저 전력 모바일 환경에서 방송 콘텐츠 서비스를 위한 ID-기반의 인증된 동적 그룹 키 교환 프로토콜+

*최규영 **이동훈

고려대학교 정보경영공학전문대학원

*young@cist.korea.ac.kr, **donghlee@korea.ac.kr

ID-based Authenticated Dynamic Group Key Agreement for TV-Content Service in Low-Power Mobile Enviroment

*Choi, Kyu Yung **Lee, Dong Hoon

Center for Information Security Technology, Korea University

요약

최근 DMB 서비스와 같이 저 전력 무선 환경에서 유료 콘텐츠 서비스가 활발히 이루어지고 있다. 이러한 콘텐츠 서비스를 정당한 서비스 수신자에게 제공하기 위해서는 서비스 제공자와 수신자 사이에 안전한 키 교환이 필요하다. 본 논문에서는 모바일 콘텐츠 서비스를 위한 효율적인 ID-기반의 그룹 키 교환, 즉 다수의 서비스 수신자들(클라이언트)과 서비스 제공자(서버) 사이의 인증된 동적 그룹 키 교환 프로토콜을 제안한다. 제안한 프로토콜은 클라이언트의 계산량이 낮아 저 전력 모바일 환경에 적합하며, 또한 가입과 탈퇴 발생 시에도 효율적으로 키 교환을 수행할 수 있다. 제안한 그룹 키 교환 프로토콜은 랜덤 오라클 모델에서 그 안전성을 제공한다.

1. 서론

현대의 많은 협업과 분산 환경들, 즉 멀티 통신, 화상 회의 그리고 협업 도구들과 같은 환경에서 신뢰 할 수 있는 그룹 통신은 중요한 문제 가운데 하나이다. 그룹 키 교환(GKE) 프로토콜은 분배된 키를 소유한 사용자들과의 비밀 통신을 목적으로 한다. 그리고 이러한 그룹 키 교환 프로토콜에 어떤 의도된 사용자들에 대한 상호 인증을 제공하는 프로토콜을 인증된 그룹 키 교환(AGKE) 프로토콜이라 한다. 다양한 인증 기법들 중 전형적인 인증서 기반의 공개키 기반 구조는(Public Key Infrastructure, PKI)는 인증하고자 하는 상대방의 공개키에 대하여 신뢰 기관으로부터 발급된 인증서가 필요하다. 이러한 이유로 2001년 Boneh가 Blinear Map을 이용한 ID-기반 암호시스템 [3]을 제안하였다. ID-기반 시스템은 단지 사용자의 메일 주소와 같은 평이한 공개 정보로 구성된 공개 확인자(Identity, ID)만 알면 된다. 따라서 인증서 기반의 PKI에 비해 ID-기반의 인증 시스템이 보다 효율적이고 간단한 인증방식을 제공한다.

최근 무선 환경이 급속도로 발달하면서 휴대폰이나 PDA와 같은 저 전력 모바일 장치를 이용한 통신이 늘어나고 있다. 이에 따라 소형 단말기를 대상으로 디지털 콘텐츠 서비스를 제공하는 업체 수도 증가하고 있다. 이렇게 늘어나고 다양화 되는 콘텐츠 서비스를 안전하게 제공하기 위해 서비스를 제공하는 서버와 서비스를 제공받는 모바일 클라이언트 사이의 안전한 키 교환 프로토콜이 요구되고 있다. 특히 서버와 다수의 저 전력 모바일 클라이언트들 사이의 인증된 그룹 키 교환은 모바일 유료 방송 시스템이나 모바일 온라인 게임 등과 같은 콘텐츠 서비스를 안전하게 제공하기 위해 꼭 필요하다. 그러나 불행하게도 대부분의 ID-기반의 그룹 키 교환 프로토콜은 연산 속도와 계산량의 복잡함 때문에 저 전력 모바일 장치와 같은 자원 제한적인 곳에 적용하기엔 적절하지 않다.

본 논문에서는 [7]에서 제시된 ID-기반의 인증된 키 교환(AKA) 프로토콜을 확장하여 모바일 콘텐츠 서비스를 위한 효율적인 ID-기반의 그룹 키 교환, 즉 다수의 클라이언트들과 서버 사이의 인증된 그룹 키 교환 프로토콜을 제안한다.

Bilinear map을 이용한 ID-기반 시스템은 Weil/Tate pairing 연산과 ID를 표현한 수를 타원곡선(elliptic) 위의 한 점으로 변환시키는 Map-To-Point 연산과 같은 계산량이 많은 복잡한 연산을 필요로 한다. 따라서 이러한 복잡한 연산 특히 pairing 연산을 줄이기 위하여 많은 연구 [4,5,8]가 되어 왔음에도 불구하고 여전히 pairing 연산은 타원곡선에서의 스칼라 곱에 비하여 계산량이 훨씬 많기 때문에 여전히 기존에 제안된 ID-기반의 키 교환 기법 [1,11,12,6,9,13]은 저 전력 모바일 장치에 사용하기엔 적합하지 않았다. 그러나 최근 Choi 외 저자들이 저 전력 모바일 환경에서 적합한 서버와 클라이언트 간의 ID-기반의 키 교환 기법 [7]을 제안하였다.

제안하는 ID-기반 AGKA는 [7]을 그룹으로 확장하여 비대칭 형태의 그룹 키 교환 프로토콜을 설계하였다. 먼저 우리는 클라이언트 측에서의 복잡한 pairing 연산과 Map-To-Point 연산을 사용하지 않기 때문에 저 전력의 모바일 장치에 적합하다. 특히 오프라인 사전 계산을 하면 초기 셋업(Setup) 과정에서 각 클라이언트는

+ 이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No.R01-2004-000-10704-0).

단지 두 번의 타원곡선 곱만을 요하게 된다. 또한 제안한 프로토콜은 클라이언트들의 가입과 탈퇴가 일어나도 그룹 키 교환이 가능하다. 또한 제안한 ID-기반의 AGKA은 제안한 프로토콜은 서버의 고정된 비밀키가 노출되면 이전의 세션키가 폭로되지만, 클라이언트의 고정된 비밀키가 노출되어도 이전의 세션키가 안전한 절반의 전방향 안전성 (half forward secrecy)을 제공하며, 프로토콜의 안전성은 랜덤 오라클 모델에서 k-CAA (collusion attack algorithm with k traitors) 문제와 k-mBIDH (modified Bilinear Inverse DH with k values) 문제의 어려움에 기반한다.

2. 프로토콜 모델

비 대칭의 ID-기반의 그룹 키 교환의 기본 구조는 다음과 같은 알고리즘으로 구성되어 있다.

- 키 생성 알고리즘 $P-KGen(1^k)$ 은 보안 상수 1^k를 입력되어 각 클라이언트의 비밀키를 출력하는 알고리즘이다.
- 셋업 알고리즘 $P-Setup(U_P)$은 프로토콜을 시행하기 위한 파라메터 생성과 초기의 프로토콜 참여하는 클라이언트들의 그룹 U_P을 생성하여 세션키를 생성한다.
- 탈퇴 알고리즘 $P-Remove(U_P)$은 이전의 참여자 그룹으로부터 탈퇴한 클라이언트들의 그룹 U_R을 제외시켜 새로운 참여자 그룹 $U_P = U_P - U_R$을 설정하여 새로운 참여자 간에 세션키를 생성한다.
- 가입 알고리즘 $P-Remove(U_P)$은 이전의 참여자 그룹에서 새로 가입한 그룹 U_J을 추가하여 새로운 참여자 그룹 $U_P = U_P \cup U_J$을 설정한하여 새로운 참여자 간에 세션키를 생성한다.

3. Bilinear Map과 암호학적 가정들

본 장에서는 이 후 제안할 프로토콜과 관련된 몇 가지 정의와 가정들에 대해서 살펴본다. 본 논문에서 우리는 G_1을 위수가 q인 덧셈 연산 군이라 하고, G_2를 같은 위수 q를 갖는 곱셈 연산 군이라 하자. 그리고 P는 G_1의 생성자이다. 이 때 G_1, G_2에서의 이산 대수 문제(DLP)는 어렵다고 가정한다. 임의의 $P, Q \in G_1$와 $a,b \in Z_q^*$에 대하여 아래와 같은 조건을 만족하는 함수 $e: G_1 \times G_1 \rightarrow G_2$를 우리는 admissible bilinear map 이라 한다.

- Bilinear : $e(aP,bQ) = e(P,Q)^{ab}$
- Non-degenerate : $e(P,Q) \neq 1$을 만족하는 $P, Q \in G_1$가 존재한다.
- Computable : $e(P,Q)$을 계산할 수 있는 효율적인 알고리즘이 존재한다.

Computational Diffie-Hellman (CDH) problem: ICDH 문제는 $a \in Z_q^*$인 P, aP, cP가 주어지면 abP를 계산하는 문제이다.

Bilinear Inverse Diffie-Hellman (BIDH) problem: BIDH 문제는 $a,c \in Z_q^*$인 P, aP, cP가 주어지면 $e(P,P)^{a^{-1}c}$를 계산하는 문제이다.

우리는 위의 CDH와 BDH 문제를 어렵다고 가정한다. 이는 다항식 시간(polynomial time) 안에 위의 두 문제를 해결하는 알고리즘이 존재하지 않는다는 것이다.

4. 제안하는 ID-기반의 인증된 동적 그룹 키 교환 프로토콜

이 절에서는 앞 장에서 제시된 ID-AKD를 서버가 존재하는 비대칭 형태의 동적 그룹으로 확장시킨 그룹 키 교환 프로토콜 ID-AGKA를 제안하고 그에 대한 안전성을 분석한다.

먼저 KGC(Key Genration Center)는 난수 $s \in Z_q^*$와 G_1의 생성자 P를 선택하고 $P_{pub} = sP$를 계산한다. 또한 암호학적 일방향 해쉬 함수 $H: \{0,1\}^* \rightarrow Z_q^*$, $H_1 : G_2 \rightarrow Z_q^*$, $H_2 : 0,1^* \rightarrow 0,1^t$그리고 $H_3 : \{0,1\}^* \rightarrow \{0,1\}^k$를 선택한다. KGC는 마스터 비밀키인 s를 비밀로 하고 공개 시스템 파라미터 $params = (e, G_1, G_2, q, P, P_{pub}, H, H_1, H_2, H_3)$를 공개한다.

가. 키 생성(Key Generation)

확인자가 ID_U인 클라이언트 U가 비밀키를 얻기를 원할 때, KGC는 $q_u = H(ID_U)$와 $g = e(P,P)$를 계산하여 비밀키 $S_U = (s+q_U)^{-1}P$를 계산한 후, (g, S_U)를 안전한 채널로 U에게 전송한다. 동일한 방법으로, 확인자가 ID_V인 서버 V도 $q_v = H(ID_V)$를 계산한 후, 비밀키 $S_V = (s+q_V)^{-1}P$를 계산하여 안전한 채널로 V에게 전송한다.

나. 초기화(Setup)

$U_P = \{U_1, U_2, ..., U_n\}$을 서버 V와 그룹 세션 키를 생성하기를 원하는 모바일 클라이언트 그룹이라 하고, $ID_P = \{ID_1, ID_2, ..., ID_n\}$를 U_P에 속하는 클라이언트들의 확인자(identity)집합이라 하자. 또한 S_i를 각 U_i의 비밀키라 하고 S_V를 서버 V의 비밀키라 하면, 셋업 알고리즘 $P-Setup(U_P)$은 다음과 같이 3단계로 이루어진다 (그림 1. 참조).

- [Round 1.] 각 클라이언트 U_i는 서버의 확인자 ID_V로부터 $q_v = H(ID_V)$를 계산한 후, 난수 $a_i \in Z_q^*$를 선택하여 $t_i = g^{a_i}$와 $Q_V = P_{pub} + q_v P$를 계산한다. 또한 각 U_i는 $h_i = H_1(t_i)$, $X_i = a_i Q_V$ 그리고 $Y_i = (a_i + h_i)S_i$를 계산하여 $\langle ID_i, (X_i, Y_i) \rangle$를 V에게 전송한다.
- [Round 2.] 서버 V는 각 클라이언트들의 확인자 ID_i로부터 각각의 $q_i = H(ID_i)$와 $Q_i = P_{pub} + q_i P$를 계산한 후, $t_i = g^{a_i}$와 $c_i = e(X_i, S_V)$를 전송받은 메시지와 자신의 비밀키 S_V를 이용하여 계산한다. 또한 $h_i = H_1(t_i)$를 계산하고 각각의 클

라이언트에 대하여 $c_i = t_i g^{h_i}$임을 확인한다. 만약 식이 하나라도 성립하지 않으면 V는 실패를 출력하고, 모든 식이 성립하면 난수 $t_v \in Z_q^*$와 카운터 ct (초기값 0)를 선택한다. 그 후 V는 각 클라이언트의 비밀 정보인 t_i를 이용하여 $f = H_2(ct \| t_1 \| \ldots \| t_n \| t_v)$와 $f_i = f \oplus H_2(ct \| t_i \| t_v)$를 계산하여 $\langle f_i, ct, t_v \rangle$를 U에게 전송한다.

- [Key Computation.] 각 클라이언트 U_i는 자신의 비밀 정보 t_i와 전송받은 카운터 ct와 서버의 난수 t_v이용하여 $H_2(ct \| t_i \| t_v)$를 계산한 후 이를 이용하여 $f = f_i \oplus H_2(ct \| t_i \| t_v)$를 계산한다. 마침내 각 클라이언트는 그룹 세션키 $sk = H_3(f \| ID_1 \| \ldots \| ID_n \| ID_V)$ 얻는다.

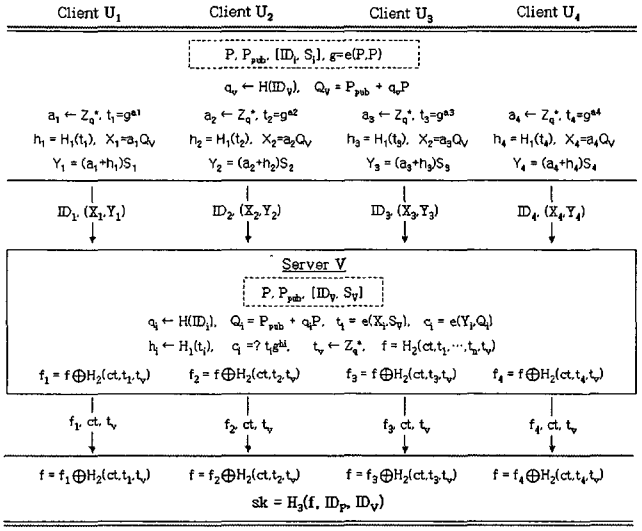

그림 1. ID-AGKA의 $P-Setup(U_P)$알고리즘 (i = 1 ~ 4)

위의 Round 2에서 서버는 매 세션마다 새로운 난수를 선택하여 f값을 계산하는데 사용한다. 이는 [2]의 기법과 같이 카운터만을 사용하면 parallel session attack [10]에 취약하기 때문에 이와 같은 공격에 안전하게 하기 위함이다.

다. 탈 퇴(Remove)

탈퇴한 클라이언트들의 집합(U_R)에 대한 탈퇴 알고리즘 $P-Remove(U_R)$은 다음과 같다(그림 2. 참조).

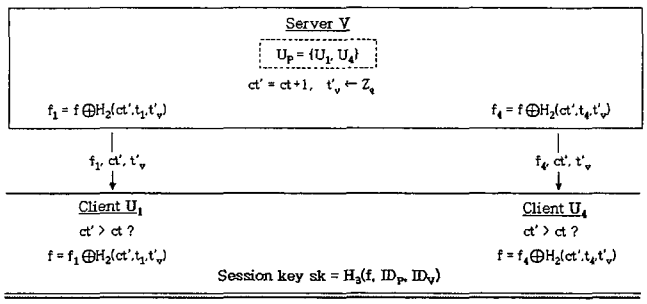

그림 2. ID-AGKA의 $P-Remove(U_R)$ 알고리즘 ($U_R = \{U_2, U_3\}$)

1. 먼저 서버가 이전의 참여자 그룹에서 탈퇴한 그룹을 제외하여 새로운 참여자 그룹 $U_P = U_P - U_R$을 설정한다.
2. 서버는 카운터 ct를 1 증가시키고 새로운 난수 $t'_v \in Z_q^*$을 선택한 후 U_P에 속하는 클라이언트들의 비밀 정보 $\{t_i\}_{i \in U_P}$를 이용하여 $f_i = H_2(ct \| t_i \| t'_v)$와 $f = f_i \oplus H_2(ct \| t_i \| t'_v)$계산한다.
3. 서버는 각 클라이언트 $\{U_i\}_{i \in U_P}$에게 $\langle f_i, ct, t'_v \rangle$를 전송하고 새로운 그룹 세션키 $sk = H_3(f \| ID_P \| ID_V)$를 계산한다.
4. 각 클라이언트는 전송받은 카운터를 이전의 카운터와 비교하여 1이 증가하였는지 확인하고 Setup 단계의 Key Computation과 동일하게 자신의 비밀정보와 서버의 난수 t'_v를 이용하여 $f_i = H_2(ct \| t_i \| t'_v)$와 $f = f_i \oplus H_2(ct \| t_i \| t'_v)$계산한 후, 새로운 그룹 세션키 $sk = H_3(f \| ID_P \| ID_V)$를 얻는다.

라. 가 입(Join)

새로 가입하려는 클라이언트들의 확인자 집합 U_J에 대한 가입 알고리즘 $P-Join(U_J)$은 다음과 같다(그림 3. 참조).

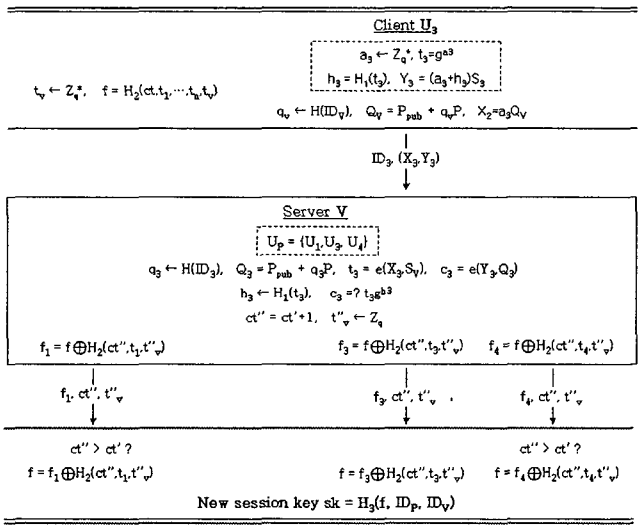

그림 3. ID-AGKA의 $P-Join(U_J)$ 알고리즘 ($U_J = \{U_3\}$)

1. 각 클라이언트 $U_j \in U_J$는 사전에 난수 $a_j \in Z_q^*$를 선택하여 $t_j = g^{a_j}$와 $h_j = H_1(t_j)$ 그리고 $Y_j = (a_j + h_j)S_j$를 계산한다. 그 후 U_j가 프로토콜에 참여하길 원한다면 서버의 확인자 ID_V를 이용하여 $q_v = H(ID_V)$를 계산한 후, $Q_V = P_{pub} + q_v P$와 $X_j = a_j Q_V$ 를 계산하여 $\langle ID_j, (X_j, Y_j) \rangle$를 V에게 전송한다.
2. 먼저 서버는 이전의 참여자 그룹에서 새로 가입한 그룹을 추가하여 새로운 참여자 그룹 $U_P = U_P \cup U_J$을 설정한다. 그 후 서버는 Setup 단계의 Round 2에서와 비슷하게 수행하여 전송받은 받은 메시지와 추가된 클라이언트들의 정당성을 확인한다.
3. 서버는 카운터 ct를 1 증가시키고 새로운 난수 $t'_v \in Z_q^*$을 선택한 후 U_P에 속하는 클라이언트들의 비밀 정보 $\{t_i\}_{i \in U_P}$를

이용하여 f_j와 f를 계산한다. 그리고 각 클라이언트는 $\{U_j\}_{j\in U_P}$에게 $\langle f_i, ct, t'_v\rangle$를 전송하고 새로운 그룹 세션키 $sk = H_3(f\|ID_P\|ID_V)$를 계산한다.

4. 각 클라이언트는 전송받은 카운터를 이전의 카운터와 비교하여 1이 증가하였는지 확인하고 Setup 단계의 Key Computation과 동일하게 자신의 비밀정보와 서버의 난수 t'_v를 이용하여 새로운 그룹 세션키 $sk = H_3(f\|ID_P\|ID_V)$를 계산한다. (물론 추가된 클라이언트는 확인과정이 없이 ct를 받아들인다. 또는 이들을 위해서 서버는 카운터를 $ct = 0$으로 초기화한다.)

5. 비교 및 결론

가. 비 교

우리는 제안한 기법과 같이 기존의 서버와 다수의 클라이언트 사이의 ID-기반의 그룹 키 교환 프로토콜인 [13]을 우리의 프로토콜과 초기화 단계에서의 통신량과 계산량을 중심으로 비교한다. 여기서 n을 프로토콜에 참여하는 전체 클라이언트의 수라 한다.

	Communication		
	Round	Unicasts	Broadcasts
Kim [13]	2	n	1
Our Protocol	2	n	1

표 1. 통신량 비교

	Computation					
	Server			Each Client		
	M	e	m(Exp)	M	e	m(Exp)
Kim [13]	3	3n	n(0)	4	1	1(0)
Our Protocol	n	2n	n(n)	2	0	0(1)

표 2. 계산량 비교(M: G_1에서의 스칼라 곱, A: G_1에서의 덧셈, e: pairing 연산, Exp: G_2에서의 지수승, m: G_2에서의 곱셈)

일반적으로 서비스를 제공하는 서버는 파워가 크다고 볼 수 있다. 따라서 서버에서의 계산량은 그리 중요하지 않다. 문제는 저 전력 모바일 환경인 클라이언트의 계산량이다. 위의 표에서 알 수 있듯이 제안한 프로토콜의 클라이언트 계산량이 기존보다 효율적임을 알 수 있다. 특히 계산량을 많이 요하는 pairing 연산이 클라이언트 측에 필요하지 않아 저 전력 모바일 환경에 적합하다고 볼 수 있다.

나. 결 론

본 논문에서 우리는 유료 방송 서비스를 위한 효율적인 ID-기반의 인증된 동적 그룹 키 교환 프로토콜을 제안하였다. 특히 서비스를 제공받는 클라이언트 측의 계산량을 줄임으로써 낮은 파워를 가진 모바일 장치에 알맞게 설계하였다. 제안한 기법의 안전성은 CDH와 BDH 문제의 어려움에 기반한다.

참 고 문 헌

[1] R. Barua, R. Dutta and P. Sarker, Extending Joux's Protocol to Multi Party Key Agreement., Proc. of Indocrypt '03.

[2] E. Bresson, O. Chevassut, A. Essiari and D. Pointcheval, "Mutual Athentication and Group Key Agreement for Low-Power Mobile Devices", In the 5th IEEE International Conference on Mobile and Wireless Communications Networks, 2003.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing", Proc. of Crypto '01, LNCS 2139, pp.213-229, Springer-Verlag, 2001.

[4] P. S. L. M. Barreto, H. Y. Kim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", Proc. of Crypto '02, LNCS 2442, pp. 354-368, Springer-Verlag, 2002.

[5] P. S. L. M. Barreto, B. Lynn and M. Scott, "Efficient implementation of pairing-based cryptosystems.", Journal of Cryptology, pp. 321-334, 2004.

[6] K. Y. Choi, J. Y. Hwang and D. H. Lee, "Efficient ID-based Group Key Agreement with Bilinear Maps", Proc. of PKC '04, LNCS 2947, pp.130-144, Springer-Verlag, 2004.

[7] K. Y. Choi, J. Y. Hwang, and In Seog Seo, "ID-based Authenticated Key Agreement for Low-Power Mobile Devices", Proc. of ACISP '05, LNCS 3574, pp.494-505, Springer-Verlag, 2005.

[8] S. D. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", Proc. of ANTS'02, LNCS 2369, pp.324-337, Springer-Verlag, 2002.

[9] N. McCullagh and P. S. L. M. Barreto, "A New Two-Party Identity-Based Authenticated Key Agreement", Proc. of CT-RSA'05, LNCS 3376, pp.262-274, Springer-Verlag, 2005.

[10] J. Nam, S. Kim and D. Won, "Attacks on Bresson-Chevassut-Essiari-Pointcheval's Group Key Agreement Scheme for Low-Power Mobile Devices", Proc. of IEEE Communications Letters, 2005.

[11] D. Nalla and K. C. Reddy, "ID-based tripartite Authenticated Key Agreement Protocols from pairings", Cryptology ePrint Archive, Report 2003/004.

[12] N.P.Smart, "An Identity based authenticated Key Agreement protocol based on the Weil pairing", Electronics Letters, vol. 38 (13): 630--632, June 2002.

[13] 김현주, 남정현, 김승주, 원동호, "유료 방송 시스템에 적합한 ID 기반의 2 라운드 그룹키 동의 프로토콜" 한국정보보호학회, 정보보호논문지, 15권 1호, 2005