유한 사람만이 암호문을 복호할 수 있다는 암호의 특성 자체가 키를 분실한 경우 정당한 사용자 조차도 암호문을 복호할 수 없으며, 암호가 범죄에 이용되는 경우 합법적인 수사를 방해할 수 있다는 역기능을 발생시킬 수 있다[2, 3].

전자상거래등 민간 부문으로 암호 사용이 확산되고 있는 현재 암호의 역기능을 해결하는 것이 시급히 요구되고 있으며, 이에 대한 대안으로 세계 각국에서 키 복구 기술에 대한 연구가 활발히 진행 중에 있다[4, 5].

본 논문에서는 무선 통신 환경에서 요구되는 안전성과 효율성을 모두 만족시키기 위해서 효율적인 키 분배 시스템을 제안하였다. 또한 암호의 역기능을 방지하기 위해서 키 복구 기능을 추가하였다[6-8]. 제안하는 방식은 기존의 방식들에 비해 효율적이며 기존의 방식과 달리 송수신자 양측에서 동일한 방법으로 키 복구를 수행하므로 구현이 간편하며 추가되는 새로운 연산이 없다. 또한 클라이언트 서버 환경뿐만 아니라 클라이어트 대 클라이언트 환경까지 다양한 응용이 가능하다.

† 정 회 원 : 국가보안기술연구소 연구원
†† 종신회원 : 성균관대학교 정보통신공학부 교수
논문접수 : 2002년 7월 26일, 심사완료 : 2002년 9월 7일

본 논문은 다음과 같이 구성된다. 2장에서는 기존의 무선 통신 환경에서의 키 복구 기능을 가진 키 분배 프로토콜을 분석하고, 3장에서는 위탁 방식을 이용하여 키 복구 기능을 가진 효율적인 키 분배 시스템을 제안하였다. 4장에서는 제안한 프로토콜의 특성을 분석하고, 마지막으로 5장에서 결론을 맺었다.

2. 기존의 무선 환경에서의 키 복구 프로토콜

2.1 KR Enhanced ASPeCT 프로토콜

UMTS(Universal Mobile Telecommunications on Information)을 위한 가장 잘 알려진 공개키 기반의 WAKE(Wireless Authentication and Key Establish) 프로토콜은 ASPeCT 프로젝트에서 제시된 ASPeCT 프로토콜이다[9].

1999년 Rantos와 Mitchel은 암호의 역기능을 방지하기 위하여 키 복구 기능이 요구됨에 따라 ASPeCT 프로토콜에 키 복구 기능을 추가하여 ASPeCT 프로토콜을 개선하였다[10].

2.1.1 프로토콜

사용자 A와 VASP(Value Added Service Provider) B는 자신이 선택한 각각의 키 복구 기관 KRA_A, KRA_B에게 자신의 정보를 위탁한다. TTP는 인증기관과 키 복구 기관의 역할을 하고 있다. 다음 (그림 1)은 Rantos와 Mitchel에 의해서 제안된 키 복구 기능을 추가한 ASPeCT 프로토콜이다.

A : 사용자, B : VASP, TTP_A : A의 신뢰기관, $K_{AB} = h_1(r_B, g^{br_A})$
A : $r_A = f(w_A, s_A)$, $L = (g^{x_A})^{r_A}$

1. $A \rightarrow B$: g^{r_A}, s_A, $\{A\}_L$, TTP_A
2. $A \leftarrow B$: r_B, $h_2(K_{AB}, r_B, B)$, B_{Cert}
3. $A \rightarrow B$: $E_{K_{AB}}(\{h_3(g^{r_A}, g^{b}, r_B, B)\}_{K_A^{-1}}, A_{Cert})$

(그림 1) KR enhanced ASPeCT 프로토콜

사용자 A는 난수 $r_A = f(w_A, s_A)$를 계산한다. 이때 f는 일방향 함수이며, s_A는 임으로 선택된 난수이다. 또한 w_A는 키복구 기관 KRA_A에게 위탁된 정보이다. $\{A\}_L$은 사용자 A가 자신의 식별정보를 L로 암호화한 값이다. 이때, $L = (g^{x_A})^{r_A}$이며, g^{x_A}는 KRA_A의 공개키를 나타낸다. 사용자 A는 토큰 1을 VASP B에게 전달하며, TTP_A는 A의 인증기관을 의미한다.

VASP B는 임의의 난수 r_B를 선택하여 세션키 $K_{AB} = h_1(r_B, g^{br_A})$를 계산한다. VASP B는 토큰 2를 사용자 A에게 전달한다. 사용자 A는 토큰 2를 수신 받아 세션키 $K_{AB} = h_1(r_B, g^{br_A})$를 계산하고 토큰 2에서 수신 받은 일방향 함수 값 $h_2(K_{AB}, r_B, B)$을 계산하여 무결성을 검사한다. 무결성이 확인되면 사용자 A는 서명 $\{h_3(g^{r_A}, g^{b}, r_B, B)\}_{K_A^{-1}}$을 생성하여 토큰 3를 VASP B에게 전송한다.

2.1.2 키 복구 과정

[A의 키 복구 기관]

KRA_A는 프로토콜로부터 공개된 값 s_A, $\{A\}_L$, r_B, g^b을 얻고, $\{A\}_L$로부터 A의 식별 정보를 복호한다. KRA_A는 식별정보를 이용하여 상응하는 위탁 정보 w_A를 찾은 후 s_A를 같이 이용하여 r_A를 계산한다.

$$r_A = f(w_A, s_A)$$

KRA_A는 세션키 $K_{AB} = h_1(r_B, g^{br_A})$를 계산한다.

[B의 키 복구 기관]

VASP B는 등록단계에서 KRA_B에게 자신의 개인키 b를 위탁한다.

KRA_B는 프로토콜에 공개된 정보 g^{r_A}, r_B와 B의 위탁된 개인키 b를 이용하여 세션키 $K_{AB} = h_1(r_B, g^{br_A})$를 계산한다.

2.1.3 분 석

이 프로토콜에서 $\{A\}_L$는 필요하지 않다. 이 정보는 익명성을 제공하기 위해서 사용되는 정보이지만, 키 복구 기능이 추가되면 감청 기관이 프로토콜을 감청하고도 사용자가 누구인지 알 수 없으므로 키 복구 기능과 모순된다. 또한 이 프로토콜은 상호 인증이 제공되지 않는다. 마지막으로 키 복구 필드는 의도적으로 잘못된 정보를 이용하여 생성할 수 있으므로 누구나 키 복구 필드의 무결성을 검증할 수 있는 키 복구 필드에 대한 공개적인 검증 기능 제공이 요구된다.

2.2 변형된 KR Enhanced ASPeCT 프로토콜

2000년 Nieto 등은 KR Enhanced ASPeCT 프로토콜에서 $\{A\}_L$이 불필요함을 지적하고, 키 복구 정보에대한 공개적인 검증 기능을 추가한 변형된 프로토콜을 제안하였다[11].

2.2.1 프로토콜

사용자 A는 키 복구 기관 KRA_A에게 자신의 위탁 정보 w_A를 생성해서 위탁한다. VASP B는 키 복구 기관 KRA_B에게 자신의 개인키 b를 위탁한다. 이때, TTP는 인증기관과 키 복구 기관의 역할을 하고 있다. 다음 (그림 2)은 변형된 KR enhanced ASPeCT 프로토콜이다.

A : 사용자, B : VASP, TTP_A : A의 신뢰기관, $K_{AB} = h_1(r_B, g^{br_A})$
A : $s_A = (w_A h(g^{r_A}) + r_A) \bmod q$, B : $r_B = f_B(w_B, s_B)$

1. $A \rightarrow B$: g^{r_A}, TTP_A
2. $A \leftarrow B$: $r_B \oplus g^{br_A}$, $h_2(K_{AB}, r_B, B)$, $E_{K_{AB}}(s_B)$, B_{Cert}
3. $A \rightarrow B$: $E_{K_{AB}}(\{h_3(g^{r_A}, g^{b}, r_B, B)\}_{K_A^{-1}}, A_{Cert})$, s_A, s_B

(그림 2) 변형된 KR enhanced ASPeCT 프로토콜

사용자 A는 위탁 정보 w_A를 생성하여 KRA_A와 공유하고 $\phi_A = g^{w_A}$를 생성하여 이를 공개한다. 단, $1 \le w_A \le q-1$이다. 또한 사용자 A는 임의의 난수 r_A를 선택하여 g^{r_A}와 $s_A = (w_A h(g^{r_A}) + r_A) \bmod q$를 계산한다. 단, $1 \le r_A \le q-1$이다.

VASP B는 $r_B = f_B(w_B, s_B)$를 계산한다. 이때 f_B는 일방향 함수이며, w_B는 KRA_B와 공유한 비밀값이고, s_B는 난수

이다.

2.2.2 키 복구 과정

[A의 키 복구 기관]

KRA_A는 다음과 같이 r_A를 계산한다.

$$r_A = s_A - w_A h(u_A) \bmod q$$

그후, KRA_A는 $K_{AB} = h_1(r_B, g^{br_A})$를 계산한다.

[B의 키 복구 기관]

KRA_B는 $r_B = f_B(w_B, s_B)$를 계산하고 g^{br_A}를 계산한다.

$$g^{br_A} = (r_B \oplus g^{br_A}) \oplus r_B$$

그후, KRA_B는 $K_{AB} = h_1(r_B, g^{br_A})$를 계산한다.

2.2.3 키 복구 정보 검증 과정

공개된 정보 g^{r_A}, s_A를 통해서 키 복구 정보의 무결성을 검증할 수 있다. 먼저 공개값 ϕ_A를 습득한 후 $c' = h(g^{r_A})$를 계산한다. $g^{s_A} = \phi_A^{c'} u_A$를 계산해서 그 값이 맞으면 검증에 성공한다.

2.2.4 분 석

이 프로토콜은 키 복구 정보를 검증할 수 있는 장점을 가지는 반면, 전송시 s_A, s_B, $\{s_B\}_{K_{AB}}$의 부가 정보가 생긴다. 또한 사용자 A가 토큰 2에서 r_B를 알게 되므로 키 복구 정보의 검증 방법을 B의 도메인에 적용시킬 수 없다. 또한, $\{A\}_L$ 사용의 불필요함을 지적하면서도 키 복구를 위해 감청 기관이 사용자 A에 대한 정보를 알 수 있는 구체적인 방법을 제시하고 있지 못하다.

2.3 PKC 2001의 프로토콜

2001년 Kim 등은 PKC 2001에서 Nieto 등의 변형된 KR Enhanced ASPeCT 프로토콜의 단점을 개선하여 사용자 A와 VASP B 양쪽 도메인에서 키 복구 정보를 검증할 수 있는 새로운 프로토콜을 제안하였다[12].

2.3.1 프로토콜

사용자 A와 VASP B는 각각 w_A, w_B를 생성하여 자신이 선택한 키 복구 기관 KRA_A, KRA_B에게 자신의 위탁 정보 w_A, w_B를 각각 위탁한 후, $\phi_A = g^{w_A}$, $\phi_B = g^{w_B}$를 계산하여 이를 공개한다. 이때, $1 \le w_A \le q-1$이다. 다음 (그림 3)은 PKC 2001에서 제안된 프로토콜이다.

A : 사용자, B : VASP, TTP_A : A의 신뢰기관, $K_{AB} = h_1(g^{br_A + r_B})$
$A : s_A = (w_A h(g^{r_A}) + r_A) \bmod q$, $B : s_A = (w_B h(g^{r_B}) + r_B) \bmod q$

1. $A \rightarrow B$: g^{r_A}, TTP_A
2. $A \leftarrow B$: g^{r_B}, $w_B \oplus r_B \oplus g^{br_A}$, $h_2(K_{AB}, g^{r_B}, B)$, $\{s_B\}_{K_{AB}}$, B_{Cert}
3. $A \rightarrow B$: $E_{K_{AB}}(\{h_3(g^{r_A}, g^b, g^{r_B}, B)\}_{K_A^{-1}}, A_{Cert})$, s_A, s_B

(그림 3) PKC 2001 프로토콜

사용자 A는 임의의 난수 r_A를 선택하여 g^{r_A}와 $s_A = (w_A h(g^{r_A}) + r_A) \bmod q$를 계산한다. 이때 $1 \le r_A \le q-1$이다.

VASP B 역시 동일한 방법으로 r_B, g^{r_A}, s_B를 생성한다.

2.3.2 키 복구 과정

[A의 키 복구 기관]

KRA_A는 다음과 같이 r_A를 계산한다.

$$r_A = s_A - w_A h(u_A) \bmod q$$

그후, KRA_A는 $K_{AB} = h_1(g^{br_A + r_B})$를 계산한다.

[B의 키 복구 기관]

KRA_B는 다음과 같이 r_B를 계산한다.

$$r_B = s_B - w_B h(u_B) \bmod q$$

KRA_B는 $g^{br_A} = (r_B \oplus g^{br_A}) \oplus r_B$를 계산하고 $K_{AB} = h_1(g^{br_A + r_B})$를 계산한다.

2.3.3 키 복구 정보 검증 과정

공개된 정보 g^{r_A}, s_A를 통해서 키 복구 정보의 무결성을 검증할 수 있다. 먼저 공개값 ϕ_A를 습득한 후 $c' = h(g^{r_A})$를 계산한다. $g^{s_A} = \phi_A^{c'} g^{r_A}$를 계산해서 그 값이 맞으면 검증에 성공한다. 이 방법은 VASP B의 도메인에서도 동일하게 적용된다.

2.3.4 분 석

이 프로토콜은 송신자 측과 수신자 측에서 다른 능력을 가지고 있다는 전제하여 설계되어 있으므로 클라이언트 대 클라이언트 사이의 통신에 적용하기에 부적합하다. 또한 부가되는 정보가 많아 전송시 부가 정보가 많다는 단점을 가지고 있으며, 키 복구를 위해 감청 기관이 사용자 A에 대한 정보를 알 수 있는 구체적인 방법을 제시하고 있지 못하다.

3. 제안하는 시스템

1996년 무선 통신 환경에서 세션키를 분배하고 사용자 인증을 수행하는 ASPeCT 프로토콜에 제시된 이후로 다양한 WAKE 프로토콜들이 제안되었다. 이후 키 복구 기능의 필요에 의해 키 복구 기능이 추가된 프로토콜들이 꾸준히 제시되었으나, 무선 환경이라는 특성은 이들 프로토콜의 효율성 개선을 요구하고 있다.

본 논문에서는 송수신자 양측에서 동일한 방법으로 키 복구 기능과 인증 기능을 가진 위탁 방식을 이용한 무선 통신 상의 키 분배 및 키 복구 시스템을 제안하였다. 이때, 위탁되는 정보는 사용자의 암호용 개인키가 아니므로 사용자의 프라이버시가 보호될 수 있으며, 송신자와 수신자가 프로토콜 상에서 생성하는 공개 정보들을 이용하여 키 복구 필드의 유효성을 검증할 수 있다.

3.1 시스템 설정

신뢰센터 TTP는 사용자의 암호용 공개키에 인증서를 발급해 주는 기관이며, 시스템을 이용하는 모든 사용자들은 위탁 정보 w를 생성하여 신뢰할 수 있는 키 복구 기관 KRA에게 이를 위탁한다. 이때 KRA는 사용자들이 임의로 선정할 수 있으며, TTP는 인증기관과 키 복구 기관의 역할을 하고 있다.

다음 <표 1>는 제안하는 시스템에서 사용되는 용어이다.

〈표 1〉 프로토콜의 약어 및 의미

약 어	의 미
A	사용자 A의 식별 정보
B	VASP B의 식별 정보
$TTP_A(KRA_A)$	사용자 A의 인증 기관 및 키 복구 기관
$TTP_B(KRA_B)$	VASP B의 인증 기관 및 키 복구 기관
A_{Cert}	사용자 A의 공개키에 대한 인증서
B_{Cert}	VASP B의 공개키에 대한 인증서
$E_{K_{AB}}$	세션키 K_{AB}를 사용하여 메시지 m을 관용 암호 방식으로 암호화
h_1, h_2, h_3	일방향 해쉬 함수

본 논문에서 제안하는 키 복구 기능을 가진 WAKE 프로토콜에서 위탁 정보는 등록 과정에서 사용자가 선택한 키 복구 기관에 위탁된다.

3.2 위탁 과정

[단계 1]

사용자 A와 VASP B는 각각의 위탁 정보는 위탁 정보 w_A, w_B를 각각의 신뢰 기관 KRA_A, KRA_B 이를 에게 위탁한다.

이때 신뢰 기관은 사용자 A 및 VASP B가 임의로 선정할 수 있다. 단, $1 \le w_A, w_B \le q-1$

[단계 2]

사용자 A와 VASP B는 각각 $\phi_A = g^{w_A}$, $\phi_B = g^{w_B}$를 생성하여 이를 공개한다.

3.2.1 키 분배 및 인증 프로토콜

사용자 A와 VASP B는 위에서 언급한 위탁 과정에 따라 키 위탁 정보를 생성하여 자신이 선택한 신뢰기관에 이를 위탁하고 다음과 같이 세션키를 공유하고 키와 사용자를 인증한다.

[단계 1]

① 사용자 A는 임의의 난수 r_A를 선택한다.

$$r_A \in_R Z_{q-1},\ 1 \le r_A \le q-1$$

이때 p는 큰 소수이며 q는 $q \mid (p-1)$인 소수이다.

② 사용자 A는 g^{r_A}을 계산하여 A_{Cert}와 함께 전달한다. 이때 g는 Z_p^* 상에서 q의 order인 원시 원소이다.

③ 사용자 A는 다음과 같이 s_A를 계산한다. 이때 f는 일방향 함수이며, w_A는 키복구 기관 KRA_A에게 위탁한 정보이다.

$$s_A = (w_A h(g^{r_A}) + r_A) \bmod q$$

[단계 2]

① VASP B는 임의의 난수 r_B를 선택한다.

$$r_B \in_R Z_{q-1},\ 1 \le r_B \le q-1$$

이때 p는 큰 소수이며 q는 $q \mid (p-1)$인 소수이다.

② VASP B는 g^{r_B}를 계산한다. 이때 g는 Z_p^* 상에서 q의 위수인 원시 원소이다.

③ VASP B는 다음과 같이 s_B를 계산한다. 이때 f는 일방향 함수이며, w_B는 키복구 기관 KRA_B에게 위탁한 정보이다.

$$s_B = (w_B h(g^{r_B}) + r_B) \bmod q$$

④ VASP B는 다음과 같이 세션키를 생성한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

⑤ VASP B는 키 복구 필드를 생성한다.

$$s_B \oplus g^{ar_B} \oplus g^{br_A}$$

⑥ VASP B는 키에대한 무결성 검사를 위해 다음의 해쉬 값을 생성한다.

$$h_2(K_{AB}, g^{r_B}, B)$$

⑦ VASP B는 자신의 인증서를 첨부하여 다음을 사용자 A에게 전송한다.

$$g^{r_B},\ s_B \oplus g^{ar_B} \oplus g^{br_A},\ h_2(K_{AB}, g^{r_B}, B),\ B_{Cert}$$

[단계 3]

① 사용자 A는 [단계 2]에서 전달받은 $h_2(K_{AB}, g^{r_B}, B)$ 값을 계산하여 무결성을 확인하고, 다음과 같이 세션키를 생성한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

② 사용자 A는 $s_B \oplus g^{ar_B} \oplus g^{br_A}$로부터 s_B를 계산한다.

$$s_B = s_B \oplus g^{ar_B} \oplus g^{br_A} \oplus g^{ar_B} \oplus g^{br_A}$$

③ 사용자 A는 다음과 같이 일방향 함수 값을 생성한다.

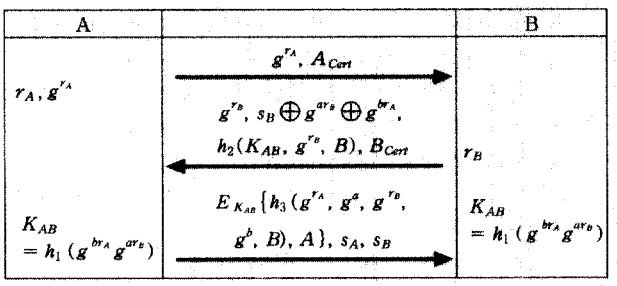
$$h_3(g^{r_A}, g^a, g^{r_B}, g^b, B)$$

④ 사용자 A는 ③에서 생성한 일방향 함수 값에 A의 식별 정보를 첨부하여 세션키로 암호화한다.

$$E_{K_{AB}}\{h_3(g^{r_A}, g^a, g^{r_B}, g^b, B), A\}$$

⑤ 사용자 A는 ④에서 생성한 값 s_A, s_B에를 첨부하여 VASP B에게 전송한다.

$$E_{K_{AB}}\{h_3(g^{r_A}, g^a, g^{r_B}, g^b, B), A\},\ s_A,\ s_B$$



(그림 4) 제안하는 키 분배 및 키 복구 프로토콜

3.3 키 복구 과정

제안하는 프로토콜에서는 사용자 A의 도메인과 VASP B의 도메인에서 동일한 방법으로 키 복구를 할 수 있다.

[A의 키 복구 기관]

① KRA_A는 다음과 같이 r_A를 계산한다.

$$r_A = s_A - w_A h(g^{r_A}) \bmod q$$

② KRA_A는 VASP B의 공개키 g^b와 r_A를 이용하여 다음을 계산한다.

$$g^{r_A b} = (g^b)^{r_A}$$

③ KRA_A 다음과 같이 g^{ar_B}를 계산한다.

$$g^{ar_B} = s_B \oplus g^{ar_B} \oplus g^{br_A} \oplus s_B \oplus g^{br_A}$$

④ KRA_A는 다음과 같이 세션키를 계산한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

[B의 키 복구 기관]

① KRA_B는 다음과 같이 r_B를 계산한다.

$$r_B = s_B - w_B h(g^{r_B}) \bmod q$$

② KRA_B는 사용자 A의 공개키 g^a와 r_B를 이용하여 다음을 계산한다.

$$g^{r_B a} = (g^a)^{r_B}$$

③ KRA_B 다음과 같이 g^{br_A}를 계산한다.

$$g^{br_A} = s_B \oplus g^{ar_B} \oplus g^{br_A} \oplus s_B \oplus g^{ar_B}$$

④ KRA_B는 다음과 같이 세션키를 계산한다.

$$K_{AB} = h_1(g^{br_A} g^{ar_B})$$

4. 제안하는 시스템의 특성

4.1 안전성

4.1.1 키 복구 정보 유효성 검증 기능

키 복구 정보의 유효성은 제 3자에게 검증 가능하도록 구성되어 키 복구 유효성을 가져야 한다. 제안하는 시스템은 프로토콜에서 사용되는 공개된 값들을 이용하여 올바른 키 복구 정보가 생성되었는지 제 3자가 확인할 수 있다. 즉, 사용자들은 부가 계산량 없이 키 복구 정보의 유효성을 확인할 수 있다. 다음은 사용자 A에 대한 키 복구 정보를 검증하는 것이며, VASP B에 대한 키 복구 정보 검증 방법도 이와 동일하다.

또한 키 복구 수행을 위한 파라미터인 s_A, s_B는 마지막 프로토콜에서 전달이 되므로 세션이 성립되었을때만 키 복구가 가능하다.

① 프로토콜로부터 g^{r_A}, s_A를 얻을 수 있으며 인증된 공개정보 ϕ_A를 이용하여 다음을 계산할 수 있다.

$$c' = h(g^{r_A}) \bmod q$$

② s_A를 이용하여 g^{s_A}를 계산한다.

③ ②에서 계산된 값과 $\phi_A^{c'} g^{r_A}$이 동일한 값인지 확인하여 키 복구 정보의 유효성을 검증할 수 있다.

$$g^{s_A} = \phi_A^{c'} g^{r_A}$$

4.1.2 동일한 키 복구 방식 적용

기존에 제안된 키 복구 시스템에서는 사용자 A와 VASP B가 서로 다른 방법으로 키를 위탁하고 있어 서로 다른 방법으로 키 복구를 해야했다. 제안한 방식에서는 B의 도메인에서도 동일한 방법으로 키 복구가 가능하다.

4.1.3 인 증

세션키는 사용자 A와 VASP B는 각각의 공개키와 난수를 결합하여 생성하며, 키 동의를 통한 세션키를 생성한다. 세션키 생성시 송수신자의 공개키를 사용하므로 공개키에 대한 소유자의 개인키 소유 여부를 묵시적으로 검증할 수 있어 사용자에대한 묵시적 인증을 수행할 수 있다.

4.1.4 무결성 및 안전성

제안하는 프로토콜에서는 사용되는 파라미터에 대한 일방향 함수 값을 생성하여 송수신자가 서로 전달하도록 하고 있어 전송시 누군가 해당 값을 변경하면 이를 통해 변경 여부를 알 수 있다. 또한 마지막 프로토콜에서 세션키 생성에 사용된 모든 파라미터에 대한 일방향 함수 값을 생성하여 이를 세션키로 암호화하므로 제 3자에게 정보가 노출되지 않는다.

4.2 효율성

〈표 2〉 프로토콜 비교

Protocol	모듈러 멱승		추가된 전송 정보	사용 연산			키복구정보 공개검증
	A	B		대칭키 암호	공개키 암호	서명	
KR enhanced ASPeCT	3	1	$s_A, \{A\}_L$	1	1	1	불 가
Modified KR enhanced	2	1	$\{s_B\}_{K_{AB}}, s_A, s_B$	2	-	1	송 신 자
PKC 2001 protocol	2	2	$\{s_B\}_{K_{AB}}, s_A, s_B, g^{r_B}$	2	-	1	송수신자
제안하는 protocol	2	2	s_A, s_B	1	-	-	송수신자

본 논문에서 제시한 프로토콜은 2번째 프로토콜에서 $\{s_B\}_{K_{AB}}$의 암호화 단계가 없으므로 암호화 1번과 전송정보 1개를 줄일 수 있다. 또한 세 번째 프로토콜에서는 서명 과정이 생략되므로 매우 효율적이다.

<표 2>는 기존의 프로토콜과 제안하는 프로토콜을 비교하였다.

5. 결 론

이동성과 편리성을 가지고 있는 무선 환경에서의 통신은 지속적으로 발전하고 있으며 향후 현재 유선 시스템의 많은 부분들이 무선 환경으로 변화할 것이다. 또한 전자상거래 등 다양한 응용 분야에서도 무선 통신이 사용되기 위해서는 정보보호가 필요하다. 그러나 무선 환경에서 사용되고 있는 단말기는 제한된 계산 능력을 가지고 있어 안전성과 효율성이라는 상반된 목적을 만족시키는 암호 시스템이 요구되며, 암호의 역기능을 방지하기 위한 대비책이 요구된다. 본 논문에서는 안전성과 효율성을 제공하고, 암호의 역기능을 방지할 수 있는 위탁 방식을 이용한 무선 통신상의 키 분배 및 키 복구 시스템을 제안하였다.

제안한 시스템은 전송되는 정보가 적어 기존의 프로토콜에 비하여 효율적이며, 키 복구 정보에 대한 유효성 검증이 가능하고, 송수신자 양측에서 동일한 키 복구 방식을 사용하고 있어 다양한 응용 분야에 적용될 수 있다. 따라서 클라이언트 대 서버 환경뿐만 아니라 클라이언트 대 클라이언트 환경 등에 적용할 수 있으므로 이에 대한 향후 연구가 필요하다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New Direction in Cryptography," IEEE Trans. Info. Theory, 22, pp.644-654, 1976.

[2] NIST, "Escrowed Encryption Standard," Federal Information Processing Standards Publication 185, 1994.

[3] David M. Balenson, Carl M. Elli son, StevenB. Lipner and Stephen T. Walker, "A New Approach to Software Key Escrow Encryption," Building in Big Brother : The Cryptographic Policy Debate, Springer-Verlag, pp.180-207, 1995.

[4] Sivio Micali, "Fair public key crypto-systems," Crypto'92, Springer-Verlag, Lecture Notes in Computer Science, LNCS 740, pp.113-138, 1992.

[5] Adam Young and Moti Yung, "Auto-Recoverablel Auto-Certifiable Cryptosystems," Advanced in Cryptology-Eurocrypto'98, Springer-Verlag, Lecture Notes in Computer Science, pp.17-31, 1998.

[6] Pascal Paillier and Moti Yung, "Self-Escrowed Public Key Infrastructures," Proceedings of ICISC '99, The 2nd International Conference Information Security and Cryptology. Springer-Verlag, Lecture Note in Computer Science, 1999.

[7] Stephen T. Walker, Steven B. Lipner, Carl M. Ellison, Dennis K. Branstad and David M. Balenson, "Commercial Key Escrow : something for everyone now and for the future," TIS Report, No.541, Trusted Information Systems Inc., 1995.

[8] Eric Verheul and Henk C. A. van Tilborg, "Binding ElGamal : A Fraud Detectable Alternative to Key-Escrow Proposals," Eurocrypto '97, Springer-Verlag, Lecture Notes in Computer Science, LNCS 1233, pp.119-133, 1997.

[9] Advanced Security for Personal Communications Technologies, http://www.esat.kuleuven.ac.be/cosic/aspect/index.html.

[10] K. Rantos and C. MItchell, "Key Recovery in ASPeCT Authentication and Initialisation of Payment Protocol," presented at ACTS Mobile Summint, Sorrento, Italy, June, 1999.

[11] J. Nieto, D. Park, C. Boyd and E. Dawson, "Key Recovery in Third Generation Wireless Communication Systems," Public Key Cryptography-PKC 2000, LNCS 1751, pp.223-237, 2000

[12] C. H. Kim, P. J. Lee, "New Key Recovery in WAKE Protocol," Public Key Cryptography-PKC 2001, LNCS 1992, pp.325-338, 2001

주 미 리

e-mail : mrjoo@etri.re.kr

1996년 성균관대학교 정보공학과(학사)

1998년 성균관대학교 대학원 정보공학과 (석사)

1999년~현재 성균관대학교 전기전자 및 컴퓨터공학부 박사과정

2001년~현재 국가보안기술연구소 연구원

관심분야 : 암호이론, 이동통신보안, PKI 등

원 동 호

e-mail : dhwon@dosan.skku.ac.kr

1976년 성균관대학교 전자공학과(학사)

1978년 성균관대학교 전자공학과 석사(공학석사)

1988년 성균관대학교 전자공학과 박사(공학박사)

1978년~1980년 한국전자통신연구원 전임연구원

1985년~1986년 일본 동경공대 객원연구원

1992년~1994년 성균관대학교 전산소장

1995년~1997년 성균관대학교 교학처장

1996년~1998년 국무총리실 정보화추진위원회 자문위원

1998년~1999년 성균관대학교 정보통신기술연구소 소장

1999년~2001년 성균관대학교 전기전자 및 컴퓨터공학부장

1999년~2001년 성균관대학교 정보통신대학원장

1982년~현재 성균관대학교 정보통신공학부 교수

2000년~현재 정통부 지정 정보보호인증기술연구센터 센터장

2002년~현재 한국정보보호학회 회장

관심분야 : 암호 이론, 정보 이론