情報保護學會論文誌
第12券 第1號, 2002. 2

약한 키를 가지는 대화식 영지식 증명의 안전성 강화 방법과 그 응용

양 대 헌*

A Method to Enhance the Security of ZKIP with Weak Keys and Its Application

Dae Hun Nyang*

요 약

본 논문에서는 약한 키를 가지는 대화식 영지식 증명을 이용한 인증 프로토콜의 안전성을 강화하는 방법을 제시한다. 일반적으로 대화식 영지식 증명을 이용한 인증 프로토콜은 충분히 길고 랜덤한 비밀키를 가정하고 그 비밀키에 대한 영지식 증명을 수행하게 된다. 하지만 때에 따라서 충분히 길지 않거나 랜덤하지 않은 비밀키가 선택될 수 있다. 즉, 좋지 않은 난수 발생기를 써야 하는 경우, 또는 패스워드처럼 의도적으로 약한 키를 사용하는 경우가 생기며, 대화식 영지식 증명은 이에 적합하지 않다고 알려져 있다. 본 논문에서는 비밀 동전 던지기(Secret Coin Tossing)라는 개념을 제시해서, 일반적인 영지식 증명을 이용한 인증 프로토콜을 약한 키를 가지는 영지식 증명 기반 인증 프로토콜로 쉽게 변환할 수 있는 프레임웍을 제안한다. 또한, 이 프레임웍을 이용해서 설계된 인증 프로토콜이 ideal cipher model에서 안전함을 보인다.

ABSTRACT

We present a systematic way to armor a zero-knowledge interactive proof based identification scheme that has badly chosen keys. Keys are sometimes mistakenly chosen to be weak(neither random nor long), and a weak key is often preferred to a strong key so that it might be easy for human to remember. Weak keys severely degrade the security of ZKIP based identification schemes. We show using off-line guessing attack how the weak key threats the security of ZKIP based identification schemes. For the proper usage of ZKIP, we introduce a specialized form of ZKIP, which has a secret coin-tossing stage. Using the secret coin tossing, a secure framework is proposed for ZKIP based identification schemes with weak keys in the ideal cipher model. The framework is very useful in password based authentication and key exchange protocol

keyword : *Zeroknoledge interactive proof, authentication protocol, password, weak keys*

Ⅰ. 서 론

대화식 영지식 증명은 암호학에서 가장 유용한 불 중의 하나가 되었고, 수많은 암호 프로토콜들이 대화식 영지식 증명에 기초하고 있다. 대화식 영지식 증명이 가장 유용하게 쓰이는 분야중의 하나가 인증 프로토콜 분야인데, 많은 좋은 프로토콜들이 제안되어왔다.[8,19,10]

대화식 영지식 증명에서 증명하려는(동시에 아무 지식도 노출시키지 않으려는) 비밀은 예외 없이 길고

* ETRI 정보보호연구본부(nyang@etri.re.kr)

랜덤한 수이어야 하며, 이는 대화식 영지식 증명의 광범위한 사용을 제한한다. 즉, 아무리 잘 설계된 대화식 영지식 증명 프로토콜이라 하더라도 그것이 증명하고 있는 비밀의 랜덤성과 충분한 길이가 보장되지 않는다면 오프라인 사전 공격(Offline Dictionary Attack or Guessing Attack)에 쉽게 깨어질 수 있다. 이 논문에서는 일반적인 대화식 영지식 증명에 기반한 인증 프로토콜에 약한 키가(weak key)가 사용되는 경우 어떻게 이런 오프라인 사전 공격이 가능한지에 대해 알아보고, 이들을 체계적으로 막을 수 있는 프레임웍을 제시한다. 약한 키를 가지는 대화식 영지식 증명의 안전한 사용을 위해서 비밀 동전 던지기(Secret coin tossing)이라는 개념을 제안하고, 이를 수용한 특별한 형태의 영지식 증명에 기반한 인증 프로토콜 프레임웍을 소개한다.

이 프레임웍을 적용할 수 있는 재미있는 응용분야가 하나 있는데 바로 패스워드에 기초한 인증 및 키 교환 프로토콜이다. 비록, 공개키 암호시스템이 이제는 매우 광범위하게 사용되려고 하고, 암호학에서는 아주 막강한 툴이 되었지만 아직 공개키/비밀키/인증서를 사용자가 가지고 다니는 것은 전혀 편리한 방법이 아니다. 어떤 특정한 분야에서 패스워드는 그 자체로 훌륭한 인증의 도구가 되고 있다. 패스워드를 이용하는 인증 프로토콜에서는 사용자가 스마트카드 등의 귀찮은 디바이스를 들고 다니지 않아도 되므로 사용자 편의성 면에서 훌륭한 프로토콜이라고 할 수 있다. 다만, 패스워드의 충분하지 않은 랜덤성과 짧은 길이로 인해 인증 및 키 교환 프로토콜의 설계에 패스워드를 사용하는 것은 많은 주의를 요한다. 1992년 Bellovin과 Merrit에 의해 처음 오프라인 사전 공격에 강한 패스워드를 이용한 인증 프로토콜(EKE)이 설계되었다.[3] 이후 Jablon의 SPEKE 그리고 Wu의 SRP등이 발표되었다.[11,21] EKE와 SPEKE는 패스워드 확인자 모델(Password verifier model)로 확장되었는데 각각 A-EKE, B-SPEKE이다.[12,4] 패스워드 확인자 모델은 서버에 패스워드를 보관해 놓지 않고, 패스워드에 프로토콜에 따른 일방향 함수를 수행한 결과값만을 보관해 놓고 인증 및 키 교환을 수행하는 모델을 말한다. 이 모델은 plaintext 모델(패스워드를 서버에 저장해 놓는 모델)에 비해 서버에게 패스워드를 알리지 않는다는 점에서 사용자에게 유리하다. 또한 서버가 해킹 당하는 경우에도 사용자의 패스워드가 직접 노출되지 않는다는 점에서 더 좋은 모델이라 할 수 있다. 초기의 패스워드를 이용한 인증 프로토콜들이 프로토콜의 안전성에 수학적 증명을 가지지 못하고 있었지만, 2000년 Bellare 등에 의해 패스워드에 기초한 인증 프로토콜에 대한 암호학적 접근이 이루어졌다.[2] 이를 계기로 수학적 안전성 증명을 가지는 프로토콜이 하나씩 설계되고 있다.[5, 3,15] 다만 이들 프로토콜들은 아직 계산량 등의 측면에서 효율적이지 않다. 이 논문에서는 ideal cipher model에서 수학적인 안전성 증명을 가지는 패스워드를 이용한 인증 및 키 교환 프로토콜을 설계하는 프레임웍을 제시한다. 이 프레임웍을 이용해서 기존의 또는 앞으로 발표될 좋은 특징을 가지는 대화식 영지식 증명 프로토콜을 쉽게 패스워드를 이용한 인증 및 키 교환 프로토콜로 변환할 수 있다. 또한 약한 키를 가지는 대화식 영지식 증명 프로토콜을 안전하게 사용할 수 있다.

II. 영지식 증명과 약한 키

일반적으로 대화식 영지식 증명에 기초한 인증 프로토콜은 크게 다음의 세 단계로 이루어진다: 시험(test), 질문(question), 목격(witness). 어떤 비밀 지식을 증명하는 증명자(knowledge prover)는 시험수(test number)를 생성해서 확인자(knowledge verifier)에게 전송하고, 확인자는 질문수(question number)를 평문으로 전송한다. 마지막으로 증명자가 자신이 알고 있는 비밀 지식을 이용해서 목격자수(witness number)를 계산하고 이를 확인자에게 전송한다. 확인자는 시험수, 질문수, 목격자수, 비밀 지식에 대응하는 공개키를 이용해 확인한다.

만약 대화식 영지식 증명이 증명하고 있는 비밀지식이 작은 집합에서 선택되었고, 랜덤하지 않거나 충분히 길지 않다면, 공격자는 쉽게 공개키(또는 패스워드 확인자)를 참조 삼아 오프라인 사전 공격을 수행할 수 있다. 이 trivial한 공격은 패스워드 확인자나 공개키를 서버의 안전한 저장소에 저장해 놓으므로써 쉽게 막을 수 있다. 하지만, 공개키 또는 패스워드 확인자가 사용자와 서버에게만 알려져있다 하더라도, 공격자는 둘 사이의 대화(transcript)를 보고서 오프라인 사전 공격을 수행할 수 있다. 다음의 대화식 영지식 증명을 보자.

- **시스템 설정**

공개키는 $V = OWF(f(S))$이며, 여기서 S는 약한

키 $f()$는 S를 충분한 길이로 늘려주는 함수 OWF는 각 대화식 영지식 증명에서 사용되는 일방향 함수를 의미한다 $f()$가 충돌회피성, 강또는 약 일방향성 등의 암호학적 성질을 가질 필요는 없지만, 잘 알려져 있는 일방향 해쉬함수를 사용할 수 있다.

- **인증 프로토콜**

a. 사용자가 자신의 아이디와 시험수 $A = OWF(r)$을 서버에게 보낸다 r은 랜덤수.
b. 서버가 질문 c를 임의로 선택해서 사용자에게 보낸다.
c. 사용자는 c, r 그리고 S를 이용해서 목격자수 B를 계산하고 이를 서버에게 보낸다.
d. 서버는 사용자가 보낸 B를 A, V, c를 이용해서 검증한다.

원래의 대화형 영지식 증명 프로토콜이 soundness, completeness, simulatability를 만족한다면, 약한키 S를 사용하는 위의 프로토콜도 안전한 것처럼 보인다. 하지만 영지식에 기반한 인증 프로토콜은 S가 충분히 길고, 랜덤할 것을 가정하고 있으므로 위의 프로토콜은 오프라인 사전공격에 약하다. 즉, 공격자는 시험수 A 질문수 c 그리고 목격자수 B를 이용해서 쉽게 S에 사전공격을 수행할 수 있다. 좀 더 명확히 말하면, B와 A를 이용하면 c로 마스킹된 공개키값을 얻을 수 있고, 알려진 정보 A, B, c를 이용해서 공개키를 추측하므로써 사전공격을 수행할 수 있게된다. 이는 질문 수 c가 공격자에게 노출되어있기 때문인데, 전통적인 대화형 영지식 증명에서는 공개키에 해당하는 비밀키가 충분히 길고 랜덤하므로 사전공격을 수행할 수 없다.

설명을 위해서 Guillous-Quisquater의 프로토콜이 약한 키를 가지는 경우 어떻게 오프라인 사전공격이 이루어지는지 살펴보자. 우선 Guillous-Quisquater의 프로토콜은 다음과 같이 요약할 수 있다.

a. 사용자 → 서버 : $x \equiv r^e \bmod n, r \in_R Z_n^*$
b. 서버 → 사용자 : c, c는 $1 < c < e$인 랜덤수
c. 사용자 → 서버 : $y \equiv r * f(S)^c \bmod n$
d. 서버 : $x \equiv V^c * y^e \bmod n$를 확인,
   여기서 $V \equiv f(S)^{-e}$

V는 사용자의 공개키, n은 RSA modulus이다. 위의 프로토콜은 트랜스크립트 (x, c, y)를 가지며 이를 이용해서 누구나 다음과 같이 오프라인 사전공격을 수행할 수 있다.

```
Procedure DictionaryAttackGQ()
Input : (x, c, y, e, n)
Return value: Guessed password
BEGIN
For each guessed secret S' in her dictionary do
   if x/y^e ≡ V'^c mod n, 여기서 V' ≡ f(S')^-e mod n
      then return S'
Endfor
return FAIL
END
```

즉, 공개키 또는 패스워드 확인자 V가 서버에 안전하게 보관된다 하더라도 위의 프로토콜은 약한 키를 가지는 경우 안전하지 않다. 지면상, 다른 프로토콜들에 대한 공격방법은 생략하지만, Schnorr의 프로토콜, Feige-Fiat-Shamir의 프로토콜 등에도 위의 공격이 가능하다.

Ⅲ. 비밀 동전 던지기

앞서 언급한 약점은 비밀 동전 던지기(Secret Coin Tossing)라는 개념을 이용해서 극복할 수 있다. II장의 추측공격이 가능한 주요한 이유는 마스킹된 공개키 또는 마스킹된 패스워드 확인자가(비록 마스킹된 채로 노출되기는 하지만) 노출된다는 것이다. 따라서 만약 이것을 노출시키지 않는다면 오프라인 사전공격을 막을 수 있다.

일반적인 대화식 영지식 증명 프로토콜에 기반한 인증 프로토콜이 공개된 동전 던지기를 하는 것은 앞서 살펴본 바와같이 증명하고자 하는 비밀수의 랜덤성과 충분한 길이에 안전성을 두고 있다. 약한 키를 가지는 대화형 영지식 증명 프로토콜의 설계를 위해서 비밀 동전 던지기라는 개념을 제시한다. 비밀 동전 던지기는 대화하는 두 주체만 동전 던지기의 결과를 알 수 있고, 그 이외에는 결과를 알 수 없는 시행이다. 따라서, II의 프로토콜에서 공개된 동전 던지기를 하는 대신 비밀 동전 던지기를 수행하므로써, 마스킹된 패스워드 확인자나 마스킹된 공개키가 노출되는 것을 막을 수 있다. 이렇게, 전통적인 대화식 영지식 증명의 공개된 동전 던지기 부분을 비밀 동전 던지기로 대체하므로써 약한 키에 대한 영지식 증명을 원래의 프로토콜이 가지는 좋은 성질(completeness, soundness, simulatability)

을 잃지 않고 수행할 수 있게 된다.

이 프로토콜이 끝난 후, 서버는 사용자가 비밀수를 알고 있음을 높은 확률로 확신할 수 있다. 하지만, 이는 사용자가 서버의 공개키 또는 패스워드 확인자에 대한 지식을 확인 할 수 없다는 점에서 일방향성을 띤다. 전통적인 대화식 영지식 증명에서는 공개키가 엔트로피가 높은 비밀키와 대응되므로 이런 일방향성이 안전성 취약점이 되지 않지만, 약한키를 가지는 대화식 영지식 증명의 경우 안전성에 위협이 된다. 따라서 서버의 공개키 또는 패스워드 확인자에 대한 지식을 사용자가 먼저 확인하고 나서 앞서 기술한 비밀 동전 던지기를 이용한 영지식 증명을 수행하여야 한다.

비밀 동전 던지기 그리고 사용자의 공개키 또는 패스워드 확인자에 대한 서버의 지식 확인을 위해서 EKE의 변형된 형태를 사용한다. EKE는 원래 패스워드에 기초한 인증 프로토콜을 위해 설계되었고, [2]에서 그 안전성의 일부분이 처음으로 증명되었다. 이 논문에서는 EKE의 일반적인 사용목적인 비밀키 또는 패스워드를 증명하는데 사용하지 않고, 비밀 동전 던지기와 공개키 또는 패스워드 확인자를 서버가 알고 있는지를 사용자가 확인하는데 사용한다. 다음의 프로토콜이 이 논문에서 제안하는 인증 프로토콜 프레임웍을 위해 변형된 EKE이다. 여기서 모든 연산은 유한 순환 그룹 $G=\langle g\rangle$에서 행해진다. 이 그룹은 $G=Z_p^*$이 될 수도 있고, 이 그룹의 소수차 서브그룹(prime order subgroup)일 수도 있다. 또한 타원 곡선 그룹이 될 수도 있다. 표기는 multiplicative group 표기를 사용하겠다.

- **변형된 EKE**

a. 사용자가 서버에게 자신의 ID와 $X=V(g^x)(x\in_R G)$를 보낸다. $V(x)(V^{-1}(x))$는 x를 키 V로 대칭키 암호(복호)화 하는 것을 의미한다.

b. 서버는 $y\in_R G$를 선택하고, 다음을 계산해서 $(auth=H(K'\|1), Y)$를 사용자에게 보낸다.

$$K\equiv[V^{-1}(X)]^y,\ Y=V(g^y)$$
$$K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

여기서 K는 임시 세션키를 생성하는데, Y는 키 교환을 위해, 그리고 K'은 K의 유효성을 검증하는데 사용된다.

c. 사용자는 다음을 계산해서 $H(K'\|1)=auth$ 인지 확인한다. 만약 성공한다면, 사용자는 서버가 V를 알고 있음을 확신할 수 있다.

$$K\equiv[V^{-1}(Y)]^x,\ K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

d. 프로토콜이 성공적으로 끝난다면, 사용자와 서버 모두 임시 세션키 $TSK=H(K'\|0)$을 갖게된다.

위의 프로토콜은 [2]의 "AddSCA(EKE2)"를 패스워드 대신 패스워드 확인자 또는 공개키에 대한 인증으로 변형한 것이다. 따라서 위의 프로토콜도 패스워드 확인자에 대한 인증에 대해서 ideal cipher 모델에서 안전하다. 이에 대한 증명을 [2]를 참고하라. 위의 프로토콜의 결과로 사용자는 서버가 패스워드 확인자 또는 공개키를 알고 있음을 확신할 수 있고, 또한 임시 세션키를 이용해서 비밀 동전 던지기를 할 수 있게된다. 이제 이 논문에서 제안하는 프로토콜 프레임웍을 살펴보자.

Ⅳ. 새로운 인증 프로토콜 프레임웍

이 장에서는 비밀 동전 던지기를 이용해서 일반적인 대화식 영지식 증명 프로토콜이 약한 키를 가지는 경우에도 안전하게 사용할 수 있는 프레임웍을 설계한다. 이 프레임웍에서 증명하려는 비밀수를 패스워드로, 공개키를 패스워드 확인자로 치환하면 이 프레임웍을 쉽게 패스워드에 기초한 인증 및 키 교환 프로토콜로 사용할 수도 있다. 이 프레임웍은 ideal cipher 모델에서 오프라인 사전공격에 안전하다.

제안하는 프레임웍은 크게 Ⅲ장의 변형된 EKE와 비밀동전던지기를 하는 대화식 영지식 증명의 두 부분으로 이루어져있다. 여기서 쓰이는 $H()$와 $h()$는 모두 일방향 해쉬함수이며, 특히 $h()$는 해쉬값의 상위 k 비트만을 돌려준다(k는 계산효율과 보안강도의 trade-off의 정도가 된다).

- **시스템 설정:**

사용자의 공개키 또는 패스워드 확인자 $V=OWF(f(S))$는 서버에 비밀리에 보관된다.

- **인증:**

a. 변형된 EKE를 수행한다.

a.1 사용자는 x를 임의로 선택해서 시험수 $A=OWF(r)$와 함께 $ID_{User}, X=V(g^x)$를 서버에 전송한다. 여기서 $x \in_R G$.

a.2 서버는 $y \in_R G$를 이용해서 다음을 계산하고 $(auth=H(K'\|1), Y)$를 사용자에게 전송한다.

$$K \equiv [V^{-1}(X)]^y,\ Y=V(g^y)$$
$$K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

a.3 사용자는 다음을 계산해서 $H(K'\|1)=auth$인지 확인한다. 맞는다면 서버가 V를 알고있다고 확신할 수 있다.

$$K \equiv [V^{-1}(Y)]^x,$$
$$K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

a.4 이 변형된 EKE가 성공적으로 끝나면, 각각은 공유하는 비밀키 $TSK=H(K'\|0)$를 갖는다. 아니라면 프로토콜 수행을 중단한다.

b. 사용자는 목격자수 B를 c, r 그리고 자신이 가지고 있는 비밀수 S를 이용해서 서버에게 보낸다. 여기서 $c=h(TSK\|A)$이고 c의 길이는 안전강도와 계산효율성의 trade-off파라미터가 된다.

c. 서버는 $c=H(TSK\|A)$를 계산하고 사용자의 목격자수를 A, V, c를 이용해서 검증한다. 성공하면 사용자 인증이 완료된다.

d. 프로토콜 종료 후, 교환된 키는 다음과 같다.

$$SK=H(K'\|A\|B\|2)$$

여기서 시험수 A가 영지식 증명 부분이 아닌 변형된 EKE 부분에서 전송됨을 주목해 보면, 사용자가 시험수를 결정할 당시에는 질문수 c를 전혀 예측할 수 없음을 알 수 있다. 이 불예측성은 서버가 랜덤하게 질문수를 선택해서 사용자에게 전송하는 것과 같은 효과를 가진다.

V. 인증프로토콜 프레임웍의 적용

이 장에서는 IV장에서 제안한 인증 프로토콜 프레임웍을 실재로 잘 알려진 대화식 영지식 증명 프로토콜에 어떻게 적용할지를 예를 통해 설명한다. 널리 알려진 Guillous-Quisquater의 프로토콜에 대해 적용해본다. 이 프로토콜 외에 Schnorr, Feige-Fiat-Shamr의 대화식 영지식 증명에 기초한 인증 프로토콜들에도 적용이 가능하다.

- **시스템 설정:**

사용자의 공개키 또는 패스워드 확인자 $V=OWF(f(S))$는 서버에 비밀리에 보관된다.

- **인증:**

a. 사용자는 x를 임의로 선택해서 시험수 $A=r^e \bmod n$와 함께 $ID_{User}, X=V(g^x)$를 서버에 전송한다. 여기서 $x \in_R G, r \in_R Z_n^*$.

b. 서버는 $y \in_R G$를 이용해서 다음을 계산하고 $(auth=H(K'\|1), Y)$를 사용자에게 전송한다.

$$K \equiv [V^{-1}(X)]^y,\ Y=V(g^y)$$
$$K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

c. 사용자는 다음을 계산해서 $H(K'\|1)=auth$인지 확인한다. 맞는다면 서버가 V를 알고있다고 확신할 수 있다

$$K \equiv [V^{-1}(Y)]^x, K'=H(K\|g^x\|g^y\|ID_{User}\|ID_{Server})$$

확인 후 목격자 수 B를 c, r 그리고 자신이 가지고 있는 비밀수 S를 이용해서 다음과 같이 계산한다.

$$B \equiv r * f(S)^c \bmod n,$$
여기서 $c=h(TSK\|A), TSK=H(K'\|0)$

d. 서버 $TSK=H(K'\|0), c=H(TSK\|A)$를 계산하고 사용자의 목격자수를 A, V, c를 이용해서 다음과 같이 검증한다. 성공하면 사용자 인증이 완료된다.

$$A \equiv B^e * V^c \bmod n;$$

e. 프로토콜 종료 후, 교환된 키는 다음과 같다.

$$SK=H(K'\|A\|B\|2)$$

VI. 안전성 증명

이 장에서는 안전성에 대해 살펴본다. 서론에서

언급했던 대로, 약한 키를 가지는 인증 및 키 교환 프로토콜에 대한 안전성 증명은 최근에야 주목받기 시작했고, 아직 안전성 증명을 가지는 효율적인 프로토콜은 많지 않다. 이 논문에서 제안하는 프레임웍은 약한 키를 가지면서 안전성 증명을 가지는 프로토콜의 설계를 이미 잘 알려진 대화식 영지식 증명 프로토콜을 체계적으로 변환하는 것으로 대체해 준다. 따라서 사용할 대화식 영지식 증명의 안전성 증명만 존재한다면, 이 프레임웍에 의해 만들어지는 새로운 프로토콜도 안전성 증명을 가지게 된다.

이 논문에서 제안한 인증 프레임웍으로 만들어진 프로토콜에 대한 오프라인 사전공격의 가능성을 평가하는데는 [2]에서 소개된 adversary 모델을 사용한다. 여기서는 중요한 표기법을 간략하게 소개한다. 자세한 내용은 [2]를 참조하기 바란다. 공격자(adversary) A는 서버 또는 클라이언트 오라클 $\Pi^i_U, U\in\{Client, Server\}$ $i\in N$, $1\le N\le\sqrt{|G|/q}$에 다음과 같은 여섯 가지 타입의 질의를 수행할 수 있다: Send U,I,M), Reveal U,i), Corrupt U,pw), Execute A,i,B,j), Test U,i), Oracle M). 여기서 $q_{se}, q_{re}, q_{co}, q_{ex}, q_{or}$ 은 각각 Send, Reveal, Corrupt, Execute, Oracle 질의의 수를 의미한다. 또한, t 는 공격자의 수행시간을 뜻한다.

[정리 1]

공격자는 ideal cipher 모델에서 앞서 제시한 프레임웍으로 생성된 변형된 GQ 프로토콜에 대해 오프라인 사전공격을 다음의 확률보다 더 높은 확률로 성공할 수 없다.

$$Adv^{ake-fs}_{P,PW,SK}\le\frac{q_{se}}{N}+q_{se}q_{or}\,Adv^{dh}_{G,g}(t',q_{or})+\frac{O(q^2)}{|G|}+\frac{O(1)}{\sqrt{|G|}}$$

여기서

$t'=t+O(q_{se}+q_{or})$, $q=q_{se}+q_{re}+q_{co}+q_{ex}+q_{or}$

[증명]

알고리즘 A*가 변형된 GQ 프로토콜에 대해서 오프라인 사전 공격을 $Adv^{ake-fs}_{P,PW,SK}$보다 큰 확률로 수행할 수 있다고 가정하자. 변형된 GQ 프로토콜을 GQ*이라하고, [2]에서 AddSCA (EKE2)가 안전함이 증명되었다는 사실을 이용한다. 만약 $Adv^{ake-fs}_{P,PW,SK}$보다 큰 확률로 GQ*에 사전공격을 할 수 있는 A*가 존재한다면 AddSCA (EKE2)를 $Adv^{ake-fs}_{P,PW,SK}$보다 높은 확률로 공격할 수 있는 알고리즘 A+가 존재함을 보인다. [2]에서 AddSCA(EKE2)는 $Adv^{ake-fs}_{P,PW,SK}$보다 높은 확률로 공격당할 수 없음을 증명했으므로, 모순을 이끌어 낼 수 있다.

GQ*의 대화(transcript)는 세 개의 플로우(flow)로 이루어져있다.

$$((X, A\equiv r^e \bmod n);(Y, auth);(B\equiv rf(S)^c \bmod n))$$

이 대화를 A*의 입력으로 주면, 가정에 의해 A*는 $Adv^{ake-fs}_{P,PW,SK}$보다 높은 확률로 S를 찾아낼 것이다. $T_{ake}=((X);(Y, auth))$를 그 비밀수가 우리가 찾고 싶어하는 AddSCA(EKE2)의 대화라고 하자. AddSCA (EKE2)는 오프라인 사전공격에 당할 확률이 $Adv^{ake-fs}_{P,PW,SK}$보다 낮다는 가정 때문에 우리는 S나 c를 추측할 수 없게된다.

다음의 대화를 보자. 이는 T_{ake}에 두 랜덤수 (A', B')를 추가해서 만들어진 대화이다.

$$T_{rand}=[(X, A'\equiv r_1^e\in_R Z_n^*);(Y, auth);(B'\in_R Z_n^*)]$$

이제 T_{rand}와 다음의 대화를 비교해보자.

$$T_{GQ*}=((X, A\equiv r^e \bmod n);(Y, auth);(B\equiv rf(S)^c \bmod n))$$

T_{rand}와 T_{GQ*}를 살펴보면 $X, Y, auth$ 는 같은 수이고 r, r_1은 랜덤수이므로 계산적으로 구별 불가능(computationally indistinguishable)하다. 따라서 B'과 B이 계산적으로 구별 불가능함을 보이면 T_{rand}와 T_{GQ*}가 계산적으로 구별 불가능함을 보이게 된다.

여기서, A*에게 c는 "알려지지 않은" 균일 분포를 갖는 랜덤수이므로, 랜덤 변수(random variable $B\equiv rf(S)^c \bmod n$은 Z_n^*에 균일하게 분포한다. 따라서 Z_n^*에서 균일한 분포를 갖는 랜덤 변수 B'과는 계산적으로 구별 불가능하다. 따라서 랜덤 변 T_{rand}는 T_{GQ*}과 계산적으로 구별 불가능하다.

비록 $f(S)$는 그 자체로 약하지만, B의 엔트로피가 c에 의해 증폭된다고 볼 수 있다.

이제 위의 결과에 따라 A+를 다음과 같이 정의하자.

a. A+ 는 다음과 같은 대화를 만든다

$$T_{rand}=[(X, A' \equiv r_1^e \in {}_R Z_n^*);$$
$$(Y, auth);(B' \in {}_R Z_n^*)]$$

b. 대화 T_{rand}를 A*에 입력한다. 가정에 의해서 A* 은 $Adv_{P,PW,SK}^{ake-fs}$보다 높은 확률로 S를 찾아낼 것이고, A+는 이 결과를 출력한다.

T_{eke}로부터 T_{rand}를 만들어내는 과정 a의 실행시간은 O(1)이므로, 알고리즘 A+은 $Adv_{P,PW,SK}^{ake-fs}$보다 높은 확률로 S를 찾아낸다. 이는 AddSCA (EKE2)가 오프라인 사전 공격에 강하다는 증명에 모순이 된다. 따라서 만약 AddSCA(EKE2)가 오프라인 사전 공격에 강하다면, GQ*도 ideal cipher model과 random oracle 가정 하에서 오프라인 사전 공격에 강하다. ■

정리 1은 비슷한 방법으로 Schnorr 프로토콜의 변형, Feige-Fiat-Shamir 프로토콜의 변형 등에도 적용할 수 있다.

[정리 2]

정직하지 못한 서버는 이 프레임웍에서 사용자로부터 공개키에 관한 아무런 정보도 얻지 못한다.

[증명]

a 단계에서 얻은 메시지 $A, X = V(g^x))$만으로는 information theoretically 공개키에 대한 아무 정보도 얻지 못한다. 또한 b 단계에서 정직하지 않은 서버는 정확한 대답을 할 수 없으므로 더 이상의 정보가 서버에게 주어지지 않는다.■

[정리 3]

정직한 서버는 GQ*가 끝난 이후에 사용자가 S를 알고 있다는 사실 이외에는 아무 추가적인 정보를 얻지 못한다.

[증명]

이는 GQ*가 기반하고 있는 대화식 영지식 증명 시스템의 시뮬레이션 성질로부터 쉽게 알 수 있다.

정직한 사용자와의 대화없이 대화 T_{GQ*}와 계산적으로 구별 불가능한 대화 T_o를 만들어 낼 수 있는 오라클이 존재한다. 이 오라클은 공개키와 질문수 c로 접근 가능하므로, 다음과 같이 T_o를 만들어 낸다.

a. 오라클은 랜덤수 $x, y \in {}_R G, r \in {}_R Z_n^*$을 생성한다.

b. 위의 랜덤수들과 공개키를 이용해서 다음과 같이 T_o를 생성한다.

$$T_o = ((V(g^x), r^e V^c \bmod n);(V(g^y), auth);(r))$$

T_o는 T_{GQ*}과 계산적으로 구별 불가능하며, 이는 정직한 사용자와 대화하지 않고 T_{GQ*}와 똑같은 확률분포를 가지는 해화를 생성하는 오라클이 존재함을 의미한다. 따라서 T_{GQ*}는 사용자가 S를 알고 있다는 사실 이외에 아무런 정보도 노출시키지 않는다. ■

마찬가지 방법으로 다른 대화식 영지식 증명에 기초한 프로토콜들에 대해서도 정리 3을 증명할 수 있다.

[정리 4]

정직한 사용자는 이 프레임웍에서 자신의 S에 대한 지식을 증명하는데 항상 성공한다.

[증명]

이 프레임웍이 기초하고 있는 대화식 영지식 증명 프로토콜의 정의에 따라 trivially 증명된다. ■

[정리 5]

정직하지 않은 사용자는 이 프레임웍에 오프라인 사전공격을 수행할 수 없다.

EKE2의 안전성 증명을 참고하라[2]. 만약 [2]의 EKE2에서 패스워드를 변형된 EKE의 공개키로 치환한다면, [2]의 증명을 이 프레임웍에 적용할 수 있다.

Ⅷ. 결 론

대화식 영지식 증명은 충분히 길고 랜덤한 비밀수를 보호하는 인증 프로토콜을 설계하는데 매우 강력한 도구이지만, 약한 키를 보호하는데 응용하는 방

법에 대해서는 많은 연구가 이루어지지 않았다. 따라서 약한 키를 보호하는데 사용하는 프로토콜들은 주로 ad hoc 설계에 의존해 왔다. 이 논문에서는 어떤 영지식 증명을 약한 키를 증명하는데 사용할 수 있는 체계적인 방법을 프레임웍 형태로 제시하였다. 이렇게 하므로써, 약한키를 쓸 수밖에 없는 환경에서도 영지식 증명을 이용해서 인증을 하거나 키 교환을 할 수 있게 되었다. 특히 유용한 분야로 패스워드를 이용한 인증과 키 교환 프로토콜 설계가 있는데, 적당한 대화형 영지식 증명 프로토콜을 쉽게 패스워드에 기초한 인증 및 교환 프로토콜로 변환할 수 있다.

이 논문에서 제시한 프레임웍은 두 번의 대칭키 연산과 한 번의 Diffie-Hellman 키교환 만큼의 연산만이 추가되므로 이론적인 면에서뿐만 아니라 실용적인 면에서도 의미를 갖는다. 만약 우리가 타원곡선 그룹 같은 좋은 finite cyclic 그룹을 선택한다면 추가적인 연산은 그다지 크지 않을 것이다.

이 논문에서 보여진 설계 방법은 "프레임웍"의 형태를 가지므로 여러 가지 대화식 영지식 증명 프로토콜에 기초한 인증 프로토콜에 적용할 수 있다. 앞으로 더 좋은 성질을 가지는 대화식 영지식 증명 프로토콜이 설계된다면 그 프로토콜을 여기서 제시한 프레임웍에 적용해서 새로운 프로토콜을 만들어 낼 수 있다. 이렇게 만들어진 프로토콜은 원래의 대화식 영지식 증명 프로토콜이 가지는 좋은 성질을 모두 가질 뿐만 아니라, 약한 키가 사용되는 경우에도 안전하게 사용될 수 있다. 또한 약한 키로 패스워드가 사용되는 경우 패스워드의 편리함도 누릴 수 있으며, 계산량의 측면에서도 기존의 안전성 증명을 가지는 프로토콜에 비해 매우 우수하다.

마지막으로, 비밀 동전 던지기와 서버의 공개키에 대한 지식을 확인하는데 AddSCA(EKE2)를 사용했다. AddSCA(EKE2)가 매우 효율적이고 편리하지만, 다른 좋은 성질을 가지는 프로토콜이 설계된다면 프레임웍에서 이 새로운 프로토콜로 교체할 수 있다.

참 고 문 헌

[1] R. Anderson and T. Lomas, Fortifying key negotiation schemes with poorly chosen passwords, Electronics Letters, 1994, Vol. 30, No. 13, pp. 1040~1041.

[2] M. Bellare, D. Pointcheval and P. Rogaway, Authenticated key exchange secure against dictionary attacks. Proceedings of EuroCrypt 2000,Lecture Notes in Computer Science, Springer-Verlag, 2000, pp. 139~155.

[3] S. Bellovin and M. Merrit, Encrypted key exchange: password based protocols secure against dictionary attacks, IEEE Comp. Society Symp. on Research in Security and Privacy, 1992, pp. 72~84.

[4] S. Bellovin and M. Merrit, Augmented encrypted key exchange: a password based protocol secure against dictionary attacks and password file compromise, ACM Conference on Comp. and Comm. Security, 1993, pp. 244~250.

[5] V. Boyko, P. MacKenzie, and S. Patel, Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman, Proceedings of EuroCrypt 2000, Lecture Notes in Computer Science, Springer-Verlag, 2000, pp. 156~171.

[6] D. E. Denning and G. M. Sacco, Timestamps in Key Distribution Protocols, Communications of the ACM, Vol. 24, No. 8, 1981, pp. 533~536.

[7] W. Diffie and M. E. Hellman, New directions in cryptography, IEEE Trans., 1976, Vol. IT-22, No. 6, pp. 650~654.

[8] U. Feige, A. Fiat and A. Shamir, Zero-knowledge proofs of identity, Journal of Cryptology, Vol. 1, No. 2, 1988, pp. 77~94.

[9] L. Gong, M. Lomas., R. Needham, and J. Saltzer, Protecting poorly chosen secrets from guessing attacks, IEEE Journal on Selected Area in Comm., 1993, Vol. 11, No. 5, pp. 648~656.

[10] L.C. Guillou and J.J. Quisquater, Protocol fitted to security microprocessor minimizing both transmission and memory, Proceedings of EuroCrypt 88, Lecture Notes in Computer Science,

Springer-Verlag, 1988, pp. 123~128.
[11] D. Jablon, Strong password-only authenticated key exchange, ACM Comp. Comm. Review, 1996, Vol. 26, No. 5, pp. 5~26.
[12] D. Jablon, Extended Password Key Exchange Protocols Immune to Dictionary Attacks, Proc. of WET-ICE 97, IEEE Computer Society, June, 1997, Cambridge, MA, pp. 248~255.
[13] J. Katz, R. Ostrovsky and M. Yung, Efficient Password-Authenticated Key Exchange Using Human-Memorable Passwords, Proceedings of Eurocrypt 2001, Lecture Notes in Computer Science, Springer-Verlag, 2001, pp. 475~494.
[14] K. McCurley, A key distribution system equivalent to factoring, Journal of Cryptology, 1988, Vol. 1, pp. 95~105.
[15] Password-Authenticated Key Exchange Based on RSA, Proceedings of Asiacrypt 2000, Lecture Notes in Computer Science, Springer-Verlag, 2000, pp. 599~613.
[16] S. Patel, Number Theoretic Attacks on Secure Password Schemes, IEEE Symposium on Security and Privacy, 1997.
[17] S. Pohlig and M. Hellman, An improved Algorithm for Computing Logarithms over GFp and its cryptographic significance, IEEE Trans., 1978, Vol. IT-24, No. 1, pp. 106~110.
[18] J. Pollard, Monte Carlo methods for index computation mod p, Mathematics of Computation, volume 32, 1978, pp 918~924.
[19] C.P. Schnorr, Efficient Identification and Signatures for Smart cards, Advances in Cryptology : Proceedings of Crypto 89, Lecture Notes in Computer Science, Springer-Verlag, New York, 1989, pp. 239~251.
[20] P. Van Oorschot and M. Wiener, On Diffie-Hellman key agreement with short exponents, Eurocrypt, 1996, pp. 332~343.
[21] T. Wu, Secure Remote Password Protocol, Internet Society Symp. Network and Distributed System Security, 1998, pp. 97~111.

〈著者紹介〉

양 대 헌 (Dae-Hun Nyang)
1994년 2월 : 한국과학기술원 과학기술대학 전기 및 전자 공학과 졸업
1996년 2월 : 연세대학교 컴퓨터 과학과 석사
2000년 8월 : 연세대학교 컴퓨터 과학과 박사
2000년 9월~현재 : 한국전자통신연구원 정보보호연구본부 재직
〈관심분야〉 암호이론, 암호프로토콜, 인증, 무선 인터넷 보안