情 報 保 護 學 會 誌
第20卷 第2號, 2010. 4

# 강화된 키 교환 프로토콜의 안전성 모델에 관한 연구

변 진 욱*

요 약

키 교환 프로토콜은 대표적인 암호화 프로토콜로서 그 안전성 모델에 관한 연구가 꾸준히 진행되어 왔다. 최근에는 기존의 안전성 모델을 강화시키고 강화된 모델을 바탕으로 키 교환 프로토콜 설계가 이루어졌다. 본 논문에서는 강화된 새로운 안전성 모델 결과들을 정리해서 살펴보고 향후 연구 방향에 대해서 논한다.

## Ⅰ. 서 론

인증된 키 교환 프로토콜(AKE: authenticated key exchange)은 인증과 키 교환이 동시에 이루어지는 프로토콜을 의미한다. 사용자들이 인증 및 키 교환을 시 도할 때 가장 중요한 부분은 개인의 비밀 정보이다. AKE 기법은 이러한 비밀 정보의 성질 및 공유 형태에 따라, 비밀 키 기반 기법, 공개키 기반 기법, 패스워드 기반 기법, 하이브리드 기법으로 나눌 수 있다. 우선, 비밀 키 기반 AKE 기법은 상호 공유된 대칭 키 및 대칭키 암호 알고리즘(예: AES, MAC)들을 이용하여 AKE를 수행한다. 이와 반면에, 공개 키 기반 AKE 기법은 사용자들의 개인키 및 공개키를 이용하여 AKE를 수행한다. 패스워드 기반 기법은 상호 공유된 비밀 값이 패스워드 형태인 것을 제외하고는 비밀 키 기반 AKE 기법과 동일하다. 사실, 패스워드 기반 AKE 기법은 비밀 키 기반 AKE 기법에 포함될 수 있지만, 따로 분류한 이유는 다음과 같다. 즉, 비밀 정보를 사전에 공유해야 한다는 사실은 동일하지만, 그 형태가 사용자가 암기 가능한 형태이므로 안전성 모델이 상이할 수 밖에 없다. 끝으로, 하이브리드 기법은 패스워드와 비밀 키 관리 기법 혹은 패스워드와 공개키 기반 기법을 병합해서 인증된 키 교환을 유도하는 방법이다.

1993년에 Bellare와 Rogaway가 처음으로 AKE 안전성 모델을 정의하였으며[1], 이를 바탕으로 다양한 AKE 프로토콜이 설계되었다[4,5]. 최근에는 기존의 AKE 안전성 모델에서 fresh session의 개념 정의를 더 유연하게 정의함으로 인해, 궁극적으로 공격자의 능력을 강화 및 계층화시키는 연구가 진행되었다. 이러한 결과는 2007년도에, LaMacchia, Lauther, 그리고 Mityagin에 의해서 처음으로 시도되었다[7]. 또한 2009년도에는 사용자들의 개인키를 하나 이상의 다른 AKE 프로토콜에서 안전하게 재사용 할 수 있는 공용의(shared) AKE 안전성 모델도 Chatterjee, Menezes, 그리고 Ustaoglu에 의해서 이루어졌다[6].

본 논문에서는 기존의 AKE 안전성 모델의 특징과 두개의 최신 결과들의[6,7] 특징들을 비교해서 살펴보고 향후 AKE 기반 프로토콜의 연구 가능한 주제에 대해서 논한다. 이를 위한 논문의 구성은 다음과 같다. 먼저, 기존 AKE 안전성 모델의 변화 과정을 세션 ID의 정의 방법, Freshness의 정의 방법, 공격자의 능력 및 안전성 모델의 측면에서 살펴본다. 그 후 강화된 AKE 안전성 모델 및 공용의 AKE 안전성 모델의 특징을 분석하고, 향후 연구 과제에 대해서 논한다.

## Ⅱ. 기존 AKE 안전성 모델의 특징

### 2.1. 세션 ID의 정의 방법

세션은 통신 흐름(flow)을 정의하기 위한 수단으로 사용된다. 즉, A에서 B로 특정 메시지를 통신 흐름에 실어

* 평택대학교 정보통신학과 조교수 (jwbyun@ptu.ac.kr)

보낼 때, 그 흐름을 지정하기 위한 고유한 값을 정의한 것이 세션 ID이다. AKE 프로토콜의 목적은 특정 세션을 보호하기 위한 세션 키를 만드는 것이 목적이므로 세션 ID를 엄밀히 정의하는 것이 굉장히 중요하다. 이러한 세션 ID를 정의하는 방법은 크게 두 가지로 나눈다. 첫째는 AKE 프로토콜 시작 전에 세션 ID가 미리 주어지는 경우다. 그래서 AKE 프로토콜이 종료되면, 미리 주어진 세션 ID의 세션 키가 두 사용자간에 만들어지게 된다. 두 번째 방법은 AKE 프로토콜을 시작하면서 고유한 세션 ID를 고유하게 만들어가는 방법이다. 이는 사용자간에 주고받는 메시지들의 연결로써 세션 ID를 구성하게 된다. 그러므로 AKE 프로토콜이 완전히 끝나야지만, 만들어진 세션 ID의 세션 키를 알 수 있게 된다. 전자의 방법은 [6]에서 정의되었고, 후자는 [3]에서 정의되었다.

## 2.2. 공격자의 능력 및 안전성 정의

### 2.2.1 공격자의 능력

공격자는 사용자들끼리 주고받는 모든 메시지들을 관찰 및 조절할 수 있다. 기존의 안전성 모델에서 공격자의 능력을 요약정리하면 다음과 같다. 표기 sid는 세션 ID를 의미한다.

- Send(M, A, sid) : 이는 사용자 A에 의해 실행되는 세션 식별자인 sid의 메시지 M을 전달하고, 출력 값은 그 프로토콜의 수행 결과 값이다. Send 질의는 공격자가 프로토콜 내에서 사용자 A에게 메시지를 전달하는 행동을 모델화 한 것이다.
- Reveal(sid, A) : 이는 사용자 A에 의해 sid의 세션 ID에 계산된 세션 키를 공격자에게 준다.
- Corrupt(A) : 이 질의를 통하여 공격자는 사용자 A의 개인 키 값(long-term secret)을 알 수 있다.
- Session-State Reveal(A, sid) : 해당 세션 sid에 포함되는 사용자 A의 세션 관련 비밀 값들을 공격자에게 준다.
- Test(A, sid) : 이 질의는 공격자의 세션 키에 관한 지식을 측정하기 위해 사용되어진다. 측정되어지는 세션은 반드시 fresh한 세션이어야 한다. 이에 대한 정의는 뒤에서 다시 살펴본다. 우선, 랜덤 비트 값 b를 결정하기 위해 동전던지기를 실시한다. b=1이면 세션 키가 공격자에게 전달되어진다. b=0인 경우는 랜덤 값이 전달된다.

### 2.2.2 안전성 정의

AKE 프로토콜을 공격하는 공격자 이점(advantage)을 수학적으로 정의함으로써 AKE 프로토콜의 안전성을 정의한다. 다음의 실험을 고려해 보자. 공격자 A가 Test 질의를 했을 때, 실험은 동전던지기를 통해 랜덤 비트 값 b를 만든다. 만약 b=1이면 실험은 세션 키를 공격자에게 전달하고, b=0이면 실험은 랜덤 값을 공격자에게 전달한다. 이러한 실험에서는 공격자는 b값을 추측함으로써, 세션 키를 알려 할 것이다. Succ를 공격자가 위의 b값을 정확히 추측한 사건이라 가정했을 때 프로토콜의 세션 키 안전성을 공격하는 공격자 A의 이점은 다항식 시간 T이내에 다음과 같이 정의된다.

$$Adv_P^{ake}(A,T) = 2\Pr[Succ] - 1$$

만약 $Adv_P^{ake}(A,T)$가 모든 확률적 다항식 시간 공격자에 대해서 무시할 수 있는 확률로 표현되어질 때 주어진 프로토콜 P는 안전하다고 말한다.

## 2.3. Bellare 기타 등의 방법의 특징

사실, AKE의 안전성 정의는 대칭키 기반 기법 환경에서 Bellare와 Rogaway에 의해서 처음 이루어졌다[1,2]. 위에서 정의된 안전성 정의 방법과 유사하며, 중요한 특징은 공격자에게 send, reveal, corrupt, test 오라클 질의를 허용하고 통신 개체의 파트너쉽(partnership) 개념을 일치되는 대화(matching conversation)라는 개념을 이용해서 정의하였다[1]. 또한 중요한 특징은, fresh 세션이 오직 reveal 질의를 이용해서 정의되었다는 점이다. 이는 잘 알려진 키 공격(known key attack)을 모델링하기 위한 것이었지만, 이후 이슈가 되었던 순방향 완전 기밀성(PFS: perfect forward secrecy)에 대한 정의를 온전히 포함 할 수 없었다. PFS는 사용자의 개인키가 노출 되었을때에도 공격자가 해당 세션 키를 구할 수 없어야 하는 성질이다. fresh 세션의 개념은 공격자가 test 질의를 통해 AKE 세션 키의 이점을 구하려 할 때에, test 질의의 대상이 되는 세션을 말한다. 공격자의 능력을 정확하게 반영하기 위해서는 fresh 세션의 세밀한 정의가 반드시 필요하다.

1) 구체적인 정의 및 내용은 참고문헌 [1,2]에 정의되어 있다.

2000년도에 Bellare, Rogaway, Pointcheval이 기존의 fresh 세션의 정의를 reveal과 corrupt 질의를 이용해서 수정하였고, 이를 통해 PFS의 이점을 정확히 안전성 모델에 반영할 수 있었다[3]. 세션 ID는 메시지들을 전달할 때마다, 사용자들의 각 통신 메시지들을 연결(concatenation)시키는 방법으로 고유하게 만들었다.

### 2.4. Canetti, Krawczyk 방법의 특징

2001년도에, Canetti와 Krawczyk는 공격자에게 session-state reveal 질의를 허용하게 함으로써, 기존의 AKE 모델 정의를 한층 강화 시켰다. 처음으로 정의되었던 session-state reveal 질의는, 공격자에게 사용자들이 세션 키를 만들 때 필요한 임시적인 비밀 값을 알 수 있게 하는 질의이다. 이와 더불어 중요한 특징은 세션의 ID를 정의하는 방법에 있었다. 즉, 세션 ID가 프로토콜 시작 전에 사용자들에게 미리 주어지도록 설계되었다. 이러한 점은 기존의 Bellare, Rogaway 모델과[1,2,3]크게 다른 점이라 할 수 있으며, 이후 두 모델의 상호 관계성 규명에 많은 어려움을 야기시키는 원인이 되었다. 그 이유는, 세션 ID를 만드는 방법에서 찾아 볼 수 있는데, 전자의 Canetti 모델은 주어진 프로토콜의 세션 ID가 프로토콜의 이전에 이미 주어지는 상황이므로, 프로토콜이 끝나야만 세션 ID를 알 수 있는 Bellare 식의 모델로 상호 변화될 수 없기 때문이다.

Krwaczyk는 2005년도에 기존의 Canetti와 Krawczyk 모델에 key compromise 가장 공격을 추가하여 정의하였다[9]. key compromise 가장 공격이란, 사용자 A의 키가 노출 되었을 때 그 키를 이용하여 다른 사용자라고 A에게 가장하는 공격을 말한다. 또 하나의 특징은, PFS를 weak PFS와 full PFS로 나누어서 정의하였다는 점이다. 우선, 기존 PFS는 세션이 끝난 후에 사용자의 개인키가 노출 되었을 때 그 해당 세션의 세션 키를 얻을 수 없는 성질이었다면, 추가 정의된, weak PFS는 세션이 끝나지 않고도 세션 중간에 수동적(passive) 공격자가 사용자의 개인키를 얻게 되었을 때 해당 세션의 세션 키를 얻을 수 없는 성질이다. full PFS는 수동적 공격자가 아니라 메시지를 변경할 수 있는 능동적(active) 공격자로 조건을 강화시킨 것이다. 2번의 메시지 전송횟수로(2-pass) full PFS를 만족시키는 AKE 프로토콜 설계는 불가능한 반면에, 3번의 메시지 전송횟수로(3-pass) full PFS를 만족하는 프로토콜 설계는 가능하다고 증명되었다.

## Ⅲ. 강화된 AKE 안전성 모델

본 장에서는 LaMacchia, Lauter, Mityagin이 제안한 강한 AKE 안전성 모델 및 그 특징을 살펴본다[8]. 특별히 강화된 AKE 모델의 특징은 크게 두 가지로 요약할 수 있다. 첫째는 ephemeral key reveal질의를 새롭게 정의한 부분이고, 둘째는, 공격자의 test 질의 대상인 fresh한 세션을 공격자의 능력을 강화시키는 관점에서 새롭게 정의했다는 점이다. 아래에서 위 두 가지에 대해서 자세히 살펴본다. 이와 더불어, 강화된 AKE 모델이 실제적으로 어떠한 공격에 안전할 수 있는지 살펴본다.

### 3.1. Ephemeral Key Reveal 질의

가장 주요한 변경 부분은 공격자의 질의 부분이다. 기존의 corrupt 질의 대신, long-term key reveal 질의를 정의하였으며, session-state reveal 그리고 reveal 질의를 기존 모델과 동일하게 허용하였다. 가장 이슈가 되는 점은 session-state reveal 질의를 더욱 세분화해서 재정의한 사실이다. session-state reveal 질의는 세션에 해당하는 임시 값들을 모두 공격자에게 허용하는 질의였지만, 사실, 기존 AKE 모델은[1] 사용자의 모든 랜덤 값들을 공격자가 알 수 있도록 허용하지 않았다. 예를 들어, AKE 프로토콜 중에서는 메시지 인증을 위해 전자서명 알고리즘을 사용하는데, 일반적으로 전자서명에는 랜덤 값 (랜덤 코인)이 반드시 사용된다. 기존의 AKE 안전성 모델은 이러한 랜덤 값들까지 공격자에게 허용하지는 않았다. 그래서 이러한 점이 기존 AKE 안전성 모델로 안전하게 설계되었다하더라도 해당 프로토콜의 취약점이 될 수 있다. 그래서 session-state reveal 대신 새로운 ephemeral key reveal 질의를 새롭게 정의했다. 그 질의를 통해 공격자는 AKE 프로토콜 중에서 발생할 수 있는 모든 랜덤 값을 얻을 수 있게 된다.

### 3.2. Freshenss의 강화된 정의

Freshness의 정의는 공격자의 이점을 측정하기 위한 대상이 되는 순수 세션의 성질을 정의한 것이다. 그러므로 freshness의 정의는 공격자에게 정당한 이점을 측정하기 위해서 반드시 피해야 하는 질의 조건을 정확히

명시하여 정의된다. 이를 위해 long-term key reveal과 ephemeral key reveal 질의들을 이용해서 다음과 같이 정의하였다. sid는 송신자 A(owner)의 시작에 의해서 수신자 B(peer)에 의해 완료된 세션 id이며, 다음의 어느 조건도 만족하지 않을 때, 해당 sid를 fresh 하다고 정의한다. (단, A에 의해서 실행된 AKE 프로토콜의 세션 id는 sid이며, B에 의해서 실행된 세션 id는 sid*이다. 두 세션이 매칭 일 때, (함께 통신하고 있는 경우), sid, sid*를 매칭세션이라 정의한다. 매칭 및 매칭 세션에 대한 구체적인 정의는 참고문헌 [6,9]를 참고한다.)

- 공격자는 sid에 해당하는 세션 키나 혹은 그와 매칭 세션에 있는 sid*의 세션 키를 노출한다.
- B가 세션 sid*에 연결되어 있고, sid와 매칭 세션일 때, 공격자는 다음의 질의를 한다.
  - long-term key reveal(A)와 ephemeral key reveal(A, sid) 혹은,
  - long-term key reveal(B)와 ephemeral key reveal(B, sid*) 질의 수행
- sid와 매칭인 세션이 존재하지 않고, 공격자가 다음의 질의를 한다.
  - long-term key reveal(A)과 ephemeral key reveal(A, sid) 혹은,
  - 세션 sid가 완료되기 전에, long-term key reveal(B)질의를 수행

위의 fresh 세션의 정의는 두 가지 경우로 나뉜다. sid와 매칭 세션인 sid*가 존재하는 경우와 그렇지 않은 경우이다. 우선, 존재하는 경우는, sid에 대해서 사용자 A의 비밀값과 랜덤 값들 모두에 대해 질의하는 것을 규제하고 있다. 마찬가지로, sid*에 대해서도 사용자 B의 개인키 값과 랜덤 값에 대해서 질의하는 것을 제한하고 있다. 즉, 공격자가 사용자 A, B의 개인 키 값과 랜덤 값들에 대해서 한 사용자들에게 동시에 질의하는 것을 허용하지 않되, 사용자 A의 개인 키 값, 사용자 B의 랜덤 값, 그리고, 사용자 A의 랜덤 값, 사용자 B의 개인 키 값 에 대해서는 공격자에게 허용하여도, 해당 세션을 fresh 세션이라 정의하였다. 이것은 공격자의 능력을 강화시킨 반면에 fresh 세션을 좀 더 유연하게 정의했다고 볼 수 있다.

위의 정의는 일반적인 3-pass 용 AKE 프로토콜을 위한 fresh 세션의 정의이고, 2-pass용 AKE 프로토콜의 정의는 다음과 같이 정의한다. 즉, 다음의 어느 조건도 만족하지 않을 때, 해당 sid를 fresh하다고 정의한다. 나머지 두 조건은 위의 fresh 세션의 정의와 동일하므로 중복적인 기술을 생략했다.

- sid와 매칭인 세션이 존재하지 않고, 공격자가 다음의 질의를 한다.
  - long-term key reveal(A)과 ephemeral key reveal(A, sid) 혹은,
  - 항상 long-term key reveal(B)질의를 수행

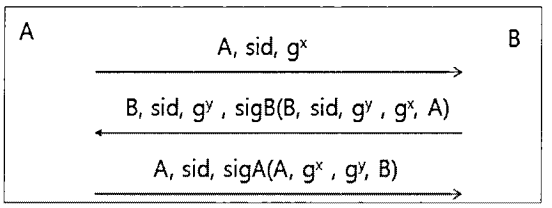
마지막 부분의 정의가 "*세션 sid가 완료되기 전*"에서 "*항상*"으로 변경된 것을 제외하고는 모든 조건이 동일하다. 세션 sid가 완료되기 전 의 의미는 사용자 A가 첫 번째 메시지를 보내기 전을 의미한다. 그리고, 항상은 사용자 A가 첫 번째 메시지를 보내는 것과 상관없이(보내기 전 보낸 후 모두 포함) long-term key reveal(B) 질의를 할 수 없음을 의미한다. 그러므로, 2-pass 용 freshness는 상대적으로 유연하지 못한 정의이다. 하지만, 2-pass용 freshness를 따로 정의한 이유는 2-pass AKE 프로토콜은 3-pass용 AKE 프로토콜의 fresh 세션의 정의에 의해 안전하지 않기 때문이다. 예를 들어, 임의의 2-pass 용 AKE 프로토콜이 있을 때, 사용자 A가 첫 번째 메시지를 보내 기 전에 long-term key reveal(B)를 허용하게 되면, 임의의 공격자는 쉽게 랜덤 값들을 생성하여서 사용자 B를 가장할 수 있고, 이후 사용자 A가 보내온 첫 번째 메시지를 이용해서 세션 키를 쉽게 구할 수 있게 된다. 그러므로 2-pass용 fresh 세션의 정의는 항상 long-term key reveal(B) 질의를 못하도록 제한하였다.

### 3.3. SIG-DH 프로토콜의 공격 및 개선 프로토콜

강화된 AKE 모델에서 가장 큰 변화는 무엇보다도 ephemeral key reveal을 새롭게 정의한 것이다. 사실, 이 질의를 통해 안전하다고 알려진 기존의 SIG-DH 프로토콜을[6] 공격할 수 있다. SIG-DH 프로토콜과 그 공격 시나리오를 아래에 간략히 소개하였다.

#### 3.3.1 SIG-DH 프로토콜

SIG-DH 프로토콜은 cannetti와 krawczyk에 의해서 제안되었다[6]. 안전성 모델에서 ephemeral key 값을 얻을 수 있는 질의를 공격자에게 허용하였지만, ephemeral의 정의에 온전한 의미의 랜덤 값을 포함하지 않았다. 이로 인해 취약점이 발생된다.



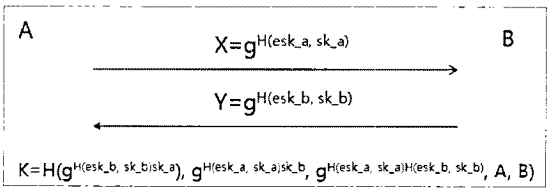

〔그림 1〕 SIG-DH 프로토콜

[프로토콜 설명] 먼저, sid는 프로토콜 시작 전에 미리 주어진다. 사용자 A는 랜덤 값 $x$를 이용해서 $g^x$를 계산해서 사용자 B에게 준다. 사용자 B는 자신도 $g^y$를 계산 한 후, $g^x, g^y, sid, A, B$를 자신의 개인키로 서명하여 A에게 주면, 사용자 A도 $A, g^x, g^y, B$를 개인 서명하여 사용자 B에게 돌려준다. 형성되는 세션 키는 $g^{xy}$이다.

[공격 시나리오] 다양한 공격 시나리오가 가능하겠지만, 먼저, 공격자가 모든 랜덤 값 (random coin 포함) 을 질의할 수 있는 상황에서는, 프로토콜에서 사용된 전자서명의 랜덤 값 까지 알 수 있다는 사실을 주목해야 한다. 이러한 랜덤 값 노출은 통해 전자사명의 개인 키 값을 쉽게 알 수 있다. 예를 들어, 잘 알려진 ElGamal, Schnorr, DSA, GQ 전자서명에서 랜덤 값의 노출은 개인 키 값의 노출로 이어짐은 자명하다. 그러므로 ephemeral key reveal 질의를 통해, 서명을 위조할 수 있으며, 이는 안전성의 결점을 야기 시킨다.

### 3.3.2 개선된 NAXOS 프로토콜

NAXOS 프로토콜은 위에서 언급한 공격에 안전하도록 설계한 AKE 프로토콜이다.




〔그림 2〕 NAXOS 프로토콜

[프로토콜 설명] 위에서 보듯이, NAXOS 프로토콜은 2-pass 프로토콜이며, 3-pass로 확장 가능하다. 먼저, 사용자 A는 자신의 비밀키 sk_a와 랜덤하게 뽑은 키 값 esk_a를 해시해서 X를 계산하고, 사용자 B도 동일한 방법으로 Y를 계산해서 서로 교환한다. 사용되는 해시 함수는 임의의 공간에서 $Z_q^*$으로 연결되는 암호학적으로 안전한 일 방향 해시 함수이다.

[세션 키에 대한 특징] 세션 키를 만드는 방법이 기존 방법과 비교했을 때 참신하다. 각각 주고받은 X, Y값에 자신의 개인키를 승하고, X, Y에 사용했던 지수 값(해시 값)을 승한 값들을 모두 해시해서 세션 키를 형성하게 된다. 이러한 방법은 첫째, 지수 승 횟수를 줄여주는 효과를 지닌다. 즉, X 및 K를 계산할 때, 해시 된 값에 대해서 지수 승을 수행하기 때문에 지수 값들이 많이 사용된 것에 비해 지수 승이 많지 않은 편이다. 둘째, 위에서 정의한 fresh한 세션에 대해서, 공격자는 세션 키에 대한 안전성을 어려운 문제로 쉽게 귀결 시킬 수 있게 된다. 즉, fresh한 세션은 공격자가 사용자들에 대해서 개인 키 값과 랜덤 값들을 모두 알지 못하는 세션이다. 설계된 세션 키 구조는 사용자들의 개인 키 값과 랜덤 값들을 동시에 알지 못하는 한 공격자가 쉽게 세션 키를 알지 못하도록 설계되었다. 그러므로 그러한 fresh한 세션에 대해서, 정의된 공격자의 질의를 통해, 세션 키를 구하기 위해서는 DH 관련 문제를 풀어야만 된다. 그러므로 쉽게 랜덤 오라클 모델에서 증명 가능한 AKE 프로토콜 설계가 가능한 장점이 있다.

## Ⅳ. 비밀 키를 재사용하는 강화된 AKE 안전성 모델

NIST SP 800-56A 표준 문서에서는 키 설정 프로토콜을 수행할 때 사용자들의 개인키를 한 개 이상의 프로토콜에서 재사용 할 수 있다고 명시되어 있다. 하지만, 지금까지 제안되었던 키 교환 프로토콜은 사용자의

개인키를 재사용했을 때, 이에 대한 안전성을 제공하지 못하였다. 즉, 각각의 AKE 프로토콜은 안전하나, 사용자의 개인키가 여러 AKE 프로토콜에 재사용 되어 질 때는 안전성의 문제가 야기되었다. 이러한 문제점이 Chatterjee, Menezes, Ustaoglu들에 의해 처음 발견되었고 이에 맞는 공용의(shared) AKE 안전성 모델이 설계되었다. 본 장에서는 그 모델의 특징에 대해서 간략히 살펴본다.

### 4.1. 공용 모델에서의 공격자의 질의 능력

우선 공용의 AKE 모델은 *d*개의 AKE 프로토콜들을 가정하고, 사용자는 동일한 개인키를 모든 프로토콜에 동일하게 사용한다. 이러한 사실을 제외하고는 기존의 AKE 환경과 동일하다. 그러므로 공격자의 질의 능력 차원에서 기존 안전성 모델과 크게 차이점은 없다. 사용자의 개인 키 값을 알 수 있는 long-term key reveal(A) 질의가 statickeyreveal(A)로 질의 이름만 변경 되었고, 나머지 질의들은 기존의 AKE 안전성 모델과 동일하다. 여러 개의 AKE 프로토콜을 수행할 수 있기에, sessionkeyreveal(sid)과 ephemeralkeyreveal(sid) 질의가 sid를 입력 값으로 받는다. 이 부분은 한 개의 AKE 프로토콜에 대한 기존의 안전성 모델에서도 sid를 입력으로 해서 질의가 수행되었던 부분이다. 비록, 여러 AKE 프로토콜을 수행한다 하더라도 각각의 세션 id는 고유하기 때문에 고유한 sid가 생성된다. 그러므로 비록 d개의 프로토콜로 대상이 증가되었지만 sessionkeyreveal과 ephemeralkeyreveal에 대해서 sid를 입력으로 해서 질의가 이루지는 것은 자연스럽다. 하지만, ephemeralkeyreveal 질의에 대해서 내용을 세분화 할 수 있는 여지는 충분히 있다. 즉, 랜덤 값을 알려주는 ephemeralkeyreveal(sid) 질의 입력 값을 (sid,사용자)의 입력 형태로 만들어주면, 특정 사용자에 대한 세션 관련 랜덤 값을 알려주므로 공격자의 능력을 세분화 할 수 있게 된다.

### 4.2. 공용 모델에서의 매칭 세션 및 fresh 세션

우선 세션 id는 sid=(P, I, R, Role, Comm)로 정의된다. P는 프로토콜 이름이며, I는 프로토콜의 시작자이며, R은 프로토콜의 응답자이다. Role은 자신이 I혹은 R인지를 나타내는 기호이며, Comm은 전달되는 메시지를 나타낸다. sid=(P, A, B, Role, Comm)와 sid*=(P*, C, D, Role*, Comm*)가 매칭 세션이다 함은 P=P*, A=D, B=C, Role $\neq$ Role*, Comm*=Comm 일 경우를 의미한다. fresh 세션은 기존의 AKE 안전성 모델에서의 정의와 동일하다.

### 4.3. 공용 모델에서의 안전성 정의

구체적인 안전성 정의에서 변화된 부분은 대상이 한 개의 프로토콜이 아니라 한 개 이상의 AKE 프로토콜로 확장되었다는 점이다. d개의 AKE 프로토콜이 존재할 때 다음의 두 조건을 만족하면, d개의 AKE 프로토콜들은 공용의 AKE 모델에서 안전하다고 정의한다.

- 어떠한 $i \in [i, d]$에 대해서 AKE 프로토콜의 세션을 완료 했을 때, 참여한 사용자는 높은 확률로 동일한 세션 키를 구할 수 있어야 한다.
- 어떠한 $i \in [i, d]$에 대해서 다항식 시간의 공격자는 랜덤한 키와 $i$의 AKE 프로토콜에서 만들어진 세션 키와 구분이 불가능해야 한다.

공용의 모델에서는 모든 사용자들은 동일한 개인키를 d개의 AKE 프로토콜에 사용한다. 이러한 특징이 위 정의에 포함되어 있다. 다시 말해, 세션 키에 대한 구분 불가능성의 대상이 d개의 프로토콜의 각 세션으로 확장된 점이 크게 틀린 점이다. 그러므로 위 정의에 안전한 d개의 AKE 프로토콜들이 공용의 안전성을 만족한다면, d개의 AKE 프로토콜 각각은 기존의 AKE 안전성 모델에 안전하다고 말할 수 있다.

## V. 향후 연구 과제 및 결론

본 논문에서는 안전성 모델에 대한 최근 두 개의 연구 결과에 대해서 그 특징을 분석하였다. 그 특징을 요약하면, fresh 세션에 대한 재 정의와 여러 개의 AKE 프로토콜에서도 사용자의 개인키를 재사용할 수 있도록

강화시켰다는 점이다. AKE 프로토콜은 대표적인 암호 프로토콜이므로 통신 환경 및 조건의 영향을 많이 받는다. 그러므로 차세대 통신 환경에 따라 더욱 다양하고 강화된 모델 연구가 진행 되어야 한다.

랜덤 오라클 하에서 설계된 AKE 프로토콜을 강화된 AKE 혹은 공용의 AKE 안전성 모델 하에서 표준 가정만을 이용하여 설계하는 것이 필요하다. 이와 더불어, 그룹 환경에서의 새로운 안전성 모델 연구 및 프로토콜 설계도 필요하다. 더 나아가 패스워드 기반의 안전성 모델 연구 및 양 자간(two-party) 혹은 그룹 환경의 AKE 프로토콜 설계도 좋은 연구 주제가 될 것이다.

## 참고문헌


[1] M. Bellare and P. Rogaway, "Provably secure session key distribution-the three party case", ACM symposium in theory of computing, 1995.

[2] M. Bellare and P. Rogaway, "Entity authentication and key distribution", In proceedings of Crypto 1993, LNCS Vol. 773, pp. 232-249. Springer-Verlag, 1994.

[3] M. Bellare, D. Pointcheval, and P. Rogaway, "Authenticated key exchange secure against dictionary attacks", In proceedings of Eurocrypt 2000, LNCS Vol.1807, pp. 139-155, Springer-Verlag, 2000.

[4] S. Blake-Wilson, D. Jhonson, and A. Menezes, "Key agreement protocols and their security analysis", In proceedings of IMA international conference, LNCS Vol. 1361, pp. 30-45, Springer-Verlag, 1997.

[5] K.-K.R. Choo C. Boyd and Y. Hitchcock, Examining Indistinguishability complexity proofs for protocols, Advances in Cryptology, Asiacrypt '05, LNCS 3788, pp. 624-643, Springer-Verlag, 2005

[6] R. Canetti and H. Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels, Advances in Cryptology, Eurocrypt '01, pp. 453-474, Springer-verlag, 2001.

[7] S. Chatterjee, A. Menezes, B. Ustaoglu, "Reusing static keys in key agreement protocols", Indocrypt '09, LNCS 5922, pp. 39-56, Springer-Verlag, 2009.

[8] B. LaMacchia, K. Lauter and A. Mityagin, "Stronger security of authenticated key exchange", ProvSec'07, LNCS 4784, pp. 1-16, Springer-Verlag, 2007.

[9] H. Krawczyk, HMQV: A High-Performance Secure Diffie-Hellman Protocol", Advances in Cryptology, Crypto'05, LNCS 3621, pp. 546-566, Springer-Verlag, 2005.


## 〈著者紹介〉


**변 진 욱 (Byun, Jin Wook)**
정회원

2001년 2월 : 고려대학교 전산학과 이학사
2003년 2월 : 고려대학교 정보보호대학원 공학석사
2006년 8월 : 고려대학교 정보보호대학원 공학박사
2006년 11월 ~ 2007년 11월: 런던대학교, Information Security Group, 박사 후 연구원
2008년 3월~현재: 평택대학교 정보통신학과 조교수
<관심분야> 암호 프로토콜 설계, 키 교환 프로토콜 설계, 스마트 카드 인증, 키워드 검색 프로토콜, 개인정보 보호 기술