情報保護學會論文誌
第15券 第3號, 2005. 6

효율성을 개선한 신원기반의 3자간 복수 키 합의 프로토콜*

박 영 호,[1†] 이 경 현[2‡]

[1]부경대학교 정보보호학과, [2]부경대학교 전자컴퓨터정보통신공학부

An Efficiency Improved ID-based Tripartite Key Agreement Protocol*

Young-Ho Park,[1†] Kyung-Hyune Rhee[1‡]

[1]Dept. of Information Security, [2]Div. of Electronic, Computer and Telecommunication Engineering, Pukyong National University

요 약

Pairing을 이용한 신원기반의 공개키 암호시스템에 대한 연구가 활발히 진행되면서 신원기반의 다양한 키 합의 프로토콜이 제안되었으나, 대부분의 기법들이 키 합의 프로토콜에서 요구되는 보안 요구사항을 만족하지 않는 것으로 분석되었다. 그리고 최근 Liu 등과 Kim 등은 한 번의 프로토콜의 수행을 통해 복수개의 키를 설정할 수 있는 키 합의 프로토콜을 제안하였다. 본 논문에서는 Liu 등의 기법을 개선한 신원기반의 3자간 복수개의 키 합의 프로토콜을 제안한다. Liu 등의 기법과 유사하게 키 교환 메시지에 서명을 추가하지만 Liu 등의 기법보다 효율적인 프로토콜의 수행이 가능하다. 그리고 제안 프로토콜은 서로 다른 여러 키 발급센터(Private key generator, PKG)들이 관여하는 환경에서도 프로토콜의 수행이 가능하며, 프로토콜에 참여하는 각 개체들이 자신의 소속에 따라 별개의 키 발급센터로부터 발행된 개인키를 사용할 수 있으므로 보다 실용적이며 효율적으로 적용될 수 있다.

ABSTRACT

As the ID-based public key cryptosystems become a very active research area, a number of ID-based key agreement protocols have been proposed, but unfortunately many of them were analyzed that there were some security flaws in the protocols. In addition to key agreement protocols, in recent, Liu et al. and Kim et al. proposed the key agreement protocols that multiple session keys are established at once among participated entities. In this paper, we propose an ID-based tripartite key agreement protocol that establishes 8 keys by improving the efficiency of the Liu et al.'s. Moreover, the proposed protocol can be used in the situation where multiple different private key generators(PKG) are involved. Therefore, because the private key issued by different PKGs belonging to each entity's domain can be used, our proposed scheme is more efficiently applicable to the practical applications.

Keywords : *key agreement, tripartite Diffie-Hellman, ID-based cryptography*

접수일 : 2005년 2월 18일 ; 채택일 : 2005년 6월 7일

* 본 연구는 정보통신부의 기초기술연구지원사업(정보통신연구진흥원)으로 수행한 연구결과물 입니다.

† 주저자, ‡ 교신저자 : khrhee@pknu.ac.kr

Ⅰ. 서 론

키 합의 프로토콜(key agreement protocol)은 보안 통신을 위해 둘 또는 그 이상의 개체들간에 공유되는 세션키(session key)를 설정하기 위한 프로토콜이다. 전형적인 키 합의 프로토콜은 Diffie-Hellman(DH) 키 교환 기법[1]을 근간으로 두 개체들간에 통신의 기밀성과 무결성을 보장하기 위한 세션키를 설정하는 프로토콜로 연구되고 있으며, 최근 다자간(multi-party) 프로토콜의 특수한 경우로서 3자간 키 합의 프로토콜도 연구되고 있다. Pairing을 이용한 3자간 키 합의 프로토콜은 Joux[2]에 의해 처음 소개되었지만, Joux의 기법은 인증 기능을 제공하지 않으므로 man-in-the-middle 공격에 대한 취약성을 가지고 있다. Joux 이후로 인증 기능을 제공하는 3자간 키 합의 프로토콜들이 제안되었고, 제안된 기법들은 크게 인증서 기반의 공개키 기법과 신원기반의 공개키 기법으로 분류될 수 있으며, 본 논문에서는 신원기반의 기법에 대해서만 고려한다.

신원기반 공개키 암호시스템의 경우 사용자의 공개키는 사용자를 유일하게 식별할 수 있는 ID로부터 유도될 수 있으며, PKG(Private Key Generator)라는 신뢰되는 키 발급센터에 의해 자신의 ID에 대한 개인키를 발급 받게 된다. 사용자를 식별할 수 있는 ID로부터 직접 그 사용자의 공개키를 계산할 수 있으므로 신원기반의 공개키 기법은 기존의 PKI 구조에서 공개키 인증서의 관리와 관련된 작업들의 부담을 줄일 수 있는 이점을 가진다. 이러한 신원기반 암호시스템에 대한 개념은 Shamir에 의해 처음 제안되었으며[3], Boneh와 Franklin의 Weil pairing을 이용한 신원기반 암호기법[4] 이후로 신원기반의 서명과 키 합의 등의 다양한 기법들이 활발히 연구되고 있다.

Boneh와 Franklin의 암호기법이 제안된 이후로 pairing을 이용한 신원기반의 다양한 키 합의 프로토콜들이 제안되었으나 대부분이 보안상 결함이 있는 것으로 분석되었다. 2자간 키 합의 프로토콜의 경우 Smart의 기법[5]이 제안된 후 Chen과 Kudla[6], Shim[7]에 의해 Smart 기법의 효율성을 개선한 새로운 프로토콜들이 제안되었으나, Shim 기법은 Sun과 Hsieh[8]에 의해 보안상 결함이 지적되었다. Nalla와 Reddy가 신원기반의 3자간 키 합의 프로토콜을[9] 제안하였지만 Chen[10]과 Shim[11]에 의해 안전하지 않은 것으로 분석되었다. Nalla에 의해 제안된 기법[12]과 Liu 등에 의해 제안된 신원기반 3자간 키 합의 프로토콜[13]은 인증을 위해 키 교환 메시지에 대한 서명을 적용하였지만, Nalla의 기법은 Shim에 의해 보안상의 결함이 지적되었다[11].

일반적인 키 합의 프로토콜은 한번의 프로토콜의 수행을 통해 단일 세션키를 설정하게 되지만 Liu 등이 제안한 기법은 3자간에 한번의 프로토콜의 수행을 통해 8개의 서로 다른 키를 생성할 수 있으며, Kim 등은 2개체간에 4개의 서로 다른 키를 생성하는 프로토콜[15]을 제안하였다. 일반적으로 보안 통신의 안전성은 사용되는 세션키에 의존하게 되며, 시스템의 안전성을 유지하기 위해 주기적으로 세션키를 갱신할 것을 권장하고 있다. 주기적인 키 갱신을 위한 방법으로 이전의 세션키를 이용하여 새로운 키를 전달하거나, 새로운 키 합의 프로토콜의 수행을 통해 새로운 키를 설정할 수 있다. 그러나 첫 번째 방법의 경우 이전의 세션키가 노출되는 경우 연쇄적으로 이후의 통신에 대한 보안성도 영향을 받게 되며, 두 번째 방법처럼 키 갱신을 위해 매번 새로운 프로토콜을 수행하는 것은 시스템의 효율성을 저하시키는 요인이 될 수 있다. 그러므로 한 번의 프로토콜의 수행을 통해 서로 다른 여러 개의 키를 생성할 수 있다면, 어느 한 키의 노출이 다른 키에 영향을 주지 않으면서 효율적으로 시스템의 안전성을 유지할 수 있는 시스템을 구성할 수 있을 것이다.

그리고 이전에 제안된 대부분의 신원기반의 키 합의 프로토콜은 프로토콜에 참여하는 모든 사용자들이 동일한 PKG로부터 사용자의 ID에 대한 개인키를 발급 받는 환경만을 고려하였다. 그러나 실질적인 응용환경에서는 동일한 조직 내부의 사용자들뿐만 아니라 다른 조직에 속한 사용자간에도 프로토콜의 수행이 필요할 것이며, 사용자들이 자신의 소속에 따라 각자 서로 다른 PKG로부터 발급 받은 개인키를 사용하는 상황도 발생하게 될 것이다. 예를 들어, 어느 회사에서 사원들의 보안 키 발급의 효율성을 위해 지점이나 부서에 따라 별도의 키 발급센터를 운영한다고 가정해보자. A지점에 근무하는 갑이라는 사원이 B지점에 근무하는 을이라는 사원과 보안 통신을 위한 키 합의 프로토콜의 수행을 필요로 한다면 각자 자신이 소속된 지점의 PKG로부터 발급 받은 키를 사용하는 것이 더 일반적이며 실용적일 것이다.

서로 다른 별개의 PKG로부터 개인키를 발급 받는 경우에 대한 키 합의 프로토콜은 Chen과 Kudla 의 기법[6]과 McCullagh와 Barreto[16]에 의해 제안되

었다. 그러나 두 기법은 두 명의 사용자에 대한 2자간 키 합의 프로토콜이며 McCullagh와 Barreto의 기법은 Xie[17]와 Choo[18]에 의해 각각 안전하지 않은 것으로 분석되었다. 따라서 Chen과 Kudla의 기법은 PKG에 독립적인 프로토콜의 수행이 가능하지만 3자간 프로토콜로는 효율적으로 확장되지 못하며, Liu 등의 기법은 3자간 프로토콜이지만 동일한 하나의 PKG로부터 개인키를 발급 받은 경우에 대해서만 고려하였으므로 역시나 서로 다른 PKG가 관여하는 경우 프로토콜이 수정되어야 하며 효율적으로 수행되지 못한다.

본 논문에서는 프로토콜에 참여하는 개체들이 동일한 PKG로부터 발급 받은 개인키뿐만 아니라 각 개체가 자신의 소속에 따라 선택된 별개의 PKG로부터 발급 받은 개인키도 이용할 수 있는 신원기반의 3자간 키 합의 프로토콜에 대해 제안한다. 여기서 별개의 PKG란 전반적인 시스템 파라미터들은 공유하지만 키 발급을 위한 마스터 키가 서로 다른 다중 PKG 환경을 의미한다. 본 논문에서 제안하는 프로토콜은 Liu 등이 제안한 프로토콜과 유사하게 키 교환 메시지에 서명을 부가하고 8개의 독립적인 키를 생성할 수 있지만, Liu 등의 기법보다 효율적으로 프로토콜의 수행이 가능하다. 비록 제안 프로토콜이 새로운 암호학적 기법을 내포하고 있지는 않지만, 3자간 DH 키 교환 프로토콜과 효율적인 신원기반 서명기법을 결합시킴으로써 Liu 등이 제안한 키 합의 프로토콜의 서명검증에 대한 효율성을 향상시킨다. 그리고 프로토콜에 참여하는 사용자들이 서로 다른 PKG로부터 자신의 ID에 대한 개인키를 발급 받는 경우에도 제안 프로토콜은 동일하게 수행될 수 있으므로, 보다 현실적인 환경에서 실용적으로 사용될 수 있을 것이며, 제안 프로토콜을 단위 프로토콜로 하여 트리기반의 그룹키 합의 프로토콜[19]로도 효율적으로 확장될 수 있을 것이다.

제안 기법을 설명하기 위해 Ⅱ장에서는 관련연구로서 pairing의 성질과 키 합의 프로토콜에 대한 요구사항들과 Liu 등이 제안한 프로토콜을 살펴본다. Ⅲ장에서는 3자간 키 합의 프로토콜을 제안하고, Ⅳ장에서 제안 기법을 분석하고 Ⅴ장에서 결론을 맺도록 한다.

Ⅱ. 관련연구

본 장에서는 최근 신원기반 시스템에 널리 사용되는 pairing의 수학적 성질과, 키 합의 프로토콜에서 요구되는 보안성질들에 대해 간략히 살펴보고 제안 기법과 효율성을 비교하기 위해 Liu 등이 제안한 신원기반의 3자간 프로토콜에 대해 간략히 살펴보도록 한다.

1. 수학적 배경

본 절에서는 신원기반 암호시스템의 구성을 위한 bilinear pairing과 암호학적 용도를 위한 몇 가지 문제들에 대한 가정에 대해 간략하게 설명하도록 한다.

G_1을 충분히 큰 소수(prime number) q를 위수(order)로 가지며 생성자 P에 의해 생성되는 덧셈군(additive cyclic group)이라 두고 G_2를 동일한 위수를 가지는 곱셈군(multiplicative cyclic group) 이라고 하면, 이 두 군에 대해 정의되는 pairing e: $G_1 \times G_1 \rightarrow G_2$는 다음 성질들을 만족한다[4].

1) *Bilinearity* : $P, Q \in G_1$와 $a, b \in Z_q^*$에 대해, $e(P_1+P_2, Q) = e(P_1, Q)e(P_2, Q)$가 되고 $e(P, Q_1+Q_2) = e(P, Q_1)e(P, Q_2)$가 된다. 그러므로 $e(aP, bP) = e(P, P)^{ab}$가 성립한다.
2) *Non-degeneracy* : $e(P, Q) \neq 1$을 만족하는 $P, Q \in G_1$가 존재한다.
3) *Computability* : 모든 $P, Q \in G_1$에 대해 $e(P, Q)$를 효율적으로 계산할 수 있는 알고리즘이 존재한다.

현재 Bilinear pairing으로 타원곡선상에서 정의된 수정된 Weil pairing[4]과 Tate pairing[20][21]이 사용되고 있으며, 암호학적인 용도를 위해 다음과 같은 문제들을 가정한다. 현재까지 타원곡선상의 점들로 구성되는 덧셈군 G_1과 유한체에서의 곱셈군 G_2에서의 DLP와 CDHP, BDHP 문제를 해결하는 것은 어렵다고 알려져 있다[4].

- 이산대수 문제(Discrete Logarithm Problem) : DLP는 $< P, aP \in G_1 >$가 주어진 경우 a를 계산하는 문제이다.
- 계산적 Diffie-Hellman 문제(Computational Diffie-Hellman Problem) : CDHP는 $a, b \in Z_q^*$에 대해 $< P, aP, bP \in G_1 >$가 주

표 1. 이전 연구들의 분류

관련연구	개체 수	세션키 수	알려진 보안 문제
Smart[5]	2	1	PKG에 대한 전방 비밀성[7]
Chen, Kudla[6]	2	1	PKG에 대한 전방 비밀성[6]
Shim[7]	2	1	중간자 공격[8]
McCullagh, Barreto[16]	2	1	위장 공격[16], 중간자 공격[18]
Kim et al.[15]	2	4	PKG에 대한 전방 비밀성
Nalla[9]	3	1	수동적 메시지 도청[10], 중간자 공격[11]
Nalla, Reddy[12]	3	1	위장 공격[11]
Liu et al.[13]	3	1, 8	-

어진 경우 abP를 계산하는 문제이다.

- Bilinear Diffie-Hellman 문제 : BDHP는 $a,b,c \in Z_q^*$에 대해 $< P,aP,bP,cP \in G_1 >$가 주어진 경우, $e(P,P)^{abc} \in G_2$를 계산하는 문제이다.

2. 보안 요구사항

키 합의 프로토콜은 프로토콜에 참여한 사용자들의 인증을 제공할 수 있어야 하고, 프로토콜에 참여한 사용자들 이외의 다른 누구도 합의된 키에 대한 정보를 획득할 수 없음을 보장할 수 있어야 한다. 그러므로 키 합의 프로토콜은 다음과 같은 보안 요구사항들[22]을 만족해야 한다.

- *알려진 세션키에 대한 안전성* (known session key security) : 매 프로토콜의 수행으로 유일한 세션키를 설정할 수 있어야 하며, 이전 세션에 대한 세션키의 노출이 현재 세션의 세션키에 영향을 끼쳐서는 안 된다. 또한 여러 개의 키를 생성하는 프로토콜의 경우, 어떤 하나의 키의 노출이 다른 키의 안전성에 영향을 끼쳐서도 안 된다.
- *전방 비밀성* (forward secrecy) : 사용자의 개인키(long-term private key)가 노출될지라도 이전에 공유된 세션키가 노출되어서는 안 되며, 모든 사용자의 개인키가 노출되더라도 이전에 설정된 세션키가 안전한 경우 완전 전방 비밀성(perfect forward secrecy)을 만족한다고 한다. 또한 신원기반 암호시스템의 경우, 일반적으로 PKG가 개인키를 발급하게 되므로 PKG에 대한 전방 비밀성도 고려되어야 한다.
- *키 노출 위장에 대한 안전성* (key-compromise impersonation resilience) : 사용자 A의 개인키가 노출되면 공격자가 A로 위장할 수는 있지만 A에게 다른 사용자로 위장할 수 없어야 한다.
- *미지의 키 공유에 대한 안전성* (unknown key- share resilience) : 사용자 A는 자신이 의도하는 사용자들하고만 키를 설정할 수 있어야 한다.
- *키 제어에 대한 안전성* (no key control) : 어느 누구도 미리 선택된 값을 세션키로 설정하도록 할 수 없어야 한다.

전통적인 키 합의 프로토콜은 DH 키 교환 기법을 토대로 두 사용자간의 프로토콜로 연구되어 왔으며, Joux에 의해 처음으로 pairing을 이용한 3자간 DH 키 교환 프로토콜[2]이 제안되었다. 그러나 Joux의 프로토콜은 인증기능을 제공하지 않으므로 man-in-the-middle 공격에 대한 취약점을 가지고 있다. 이 후로 Joux의 프로토콜을 개선한 프로토콜들이 인증서 기반의 기법과 신원기반의 기법으로 분류되어 제안되었으나 대부분의 기법들이 보안상 결함이 있는 것으로 분석되어 졌다. 표 1은 이전에 제안된 신원기반 키 합의 프로토콜들을 분류하여 나타내고 있다.

3. Liu 등의 3자간 키 합의 프로토콜

Liu 등은 [13]에서 신원기반의 3자간 프로토콜을 제안하였으며 Ⅳ장에서 제안기법과의 비교를 위

해 본 절에서는 Liu 등이 제안한 복수개의 키 합의 프로토콜을 간단히 살펴보며 단일 세션키를 설정하기 위한 간소화된 버전에 대한 설명은 생략한다.

Setup : PKG는 임의의 값 $s \in Z_q^*$를 선택하여 자신의 마스터 비밀키로 두고 공개키 $P_{PKG} = sP$를 계산한다. 그리고 시스템 파라미터 $params = < G_1, G_2, q, e, P, P_{PKG}, H_1, H_2 >$을 공개한다. 이때 P는 G_1의 생성원(generator)이고, $H_1 : 0,1^* \rightarrow G_1$, $H_2 : G_1 \times G_1 \rightarrow G_2$는 암호학적 해시함수이다.

Private Key Extract : 사용자가 자신의 신원정보 ID를 PKG에게 등록하면 PKG 는 사용자의 식별과정을 처리하고 ID에 대한 개인키 $S_{ID} = sQ_{ID} = sH_1(ID)$를 안전한 채널을 통해 제공한다. 이때 $Q_{ID} = H(ID)$가 사용자의 ID로부터 유도된 개인키 S_{ID}에 대응되는 공개키가 된다.

Key exchange : 세 사용자 A, B, C가 각각 PKG로부터 자신의 개인키 S_A, S_B, S_C를 발급받았다고 가정할 때, A, B, C는 각각 세션 비밀값 $a, a' \in Z_q^*$, $b, b' \in Z_q^*$, $c, c' \in Z_q^*$ 를 선택하고 키 합의 프로토콜의 수행을 위해 다음과 같이 메시지를 교환한다.

$A \rightarrow B,\ C : P_A = aP,\ P_A' = a'P,$

$V_A = H_2(P_A, P_A')S_A + aP_A'$

$B \rightarrow A,\ C : P_B = bP,\ P_B' = b'P,$

$V_B = H_2(P_B, P_B')S_B + bP_B'$

$C \rightarrow B,\ A : P_C = cP,\ P_C' = c'P,$

$V_C = H_2(P_C, P_C')S_C + cP_C'$

사용자들은 자신의 개인키를 이용하여 키 교환 메시지에 대한 서명 $V_{i=A,B,C}$을 함께 전달하며, 수신자들은 서명 검증이 올바른 경우 각각 세션키를 계산한다. 프로토콜이 성공적으로 수행되면 사용자 A, B, C는 그림 1의 계산과정에 따라 모두 8개의 키 $K_{ABC}^i = K_A^i = K_B^i = K_C^i$ $(1 \leq i \leq 8)$ 를 설정하게 된다.

Liu 등이 제안한 3자간 키 합의 프로토콜은 사용자들이 한 번의 브로드캐스트를 통해 키를 계산할 수 있지만 프로토콜에 참여하는 모든 사용자들이 동일한 PKG를 통해 자신의 ID에 대한 개인키를 발급 받아야 한다. 만약 서로 다른 별개의 PKG로부터 사용자의 개인키가 발급된다면 서명 검증에 동일한 PKG의 공개키 P_{PKG}가 사용되지 못하고 각각의 PKG의 공개키가 사용되어야 하므로 서명 검증연산의 수정을 요구하게 되고, 이 경우 pairing e의 연산 횟수가 증가하게 되어 프로토콜의 수행에 대한

A verifies : $e(V_B + V_C, P) = e(H_2(P_B, P_B')Q_B + H_2(P_C, P_C')Q_C, P_{PKG}) \cdot e(P_B, P_B') \cdot e(P_C, P_C')$

A computes key :

$K_A^1 = e(P_B, P_C)^a = e(P,P)^{abc}$, $K_A^2 = (P_B, P_C')^a = e(P,P)^{abc'}$, $K_A^3 = e(P_B', P_C)^a = e(P,P)^{ab'c}$,

$K_A^4 = e(P_B', P_C')^a = e(P,P)^{ab'c'}$, $K_A^5 = (K_A^1)^{a^{-1}a'} = e(P,P)^{a'bc}$, $K_A^6 = (K_A^2)^{a^{-1}a'} = e(P,P)^{a'bc'}$,

$K_A^7 = (K_A^3)^{a^{-1}a'} = e(P,P)^{a'b'c}$, $K_A^8 = (K_A^4)^{a^{-1}a'} = e(P,P)^{a'b'c'}$

B verifies : $e(V_A + V_C, P) = e(H_2(P_A, P_A')Q_A + H_2(P_C, P_C')Q_C, P_{PKG}) \cdot e(P_A, P_A') \cdot e(P_C, P_C')$

B computes key :

$K_B^1 = e(P_A, P_C)^b = e(P,P)^{abc}$, $K_B^2 = (P_A, P_C')^b = e(P,P)^{abc'}$, $K_B^3 = (K_B^1)^{b^{-1}b'} = e(P,P)^{ab'c}$,

$K_B^4 = (K_B^2)^{b^{-1}b'} = e(P,P)^{ab'c'}$, $K_B^5 = e(P_A', P_C) = e(P,P)^{a'bc}$, $K_B^6 = e(P_A', P_C') = e(P,P)^{a'bc'}$,

$K_B^7 = (K_B^5)^{b^{-1}b'} = e(P,P)^{a'b'c}$, $K_B^8 = (K_B^6)^{b^{-1}b'} = e(P,P)^{a'b'c'}$

C verifies : $e(V_A + V_B, P) = e(H_2(P_A, P_A')Q_A + H_2(P_B, P_B')Q_B, P_{PKG}) \cdot e(P_A, P_A') \cdot e(P_B, P_B')$

C computes key :

$K_C^1 = e(P_B, P_A)^c = e(P,P)^{abc}$, $K_C^2 = (K_C^1)^{c^{-1}c'} = e(P,P)^{abc'}$, $K_C^3 = e(P_B', P_A)^c = e(P,P)^{ab'c}$,

$K_C^4 = (K_C^3)^{c^{-1}c'} = e(P,P)^{ab'c'}$, $K_C^5 = e(P_B, P_A')^c = e(P,P)^{a'bc}$, $K_C^6 = (K_B^5)^{c^{-1}c'} = e(P,P)^{a'bc'}$,

$K_C^7 = e(P_B', P_A')^c = e(P,P)^{a'b'c}$, $K_C^8 = (K_C^7)^{c^{-1}c'} = e(P,P)^{a'b'c'}$

그림 1. Liu 등의 프로토콜에서 서명검증과 키 생성

효율성을 저하시키게 된다.

Ⅲ. 제안 프로토콜

본 장에서는 Liu 등이 제안한 프로토콜의 효율성을 개선한 신원기반의 3자간 키 합의 프로토콜을 제안한다. 제안 기법도 인증된 프로토콜의 수행을 위해 키 교환 메시지에 대한 서명을 부가하며 이때 사용되는 서명기법은 DH형태의 키 교환 메시지와 부합될 수 있는 Yi의 신원기반 서명기법[23]을 가정한다. 그러나 모듈화된 프로토콜의 설계측면에서, DH 메시지와 부합될 수 있는 새로운 효율적인 서명기법이 제안된다면 서명기법만 교체하여 그대로 적용할 수도 있다.

그리고 프로토콜에 참여하는 사용자들이 모두 동일한 PKG를 통해 자신의 개인키를 발급 받을 필요는 없으며, 한 번의 브로드캐스트를 통해 동시에 키 교환 메시지를 교환함으로써 3자간에 8개의 세션키를 설정할 수 있다. 최근 신원기반 암호시스템의 연구에서 PKG의 개인키 발급에 대한 키 위탁(escrow) 성질을 방지할 수 있는 개인키 발급에 대한 연구가 주요 이슈가 되고 있지만 제안 기법에서는 PKG의 신뢰성을 가정하여 개인키 자체에 대한 위탁에 대해서는 고려하지 않는다. 그러나 비록 PKG가 사용자의 개인키를 발급하더라도 사용자들간에 교환되는 메시지로부터 세션키를 획득할 수는 없다.

본 장에서는 먼저 프로토콜에 참여하는 사용자들이 모두 동일한 PKG로부터 개인키를 발급 받는 환경에서의 프로토콜을 설명하고, 서로 다른 PKG가 관여하는 경우의 프로토콜을 설명한다.

1. 단일 PKG 환경

제안 프로토콜은 PKG가 시스템 파라미터들을 생성하는 Setup 단계와 사용자들이 PKG의 식별과정을 거쳐 자신의 ID에 대한 개인키를 발급하는 Private key extract 단계, 그리고 사용자들간에 키를 교환하는 Key exchange 단계로 구성된다.

Setup : PKG는 시스템 파라미터 $Params = < G_1, G_2, q, e, P, P_{PKG}, H_1, H_2 >$ 생성하여 공개하고, $s \in Z_q^*$는 PKG의 마스터 비밀키로 안전하게 보관한다. 여기서 P는 G_1의 생성원이며, $P_{PKG} = sP$는 PKG의 공개키이다. 그리고 $H_1 : 0,1^* \rightarrow G_1$과

A verifies : $e(P, V_B + V_C) = e(P_{PKG}, H_2(P_B, P_B')Q_B + H_2(P_C, P_C')Q_C + P_B' + P_C')$

A computes :

$K_A^1 = (P_B, P_C)^a = e(P,P)^{abc}$, $K_A^2 = (P_B, P_C')^a = e(P,P)^{abc'}$, $K_A^3 = e(P_B', P_C)^a = e(P,P)^{ab'c}$,

$K_A^4 = e(P_B', P_C')^a = e(P,P)^{ab'c'}$, $K_A^5 = (K_A^1)^{a^{-1}a'} = e(P,P)^{a'bc}$, $K_A^6 = (K_A^2)^{a^{-1}a'} = e(P,P)^{a'bc'}$,

$K_A^7 = (K_A^3)^{a^{-1}a'} = e(P,P)^{a'b'c}$, $K_A^8 = (K_A^4)^{a^{-1}a'} = e(P,P)^{a'b'c'}$

B verifies : $e(P, V_A + V_C) = e(P_{PKG}, H_2(P_A, P_A')Q_A + H_2(P_C, P_C')Q_C + P_A' + P_C')$

B computes :

$K_B^1 = (P_A, P_C)^b = e(P,P)^{abc}$, $K_B^2 = (P_A, P_C')^b = e(P,P)^{abc'}$, $K_B^3 = (K_B^1)^{b^{-1}b} = e(P,P)^{ab'c}$,

$K_B^4 = (K_B^2)^{b^{-1}b} = e(P,P)^{ab'c'}$, $K_B^5 = e(P_A', P_C)^b = e(P,P)^{a'bc}$, $K_B^6 = e(P_A', P_C')^b = e(P,P)^{a'bc'}$

$K_B^7 = (K_B^5)^{b^{-1}b} = e(P,P)^{a'b'c}$, $K_B^8 = (K_B^6)^{b^{-1}b} = e(P,P)^{a'b'c'}$

C verifies : $e(P, V_B + V_A) = e(P_{PKG}, H_2(P_B, P_B')Q_B + H_2(P_A, P_A')Q_A + P_B' + P_A')$

C computes :

$K_C^1 = e(P_B, P_A)^c = e(P,P)^{abc}$, $K_C^2 = (K_C^1)^{c^{-1}c} = e(P,P)^{abc'}$, $K_C^3 = e(P_B', P_A)^c = e(P,P)^{ab'c}$,

$K_C^4 = (K_C^2)^{c^{-1}c} = e(P,P)^{ab'c'}$, $K_C^5 = e(P_B, P_A')^c = e(P,P)^{a'bc}$, $K_C^6 = (K_C^5)^{c^{-1}c} = e(P,P)^{a'bc'}$

$K_C^7 = e(P_B', P_A')^c = e(P,P)^{a'b'c}$, $K_C^8 = (K_C^7)^{c^{-1}c} = e(P,P)^{a'b'c'}$

그림 2. 단일 PKG 환경에서의 키 교환 메시지의 검증과 키 생성 과정

$H_2 : G_1 \times G_1 \rightarrow Z_q^*$는 암호학적 일방향 해시함수이다.

Private key extract : PKG는 사용자 A에 대한 ID_A를 확인하고 A의 개인키를 다음과 같이 생성하여 안전하게 전달한다.

$$S_A = sQ_A = sH_1(ID_A)$$

이 경우 PKG에 연관되는 사용자 A의 ID_A에 대한 공개키는 $Q_A = H_1(ID_A)$로 계산될 수 있다.

Key exchange : 사용자 A, B, C가 각각 PKG로부터 자신의 개인키 S_A, S_B, S_C를 발급받았다고 가정할 때, 각자 자신의 세션 비밀값 $a, a' \in Z_q^*$, $b, b' \in Z_q^*$, $c, c' \in Z_q^*$ 를 선택하고 다음과 같이 키 교환 메시지를 전달한다.

$A \rightarrow B,\ C : P_A = aP,\ P_A' = a'P,$

$V_A = H_2(P_A, P_A')S_A + a'P_{PKG}$

$B \rightarrow A,\ C : P_B = bP,\ P_B' = b'P,$

$V_B = H_2(P_B, P_B')S_B + b'P_{PKG}$

$C \rightarrow B,\ A : P_C = cP,\ P_C' = c'P,$

$V_C = H_2(P_C, P_C')S_C + c'P_{PKG}$

이때 $\langle P_A', V_A \rangle$는 3자간 DH 파라미터 $P_A = aP$를 메시지로 하는 서명[22]이 되고, $P_A = a'P$ 를 DH 파라미터로 하는 경우 aP_{PKG}를 이용하여 서명 V_A'를 계산함으로써 $\langle P_A, V_A' \rangle$를 $P_A = a'P$ 에 대한 서명으로 구성할 수도 있다.

상대방으로부터 메시지를 수신하고 나면 각 사용자는 수신한 메시지를 그림 2와 같이 검증한다. 만일 서명 검증이 실패하는 경우 프로토콜의 수행은 중단되며, 서명 검증에 대한 정확성(correctness)은 그림 3의 검증식에 의해 증명된다.

서명 검증이 올바른 경우 각 사용자는 세션키를 그림 2의 계산식에 따라 계산한다. 프로토콜이 성공적으로 수행되면 사용자 A, B, C는 모두 8개의 공유키 $K_{ABC}^i = K_A^i = K_B^i = K_C^i$ $(1 \le i \le 8)$를 설정하게 된다.

그림 2의 계산과정에서도 알 수 있듯이 제안 프로토콜은 서명 검증에 2번, 키 계산에 4번의 pairing 연산이 사용된다. Liu 등의 기법과 세부적인 효율성 비교는 Ⅳ장에서 다루도록 한다. 그리고 Liu 등의 간소화된 프로토콜과 마찬가지로 제안 프로토콜도 각 사용자가 하나의 세션 비밀값 a, b, c를 각각 이용하여 단일 공유키 $K_{ABC} = e(P,P)^{abc}$를 설정하도록 구성할 수도 있지만 본 논문에서는 단일 세션키 설정에 대한 설명은 생략한다.

2. 다중 PKG 환경

본 절에서는 프로토콜에 참여하는 사용자들이 동일한 PKG가 아닌 서로 다른 PKG로부터 자신의 ID에 대한 개인키를 발급 받는 환경에서도 제안 프로토콜이 가능함을 보이도록 한다. 다중 PKG 환경을 고려함에 있어서 모든 PKG가 서로 다른 시스템 파라미터들을 사용하여 완전히 독립적으로 구성된다면 수학적 계산의 불일치로 인해 프로토콜이 효율적으로 수행될 수 없으므로, 본 논문에서는 각 PKG가 서로 다른 마스터 비밀키를 이용하여 사용자의 개인키를 발급함을 의미하며, PKG들간에 프로토콜의 구성을 위한 타원곡선의 명세와 생성원 $P \in G_1$ 그리고 암호학적 해시함수 등에 대한 동의가 이루어져 있다고 가정한다[6,16]. 이러한 가정들은, 예를 들어, 회사에서 지점이나 부서별로 PKG를 두는 것처럼 서브 도메인별로 별개의 PKG를 두는 환경에서는 타당할 것이다. 그리고 사용자의 식별정보나 이메일 주소처럼 통신 상대방을 식별할 수 있는 정보

$$\begin{aligned} e(P, V_B + V_C) &= e(P, V_B)e(P, V_C) \\ &= e(P,\ H_2(P_B, P_B')S_B + b'P_{PKG})e(P,\ H_2(P_C, P_C')S_C + c'P_{PKG}) \\ &= e(P_{PKG},\ H_2(P_B, P_B')Q_B + b'P)e(P_{PKG},\ H_2(P_C, P_C')Q_C + c'P) \\ &= e(P_{PKG},\ H_2(P_B, P_B')Q_B + H_2(P_C, P_C')Q_C + P_B' + P_C') \end{aligned}$$

그림 3. 서명검증에 대한 정확성 증명식

가 공개키로 사용될 수 있고 신원에 대한 공개키는 사용자가 속한 PKG의 공개키에 대한 유효성과도 결부되므로, PKG들의 공개키에 대한 신뢰성은 일반적인 PKI기반의 인증서를 사용하여 보장할 수 있을 것이다.

본 절에서는 다중의 PKG 환경에서의 프로토콜 수행을 설명하기 위해 사용자 A, B, C가 각각 PKG_1, PKG_2, PKG_3로부터 개인키를 발급 받는다고 가정한다.

Setup : PKG_i는 자신의 마스터 비밀키 $s_i \in Z_q^*$를 선택하여 공개키 $P_{PKG_i} = s_i P$를 계산하고, 공개 파라미터 $Params = < G_1, G_2, q, e, P, P_{PKG_i}, H_1, H_2 >$ 를 공개한다. 이때 s_i는 각 PKG_i의 비밀값이며, PKG_i의 공개키는 인증된 형태로 배포된다고 가정한다.

Private key extract : $PKG_i (i = 1,2,3)$는 각각 사용자 A, B, C에 대한 ID_A, ID_B, ID_C를 확인하고 각 사용자의 개인키를 아래와 같이 생성하여 안전하게 전달한다.

$$PKG_1 : S_A = s_1 Q_A = s_1 H_1(ID_A)$$
$$PKG_2 : S_B = s_2 Q_B = s_2 H_1(ID_B)$$
$$PKG_3 : S_C = s_3 Q_C = s_3 H_1(ID_C)$$

Key exchange : 사용자 A, B, C가 각각 PKG_i로부터 자신의 개인키 S_A, S_B, S_C를 발급 받았다고 가정할 때, 각자 자신의 세션 비밀값 $a, a' \in Z_q^*$, $b, b' \in Z_q^*$, $c, c' \in Z_q^*$ 를 선택하고 다음과 같이 키 교환 메시지를 전달한다. 이 경우, 단일 PKG 환경과의 차이점은 서명을 계산할 때 각 사용자가 소속된 해당 PKG_i의 공개키 P_{PKG_i}가 사용된다는 것이다.

$$A \rightarrow B,\ C : P_A = aP,\ P_A' = a'P,$$
$$V_A = H_2(P_A, P_A') S_A + aP_{PKG_1}$$
$$B \rightarrow A,\ C : P_B = bP,\ P_B' = b'P,$$
$$V_B = H_2(P_B, P_B') S_B + bP_{PKG_2}$$
$$C \rightarrow B,\ A : P_C = cP,\ P_C' = c'P,$$
$$V_C = H_2(P_C, P_C') S_C + cP_{PKG_3}$$

상대방으로부터 메시지를 수신하고 나면 각 사용자는 수신한 메시지를 그림 4와 같이 검증한다. 검증에 실패하면 프로토콜을 중단하게 되고, 서명 검증에 성공하면 3.1절의 키 계산과 동일한 방법으로 8개의 공유키를 생성할 수 있다.

Ⅳ. 제안기법 분석

본 장에서는 3장에서 제안한 프로토콜의 안전성과 효율성에 대해 분석한다. 안전성 분석과 관련하여 3장에서 서술한 요구사항에 따라 발생 가능한 몇 가지 공격들을 가정하여 제안 기법의 안전성을 분석하도록 한다. 그리고 효율성 비교를 위해 Liu의 기법과 연산량의 횟수를 비교한다.

1. 안전성

제안 프로토콜의 안전성은 DLP와 BDHP의 어려움을 근간으로 하며, 키 교환 메시지에 대한 인증은 서명을 통해 제공되고, 세션키에 대한 안전성은 각 사용자들이 해당 세션마다 임의적으로 선택한 세션 비밀값에 의해 결정된다. 비록 공격자가 도청 등을 통해 각 사용자들의 $\langle aP, bP, cP \in G_1 \rangle$를 알고 있다고 하더라도 BDHP 문제의 어려움으로 인해 $e(P,P)^{abc}$를 계산하는 것은 어렵다. 제안 프로토콜의 키 교환 과정에서 사용자 A는 자신의 세션 비밀값 $(a, a') \in Z_q^*$ 를 선택하여 $P_A = aP$, $P_A = a'P$ 를 계산하고 이에 대한 서명값으로 $V_A = H_2(P_A, P_A') S_A + aP_{PKG}$를 부가하여 전송하고, 사용자 B와 C로부터 수신된 메시지를 $e(P, V_B + V_C) = e(P_{PKG}, H_2(T_B, T_B') Q_B + H_2(T_C, T_C') Q_C + T_B + T_C)$로 검증하

A verifies : $e(P, V_B + V_C) = e(P_{PKG_2}, H_2(P_B, P_B') Q_B + P_B) e(P_{PKG_3}, H_2(P_C, P_C') Q_C + P_C)$
B verifies : $e(P, V_A + V_C) = e(P_{PKG_1}, H_2(P_A, P_A') Q_A + P_A) e(P_{PKG_3}, H_2(P_C, P_C') Q_C + P_C)$
C verifies : $e(P, V_B + V_A) = e(P_{PKG_2}, H_2(P_B, P_B') Q_B + P_B) e(P_{PKG_1}, H_2(P_A, P_A') Q_A + P_A)$

그림 4. 다중 PKG 환경에서의 키 교환 메시지의 검증과정

였다. 이 때, 본 논문에서 사용된 서명은 Yi가 제안한 서명기법[23]을 제안된 키 합의 프로토콜에 적용한 것이며, 각 사용자의 개인키를 모르는 공격자가 해당 사용자로 위장하여 서명을 위조할 수는 없다. 그리고 제안 기법에서의 차이점은 다중 PKG 환경을 가정할 때, 서명의 생성과 검증에 동일한 키 발급 센터의 공개키 대신에 각 사용자들의 소속에 따라 서로 다른 키 발급 센터의 공개키가 사용될 수도 있다는 것이다.

이전에 제안된 프로토콜에서 발견된 보안 문제처럼, 만일 공격자가 다른 상대방들에게는 투명하도록 키 교환 메시지를 제어함으로써 상대방과 세션키를 공유하게 하는 공격도 가능할 것이다[2]. 제안 기법은 키 합의 프로토콜이 만족해야 하는 보안 요구사항들을 다음과 같이 제공할 수 있다.

- *알려진 세션키 안전성* (known session key security) : 제안 기법에 대한 이 성질은 매 세션마다 각 사용자들에 의해 선택되는 세션 비밀값에 의존한다. 만약 어떤 공격자가 이전의 세션키 $K=e(P,P)^{abc}$에 대한 정보를 획득했다 할지라도 $e(P,P)^{abc}$에서 세션 비밀값을 계산하는 것은 DLP 문제에 의해 어려우므로 이전 세션키에 대한 정보로 현재 세션키를 획득할 수 없다. 그리고 사용자들이 매 세션마다 새로운 비밀값을 사용할 경우 공격자가 이전의 세션 비밀값을 알고 있다 할지라도 새로운 세션에 대한 키를 계산할 수 없다. 또한 복수개의 공유키를 설정하는 경우, 공격자가 어떤 키, 예를 들어, $K^1=e(P,P)^{abc}$를 알고 있다고 할지라도 역시 DLP 문제를 해결할 수 없다면 a나 b 또는 c가 사용된 다른 어떤 키도 획득할 수 없다.
- *전방 비밀성* (forward secrecy) : 어떤 사용자 A의 개인키 S_A가 노출되었다고 가정할 때, 공격자는 수집된 A의 브로드캐스트 메시지 $P_A=aP$, $P_A=a'P$ 와 $V_A=H_2(P_A,P_A')S_A+aP_{PKG}$를 이용하여 $aP_{PKG}=V_A-H(P_A,P_A)S_A$를 계산할 수 있다. 그러나 공격자가 비록 aP_{PKG}는 계산할 수 있을지라도 이산대수문제(DLP)의 어려움에 의해 a를 구하는 것은 어려우며, a를 모르는 경우 $e(P_B,P_C)^a=e(P,P)^{abc}$를 획득할 수 없다. 그러므로 제안 기법은 전방 비밀성을 제공한다. 만일 모든 사용자의 비밀키 S_A, S_B, S_C가 노출되었다고 가정하더라도, $\{aP_{PKG}, bP_{PKG}, cP_{PKG}\}$에서 각 사용자의 세션 비밀값 a, b, c 중 어느 하나도 구할 수 없다면 이전의 세션키를 계산할 수 없다.
- *키 노출 위장에 대한 안전성*(key-compromise impersonation resilience) : 어느 사용자 A의 개인키 S_A가 노출된 경우 공격자는 다른 사용자들에게 사용자 A로 위장하여 프로토콜에 참여 할 수 있다. 그러나 공격자가 A에게 다른 사용자 B나 C로 위장하기 위해서는 B나 C의 서명을 위조할 수 있어야 한다. 그러나 서명 기법에 대한 안전성을 가정할 때, A의 개인키 S_A에 대한 정보만으로 B나 C의 서명을 생성할 수 없으므로 공격자는 A이외의 다른 사용자로 위장할 수는 없다.
- *미지의 키 공유에 대한 안전성* (unknown key-share resilience) : 공격자가 프로토콜에 참여한 사용자들에게 사용자 자신들이 의도한 상대방과 키를 설정했다고 확신시키기 위해서는 공격자가 다른 사용자로 위장하는 것이 가능해야 한다. 즉 사용자 A에 대해, A가 B와 C라고 생각하는 사용자들과 공유한 키가 실제로는 B′, C′와 공유되는 키가 되도록 하기 위해서 공격자는 B, C의 공개키로 사용되는 ID_B, ID_C를 $ID_{B'}$, $ID_{C'}$로 대체할 수 있거나 B′와 C′의 개인키를 알고있어야만 가능하다. 그러나 신원기반 기법에서 어떤 개체가 B나 C라고 주장하기 위해서는 PKG에게 자신의 신원을 증명할 수 있어야만 B나 C의 신원에 대한 올바른 개인키를 발급 받을 수 있으므로 PKG가 올바른 신원에 대한 개인키를 발급한다고 가정할 때, 공격자가 프로토콜에 참여한 다른 사용자의 개인키를 알지 못하는 한 제안된 프로토콜은 이 성질을 만족한다.
- *키 제어에 대한 안전성* (no key control) : 제안 프로토콜의 수행을 통해 합의된 키는 각 사용자들이 임의적으로 선택한 세션 비밀값에 의해 결정되므로, 어느 특정 사용자가 미리 선택된 값을 세션키로 도출하도록 프로토콜에 영

2) 공격자는 조작된 메시지를 이용하여 비정상적으로 프로토콜을 수행할지라도 상대방은 이를 인지하지 못하고 정상적인 프로토콜과 동일한 계산과정을 수행함으로써 공격자와 키를 공유하게 되는 공격.

향을 끼치지 못한다.

일반적으로 신원기반 암호시스템에서는 PKG가 사용자의 개인키를 발급하므로 PKG에 대한 키 위탁(key escrow) 성질을 가지게 된다. 최근 신원기반 암호시스템에서 이러한 키 위탁 성질을 방지하기 위한 연구도 이슈로 부각되고 있지만 제안 기법에서는 키 위탁에 대해서는 고려하지 않았다. 전방향 비밀성과 관련하여 PKG가 개인키를 발급하는 신원기반 기법의 성질을 고려할 때, 비록 PKG가 사용자의 개인키를 알고 있다 할지라도 역시 DLP 문제의 어려움에 의해 어느 사용자의 세션 비밀값을 계산할 수 없다면 PKG도 사용자들간에 합의된 세션키를 획득할 수 없으므로 PKG에 대한 전방 비밀성도 제공할 수 있다. 그렇지만 PKG가 자신이 발급한 개인키들을 이용하여 자신에게 등록된 다른 사용자들로 위장하는 것은 가능하므로, 본 논문에서는 PKG를 신뢰센터로 간주하여 다른 사용자로 위장하여 프로토콜에 관여하지 않을 것이라는 신뢰성을 가정한다.

2. 효율성 비교

제안 기법의 효율성을 Liu 등이 제안한 3자간 키 합의 프로토콜 중 간소화된 버전과 비교하여 pairing 연산, 타원곡선상의 점들에 대한 G_1에서의 스칼라 곱셈연산, G_2에서의 지수연산의 횟수에 대해 표 2에 정리하였다. Liu 등의 기법은 서명 검증에 4번, 키 계산에 4번의 pairing 계산을 수행하며, 제안 기법은 서명 검증에 단일 PKG인 경우 2번, 다중 PKG인 경우 3번이 필요하고 키 계산에 4번의 pairing 연산을 수행한다. Pairing을 이용한 암호시스템에서 연산의 대부분은 pairing이 차지하게 되므로 제안 기법이 Liu 등의 기법보다 효율적으로 수행될 수 있다.

표 2에 나타나듯이 프로토콜의 효율성은 서명 검증연산의 차이에 의해 나타나고 있음을 알 수 있다. 제안 프로토콜에 사용된 서명 검증 절차는 두 개의 신원기반 서명에 대한 일종의 일괄검증(Batch verification)[24]이며, pairing의 bilinearity 성질로 인해 2(또는 n)개의 서명에 대한 일괄검증은 2번(또는 n번)의 개별 서명 검증보다 효율적으로 수행될 수 있는 특징을 가지게 된다. 제안 프로토콜은 3자간 DH 키 교환 파라미터인 $<aP, a'P>$를 메시지로 하면서 동시에 생성된 서명의 일부로 적용된 것이므로, 3자간 DH 프로토콜과 부합될 수 있는 새로운 효율적인 서명기법이 제안된다면 시스템의 서명모듈만 변경함으로써 더 효율적으로 적용될 수 있을 것이다.

표 2. Liu 등의 프로토콜과 제안 프로토콜 비교

	Liu et al.		제안 프로토콜	
Pairing	검증	키 계산	검증	키 계산
	4	4	2 (3)	4
스칼라 곱셈	6		6	
지수연산	8		8	
라운드	1		1	
대역폭	$3\|G_1\|$		$3\|G_1\|$	
다중 PKG	X		O	

제안 프로토콜과 Liu 등의 프로토콜 모두 1라운드 프로토콜이므로 사용자들은 프로토콜의 수행을 위해 순차적인 메시지 교환이 필요가 없으며 다른 사용자들에게 한 번의 브로드캐스트를 통해 3개의 메시지를 전송함으로써 키를 계산할 수 있다. 그러나 제안 프로토콜은 별개의 PKG로부터 독립적으로 개인키를 발급 받는 경우에도 프로토콜의 수행이 가능하다는 특징을 가진다. Liu 등이 제안한 프로토콜도 서로 다른 PKG가 관여하는 형태로 변형이 가능하지만, 이 경우 서명 검증 연산의 수정이 불가피하며 pairing의 연산이 증가하게 되어 역시 제안기법보다 효율성이 저하된다.

V. 결 론

최근 공개키 암호분야에서는 신원기반의 암호시스템에 대한 연구가 활발히 진행되어 오고 있다. 이에 따라 신원기반의 암호기법과 서명기법뿐만 아니라 키 합의 프로토콜이 제안되고 있으나 대다수의 연구들이 안전하지 않은 것으로 판명되었다. 본 논문에서는 신원기반의 3자간 키 합의 프로토콜을 제안하였으며, 제안 기법은 키 교환 메시지에 송신자의 서명을 추가함으로써 인증을 제공하도록 하였다. 또한 프로토콜에 참여한 사용자들이 모두 동일한 PKG로부터 자신의 개인키를 발급 받을 필요는 없으며 프로토콜에 참여하는 사용자들이 자신의 소속에 따라 서로 다른 PKG로부터 발급 받은 개인키를 이용하

는 경우에도 프로토콜의 수행이 가능하다. 따라서 사용자들이 특정 PKG에 의존하지 않고 자신이 의도하는 PKG로부터 키를 발급 받음으로써 보다 실용적으로 적용될 수 있을 것이다. 그러나 이 경우 PKG들간에 시스템 파라미터에 대한 동의를 전제로 하고 있으며, PKG들이 완전히 서로 다른 시스템 파라미터를 사용하여 개인키를 발급하는 환경에서의 키 합의 프로토콜에 대한 연구는 계속 연구되어야 할 과제이다. 또한 다중 PKG가 관여하는 신원기반 기법의 응용의 경우, 서로 다른 PKG에 소속된 사용자들의 ID에 대한 유효성의 검증이 필요하게 되므로 이에 대해서도 고려되어야 할 것이다. 향후 제안된 3자간 키 합의 프로토콜을 기반으로 다자간(multi-party) 또는 그룹 키(group key) 합의 프로토콜로의 확장에 대해 연구과제로 남겨두고 있다.

참 고 문 헌

[1] W. Diffie and M. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, No 22, pp.644-654, 1976.

[2] A. Joux, "A one-round protocol for tripartite Diffie-Hellman", Springer, Algorithm Number Theory Symposium-ANTS, Lecture Notes in Computer Science 1983, pp.385-394, 2000.

[3] A. Shamir, "Identity-based cryptosystems and signature schemes", Springer, Advances in Cryptology - CRYPTO '84, Lecture Note in Computer Science 196, pp.47-53, 1984.

[4] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing. Springer, Advances in Cryptology - CRYPTO 01, Lecture Notes in Computer Science 2139, pp.213-229, 2001.

[5] N. P. Smart, "An identity based authenticated key agreement protocol based on the Weil pairing", IEE Electronics Letters, 38: pp.630-632, 2002.

[6] L. Chen and C. Kudla, "Identity-based authenticated key agreement protocols from pairings", Proceedings of the 16th IEEE Computer Security Foundations Workshop, pp.219-233, 2003

[7] K. Shim, "Efficient ID-based authenticated key agreement protocol based on Weil pairing", IEE Electronics Letters, 39(8), pp653-654, 2002.

[10] Z. Chen, "Security analysis on Nalla-Reddy's ID-based tripartite authenticated key agreement protocols", Cryptology ePrint Archive, Report 2003/103, 2003. available at http://eprint.iacr.org/2003/103.

[9] D. Nalla, K. C. Reddy, "ID-based tripartite authenticated key agreement protocols from pairings", Cryptology ePrint Archive, Report 2003/004, 2003, available at http://eprint.iacr.org/2003/004.

[10] Z. Chen, "Security analysis on Nalla-Reddy's ID-based tripartite authenticated key agreement protocols", Cryptology ePrint Archive, Report 2003/103, 2003. available at http://eprint.iacr.org/2003/103.

[11] K. Shim, "Cryptanalysis of ID-based tripartite authenticated key agreement protocols", Cryptology ePrint Archive, Report 2003/115, 2003, available at http://eprint.iacr.org/2003/115.

[12] D. Nalla, "ID-based tripartite key agreement with signatures", Cryptology ePrint Archive, Report 2003/144, 2003, available at http://eprint.iacr.org/2003/144.

[13] F. Zhang, S. Liu and K. Kim, "ID-based One Round Authenticated Tripartite Key Agreement Protocol with Pairings", Cryptology ePrint Archive, Report 2002/122, 2002, available at http://eprint.iacr.org/2002/122

[14] S. Liu, F. Zhang, K. Chen, "ID-based tripartite key agreement protocol

with pairings", Proceedings of IEEE International Symposium on Information Theory, pp.136, 2003.

[15] K. Kim, E. Ryu and K. Yoo, "ID-Based Authenticated Multiple-Key Agreement Protocol from Pairings", Springer, International Conference on Computational Science and its Applications(ICCSA 2004), Lecture Notes in Computer Science 3046, pp.672-689, 2004.

[16] N. McCullagh, P. S. L. M. Barreto, "A new two-party identity-based authenticated key agreement", Cryptology ePrint Archive, Report 2004/122, available at http://eprint.iacr.org/2004/122.

[17] G. Xie, "Cryptanalysis of Noel McCullagh and Paulo S. L. M. Barreto Two-Party Identity-Based Key Agreement", Cryptology ePrint Archive, Report 2004/308, 2004. available at http://eprint.iacr.org/2004/308.

[18] K. R. Choo, "Revisit of McCullagh-Barreto Two-Party Identity-Based Authenticated Key Agreement Prot ocols", Cryptology ePrint Archive, Report 2004/343, 2004, available at http://eprint.iacr.org/2004/343.

[19] 이상원, 천정희, 김용대, "Pairing을 이용한 트리기반의 그룹키 합의 프로토콜", 정보보호학회, 정보보학회논문지 13권 3호, pp.101-110, 2003.

[20] G. Frey, M. Muller, and H. Ruck, "The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems", IEEE Transactions on Information Theory, 45(5): pp. 1717-1719, 1999.

[21] S. Galbraith, "Supersingular curves in cryptography", Springer, Advances in Cryptology-Asiacrypto '01, Lecture Notes in Computer Science 2248, Springer-Verlag, pp.495-513, 2001.

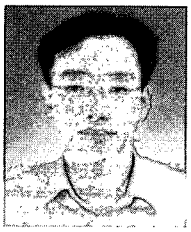
[22] S. Blake-Wilson, D. Johnson, A. Menezes, "Key agreement protocols and their security analysis", Springer, The 6th IMA International Conference on Cryptography and Coding, Lecture Notes in Computer Science 1355, pp.30-45, 1997.

[23] X. Yi, "An identity-based signature scheme from the Weil pairing", IEEE Communications Letters, Vol. 7, Issue 2, pp.76-78, 2003.

[24] H. Yoon, J. Cheon, and Y. Kim, "Batch Verifications with ID-based Signatures", Pre-Proceedings of The 7th International Conference on Information Security and Cryptology, pp.171-186., 2004.

〈著者紹介〉

이 경 현 (Kyung-Hyune Rhee)
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 8월: 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구소 연구원, 선임연구원
1993년 3월~현재: 부경대학교 전자컴퓨터정보통신공학부 전임, 조교수, 부교수, 교수
〈관심분야〉 암호이론, 암호 프로토콜, 네트워크 보안, 키 관리



박 영 호 (Young-Ho Park)
2000년 2월: 부경대학교 전자계산학과 졸업
2002년 2월: 부경대학교 전자계산학과 석사
2002년 3월~현재: 부경대학교 정보보호 박사과정
〈관심분야〉 암호 프로토콜, 암호기술 응용, 키 관리, 이동네트워크