情報保護學會論文誌
第15券 第1號, 2005. 2

유료 방송 시스템에 적합한 ID 기반의 2 라운드 그룹키 동의 프로토콜

김 현 주,†‡ 남 정 현, 김 승 주, 원 동 호
성균관대학교

Two-round ID-based Group Key Agreement Fitted for Pay-TV System

Hyunjue Kim,†‡ Junghyun Nam, Seungjoo Kim, Dongho Won
Sungkyunkwan University

요 약

그룹키 동의 프로토콜은 일련의 그룹을 형성하는 다수의 통신 참여자들이 공개된 통신망을 통해 안전하고 효율적인 방법으로 그룹의 세션키를 설정하기 위한 목적으로 설계된다. 본 논문에서는 유료 방송 시스템과 같은 그룹중심의 응용이나 서비스에 적합한 ID 기반의 2 라운드의 그룹키 동의 프로토콜을 제안하고, 이의 안전성을 CDH 가정과 BDDH 가정에 기반하여 랜덤 오라클 모델에서 증명한다. 제안하는 프로토콜은 Nam이 제안한 3 라운드 그룹키 동의 프로토콜을 기초로 설계된 것으로, 개인식별정보에 기반한 암호 시스템을 사용하여 키 관리 절차를 보다 간단히 하였으며, 새로운 인증 메카니즘을 사용하여 키 전송 메시지들의 길이를 줄이고 결합적 단순성을 제공하였다. 또한 제안하는 프로토콜은 전송되는 메시지들에 대한 인증을 묶음(batch) 기법을 사용하여 검증하도록 설계하여 효율성을 더욱 개선시켰다.

ABSTRACT

A group key agreement protocol allows a group of users to share a key which may later be used to achieve certain cryptographic goals. In this paper, we propose a new scalable two-round ID-based group key agreement protocol which would be well fit to a Pay-TV system, additionally, to the fields of internet stock quotes, audio and music deliveries, software updates and the like. Our protocol improves the three round group key agreement protocol of Nam et al., resulting in upgrading the computational efficiency by using the batch verification technique in pairing-based cryptography. Also our protocol simplifies the key agreement procedures by utilizing ID-based system. We prove the security of our protocol under the Computational Diffie-Hellman assumption and the Bilinear Decisional Diffie-Hellman assumption. Also we analyze its efficiency.

Keywords : *Group key agreement protocol, Pay-TV system, Pairing, CDH assumption, BDDH assumption*

접수일 : 2004년 10월 16일 ; 채택일 : 2005년 1월 26일
* 본 연구는 정보통신부 지원 대학 IT 연구센터 육성지원 사업(C1090-0403-0005)으로 수행하였습니다.
† 주저자, ‡ 교신저자 : hjkim@dosan.skku.ac.kr

Ⅰ. 서 론

최근, 급속한 정보 통신 기술의 발달에 힘입어 인터넷의 활용 영역이 확대됨에 따라 원격회의, 실시간 정보 서비스, 유료 영상 서비스, 대화형 분산 시뮬레이션, 네트워크를 통한 공동작업, 다중 사용자 게임 등 여러 명의 사용자들에게 동일한 서비스를 제공해주기 위한 그룹중심의 응용이나 서비스가 증가하고 있다. 이 중 디지털 데이터 방송기술은 그룹중심 서비스로서 차세대 핵심 산업의 하나로 크게 주목받고 있다. 디지털 데이터 방송 서비스의 활성화를 위해서는 방송 콘텐츠의 보호, 송수신자간의 상호 인증 등 여러 가지 보안 서비스가 제공되어야 한다. 그러나 네트워크 상의 모든 통신은 언제 어디서든지 접근 가능하여 그룹내의 사용자에게 편리하게 이용될 수 있는 반면 누구든지 접근 가능하기 때문에 정보의 도청, 오남용, 변조 등 불법적인 행위가 발생할 위험에 노출되어 있다. 따라서 안전하고 실질적인 디지털 데이터 방송 시스템을 구축하기 위해서는 안전한 그룹 통신의 보장이 매우 절실히 필요하다. 안전한 그룹 통신이란 그룹에 속한 멤버들만이 안전하면서도 비밀스럽게 서비스를 받을 수 있도록 보장하는 것이다.

유료 방송 시스템은 방송 프로그램이나 데이터 서비스를 요금을 지불한 가입자들에게만 정상적으로 제공하고 그렇지 않은 미가입자들은 시청할 수 없도록 하는 상업적인 디지털 데이터 방송 시스템으로 서비스 제공자(service provider)인 방송국, 가입자(subscriber)들과 방송 프로그램으로 구성되어 있다. 유료 방송 시스템은 가입자(subscriber)들이 낸 시청료에 의존하기 때문에 방송 수신이 비허가된 미가입자들이나 시청료를 지불하지 않은 가입자들의 방송 도청 문제는 유료 방송 업계의 커다란 문제점이 된다. 그러므로 유료 방송 시스템의 재정적 안정을 유지하기 위해서는 시청료를 지불하지 않은 미가입자들은 정상적인 방송 신호를 수신할 수 없도록 하는 보안 서비스가 반드시 제공되어야 한다. 방송 콘텐츠의 보호, 송수신자간의 상호 인증 등 여러 가지 보안 서비스는 암호 기술을 이용하여 효율적으로 제공할 수 있다.

유료 방송 시스템에 적용되는 암호방식은 브로드캐스트 암호 방식과 그룹키 분배 프로토콜이 있다.[1] 1994년 Fiat와 Naor[2]에 의해 소개된 브로드캐스트 암호 방식은 하나의 암호화키와 무수히 많은 복호화키가 존재하는 방식으로 유료 방송 시스템에 일반적으로 많이 적용된다.[3-10] 브로드캐스트 암호 방식을 사용하는 유료 방송 시스템에서 브로드캐스트 메시지는 세션키를 암호화한 암호문이 포함되어 있는 권한블록(enabling block)과 이 세션키를 이용하여 방송 프로그램을 암호화한 메시지가 포함되어 있는 암호블록(cipher block)으로 구성되어 있으며, 방송국은 하나의 암호화키로 세션키를 암호화하고 각 사용자들은 사전에 부여받은 서로 다른 복호화키를 이용하여 이를 복호화한 후 이 세션키를 통하여 방송프로그램을 시청할 수 있도록 되어있다. 그러나 기존의 브로드캐스트 암호방식은 완전한 전방향 안전성을 만족하지 않는다는 단점을 가지고 있다. 그러므로 방송국이나 각 사용자들의 비밀키(long-term private key)가 노출이 된다면 권한이 없는 사용자들이 이전 세션에서 암호화되어 전송된 방송내용을 복호화하여 시청하는 문제점이 야기된다. 본 논문에서는 그룹키 분배 프로토콜을 유료 방송 시스템에 적용함으로서 이러한 문제를 해결한다.

유료 방송 시스템에 적합한 그룹키 분배 프로토콜을 설계할 때는 완전한 전방향 안전성을 만족하는 것 이외에 다음과 같은 유료 방송 시스템의 특징들이 모두 고려되어야 한다.

① 네트워크 토폴로지(Network topology)
- 성형 네트워크(Star network): 유료 방송 시스템에서의 유·무선 방송 네트워크의 토폴로지나 구성은 성형이고, 방송국은 방송 프로그램을 모든 가입자들에게 일대다(one-to-all)로 브로드캐스트(broadcast)한다. 프로토콜을 설계 시 이러한 유료 방송 시스템의 네트워크 구조를 충분히 고려하여 설계해야한다.

② 효율성(Efficiency)
- 가입자의 연산량 최소화: 유료 방송 시스템에서 시스템을 구성하는 방송국과 가입자는 메모리나 계산적 능력 면에서 비대칭적(asymmetry) 관계에 있다. 방송국의 서버(broadcasting server)는 연산능력과 메모리와 같은 시스템 자원이 풍부하지만, 가입자들이 사용하는 이동 단말기와 같은 CPU나 셋톱박스(STB: Set-top box)등은 방송국의 서버에 비해 상대적으로 제한된 연산능력과 메모리를 보유하고 있다. 그러므로 프로토콜 설계 시 각 사용자들이 보유

하고 있는 시스템 자원을 충분히 고려하여 설계해야 한다.

- 키 관리(Key management): 사용자가 유료 방송을 시청하기 위해서는 먼저 유료 방송 시스템에 가입한 후 암호화되어 전송되는 방송 프로그램을 시청할 수 있는 세션키를 발급 받아야 한다. 키는 암호학적 기술에 의존하는 보안시스템에서 가장 중요한 요소이므로 세션키에 대한 효율적인 관리가 매우 중요하다. 암호 방식은 사용하는 공개키의 형태에 따라 공개키 인증서에 기반한 방식과 개인식별정보에 기반한 방식으로 나뉜다. 1984년 Shamir[11]에 의해 소개된 개인식별정보에 기반한 암호 방식은 사용자의 개인식별 정보인 ID자체가 공개키의 역할을 하는 암호 방식으로, 인증서에 기반한 암호방식에서처럼 저장하거나 검증할 인증서가 별도로 없기 때문에 계산량이나 사용되는 메모리 면에서 효율적이며 송·수신자간에 공개키를 교환할 필요가 없는 암호방식이다. 유료 방송 시스템에서 ID는 STB의 고유번호(Serial number)로 사용가능하므로 개인식별정보에 기반한 암호 방식을 사용함으로서 키관리 절차를 보다 간단히 할 수 있다.

③ 안전성(Security)

- 완전한 전방향 안전성(PFS: Perfect Forward Secrecy): 일반적으로 각 사용자들은 자신만이 알고 있는 비밀키를 소유하고 있으며, 유료 방송 시스템의 한 세션에서, 방송 프로그램을 암·복호화할 때 사용되는 세션키를 생성하는 과정에서 이 비밀키를 사용하게 된다. 만약 이 비밀키들이 노출된다고 하더라도 공격자는 이전 세션에서 암호화되어 전송된 방송내용을 복호화하여 시청할 수 없어야 한다. 방송국이나 가입자들의 비밀키가 노출되더라도 공격자가 과거에 사용된 세션키를 알아 낼 수 없을 때 완전한 전방향 안전성을 만족한다고 말한다.[12]
- 키 기여(Key contribution): 그룹키 분배 프로토콜을 설계 할 때, PFS를 만족하기 위해서는 기여하는 키 동의 프로토콜(contributory key agreement protocol)에 초점을 맞추어서 설계하여야 한다.[13,14] 분담하는 키 동의 프로토콜은 세션키를 공유하고자하는 그룹내의 모든 사용자들의 합의에 의해서 비밀 세션키를 생성하는 방식으로, 어느 누구도 사전에 세션키 값을 결정할 수 없는 방식이다. 그리고 정직하게 행동하는 사용자는, 세션키를 생성하는 과정에서 랜덤한 값을 선택한다면, 그룹에 속한 모든 다른 사용자들이 협력하더라도 생성된 세션키를 알아낼 수 없다는 사실을 보장할 수 있게 된다.

본 논문에서는 위의 열거된 모든 조건들을 모두 만족하는 안전한 그룹키 동의 프로토콜을 제안한다. 그룹키 설정에 관한 연구는 1982년 I. Ingemarsson, D. Tang와 C. Wong[15]에 의해서 처음으로 시작되었다. 이후 많은 프로토콜들이 발표되었으며[16-26], 안전성이 증명 가능한 그룹키 설정 프로토콜에 관한 연구는 2001년 Bresson[27-29]에 의해 이루어졌다. 그러나 Bresson이 제안한 프로토콜은 라운드 복잡도가 그룹 구성원들의 수에 관하여 선형(linear)이 된다는 문제점이 있기 때문에 그룹 사이즈가 커지면 현실적으로 실용화되기 어렵다. 2003년 Boyd와 Bresson[30]은 이러한 문제점을 해결한 안전성이 증명 가능한 효율적인 프로토콜을 제안하였다. 그러나 이들의 프로토콜들은 PFS를 만족하지 못한다. PFS를 만족하면서 상수 라운드를 갖는 프로토콜은 2003년 Katz와 Yung[31]에 의하여 제안되었다. 이들은 또한 [17]의 2라운드 프로토콜에 대한 안전성을 증명하였다. 그리고 최근 2004년 Choi[32]가 [17]의 프로토콜을 타원곡선 암호 시스템에 적용시켜, Pairing을 이용한 ID 기반 그룹키 동의 프로토콜을 제안하였다. 그러나 이들이 제안한 프로토콜들은 매우 효율적이긴 하지만 프로토콜이 완전 대칭적(symmetry)인 특징을 가지고 있기 때문에 비대칭적 관계에 있는 유료 방송 시스템에 적용하기에는 적당하지 않다. 더구나 이들이 제안한 프로토콜은 Zhang과 Chen[33]에 의해서 합법적 사용자 가장 공격(impersonation attack)에 안전하지 않음이 밝혀졌다. 비대칭적 환경에 적합한 그룹키 동의 프로토콜은 2003년 Bresson, Chevassut, Essiari와 Pointcheval[34]에 의해서 제안되었다. 이들은 저전력 모바일 장치에 적합한 그룹키 동의 프로토콜을 제안하였으나, 불행하게도 [34]의 프로토콜은 PFS를 만족하지 못한다. 또한[34]의 프로토콜은 Nam, Kim과 Won[35]에 의해서 안전하지 않음이 밝혀졌다.

Pairing은 처음 타원곡선상에서의 이산대수문제

의 공격에 사용되었으며, 2000년 Joux[36]에 의해 3자간 Diffie-Hellman 프로토콜 설계 시 이용 될 수 있음이 제안되어졌다. 그 후, 2001년, Boneh[37,38]은 실제로 구현 가능한 새로운 암호방식과 서명방식을 제안하였다. 이 제안이 이루어진 이후, Pairing을 이용한 새로운 형태의 암호 방식들이 활발히 연구되고 있다.[25,32,33,39-44]

본 논문에서는 최근 이슈가 되고 있는 Pairing을 사용하여 유료 방송 시스템에 적용 가능한 비대칭 그룹키 동의 프로토콜을 제안한다. 제안하는 프로토콜은 Nam[45,46]의 프로토콜을 기반으로 한 방식으로 위의 열거한 유료 방송 시스템의 특징들을 모두 만족하는 ID 기반의 인증된 그룹키 동의 프로토콜이다. 본 논문에서 사용된 인증 메카니즘은 [45,46]에서처럼 단순히 서명 기법을 사용한 것이 아니라 키 교환과 결합하여 전송 메시지들을 새롭게 구성한 방법이며, 또한 그룹키 생성시에 필요한 정보를 새로운 난수로 선택하도록 설계함으로써, 기존 방식에 비하여 강화된 안전성을 가지며 결합적 단순성을 제공한다. 또한 제안하는 프로토콜에서 방송국은 가입자들이 전송하는 메시지들에 대한 인증을 묶음(batch) 기법을 사용하여 검증함으로써 보다 계산적으로 효율적인 인증과정을 제공한다. 추가적으로, 본 논문에서는 사용자들의 가입이나 기존 가입자들의 탈퇴 또는 규약 위반 등에 의해 퇴출될 경우가 발생할 때 효율적으로 세션키를 갱신하는 프로토콜들을 제안함으로서, 새롭게 가입한 가입자들이 가입 이전의 통신에 대해 정보를 얻을 수 없으며 탈퇴·퇴출된 가입자들이 탈퇴·퇴출 이후의 통신에 대해 정보를 얻을 수 없도록 한다.

본 논문의 구성은 다음과 같다. 1장의 서론에 이어 2장에서는 본 논문에서 제안하는 프로토콜에 사용된 안전성 기반 문제에 대하여 설명하고, 3장에서는 본 논문에서 제안하는 ID 기반의 2 라운드 그룹키 동의 프로토콜을 소개하고, 4장에서는 제안한 방식의 안전성을 증명한다. 그리고 5장에서는 제안한 프로토콜의 효율성에 대하여 살펴보고 마지막으로 6장에서 결론을 도출한다.

Ⅱ. 안전성 기반 문제: CDH와 BDDH 문제

이 장에서는 본 논문에서 사용된 안전성 기반 문제들을 살펴본다. 본 논문에서 제안하는 프로코콜의 안전성은 계산적 Diffie-Hellman (CDH) 문제와 Bilinear 결정적 Diffie-Hellman (BDDH) 문제의 어려움에 기반을 두었으며, 이 문제들에 대한 정의는 다음과 같다.

G_1과 G_2는 위수가 임의의 k-bit의 큰 소수 p인 순환군으로, G_1은 타원곡선 $E(F_p)$위의 점들로 이루어진 덧셈군이고, G_2는 F_{p^2}의 부분군으로 곱셈군이다. 이때 k는 안전성 파라미터이다. 그리고 P는 G_1의 생성원이다.

- CDH(Computational Diffie-Hellman) 문제: 임의의 $a,b \in Z_p$에 대하여, P, aP와 bP로부터 abP를 구하는 문제

- CDH 가정: 임의의 확률적 다항식 시간(polynomial-time) 알고리즘 A에 대하여, 만일 아래의 정의된 A의 이점(advantage)이 무시할 수 있을 만큼(negligible) 아주 작다면 CDH 생성자 IG_{CDH}는 CDH 가정을 만족한다고 말한다.

$$\mathrm{Adv}_{G_1}^{CDH}(A) = \left| \Pr\left[A(G_1, P, aP, bP) = abP \;\middle|\; \begin{array}{l} G_1 \leftarrow IG_{CDH}(1^k); \\ P \leftarrow G_1; \\ a,b \leftarrow Z_p^* \end{array} \right] \right|$$

이때, t 수행시간 내에서 실행되는 모든 확률적 다항식 시간 알고리즘 A의 이점 $\mathrm{Adv}_{G_1}^{CDH}(A)$의 최대값은 $\mathrm{Adv}_{G_1}^{CDH}(t)$로 표시한다.

- Bilinear-pairing: 임의의 $Q, R \in G_1$와 $a, b \in Z_p$에 대하여, 함수 $e: G_1 \times G_1 \rightarrow G_2$가 다음의 조건들을 만족하면 e를 bilinear-pairing이라고 한다.
  - Bilinearity
    : $e(aP, bQ) = e(P, Q)^{ab}$ 또는
    $e(P+Q, R) = e(P, R) \cdot e(Q, R)$,
    $e(P, Q+R) = e(P, Q) \cdot e(P, R)$를 만족한다.
  - Non-degeneracy
    : $e(P, Q) = 1$ 이면 P는 무한원점(O) 이다.
  - Efficiency

: $e(P,Q)$의 계산이 효율적인 알고리즘이 존재한다.

- BDDH(Bilinear Decisional Diffie-Hellman) 문제 : 임의의 $a,b,c,d \in Z_p$에 대하여, P, aP, bP, cP와 $e(P,P)^d$로부터 $d=abc$인지를 결정하는 문제

- BDDH 가정: 임의의 확률적 다항식 시간 알고리즘 A에 대하여, 만일 아래의 정의된 A의 이점(advantage)이 무시할 수 있을 만큼(negligible) 아주 작다면 BDDH 파라미터 생성자 IG_{BDDH}는 BDDH 가정을 만족한다고 말한다.

$$\mathrm{Adv}^{BDDH}_{(e,G_1,G_2)}(\mathrm{A}) = \left| \Pr\left[\mathrm{A}\left(\begin{matrix} e, G_1, G_2, P, \\ aP, bP, cP, \\ e(P,P)^{abc} \end{matrix} \right) = 1 \;\middle|\; \begin{matrix} \langle G_1, G_2, e \rangle \\ \leftarrow IG_{BDH}(1^k); \\ |G_1| = |G_2| = p; \\ P \leftarrow G_1^*; \\ a, b, c \leftarrow Z_P \end{matrix} \right] - \Pr\left[\mathrm{A}\left(\begin{matrix} e, G_1, G_2, P, \\ aP, bP, cP, \\ e(P,P)^{d} \end{matrix} \right) = 1 \;\middle|\; \begin{matrix} \langle G_1, G_2, e \rangle \\ \leftarrow IG_{BDH}(1^k); \\ |G_1| = |G_2| = p; \\ P \leftarrow G_1^*; \\ a, b, c, d \leftarrow Z_P \end{matrix} \right] \right|$$

이때, t 수행시간 내에서 실행되는 모든 확률적 다항식 시간 알고리즘 A의 이점 $\mathrm{Adv}^{BDDH}_{(e,G_1,G_2)}(A)$의 최대값은 $\mathrm{Adv}^{BDDH}_{(e,G_1,G_2)}(t)$로 표시한다.

Ⅲ. 제안하는 그룹키 동의 프로토콜 : ID-AGKA

이 장에서는 ID 기반의 인증된 그룹키 동의 프로토콜을 제안한다. 편의상 ID-AGKA (ID-based Authenticated Group Key Agreement) 프로토콜이라고 표시한다. $MG=\{U_1, U_2, \cdots, U_n\}$는 ID-AGKA 프로토콜에 참가하는 n명의 사용자 U_i ($i=[1,n]$)들로 이루어진 멀티캐스트 그룹으로, U_n은 방송국이며 $U_1, U_2, \cdots, U_{n-1}$은 가입자들이다. 제안하는 ID-AGKA 프로토콜은 두 개의 라운드(round)로 그룹키를 설정하며, 첫 번째 라운드는 $n-1$번의 유니캐스트로, 두 번째 라운드에서는 한 번의 브로드캐스트로 설계되어 있다. 다음은 ID-AGKA 프로토콜의 초기화단계, 키 추출단계, 그룹키 설정 단계이다.

1) 초기화단계: 시스템 파라미터는 $< G_1, G_2, e, p, P, H, H_Q >$이다. 여기서 G_1, G_2, e, p와 P는 2장에서 정의한 값들이며, $H: \{0,1\}^* \rightarrow Z_p^*$와 $H_Q: \{0,1\}^* \rightarrow G_1$는 암호 해쉬 함수들이다.

2) 키 추출단계: 프로토콜의 초기 단계에서, 각 사용자 $U_i \in MG$들은 키 생성 알고리즘에 의해 각자의 개인식별정보 ID_i에 대응되는 공개키와 비밀키 쌍 ($Q_i = H_Q(ID_i)$, $D_i = wQ_i$)을 얻는다. 여기서 $w \in_R Z_p^*$는 마스터키이고, $P_{pub} = wP$는 키 발급 기관의 공개키이다.

3) 그룹키 설정 단계: 멀티캐스트 그룹 MG에서의 그룹키를 생성하기 위하여 다음의 알고리즘을 수행한다.

[라운드 1]

방송국 U_n은 임의의 정수 $s, v \in_R Z_p^*$를 선택하고, $P_S = sP$와 $P_V = vP$를 계산한다. s와 v는 방송국이 비밀로 간직한다.

$n-1$명의 가입자 $U_i \neq U_n$는 임의의 정수 $r_i \in_R Z_p^*$를 선택하여 부분키 $P_i = r_i P$를 생성한다. 그리고 자신의 공개키 Q_i와 비밀키 D_i를 사용하여 $O_i = H(P_i)D_i + r_i Q_i$를 계산하고 $M_i = U_i \| P_i \| O_i$를 방송국 U_n에게 전송한다. r_i는 각 가입자가 비밀로 간직한다.

[라운드 2]

$n-1$개의 메시지 M_i를 모두 전달받은 방송국은 가입자들로부터 전달받은 P_i가 정당한지를 확인하기 위하여 다음 방정식이 성립하는지를 체크한다.

$$\prod_{i=1}^{n-1} e(O_i, P) = \prod_{i=1}^{n-1} e(Q_i, H(P_i)P_{pub} + P_i)$$

만약 위의 방정식이 성립하지 않는다면 방송국은 P_i를 거부한다. P_i의 정당성 유무를 모두 확인한 후, 방송국은 임의의 정수 $z \in_R Z_p^*$를 선택하고, 각

가입자들이 그룹키 K를 생성하도록 하기 위하여, 방송국 U_n은 $T_i = z \cdot e(P_i, -svP)$를 계산하여 집합 $T = \{T_i \mid i \in [1, n-1]\}$를 생성한다. 그리고 $M_n = P_S \| P_V \| T$를 그룹내의 모든 가입자 U_i에게 브로드캐스트를 한다. (여기서 만약 방송국으로부터 전송되는 메시지 M_n에 대한 인증이 필요하다면, 기존의 서명 방식을 사용하여 인증절차를 수행하면 된다. 즉, 방송국은 M_n에 대한 서명 σ을 생성하여 각 가입자들에게 M_n대신에 $M_n^* = P_S \| P_V \| T \| \sigma$을 가입자 U_i에게 브로드캐스트함으로서, 각 가입자들은 통신 상대방인 방송국의 신원과 방송국으로부터 전송된 메시지 M_n의 변경 유무를 확인할 수 있다.)

방송국으로부터 메시지 M_n를 전달받은 각 가입자 $U_i \neq U_n$는 $z = T_i \cdot e(P_S, P_V)^{r_i}$를 계산하고, 그룹 MG의 모든 구성원들은 이를 사용하여 그룹키 $K = H(z \| T)$를 생성한다.

위 프로토콜에 의하여 그룹 MG의 모든 구성원은 안전하게 그룹키 $K = H(z \| T)$를 생성할 수 있고, 이를 이용하여 그룹에서의 비밀 통신이나 유료 서비스를 제공할 수 있다.

그리고 본 논문에서 제안한 위의 ID-AGKA 프로토콜에서 사용된 ID 기반의 인증 방식 Γ은 다음과 같이 정의된다.

1) 생성: 임의의 정수 $r \in_R Z_p^*$를 선택하여 $R = rP$를 계산한다. 그리고 $O = H(R)D_{ID} + rQ_{ID}$를 계산하여 R에 대한 인증정보 $Auth = < R, O >$를 생성한다.
2) 검증: R에 대한 인증정보 $Auth = < R, O >$가 정당한지를 확인하기 위하여, $U = H(R)P_{pub} + R$을 계산하여 방정식 $e(O,P) = e(Q_{ID}, U)$이 성립하는지 확인한다.

Ⅳ. ID-AGKA의 안전성

이 장에서는 랜덤 오라클 모델에서 능동적 공격자에 대한 ID-AGKA 프로토콜의 안전성을 살펴본다. 본 논문에서 사용한 안전성 모델은 [32,45,46]에서와 같다. 본 논문에서의 공격자는 브로드캐스트상의 메시지를 볼 수 있고 위조 할 수 있는 능력을 가지고 있으며, 다양한 쿼리(*Send*, *Execute*, *Reveal*, *Corrupt*, *Test*)를 통해 ID-AGKA 프로토콜 참가자들과 상호 작용하여 $b \in \{0,1\}$의 값을 정확히 추측하는 것이다.

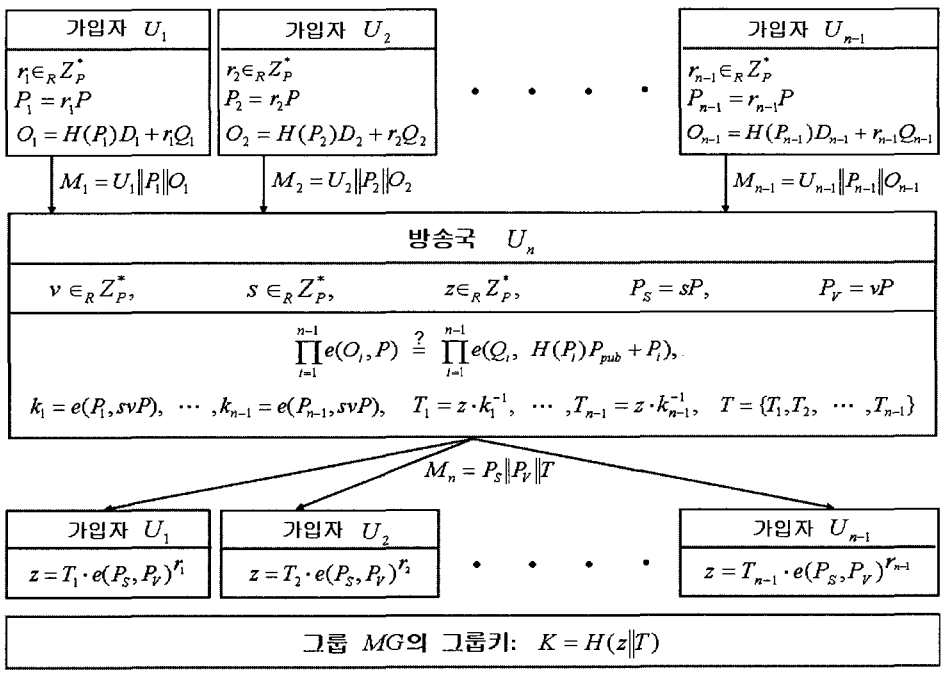


그림 1. 제안하는 ID 기반 그룹키 동의 프로토콜

제안하는 ID-AGKA 프로토콜은 CDH 가정과 BDDH 가정에 기반한 안전한 그룹 키 설정 프로토콜이다. 우선 본 논문에서 제안하는 ID-AGKA 프로토콜에서 사용된 ID 기반의 인증 방식 Γ은 [47]의 ID 기반 서명 방식을 토대로 한 방식으로, CDH 문제가 어렵다면, 제안하는 ID 기반의 인증 방식 Γ은 적응적 선택 ID에서의 존재 위조 공격(Existential forgery on adaptive chosen ID attack)에 대하여 안전하다.[47] 즉, t의 수행시간을 갖는 모든 능동적 공격자 A가 Γ에 대하여 가질 수 있는 최대 이익 $Adv_{\Gamma}(t)$은 무시할 수 있을 만큼(negligible) 아주 작다.

[정리1] q_{er}와 q_s를 공격자 A가 요구할 수 있는 *Execute*와 *Send*에 대한 각각의 최대 쿼리수라고 가정하자. 그러면 t의 수행시간을 갖는 모든 능동적 공격자 A가 프로토콜 ID-AGKA에 대하여 가질 수 있는 최대 이익 $\mathrm{Adv}_{\mathrm{ID-AGKA}}(t, q_{er}, q_s)$ 은 다음과 같다.

$$\mathrm{Adv}_{\mathrm{ID-AGKA}}(t, q_{er}, q_s) \leq$$

$$2q_{er}\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(t) + (n-1)\mathrm{Adv}_{\Gamma}(t)$$

증명) 공격자 A가 ID-AGKA 프로토콜을 공격하는 방법은, 공격자 A가 인증 메시지를 위조하여 정당한 사용자처럼 가장하는 경우와 공격자 A가 전송되는 메시지의 위조 없이 ID-AGKA 프로토콜을 공격하는 경우, 두 가지 경우로 나누어서 생각할 수 있다.

먼저 공격자 A가 인증 메시지를 위조하여 정당한 사용자처럼 가장하는 첫 번째 경우, ID-AGKA 프로토콜의 안전성은 ID 기반의 인증 방식 Γ의 안전성으로 귀결된다.

[보조정리 1] *Forge*를 공격자 A가 ID 기반의 인증 방식 Γ과 관계있는 정당한 인증 메시지를 생성하는 사건이라고 가정하자. 그러면 t의 수행시간을 갖는 모든 공격자 A가 *Forge*에 대하여 가질 수 있는 최대 확률은 다음과 같다.

$$\Pr[Forge] \leq (n-1)\mathrm{Adv}_{\Gamma}(t)$$

이때, t는 정리 1에서와 같다.

증명) A를 무시하지 못할 이익을 가지고 인증 메시지를 위조하는 공격자라고 가정한다. 그러면 공격자 A로부터 ID 기반의 인증 방식 Γ과 관계 있는 유효한 인증정보(ID, rP, O)를 생성하는 위조자 B를 건설할 수 있다. 모든 사용자들에 대하여, 위조자 B는 *Extract* 알고리즘을 실행하여 공개키와 비밀키 쌍을 생성한다. 그리고 B는 A와의 상호작용에 의하여 공격환경을 시뮬레이트한다. A가 *Corrupt*(ID)를 요청하지 않는 한 B는 이 시뮬레이션에서 성공하게 되며, A가 ID 기반의 인증 방식 Γ과 관계 있는 유효한 인증정보(ID, rP, O)를 출력한다면 B도 ID에 대한 정당한 인증정보 (ID, rP, O)를 생성할 수 있게 된다. 이때의 B의 성공 확률은

$$\mathrm{Adv}_{B,\Gamma}(t) = \frac{1}{n-1} Pr[Forge]$$

이 되며 $\mathrm{Adv}_{B,\Gamma}(t) \leq \mathrm{Adv}_{\Gamma}(t)$ 에 의하여 $\Pr[Forge] \leq (n-1)\mathrm{Adv}_{\Gamma}(t)$ 을 얻을 수 있다. □

두 번째 경우인 공격자 A가 전송되는 메시지의 변조 없이 ID-AGKA 프로토콜을 공격하는 경우, ID-AGKA 프로토콜의 안전성은 BDDH 문제로 귀결된다.

우선 ID-AGKA 프로토콜에 대응되는 실제 분포 *Real*과 랜덤한 난수로 전달된 메시지의 분포인 *Rand*를 먼저 생각해 보자. n은 프로토콜 참가자의 수이며 $W=(P_1, \cdots, P_{n-1}, O_1, \cdots, O_{n-1}, P_S, P_V, T_1, \cdots, O_{n-1}, P_S, P_V, T_1, \cdots, T_{n-1})$는 전달 메시지이고 $K=H(z \| T)$는 그룹키이다. *Real*은 다음과 같이 나타난다.

$$Real = \left\{ (W,K) \;\middle|\; \begin{array}{l} r_1, \cdots\cdots, r_{n-1}, s, v, z \in_R Z_p^* ; \\ P_1 = r_1 P, \cdots\cdots, P_{n-1} = r_{n-1} P,\ P_S = sP,\ P_V = vP ; \\ O_1 = H(P_1) D_1 + r_1 Q_1, \cdots \\ \quad \cdots, O_{n-1} = H(P_{n-1}) D_{n-1} + r_{n-1} Q_{n-1} ; \\ k_1 = e(P,P)^{zr_1}, \cdots\cdots, k_{n-1} = e(P,P)^{zr_{n-1}} ; \\ T_1 = z \cdot k_1^{-1}, \cdots\cdots, T_{n-1} = z \cdot k_{n-1}^{-1} ; \end{array} \right\}$$

*Rand*를 생각하는 데에 있어서는, 공격자 A가 *Corrupt* 쿼리와 H 쿼리를 요청하여 각각 비밀키 D_i와 해쉬함수값 $H(P_i)$를 얻음으로써 $r_iQ_i = O_i - -H(P_i)D_i$ ($i=1,\cdots,n-1$)를 구할 수 있다는 사실에 대하여 먼저 고려해 볼 필요가 있다. 그러나 이러한 사실은 공격자 A가 ID-AGKA 프로토콜을 공격하는데에 별다른 이득이 되지 않는다. 즉, r_iQ_i를 구한다고 하더라도 공격자 A는 r_iQ_i로부터 ID-AGKA 프로토콜을 공격하는 데에 필요한 어떠한 이익도 얻을 수 없다. 그러므로 *Rand*는 다음과 같이 정의된다.

$$Rand=\left\{(W,K)\left|\begin{array}{l} r_1,\cdots\cdots,r_{n-1},s,v,z,x_1,\cdots\cdots,x_{n-1}\in_R Z_p^* ;\\ P_1=r_1P,\cdots\cdots,P_{n-1}=r_{n-1}P,\ P_S=sP,\ P_V=vP ;\\ O_1=H(P_1)D_1+r_1Q_1,\cdots\\ \cdots,O_{n-1}=H(P_{n-1})D_{n-1}+r_{n-1}Q_{n-1} ;\\ k_1=e(P,P)^{x_1},\cdots\cdots,k_{n-1}=e(P,P)^{x_{n-1}} ;\\ T_1=z\cdot k_1^{-1},\cdots\cdots,T_{n-1}=z\cdot k_{n-1}^{-1} ; \end{array}\right.\right\}$$

그리고 공격자 A가 b의 값을 추측할 수 있는 확률을 $\frac{1}{2}+\epsilon$이라고 놓자. 그러면 공격자 A로부터 $\frac{\epsilon}{q_{t,r}}$의 확률을 가지고 (e,G_1,G_2)에서 BDDH 문제를 해결하는 식별자(distinguisher) Đ를 건설할 수 있다. 식별자 Đ를 설명하기에 앞서 다음의 두 보조정리를 먼저 살펴보자.

[보조정리 2] C를 *Real*과 *Rand*를 구별하는 임의의 확률론적 다항식 시간 알고리즘이라고 가정하자. 그러면 알고리즘 C의 능력은 다음과 같이 BDDH 문제의 어려움에 의해서 제한된다.

$$\left|\begin{array}{l}\Pr[C(W,K)=1]\mid(W,K)\leftarrow Real]\\ -\Pr[C(W,K)=1]\mid(W,K)\leftarrow Rand]\end{array}\right|\leqq$$

$$\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(t+(2n-4)t_{sm}+(2n-6)t_{\exp}+t_{pa})$$

여기서 t_{sm}, $t_{\exp}$, t_{pa}는 각각 그룹 G_1에서 스칼라 곱(scalar multiplication)을 계산하는데 걸리는 시간, 그룹 G_2에서 지수(exponentiation)를 계산하는데 걸리는 시간, Pairing 연산을 하는데 걸리는 시간을 나타낸다.

증명) 주어진 알고리즘 C를 이용하여 BDDH 문제를 푸는 알고리즘 F를 구성할 수 있다. $(sP, vP, r_1P, e(P,P)^{r\cdot r_1})$가 알고리즘 F의 입력값으로 주어졌을 때, 우리는 다음과 같은 분포를 구성할 수 있다.

$$Dist=\left\{(W,SK)\left|\begin{array}{l} r_2,r_3,z,a_4,\cdots,a_n,b_4,\cdots,b_n,c_4,\cdots,c_n\in_R Z_p^* ;\\ P_1=r_1P,P_2=r_2P,P_3=r_3P,\\ P_4=(r_1a_4+r_2b_4+r_3c_4)P,\cdots\\ \cdots,P_{n-1}=(r_1a_{n-1}+r_2b_{n-1}+r_3c_{n-1})P,\ P_S=sP,\ P_V=vP ;\\ O_1=H(P_1)D_1+r_1Q_1,\cdots\\ \cdots,O_{n-1}=H(P_{n-1})D_{n-1}\\ \qquad +(r_1a_{n-1}+r_2b_{n-1}+r_3c_{n-1})Q_{n-1} ;\\ k_1=e(P,P)^{sv},k_2=e(P,P)^{r'r_2},k_3=e(P,P)^{sv},\\ k_4=e(P,P)^{sv(r_1a_4+r'r_2b_4+sv)r_3c_4},\cdots\\ \cdots,k_{n-1}=e(P,P)^{sv(r_1a_{n-1}+r'r_2b_{n-1}+sv)r_3c_{n-1}} ;\\ T_1=z\cdot k_1^{-1},\cdots\cdots,T_{n-1}=z\cdot k_{n-1}^{-1} ; \end{array}\right.\right\}$$

여기서 W와 K는 *Real*과 *Rand*에서 정의된 것과 같다. 알고리즘 F는 *Dist*에서 계산되어 나온 결과 값 (W,K)를 알고리즘 C의 입력 값으로 준다. 이때 만약 주어진 $vP, r_1P, e(P,P)^{r\cdot r_1})$이 BDDH 인스턴스(즉, $r'=sv$)라면 $i\in[1,n]$에 대하여 $k_i=E_i^{sv}$이기 때문에 $Dist=Real$이 되고 (여기서 $E_i=e(P,P_i)$이다), 반면에 만약 $(sP, vP, r_1P, vP, r_1P, e(P,P)^{r\cdot r_1})$이 임의의 랜덤한 인스턴스라면 $Dist=Rand$이 된다. 결국 *Real*과 *Rand*를 구별하는 알고리즘 C의 능력은 BDDH 문제의 어려움에 의해서 제한되며 기껏해야 $\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(t+(2n-4)t_{sm}+(2n-6)t_{\exp}+t_{pa}$의 성공확률을 가지게 된다.

□

[보조정리 3] *Rand*에서 공격자 A가 b를 올바르게 추측할 확률은 다음과 같다.

$$\Pr\left[A(W,K_b)=b\left|\begin{array}{l}(W,K_1)\leftarrow Rand ;\\ K_0\leftarrow\{0,1\}^k ;\\ b\leftarrow\{0,1\}\end{array}\right.\right]=\frac{1}{2}$$

증명) *Rand*에서의 전달 메시지 W를 살펴보면,

W는 다음의 $n-1$개의 방정식

$$\begin{aligned}\log_E T_1 &= \log_E z - x_1\\ &\vdots\\ \log_E T_{n-1} &= \log_E z - x_{n-1}\end{aligned}$$

으로 나타난다. 여기서 $E=e(P,P)$이다. 위의 $n-1$개의 방정식의 선형 조합(linear combination)으로 $\log_E z$를 표시할 수 없기 때문에 전달 메시지 W와 z는 서로 독립적임을 알 수 있다. 이로부터 다음의 방정식

$$\Pr\left[A(W,z_b)=b \,\middle|\, \begin{array}{l}(W,z_1)\leftarrow Rand;\\ z_0\leftarrow_R Z_p^*;\\ b\leftarrow\{0,1\}\end{array}\right]=\frac{1}{2}$$

을 얻을 수 있으며, H가 랜덤 오라클이므로 원하는 아래의 방정식을 얻을 수 있다.

$$\Pr\left[A(W,K_b)=b \,\middle|\, \begin{array}{l}(W,K_1)\leftarrow Rand;\\ K_0\leftarrow\{0,1\}^k;\\ b\leftarrow\{0,1\}\end{array}\right]=\frac{1}{2}$$

□

위의 두 보조정리 2와 보조정리 3에 의해 식별자 Ð의 구성을 알 수가 있다: 공격자 A가 하나의 *Test* 쿼리를 생성하여 δ번째 *Execute* 쿼리에 응답하였던 오라클에게 질문한다고 가정하자. 우선 식별자 Ð는 δ의 추측 값으로 $d\in\{1,\cdots,q_{ex}\}$을 선택한다. 그리고 식별자 Ð는 공격자 A의 공격 환경을 시뮬레이션(simulation)하고 A의 모든 쿼리들에 대하여 답한다. 다만 d번째 *Execute* 쿼리일 경우는 예외이다. 즉, $vP,r_1P,e(P,P)^{r_1r_2}$가 주어지면, 식별자 Ð는 *Dist*에 따라 (W,K)를 생성하고 W를 가지고 공격자 A의 d번째 *Execute* 쿼리에 답을 한다. 만약 $d\neq\delta$이라면 식별자 Ð는 실행을 중지하고 랜덤 비트를 출력한다. 반면에 만약 $d=\delta$이라면 식별자 Ð는 K를 가지고 공격자 A의 *Test* 쿼리에 답을 한다. 공격 마지막 시점에서, 공격자 A는 비트 b의 추측 값인 b'을 출력한다. 그리고 $b'=b$이라면 식별자 Ð는 1을 출력하고 $b'\neq b$이라면 식별자 Ð는 0을 출력한다.

$d=\delta$일 확률은 $1/q_{ex}$이고 보조정리 2, 보조정리 3 그리고 방정식

$$\Pr\left[A(W,K_b)=b \,\middle|\, \begin{array}{l}(W,K_1)\leftarrow Rand;\\ K_0\leftarrow\{0,1\}^k;\\ b\leftarrow\{0,1\}\end{array}\right]=\frac{1}{2}+\epsilon$$

에 의해서 방정식

$$\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(Ð)=\frac{\epsilon}{q_{ex}}$$

을 얻을 수 있다. 따라서 두 번째 경우인 t의 수행시간을 갖는 모든 공격자 A가 전송되는 메시지의 변조 없이 ID-AGKA 프로토콜을 공격하는 경우에 가질 수 있는 최대 이익은 $2q_{ex}\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(t)$이 된다.

그러므로 첫 번째 경우와 두 번째 경우에 의해서, t의 수행시간을 갖는 모든 능동적 공격자가 ID-AGKA 프로토콜에 대하여 가질 수 있는 최대 이익은

$$\begin{aligned}&\mathrm{Adv}_{\mathrm{ID-AGKA}}(t,q_{ex},q_s)\leqq\\ &2q_{ex}\mathrm{Adv}^{\mathrm{BDDH}}_{(e,G_1,G_2)}(t)+(n-1)\mathrm{Adv}_I(t)\end{aligned}$$

이 됨을 보임으로써 정리 1을 증명하였다. □

V. ID-AGKA의 효율성

Pairing을 사용한 ID 기반 그룹키 동의 프로토콜은 2002년과 2003년에 각각 Nalla[39]와 Barua[44]에 의해서 제안되었다. 그러나 이들은 안전성에 대한 증명을 하지 못하였고 프로토콜의 라운드 수가 사용자 수에 의존하여 선형적으로 증가한다는 단점이 있다. 이후 2004년 Choi[32]가 랜덤 오라클 아래에서 안전성이 증명된 2 라운드의 효율적인 ID 기반 그룹키 동의 프로토콜을 제안하였지만, 이 프로토콜은 [17]을 기반으로 하여 설계되었기 때문에 완전 대칭적(symmetry)인 특징을 지닌다. 그러므로 비대칭적 관계에 있는 유료 방송 시스템에 적용하기에는 현실적으로 적당하지 않다. 뿐만 아니라 Choi의 프로토콜은 그룹 크기에 따라 브로드캐스트

되는 메시지의 수가 선형적으로 증가한다는 단점을 가지고 있다. 그러므로 가입자들의 증가에 따라 방송국 규모(그룹 사이즈)가 커지면 가입자들의 통신량과 연산량도 함께 증가되기 때문에, 이동단말기의 소형화 경향으로 인해 제한된 시스템자원을 고려해야하는 차세대 이동 방송 환경에는 적합하지 않다. 반면에 본 논문에서 제안하는 ID-AGKA 프로토콜은 가입자들이 보유하고 있는 제한된 시스템 자원을 고려하여 설계된 2 라운드의 효율적인 그룹키 동의 프로토콜이다. 특히, 제안하는 프로토콜의 [라운드 2]는 안전성의 변화 없이 다음과 같이 변형이 가능하므로 사용자(방속국과 가입자)측의 연산량에 대한 효율성을 더욱 증가시킬 수 있다.

[라운드 2]

가입자 $U_1,\cdots,U_{n-1}$로부터 $n-1$개의 메시지 M_i를 전달받은 방송국은 P_i가 정당한지를 확인하기 위하여 다음 방정식이 성립하는지를 체크한다.

$$e(\sum_{i=1}^{n-1} Q_i,\ P)=\prod_{i=1}^{n-1} e(Q_i,\ H(P_i)P_{pub}+P_i\ )$$

P_i의 정당성 유무를 모두 확인한 후, 방송국은 임의의 정수 $z \in {}_R Z_p^*$를 선택하고 $g=e(P,\ svP)$와 $T=\{T_i \mid i\in[1,n-1]\}$를 계산하여 $M_n=g \parallel T$를 그룹내의 모든 가입자 U_i에게 브로드캐스트를 한다. 이때, $T_i=z\cdot e(P_i,-svP)$이다. (여기서 만약 전송 메시지 M_n에 대한 인증이 필요하다면, 3장에서 언급한바와 같이, 기존의 서명 방식을 사용한다.)

방송국으로부터 메시지 M_n를 전달받은 각 가입자 $U_i \neq U_n$는 $z=T_i\cdot g^{r_i}$를 계산하고, 그룹 MG의 모든 구성원들은 이를 사용하여 그룹키 $K=H(z \parallel T)$를 생성한다.

그리고 제안하는 ID-AGKA 프로토콜에서 사용된 인증 메카니즘은 [45,46]에서처럼 단순히 서명 기법을 사용한 것이 아니라 키 교환과 결합하여 전송 메시지들을 새롭게 구성한 방법으로, 기존 방식에 비하여 전송 메시지들의 길이가 짧으며 결합적 단순성을 제공한다. 더구나 제안하는 프로토콜은, [45,46]와는 달리, 방송국이 그룹키 생성시에 필요한 정보를 새로운 난수로 선택하도록 설계함으로써, 방송국측의 연산량에 대한 효율성 및 프로토콜의 안전성을 더욱 더 증가시켰다. 또한 제안하는 프로토콜에서 방송국은 가입자들이 전송하는 메시지들에 대한 인증을 묶음(batch) 기법을 사용하여 검증함으로써 [45,46]에서보다 계산적으로 효율적인 인증 과정을 제공한다. 추가적으로, 제안하는 ID-AGKA 프로토콜은 완전한 전방향 안전성과 최적의 메시지 복잡도를 제공하면서도 유료 방송 시스템에서의 멤버쉽의 변화 즉, 사용자들의 가입이나 기존 가입자들의 탈퇴 또는 규약 위반 등에 의해 퇴출될 경우가 발생할 때에도 효율적인 세션키의 갱신이 가능하도록 하여 새롭게 가입한 가입자들이 가입 이전의 통신에 대해 정보를 얻을 수 없으며 탈퇴·퇴출된 가입자들이 탈퇴·퇴출 이후의 통신에 대해 정보를 얻을 수 없도록 한다. 사용자들의 탈퇴·퇴출과 가입이 발생할 경우에 세션키를 갱신하는 프로토콜은 다음과 같다.

가. ID-AGKA 탈퇴·퇴출 프로토콜

멀티캐스트 그룹 $MG=\{U_1,U_2,\cdots,U_n\}$에서 사용자 집합 L이 그룹을 탈퇴한다고 가정한다. 제안하는 탈퇴 프로토콜은 하나의 라운드로 그룹키를 갱신하며 한 번의 브로드캐스트로 설계되어 있으며 자세한 동작과정은 다음과 같다.

[라운드 1]

방송국 U_n은 새로운 임의의 정수 $s', v', z' \in {}_R Z_p^*$를 선택하고, $P_S'=s'P$와 $P_V'=v'P$를 계산한 후, ID-AGKA 프로토콜을 그대로 수행하여 T'를 계산하여 새로운 그룹 MG_L의 그룹키 $K=K=H(z' \parallel T')$를 생성한다. 그리고 방송국 U_n은 각 가입자 $U_i \in MG_L \setminus \{U_n\}$들이 그룹키를 갱신하도록 하기 위하여 $M_n'=T' \parallel g'$를 새로운 그룹 MG_L내의 모든 가입자에게 브로드캐스트 한다. 이때, $g'=e(P,s'v'P)$이다. (여기서 만약 전송 메시지 M_n'에 대한 인증이 필요하다면, 3장에서 언급한바와 같이, 기존의 서명 방식을 사용한다.)

각 가입자 $U_i \in MG_L \setminus \{U_n\}$는 ID-AGKA 프로토콜을 그대로 수행하여 $z'=T_i'\cdot g'^{r_i}$ ($i=[1,n-1] \setminus \{L\}$)를 계산한 후, 새롭게 형성된 멀티캐스트 그룹 MG_L에 대한 그룹키 $K=H(z' \parallel T')$를 생성한다.

위 프로토콜에 의하여 새롭게 형성된 멀티캐스트

그룹 $MG_L = MG \setminus L$의 모든 구성원은 새로운 그룹키 $K = H(z' \| T')$를 갱신할 수 있다.

나. ID-AGKA 가입 프로토콜

사용자 집합 J가 멀티캐스트 그룹 $MG=\{U_1, U_2, \cdots, U_n\}$에 새롭게 가입한다고 가정한다. 제안하는 가입 프로토콜은 두 개의 라운드로 구성되어 있으며, 첫 번째 라운드는 j번의 유니캐스트로, 두 번째 라운드에서는 한 번의 브로드캐스트로 설계되어 있다. 여기서 j는 새로 가입하는 사용자의 수 즉, $|J|=j$이다.

[라운드 1]

새롭게 그룹에 가입하는 가입자 $U_j \in J$들은 임의의 정수 $r_j \in Z_p$를 선택하여 부분키 $P_j = r_j P$를 계산한다. 그리고 ID-AGKA 프로토콜에서와 같이 $O_j = H(P_j)D_j + r_j Q_j$를 계산하고 $M_j = U_j \| P_j \| O_j$를 방송국 U_n에게 전송하여 자신을 인증한다.

[라운드 2]

방송국 U_n는 ID-AGKA 프로토콜과 동일한 방법으로 가입자 $U_j \in J$로부터 전달받은 P_j가 정당한지를 확인한 후, 새로운 임의의 정수 $s'', v'', z'' \in_R Z_p^*$를 선택하고, $P_S'' = s''P$와 $P_V'' = v''P$를 계산한 후, ID-AGKA 프로토콜을 그대로 수행하여 T''를 계산하여 새로운 그룹 MG_J의 그룹키를 생성한다. 그리고 방송국 U_n는 각 가입자 $U_i \in MG_J \setminus \{U_n\}$들이 그룹키를 갱신하도록 하기 위하여 $M_n'' = T'' \| g''$를 새로운 그룹 MG_J내의 모든 가입자에게 브로드캐스트 한다. 이때, $g'' = e(P, s''v''P)$이다. (여기서 만약 전송 메시지 M_n''에 대한 인증이 필요하다면, 3장에서 언급한바와 같이, 기존의 서명 방식을 사용한다.)

각 가입자 $U_i \in MG_J \setminus \{U_n\}$는 ID-AGKA 프로토콜을 그대로 수행하여 $z'' = T_i'' \cdot g''^{r_i}$ $(i = [1, n-1] \bigcup \{J\})$를 계산한 후, 새롭게 형성된 멀티캐스트 그룹 MG_J에 대한 그룹키 $K = H(z'' \| T'')$를 생성한다.

위 프로토콜에 의하여 새롭게 형성된 멀티캐스트 그룹 $MG_J = MG \bigcup J$의 모든 구성원은 새로운 그룹키 $K = H(z'' \| T'')$를 갱신할 수 있다.

Ⅵ. 결 론

본 논문에서는 안전성이 증명된 2 라운드의 효율적인 ID-AGKA 프로토콜을 제안하였다. 제안한 프로토콜은 비대칭적 관계에 있는 유료 방송 시스템에 현실적으로 적용할 수 있는 프로토콜로서 유료 방송 시스템의 특징들을 모두 만족하는 실용적인 프로토콜이다. 그리고 제안한 ID-AGKA 프로토콜은 프로토콜 수행시간을 주로 결정하는 핵심 요소인 라운드 수와 메시지 수를 줄인 효율적인 프로토콜이며, 또한 완전한 전방향 안전성과 최적의 메시지 복잡도를 제공하면서도 상수 라운드만에 유료 방송 시스템에서의 멤버쉽의 변화에 따른 효율적인 세션키의 갱신도 수행한다.

참 고 문 헌

[1] B.-M. Macq and J.-J. Quisquater, "Cryptology for Digital TV Broadcasting," Proc. of the IEEE, 83(6):944-57, 1995.

[2] A. Fiat and M. Naor, "Broadcast Encryption," Advances in Cryptology-Crypto'93, LNCS 773, pp. 480-491, Springer Verlag, 1994.

[3] C. Blundo, Luia A. Frota Mattos and D.R. Stinson, "Generalized Beimel-Chor Schemes for Broadcast Encryption and Interactive Key Distribution," Theoretical Computer Science, Vol. 200, pp. 313-334, 1998.

[4] C. Blundo, Luia A. Frota Mattos and D. R. Stinson, "Trade-offs Between Communication and Storage in Unconditionally Secure Schemes for Broadcast Encryption and Interactive Key Distribution," Advances in Cryptology-Crypto'96, LNCS 1109, pp. 387-400, 1996.

[5] D. Lee, H. Kim and J. Lim, "Efficient Public-Key Traitor Tracing in Provably Secure Broadcast Encryption

with Unlimited Revocation Capability," KoreaCrypto'02, 2003.
[6] D. Boneh and M. Franklin, "An Efficient Public-Key Traitor Tracing Scheme," Crypto'99, LNCS 1666, pp. 338-353, 1999.
[7] Y. Mu and V. Varadharajan, "Robust and Secure Broadcasting," Advances in Cryptology-Indocrypt'01, LNCS 2247, pp. 223-231, Springer-Verlag, 2001.
[8] A. Wool, "Key Management for Encrypted Broadcast," Proc. of the 5th ACM conference on Computer and Communications Security, pp. 7-16, Springer-Verlag, 1998.
[9] Y. Mu, W. Susilo and Y.-X. Lin, "Identity-Based Broadcasting," Advances in Cryptology-Indocrypt'03, LNCS 2904, pp. 177-190, Springer-Verlag, 2003.
[10] A. Narayanan, C.P. Rangan, and K. Kim, "Practical Pay TV schemes," Proc. of the 9th Australasian Conference on Information Security and Privacy, LNCS 2727, pp. 192-203, Springer-Verlag, 2003.
[11] A. Shamir, "Identity-based Cryptosystems and Signature Schemes," Advances in Cryptology-Crypto'84, LNCS 196, pp. 47-53, Springer-Verlag, 1984.
[12] W. Diffie, P. van Oorschot, and M. Wiener, "Authentication and Authenticated Key Exchanges," Designs, Codes and Cryptography, 2(2):107-125, 1992.
[13] G. Ateniese, M. Steiner, and G. Tsudik, "New Multiparty Authentication Services and Key Agreement Protocols," IEEE Journal on Selected Areas in Communications, 18(4):628-639, 2000.
[14] C. J. Mitchell, M. Ward, and P. Wilson, "Key Control in Key Agreement Protocols," Electronics Letters, 34(10):980-981, 1998.
[15] I. Ingemarsson, D. Tang, and C. Wong, "A Conference Key Distribution System," IEEE Transactions on Information Theory, 28(5):714-720, 1982.
[16] G.H. Chiou and W.-T. Chen, "Secure Broadcasting Using the Secure Lock," IEEE Transactions on Software Engineering, 15(8):929-934, 1989.
[17] M. Burmester and Y. Desmedt, "A Secure and Efficient Conference Key Distribution System," Advances in Cryptology-Eurocrypt'94, LNCS 950, pp. 275-286, Springer-Verlag, 1994.
[18] M. Just and S. Vaudenay, "Authenticated Multi-party Key Agreement," Advances in Cryptology-Asiacrypt'96, LNCS 1163, pp. 36-49, Springer-Verlag, 1996.
[19] K. Becker and U. Wille, "Communication Complexity of Group Key Distribution," Proc. of 5th ACM Conference on Computer and Communications Security, pp. 1-6, Springer-Verlag, 1998.
[20] Y. Kim, A. Perrig, and G. Tsudik, "Simple and Fault-tolerant Key Agreement for Dynamic Collaborative Groups," Proc. of 7st ACM Conference on Computer and Communications Security, pp. 235-244, Springer-Verlag, 2000.
[21] M. Steiner, G. Tsudik, and M. Waidner, "Key Agreement in Dynamic Peer Groups," IEEE Transactions on Parallel and Distributed Systems, 11(8):769-780, 2000.
[22] W.G. Tzeng and Z.J. Tzeng, "Round-efficient Conference Key Agreement Protocols with Provable Security," Advances in Cryptology-Asiacrypt'00, LNCS 1976, pp. 614-627, Springer-Verlag, 2000.
[23] Y. Kim, A. Perrig, and G. Tsudik, "Communication-efficient Group Key Agreement," Proc. of International Fe-

deration for Information Processing, LNCS 1163, pp. 229-244, Springer-Verlag, 2001.

[24] 박영호, 이경현, "이동네트워크 환경에서 그룹키 관리구조," 정보보호학회논문지, 12(2), pp. 89-100, 2002.

[25] 이상원, 천정희, 김용대, "Pairing을 이용한 트리 기반 그룹키 합의 프로토콜," 정보보호학회논문지, 13(3), pp. 101-110, 2003.

[26] 박영희, 정병천, 이윤호, 김희열, 이재원, 윤현수, "Diffie-Hallman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜," 정보보호학회논문지, 13(5), pp. 3-15, 2003.

[27] E. Bresson, O. Chevassut, D. Pointcheval, and J.-J. Quisquater, "Provably Authenticated Group Diffie-Hellman Key Exchange," Proc. of the 8st ACM Conference on Computer and Communications Security, pp. 255-264, Springer-Verlag, 2001.

[28] E. Bresson, O. Chevassut, and D. Pointcheval, "Provably Authenticated Group Diffie-Hellman Key Exchange the Dynamic Case," Advances in Cryptology-Asiacrypt'01, LNCS 2248, pp. 290-309, Springer-Verlag, 2001.

[29] E. Bresson, O. Chevassut, and D. Pointcheval, "Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions," Advances in Cryptology-Eurocrypt'02, LNCS 2332, pp. 321-336, Springer-Verlag, 2002.

[30] C. Boyd and J.M.G. Nieto, "Round-optimal Contributory Conference Key Agreement," Proc. of the 6th International Workshop on Practice and Theory in Public Key Cryptography, LNCS 2567, pp. 161-174, 2003.

[31] J. Katze and M. Yung, "Scalable Protocols for Authenticated Group Key Exchange," Advances in Cryptology-Crypto'03, LNCS 2729, pp. 110-125, Springer-Verlag, 2003.

[32] K.Y. Choi, J.Y. Hwang, and D.H. Lee, "Efficient ID-based Group Key Agreement with Bilinear Maps," Proc. of the 7th International Workshop on Practice and Theory in Public Key Cryptography, LNCS 2947, pp. 130-134, Springer-Verlag, 2004.

[33] F. Zhang and X. Chen, "Attack on Two ID-based Authenticated Group Key Agreement Schemes," Cryptology ePrint Archive, Report 2003/256, available at iacr.org/2003/256/.

[34] E. Bresson, O. Chevassut, A. Essiari and D. Pointcheval, "Mutual authentication and group key agreement for low-power mobile devices," *Computer Communications*, vol. 27(17), 2004, pp. 1730-1737, A preliminary version appeared in Proc. of the 5th IFIP-TC6/IEEE International Conference on Mobile and Wireless Communications Networks (MWCN 03), pp. 59-62, 2003.

[35] J. Nam, S. Kim and D. Won, "An Attack on Bresson-Chevassut-Essiari-Pontcheval's Group Key Agreement Scheme for Low-Power Mobile Devices," Cryptology ePrint Archive, Report 2004/251, available at iacr.org/2004/251/.

[36] A. Joux, "A One Round Protocol for Tripartite Diffie-Hellman," In W. Bosma, editor, Proc. of Algorithmic Number Theory Symposium, LNCS 1838, pp. 385-394, Springer-Verlag, 2000.

[37] D. Boneh and D. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. of Crypto'01, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[38] D. Bonech, B. Lynn, H. Shacham, "Short Signatures from the Weil Pairing," Advances in Cryptology-Asiacrypt'01, Springer-Verlag, 2001.

[39] D. Nalla and K.C. Reddy, "Identity Based Authenticated Group Key Agree-

ment Protocol," Proc. of Indocrypt'02, LNCS 2551, pp. 215-233, Springer-Verlag, 2002.

[40] N.P. Smart. "An Identity-based Authenticated Key Agreement Protocol based on the Weil Pairing," Electronics Letters, 38(13):630-632, 2002.

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

[42] H. Kim, S. Kim, D. Won, "ID-Based Partially Blind Signatre under GDH Group," Proc. of the International Conference on Number Theory for Secure Communications 20th, pp. 159, 2003.

[43] S. S. Al-Riyami, K. G. Paterson, "Certificateless Public Key Cryptography," Advances in Cryptology-Asiacrypt'03, LNCS 2784, Springer Verlag, 2003.

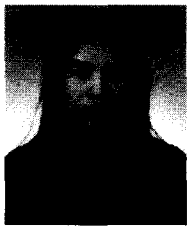
[44] R. Barua, R. Dutta and P. Sarker, "Extending Joux's Protocol to Multi Party Key Agreement," Proc. of Indocrypt'03, LNCS 2904, pp. 205-217, Springer-Verlag, 2003.

[45] J. Nam, S. Kim, S. Kim, and D. Won, "Provably-secure and Communication-efficient Scheme for Dynamic Group Key Exchange," Cryptology ePrint Archive, Report 2004/115, available at iacr.org/2004/115/.

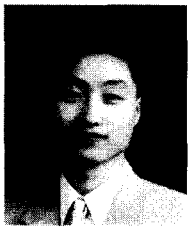
[46] J. Nam, J. Lee, S. Kim, and D. Won, "DDH-based Group Key Agreement for Mobile Computing," Cryptology e-Print Archive, Report 2004/127, available at iacr.org/2004/127/.

[47] J. Cheon, Y. Kim, and H. Yoon, "A New ID-based Signature with Batch Verification," Cryptology ePrint Archive, Report 2004/131, available at iacr.org/2004/131/.

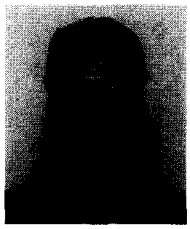
〈著者紹介〉



김 현 주 (Hyunjue Kim) 학생회원
1995년 2월 : 세명대학교 수학과(이학사)
1997년 2월 : 서강대학교 대학원 수학과(이학석사)
2005년 2월 : 성균관대학교 대학원 전자전자 및 컴퓨터공학과(공학박사)
<관심분야> 암호이론, 이동통신 보안



남 정 현 (Junghyun Nam) 학생회원
1997년 2월 : 성균관대학교 정보공학과(공학사)
2002년 5월 : Computer Science. University of Louisiana. Lafayette(M.S.)
2003년 3월~현재 : 성균관대학교 대학원 정보통신공학부 박사과정
<관심분야> 암호 프로토콜, 암호이론, 네트워크 보안



김 승 주 (Seungjoo Kim) 종신회원
1994년 2월 : 성균관대학교 정보공학과(공학사)
1996년 2월 : 성균관대학교 대학원 정보공학과(공학석사)
1999년 2월 : 성균관대학교 대학원 정보공학과(공학박사)
1998년 12월~2004년 2월 : 한국정보보호진흥원(KISA) 팀장
2001년 1월~현재 : 한국정보보호학회 논문지편집위원
2002년 4월~현재 : 한국정보통신기술협회(TTA) IT 국제표준화 전문가
2004년 3월~현재 : 성균관대학교 정보통신공학부 교수
2005년 1월~현재 : 한국정보과학회 논문지편집위원
<관심분야> 암호이론, 정보보호제품 및 스마트카드 보안성 평가, PET

원 동 호 (Dongho Won) 종신회원
성균관대학교 전자공학과(학사, 석사, 박사)
1978년~1980년 : 한국전자통신연구원 전임연구원
1985년~1986년 : 일본 동경공업대 객원연구원
1988년~1999년 : 성균관대학교 교학처장, 전기전자 및 컴퓨터공학부장, 정보통신대학원장, 정보통신기술연구소장
1996년~1998년 : 국무총리실 정보화추진위원회 자문위원
2002년~2003년 : 한국정보보호학회장
2003년~2004년 : 성균관대학교 연구처장
1982년~현재 : 성균관대학교 정보통신공학부 교수
2000년~현재 : 정보통신부 지정 정보보호인증기술연구센터장
<관심분야> 암호이론, 정보시스템 보안 등