Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.26, NO.6, Dec. 2016 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2016.26.6.1387

효율적인 ID 기반 인증 및 키 교환 프로토콜*

엄 지 은,[1†] 서 민 혜,[1] 박 종 환,[2] 이 동 훈[1‡]
[1]고려대학교, [2]상명대학교

Efficient ID-Based Authentication and Key Exchange Protocol*

Jieun Eom,[1†] Minhye Seo,[1] Jong Hwan Park,[2] Dong Hoon Lee[1‡]
[1]Graduate School of Information Security, Korea University,
[2]Department of Computer Science, Sangmyung University

요 약

사물인터넷 기술을 기반으로 한 초연결 사회에서는 다양한 성능의 기기들로부터 데이터가 수집되고, 이를 가공하여 사용자에게 새로운 서비스를 제공한다. 이 경우, 사용자의 프라이버시를 보호하고 악의적인 공격자로부터 안전한 서비스를 제공하기 위하여 기기 간 상호 인증이 필수적으로 수행되어야 한다. ID 기반 서명을 이용하면 기기 고유의 ID를 이용하여 기기 간 인증 및 키 교환을 수행할 수 있다. 그러나 기존 RSA 구조의 ID 기반 서명 기법을 이용하면 인증 단계 이후에 키 교환을 위한 추가적인 파라미터 공유가 필요하기 때문에 효율성 측면에서 IoT 환경의 저성능 기기에 적용하기에 어려움이 있었다. 본 논문에서는 효율적인 ID 기반 서명을 설계하고, 이를 이용하여 인증 및 키 교환이 동시에 수행되는 효율적인 ID 기반 인증 및 키 교환 프로토콜을 제안한다. 그리고 제안하는 기법의 안전성을 RSA 일방향성에 기반하여 증명하고, 기존 기법들과의 비교를 통해 효율성을 분석한다.

ABSTRACT

In a hyper-connected society realized through IoT-enabled technology, a large amount of data is collected by various devices and is processed to provide new services to users. While communicating through a network, it is essential for devices to execute mutual authentication since users' privacy can be infringed by malicious attackers. ID-based signature enables authentication and key exchange with a unique ID of a device. However, most of the previous ID-based signature schemes based on RSA require an additional step to share parameters for key exchange so that they are not suitable for resource-constrained devices in terms of efficiency. In this paper, we design an efficient ID-based signature and thereby propose an efficient ID-based authentication and key exchange protocol in which sessions for both an authentication and a key exchange are executed simultaneously. In addition, we prove the security of our scheme under the RSA onewayness problem and analyze the efficiency by comparing with the previous schemes.

Keywords: ID-based Signature, RSA Onewayness, Authentication and Key exchange protocol, Identification, IoT

I. 서 론

ICT 산업의 발전과 스마트 기기의 확산으로 인해 기기 간 융합 및 연결이 가능해지면서 생활 속 모든 것들을 상호 연결시키려는 사물인터넷(Internet of Things, IoT) 기술에 대한 관심이 고조되고 있다. 스마트폰, 태블릿 PC, 스마트 TV 뿐만 아니라 자동차, 가전, 조명 등 다양한 기기가 네트워크에 연결되

Received(08. 24. 2016), Modified(09. 30. 2016), Accepted(10. 21. 2016)
* 이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.R0126-16-1090, 계층적 식별자를 가진 인터넷 개체의 공개키 인증 구조 연구)
† 주저자, jieunn.eom@gmail.com
‡ 교신저자, donghlee@korea.ac.kr(Corresponding author)

면서 모든 것이 연결되는 초연결 사회(hyper-connected society)가 실현되고 있으며, 이러한 변화의 중심에서 사물인터넷 기술은 빠른 속도로 발전하고 있다.

사물인터넷 기술을 이용하면 센서와 같은 저성능 기기부터 스마트폰과 같은 고성능 기기까지 다양한 종류의 기기들로부터 수집된 데이터를 가공하여 사용자에게 새로운 서비스를 제공할 수 있다. 이때, 악의적인 공격자가 변조된 데이터를 제공하여 사용자에게 경제적 손실을 야기하거나 물리적 피해를 입힐 수 있으며, 비인가된 접근을 통해 정보를 탈취하여 사용자의 프라이버시를 침해할 수도 있다. 따라서 안전한 사물인터넷 서비스 제공을 위해서는 기기 간 상호 인증이 필수적으로 수행되어야 한다.

기본적으로 기기 간 인증을 위해서 사전에 공유된 비밀키를 이용하는 방법이 있다. 비밀키 방식의 인증은 저성능 기기에서 수행하기에 효율적이나, 인증을 수행하는 각 개체마다 서로 다른 비밀키를 공유해야 하는 단점이 있다. 특히, 사물인터넷 환경에서는 기기의 수가 매우 많기 때문에 각 기기는 많은 수의 비밀키를 저장하고 관리해야 한다. 이러한 문제를 해결하기 위해 공개키 방식을 이용할 수 있다. 공개키 방식을 이용하면 각 기기는 공개 파라미터와 자신의 개인키만 저장 및 관리하면 되지만, 공개키 검증을 위해 인증서를 사용해야 한다는 단점이 있다. 센서와 같은 저성능 기기에서는 인증서를 관리하는 것이 매우 어렵다. 또한, 사물인터넷 기술을 통해 연결되는 기기들의 수는 시간이 지날수록 기하급수적으로 증가할 것이기 때문에 인증기관이 모든 기기들에 인증서를 발급하고 이를 지속적으로 관리하는 것은 막대한 비용을 유발한다. 이러한 문제는 ID 기반 서명을 이용한 인증 방법을 통해 해결할 수 있다. ID 기반 서명을 이용하는 경우 각 기기는 자신의 고유 식별 번호를 ID로 하여 이에 대응하는 서명키를 발급받기 때문에 인증서를 필요로 하지 않는다.

ID 기반 서명을 이용한 인증 방법에서는 질의-응답(challenge-response)과 서명 검증을 통해 상호 인증을 수행하고, 디피-헬만(Diffie-Hellman) 파라미터를 공유하여 키 교환을 수행한다[1]. 따라서 효율적인 ID 기반 서명을 설계함으로써 효율적인 ID 기반 인증 및 키 교환 프로토콜을 설계할 수 있다. 기존 RSA 구조의 ID 기반 서명을 이용하면 키 교환을 위한 추가적인 디피-헬만 파라미터 공유가 필요하기 때문에 인증과 키 교환 단계가 독립적으로 이

Fig. 1. Internet of Things

루어진다. 따라서 이를 동시에 수행되도록 하여 효율성을 높일 수 있다.

본 논문에서는 ID 기반 서명을 이용하여 인증과 동시에 키 교환을 수행하는 새로운 인증 및 키 교환 프로토콜을 제안한다. 이를 위해, 먼저 RSA 구조의 새로운 ID 기반 서명 기법을 설계하고 그 안전성을 증명한다. 이후 설계한 ID 기반 서명 기법을 이용하여 ID 기반 인증 및 키 교환 프로토콜을 설계한다.

1.1 관련연구

1984년 Shamir는 PKI(Public Key Infrastructure) 시스템을 대체할 수 있는 기술로 ID 기반 암호 시스템에 대한 개념을 소개하고, ID 기반 서명 기법을 제안하였다[2]. 1986년과 1989년에 Fiat 등과 Guillou 등은 각각 인수분해 문제에 기반하여 ID 기반 서명 기법을 설계하였으나 안전성에 대한 분석은 2003년 Dodis 등에 의해 이루어졌다[3, 4, 5]. Dodis 등은 안전한 공개키 기반 서명 기법으로부터 안전한 ID 기반 서명 기법을 설계할 수 있는 변형 방법을 정의하고, 이를 바탕으로 Fiat 등과 Guillous 등이 제안한 ID 기반 서명 기법의 안전성을 증명하였다. 2004년 Bellare 등은 공개키 기반 신원 확인 기법과 ID 기반 신원 확인 기법, 그리고 ID 기반 서명 기법 간의 변형 방법을 정의하고, 이를 바탕으로 Shamir가 제안했던 ID 기반 서명 기법의 안전성을 처음으로 증명하였다[6]. Shamir의 기법 뿐만 아니라, 해당 변형 방법을 통해 이전에 제안된 대부분의 ID 기반 서명 기법의 안전성이 증명되었고, Bellare 등은 해당 논문에서 효

율성을 향상시킨 새로운 ID 기반 서명 기법을 제안하였다. 2009년 Galindo 등과 2015년 Hwang 등은 Schnorr 서명을 이용하여 효율적인 ID 기반 서명 기법을 설계하였다[7, 8]. 한편, 2000년에 Boneh와 Franklin이 겹선형 함수(bilinear map)를 이용하여 ID 기반 암호 시스템을 설계한 이후[9], Sakai 등과 Cha와 Cheon의 연구를 포함하여 많은 ID 기반 서명 기법들이 겹선형 함수를 이용하여 설계되었다[10, 11]. 이후에는 모듬(aggregate) 검증, ID 폐기(revocation), 사인크립션(signcryption) 등 ID 기반 서명 기법에 새로운 기능을 추가하는 연구가 진행되었으나, 기본적인 ID 기반 서명 기법의 효율성을 높이는 연구는 이루어지지 않았다[12, 13, 14, 15, 16].

이와 함께 ID 기반 인증 및 키 교환 프로토콜은 대부분 겹선형 함수를 기반으로 설계되었다[17, 18, 19, 20]. 겹선형 함수는 추가적인 연산을 지원하기 때문에 기법이 새로운 기능을 제공하도록 확장하는 데에 매우 유용하게 활용될 수 있으나, 연산이 비효율적이라는 단점이 있다. 겹선형 함수를 사용하지 않고, 효율적인 ID 기반 서명 기법을 이용하는 경우에는 키 교환을 위한 디피-헬만 파라미터 공유가 필요하다. Schnorr 구조의 ID 기반 서명 기법을 이용하면, 디피-헬만 파라미터를 추가적으로 공유할 필요가 없지만, RSA 구조의 ID 기반 서명 기법의 경우 추가적인 파라미터 공유가 필요하며, 이에 대한 효율성을 높이기 위한 연구는 진행되지 않았다.

본 논문의 구성은 다음과 같다. 제2장에서는 ID 기반 서명 기법 설계 및 안전성 증명에 필요한 배경지식을 설명하고, 제3장에서는 ID 기반 서명 기법의 알고리즘 및 안전성 모델을 정의한다. 제4장에서는 새로운 ID 기반 서명 기법을 제안하고, 제안한 기법에 대한 안전성을 증명한다. 제5장에서는 제안한 ID 기반 서명 기법을 이용하여 ID 기반 인증 및 키 교환 프로토콜을 설계하고, 그 효율성을 분석한다. 마지막으로 제6장에서 결론을 맺는다.

II. 배경지식

본 장에서는 기법 설계에 필요한 배경지식과 각 기법을 구성하는 알고리즘 및 안전성의 정의를 설명한다.

2.1 RSA 파라미터

RSA 키 생성 알고리즘 $KG_{RSA}(1^{\lambda})$는 보안 상수(security parameter) 1^{λ}을 입력으로 하여 서로 다른 두 소수 p, q를 선택하고, $n = pq$에 대한 $ed \equiv 1 \bmod \phi(n)$을 만족하는 e, d를 계산하여 RSA 파라미터 (n, p, q, e, d)를 출력하는 알고리즘이다. 여기서 $\phi(n) = (p-1)(q-1)$이다.

2.2 RSA 암호학적 가정

RSA 파라미터로부터 설계된 기법의 안전성은 RSA 일방향성(RSA onewayness)을 통해 증명된다. 임의의 공격자에게 $KG_{RSA}(1^{\lambda})$로부터 생성된 (N, e)와 $x^e \equiv y \bmod n$을 만족하는 y가 주어졌을 때, x를 다항 시간 안에 계산할 수 있는 확률이 무시할 만큼 낮을 때(negligible), RSA는 일방향성을 만족한다.

2.3 확장 유클리드 알고리즘

두 정수 $a, b \in Z$에 대해 $ax + by = \gcd(a,b)$를 만족하는 정수 x, y가 존재하며, 확장 유클리드 알고리즘(extended Euclidean algorithm)을 이용하여 구할 수 있다. a와 b가 서로소($\gcd(a,b) = 1$)일 때, $ax + by = 1$을 만족하는 정수 x, y가 존재하며, 여기서 x는 mod b에 대한 a의 역원이다.

III. 시스템 모델 및 안전성 정의

본 장에서는 ID 기반 서명 기법의 알고리즘을 정의하고, 공개키 기반 신원 확인 기법으로부터 ID 기반 서명 기법을 설계하는 변형에 대하여 설명한다. 그리고 ID 기반 서명의 안전성 모델을 정의한다.

3.1 ID 기반 서명

ID 기반 서명 기법(ID-based signature, IBS)은 (Setup, KeyGen, Sign, Verify)의 네 개의 다항 시간(polynomial-time) 알고리즘으로 구성된다.

• **Setup**$(1^{\lambda}) \rightarrow$ (pp, msk): 셋업 알고리즘은 보안 상수 1^{λ}를 입력으로 받아서 공개 파라미터

pp(public parameter)와 마스터 비밀키 msk (master secret-key)를 출력한다.

• **KeyGen**(ID, msk, pp) → sk_{ID}: 키 생성 알고리즘은 마스터 비밀키 msk와 사용자의 ID를 입력으로 받아서 사용자 서명키 sk_{ID}를 출력한다.

• **Sign**(m, sk_{ID}, pp) → σ: 서명 생성 알고리즘은 메시지 m과 사용자 서명키 sk_{ID}를 입력으로 받아서 서명 σ를 출력한다.

• **Verify**(σ, m, ID, pp) → T/F: 검증 알고리즘은 서명 σ, 메시지 m과 ID를 입력으로 받아서 T(True) 또는 F(False)를 출력한다.

정확성(Correctness). 임의의 보안 상수 1^{λ}를 입력으로 하여 Setup으로부터 생성된 (pp, msk), msk와 사용자의 ID를 입력으로 하여 KeyGen으로부터 생성된 sk_{ID}에 대하여, 다음 검증식을 만족할 확률은 1이다.

Verify(Sign(m, sk_{ID}, pp), m, ID, pp) = T

3.1.1 ID 기반 서명의 안전성 모델

IBS 기법의 안전성 모델은 다음과 같이 정의된다.

정의 1. [선택 메시지 공격에 대한 위조 불가능성]. 공격자 A는 챌린저 S와 다음과 같이 가상의 게임(game)을 수행한다.

• **Setup**: S는 보안 상수 1^{λ}를 입력으로 하여 공개 파라미터 pp와 마스터 비밀키 msk를 생성하고, A에게 공개 파라미터 pp를 전송한다.

• **Query**: A는 S에게 다음의 질의를 한다.

1. Corrupt: A는 사용자 ID를 S에게 질의하고, S는 그에 대응하는 서명키 sk_{ID}를 생성하여 A에게 전송한다.
2. Sign: A는 사용자 ID와 메시지 m을 S에게 질의하고, S는 해당 ID와 메시지 m에 대한 서명 σ를 생성하여 A에게 전송한다.

• **Output**: A는 사용자의 ID^*, 메시지 m^*와 서명 σ^*를 생성하여 S에게 전송한다. 이때, ID^*는 Corrupt에서 질의된 적이 없어야 하며, (ID^*, m^*)는 Sign에서 질의된 적이 없어야 한다. 또한 서명 σ^*는 (ID^*, m^*)에 대하여 검증 알고리즘을 통과해야 한다.

공격자 A가 질의된 적 없는 사용자 ID와 메시지 M에 대하여 검증을 통과하는 서명 σ를 출력하면 A가 게임을 이긴 것(win)으로 간주한다. 이때, 게임에서 공격자 A가 얻는 이점(advantage)은 다음과 같이 정의한다.

$$Adv_{IBS,A}^{uf-cma}(1^{\lambda}) = \Pr[A\ wins]$$

정의 2. IBS 기법에 대한 임의의 다항식 시간 공격자 A에 대하여 공격자의 이점 $Adv_{IBS,A}^{uf-cma}(1^{\lambda})$이 무시할 만큼 작은(negligible) 값이라면, IBS 기법은 선택 메시지 공격에 대하여 위조 불가능(unforgeability under chosen-message attacks)하다.

3.2 ID 기반 서명 기법으로의 변형

3.2.1 공개키 기반 신원 확인

공개키 기반 신원 확인 기법(Public-key based Identification, PI)은 증명자 P(Prover)가 비밀정보를 이용하여 검증자 V(Verifier)에게 자신의 신원을 증명하는 프로토콜이며, (PI.KeyGen, PI.Prove, PI.Verify)의 세 개의 다항 시간 알고리즘으로 구성된다.

• **PI.KeyGen**(1^{λ}) → (pk, sk): 키 생성 알고리즘은 보안 상수 1^{λ}를 입력으로 받아서 공개키 pk와 비밀키 sk를 출력한다.

• **PI.Prove/PI.Verify**: 비밀키 sk를 알고 있는 증명자와 공개키 pk를 알고 있는 검증자는 각각 PI.Prove와 PI.Verify 알고리즘을 이용하여 상호(interactive) 프로토콜을 수행하고, 검증자는 공개키 pk와 상호 프로토콜의 트랜스크립트(transcript)를 입력으로 하여 결정적 알고리즘으로부터 0(accept) 또는 1(reject)을 출력한다.

정확성(Correctness). 임의의 보안 상수 1^{λ}를 입력으로 하여 PI.KeyGen으로부터 생성된 (pk, sk)에 대하여, 검증자가 PI.Prove/PI.Verify 상호 프로토콜을 통해 0(accept)을 출력할 확률은 1이다.

3.2.2 캐노니컬한 공개키 기반 신원 확인 기법

캐노니컬한 PI 기법(Canonical PI, cPI)은 다음과 같이 정의된다.

정의 3. [canonical PI] PI 기법이 다음과 같은 증명자 P와 검증자 V 간의 세 단계(move)로 구성되는 경우, 해당 기법이 캐노니컬하다고 한다.

- **1st move** (P → V): 비밀키를 알고 있는 증명자는 커밋먼트(Commitment, Cmt) 공간(CmtSet)에서 임의의 커밋먼트를 선택하여 검증자에게 전송한다. 이때, 생성되는 커밋먼트는 커밋먼트 공간에서 uniform 분포를 따른다.
- **2nd move** (V → P): 공개키를 알고 있는 검증자는 챌린지(Challenge, Ch) 공간(ChSet)에서 임의의 챌린지를 선택하여 증명자에게 전송한다. 이때, 생성되는 챌린지는 챌린지 공간에서 uniform 분포를 따른다.
- **3rd move** (P → V): 증명자는 전송받은 챌린지를 이용하여 응답(Response, Rsp)을 생성하고, 이를 검증자에게 전송한다. 검증자는 공개키와 트랜스크립트 (Cmt, Ch, Rsp)를 입력으로 하여 결정적 알고리즘으로부터 0 또는 1을 출력한다.

3.2.3 공개키 기반 서명

공개키 기반 서명 기법(Public-key based Signature, PS)은 PS = (PS.KeyGen, PS.Sign, PS.Verify)의 세 개의 다항 시간 알고리즘으로 구성된다.

- **PS.KeyGen**(1^λ) → (vk, sk): 키 생성 알고리즘은 보안 상수 1^λ를 입력으로 받아서 검증키 vk와 서명키 sk를 출력한다.
- **PS.Sign**$(m,$ sk$)$ → σ: 서명 생성 알고리즘은 메시지 m과 서명키 sk를 입력으로 받아서 서명 σ를 출력한다.
- **PS.Verify**$(\sigma, m,$ vk$)$ → T/F: 검증 알고리즘은 서명 σ, 메시지 m과 검증키 vk를 입력으로 받아서 T 또는 F를 출력한다.

정확성(Correctness). 임의의 보안 상수 1^λ를 입력으로 하여 PS.KeyGen으로부터 생성된 (vk, sk)와 임의의 메시지 m에 대하여, 다음과 같은 검증식을 만족할 확률은 1이다.

$$\text{PS.Verify}(\text{PS.Sign}(m,\ \text{sk}), m,\ \text{vk}) = \text{T}$$

3.2.4 공개키 기반 신원 확인 기법의 공개키 기반 서명 기법으로의 변형

캐노니컬한 PI 기법은 Fiat-Shamir 변형[3]을 이용하여 PS 기법으로 변형 가능하다. 본 절에서 정의한 변형 방법을 통해 설계된 PS 기법의 안전성은 캐노니컬한 PI 기법의 안전성에 기반하여 증명 가능하다.

정의 4. [cPI-2-PS 변형] 캐노니컬 PI 기법 PI = (PI.KeyGen, PI.Prove, PI.Verify)에 대하여, 다음과 같이 PS 기법 PS = (PS.KeyGen, PS.Sign, PS.Verify)를 설계할 수 있다[6, Construction 4.8].

- **PS.KeyGen**(1^λ) → (vk, sk): PI.KeyGen(1^λ)을 수행하여 공개키 pk'과 비밀키 sk'를 생성하고, PS 기법의 검증키 vk=(pk', H)와 서명키 sk=sk'를 출력한다. 여기서 H: $\{0,1\}^*$→ChSet는 해시함수로 ChSet은 챌린지 공간을 의미한다.
- **PS.Sign**$(m,$ sk$)$ → σ: 알고리즘 PI.Prove와 함수 H를 이용하여 다음과 같이 서명 σ를 출력한다.
  1. PI.Prove(sk)를 수행하여 커밋먼트 Cmt와 상태 정보 St_P를 생성한다.
  2. H(Cmt ‖ m)을 계산하여 챌린지 Ch를 생성한다.
  3. PI.Prove(Ch, St_P)를 수행하여 응답 Rsp와 새로운 상태 정보 St_P를 생성한다.
  4. 서명 σ=(Cmt ‖ Rsp)를 출력한다.
- **PS.Verify**$(\sigma, m,$ vk$)$ → T/F: 알고리즘 PI.Verify와 함수 H를 이용하여 다음과 같이 T 또는 F를 출력한다.
  1. 서명 σ을 이용하여 커밋먼트 Cmt와 응답 Rsp를 생성한다.
  2. H(Cmt ‖ m)을 계산하여 챌린지 Ch를 생성한다.
  3. PI.Verify(vk, Cmt ‖ Ch ‖ Rsp)를 수행하여 0 또는 1을 출력한다. 0이 출력된 경우 T를, 1이 출력된 경우 F를 출력한다.

정리 1. PI 기법이 캐노니컬하고 수동적 위장 공격(impersonation under passive attacks)에 안

전하면, 정의 4에서 정의한 변형을 통해 설계된 PS 기법은 선택 메시지 공격에 대하여 위조 불가능하다[6, Theorem 4.9].

3.2.5 공개키 기반 서명 기법의 ID 기반 서명 기법으로의 변형

PS 기법은 IBS 기법으로 변형 가능하다. 본 절에서 정의한 변형 방법을 통해 설계된 IBS 기법의 안전성은 PS 기법의 안전성에 기반하여 증명 가능하다.

정의 5. [PS-2-IBS 변형] PS 기법 PS=(PS.KeyGen, PS.Sign, PS.Verify)에 대하여, 다음과 같이 IBS 기법 IBS=(Setup, KeyGen, Sign, Verify)를 설계할 수 있다[6, Construction 4.6].

- **Setup**(1^{λ}) → (pp, msk): PS.KeyGen (1^{λ})을 수행하여 검증키 vk'와 서명키 sk'를 생성하고, IBS 기법의 공개 파라미터 pp=(vk', H)와 마스터 비밀키 msk=sk'를 출력한다. 여기서 H: $\{0,1\}^{*}$→Rng(**R**)는 해시함수로 Rng(**R**)=$\{y|(x,y) \in R\}$이고, x는 relation **R**에 대한 y의 역(inverse)을 의미한다.
- **KeyGen**(ID, msk, pp) → sk_{ID}: msk를 이용하여 **R**에 대한 $H(ID)$의 역을 계산하고, 이를 IBS 기법의 서명키 sk_{ID}로 출력한다.
- **Sign**(m, sk_{ID}, pp) → σ: PS.Sign(m, (sk_{ID}, pp))을 수행하여 서명 σ'를 생성하고, 이를 IBS 기법의 서명 $\sigma=\sigma'$으로 출력한다.
- **Verify**(σ, m, ID, pp) → T/F: PS.Verify (σ, m, ($H(ID)$, pp))를 수행하여 IBS 기법의 결과값 T 또는 F로 출력한다.

정리 2. PS 기법이 선택 메시지 공격에 대하여 위조 불가능하면, 정의 5에서 정의된 변형을 통해 설계된 IBS 기법 역시 선택 메시지 공격에 대하여 위조 불가능하다[6, Theorem 4.7].

3.3 ID 기반 서명의 안전성 증명

IBS 기법이 선택 메시지 공격에 대하여 위조 불가능함을 보임으로써 안전성을 증명한다. 본 논문에서는 정의 4와 정의 5에서 정의된 변형을 통해 IBS 기법을 설계하기 때문에, 기반하는 PI 기법의 안전성 증명을 통해 IBS 기법의 안전성을 보인다.

정리 3. PI 기법이 캐노니컬하고 수동적 위장 공격에 안전하면, 3.2절에서 정의한 변형을 통해 설계된 IBS 기법은 정리 1과 정리 2에 의해 선택 메시지 공격에 대하여 위조 불가능하다[6, Corollary 4.10].

3.3.1 공개키 기반 신원 확인 기법의 안전성

PI 기법의 수동적 위장 공격에 대한 안전성은 해당 기법이 정직한 검증자 영지식(statistical honest verifier zero-knowledge)을 만족하고, 비밀값에 대한 지식 증명(proof of knowledge)이 가능함을 보임으로써 증명 가능하다[6, Theorem 5.2].

정리 4. PI 기법이 정직한 검증자 영지식을 만족하고 비밀값에 대한 지식 증명이 가능하면, 해당 기법은 수동적 위장 공격에 안전하다.

정직한 검증자 영지식은 공개된 정보만을 이용하여 올바른 분포를 가지는 트랜스크립트를 생성할 수 있는 시뮬레이터(simulator)를 설계함으로써 보일 수 있다. 그리고 동일한 커밋먼트에 대한 두 개의 정당한 질의-응답 쌍으로부터 비밀값을 추출할 수 있음을 보임으로써 PI 기법의 비밀값에 대한 지식 증명이 가능함을 보일 수 있다.

정의 6. PI 기법의 트랜스크립트 T, 시뮬레이터의 트랜스크립트 T'이 무시할 만큼(negligible) 낮은 확률 ε에 대하여 다음의 식을 만족할 때, PI 기법은 정직한 검증자 영지식을 만족한다.

$$\Pr[\mathrm{dist}(T) = \mathrm{dist}(T')] \leq 1-\varepsilon$$

정의 7. PI 기법의 커밋먼트 Cmt와 이에 대한 두 개의 질의-응답 쌍 (Ch1, Rsp1), (Ch2, Rsp2)이 무시할 만큼(negligible) 낮은 확률 ε에 대하여 다음의 식을 만족할 때, PI 기법은 비밀값 x에 대한 지식 증명이 가능하다.

$$\Pr[\text{Find } x|(\mathrm{Rsp1}, \mathrm{Rsp2}) \leftarrow \mathrm{PI.Prove}(x)] \leq 1-\varepsilon$$

IV. 효율적인 ID 기반 서명

본 장에서는 공개키 기반 신원 확인 기법을 설계하고, 이를 기반으로 효율적인 ID 기반 서명 기법을 제안한다.

4.1 공개키 기반 신원 확인

제안하는 PI 기법은 RSA 파라미터를 기반으로 설계되며, 기법은 다음과 같다.

• **PI.KeyGen**(1^λ): 증명자는 $\mathrm{KG}_{\mathrm{RSA}}(1^\lambda)$ 알고리즘으로부터 RSA 파라미터 (n,p,q,e,d)를 생성한다. p와 q는 소수 p_1과 q_1에 대해 $p=2p_1+1$와 $q=2q_1+1$의 형태로 생성하고, 위수가 p_1q_1인 임의의 $g,k\in Z_n^*$를 선택한다. 그리고 $K\leftarrow k^e \bmod n$을 계산하여 공개키 $\mathrm{pk}=(n,e,g,K)$와 개인키 $\mathrm{sk}=(n,p,q,k)$를 출력한다. pk는 공개하고 sk는 안전하게 저장한다.

• **PI.Prove/PI.Verify**: 증명자와 검증자가 수행하는 각 알고리즘과 상호 프로토콜은 아래와 같이 동작한다.

1. 증명자는 임의의 $r\in Z_n$을 선택하고, $A\leftarrow g^{er} \bmod n$을 계산하여 검증자에게 전달한다.
2. 검증자는 임의의 $c\leftarrow$ ChSet(pk)를 선택하여 증명자에게 전달한다.
3. 증명자는 $c\in$ ChSet(pk)를 확인하고, 성립하지 않을 경우 프로토콜을 종료한다. 성립하는 경우 개인키를 이용하여 $z\leftarrow k^c\cdot g^r \bmod n$을 계산한 뒤 검증자에게 전달한다.
4. 검증자는 $A,z\in Z_n^*$와 $z^e\equiv K^c\cdot A \bmod n$이 성립하는지 확인한다. 만약 성립하면 0(accept)을, 성립하지 않으면 1(reject)을 출력한다.

간략한 흐름도는 [Fig. 2]와 같으며, 여기서 (n)은 모듈러 n$(\bmod n)$ 연산을 의미한다.

4.2 효율적인 ID 기반 서명

효율적인 IBS 기법은 제안한 PI 기법을 기반으로 정의 4와 정의 5에서 정의한 변형 방법에 따라 다음과 같이 설계된다.

• **Setup**(1^λ): $\mathrm{KG}_{\mathrm{RSA}}(1^\lambda)$ 알고리즘으로부터 RSA 파라미터 (n,p,q,e,d)를 생성한다. p와 q는 소수 p_1과 q_1에 대해 $p=2p_1+1$와 $q=2q_1+1$의 형태로 생성하고, 위수가 p_1q_1인 임의의 $g\in Z_n^*$를 선택한다. 공개 파라미터 $\mathrm{pp}=(n,e,g,H,h)$와 마스터 비밀키 $\mathrm{msk}=(n,p,q,d)$를 출력한다. 여기서 $H:\{0,1\}^*\rightarrow Z_n^*$와 $h:Z_n\|\{0,1\}^*\rightarrow Z_{2^{l(\lambda)}}$는 해시함수이다. pp는 공개하고 msk는 안전하게 저장한다.

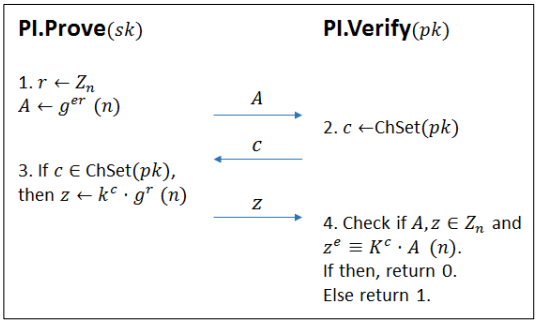

Fig. 2. Public-key based Identification

• **KeyGen**$(ID,\ \mathrm{msk},\ \mathrm{pp})$: 사용자 서명키 $sk_{ID}=H(ID)^d \bmod n$을 출력한다. sk_{ID}는 사용자에게 안전하게 전달한다.

• **Sign**$(m,\ sk_{ID},\ \mathrm{pp})$: 먼저 임의의 $r\in Z_n$을 선택하여 $c\leftarrow h(g^{er} \bmod n\|m)$을 계산한다. 그리고 $z\leftarrow sk_{ID}^c\cdot g^r \bmod n$을 계산하여 m에 대한 서명 $\sigma=(c,z)$를 출력한다.

• **Verify**$(\sigma,m,ID,\ \mathrm{pp})$: $\sigma=(\sigma_1,\sigma_2)$라 하자.

1. $A\leftarrow\sigma_2^e\cdot H(ID)^{-\sigma_1} \bmod n$을 계산한다.
2. 등식 $\sigma_1=h(A\|m)$을 확인하여 성립하면 T를 출력하고, 그렇지 않으면 F를 출력한다.

정확성(Correctness). IBS 기법의 정확성은 다음을 통해 확인할 수 있다.

Setup(1^λ)으로부터 생성된 임의의 pp와 msk에 대해 sk_{ID}가 KeyGen$(ID,\ \mathrm{msk},\ \mathrm{pp})$ 알고리즘을 통해 생성되었다고 가정하자. 임의의 메시지 m에 대한 서명 $\sigma=(\sigma_1,\sigma_2)$가 Sign$(m,\ sk_{ID},\ \mathrm{pp})$ 알고리즘으로부터 생성되었다면, Verify$(\sigma,m,ID,\ \mathrm{pp})$를 통한 검증이 올바르다는 것을 아래와 같이 확인할 수 있다.

$$\begin{aligned} A &\equiv \sigma_2^e \cdot H(ID)^{-c} \\ &\equiv (sk_{ID}^c \cdot g^r)^e \cdot H(ID)^{-c} \\ &\equiv (H(ID)^{dc} \cdot g^r)^e \cdot H(ID)^{-c} \\ &\equiv H(ID)^{edc} \cdot g^{er} \cdot H(ID)^{-c} \\ &\equiv g^{er} \bmod n \end{aligned} \quad (1)$$

마지막 등식은 RSA 파라미터의 성질 $ed \equiv 1 \bmod \phi(n)$에 의해 성립한다.

4.2.1 ID 기반 서명의 안전성

IBS 기법의 안전성은 PI 기법의 안전성을 기반으로 증명된다.

정리 5. KG_{RSA}에 대한 RSA 파라미터가 일방향성을 만족하면, 제안한 IBS 기법은 선택 메시지 공격에 대하여 위조 불가능하다.

증명. 정리 3에 의해 기반이 되는 PI 기법이 캐노니컬하고 수동적 위장 공격에 안전하면, 제안한 IBS 기법은 선택 메시지 공격에 대하여 위조 불가능하다. 보조정리 1에서 기반이 되는 PI 기법이 캐노니컬함을 증명하고, 보조정리 2에서 수동적 위장 공격에 안전함을 보인다. □

보조정리 1. 제안한 PI 기법은 캐노니컬하다.

증명. 개인키 sk를 알고 있는 증명자가 생성한 커밋먼트 $A \equiv g^{er} \bmod n$은 Z_n에서 임의로 선택된 r로부터 계산되며, 여기서 r은 uniform 분포를 따르기 때문에 A 또한 uniform 분포를 따른다(1st move). 공개키 $pk=(n,e,g,K)$ 정보를 아는 검증자로부터 챌린지 c는 uniform 분포를 갖도록 임의로 선택된다(2nd move). 증명자의 응답 z에 대해 검증자의 최종 출력은 pk와 (A,c,z)를 입력으로 하여 검증식 $z^e \equiv K^c \cdot A \bmod n$의 성립 여부에 따라 결정된다(3rd move). 따라서, 제안한 PI 기법은 정의 3에 의해 캐노니컬하다. □

보조정리 2. KG_{RSA}에 대한 RSA 파라미터가 일방향성을 만족하고, 챌린지 사이즈가 $|c| < e$를 만족하면, 제안한 PI 기법은 수동적 위장 공격에 안전하다.

증명. PI 기법의 안전성은 크게 두 단계로 나누어 증명한다. 먼저 실제 PI 기법에서 전송되는 정보들과 동일한 분포를 가지는 트랜스크립트 (A,c,z)를 공개된 정보만을 가지고 생성할 수 있음을 보임으로써 정직한 검증자 영지식을 만족함을 보인다. 공개키 $pk=(n,e,g,K)$에 대해 다음 절차를 수행한다.

1. $c \in Z_{2^{l(\lambda)}}$와 $r \in Z_n$을 uniform 분포를 갖도록 임의로 선택한다. (단, r과 e는 서로소이다.)
2. 확장 유클리드 알고리즘을 이용하여 $xr+ye=1$을 만족하는 $x,y \in Z$를 계산한다.
3. $a \leftarrow g^r \bmod n$을 계산한다.
4. $A \leftarrow K^{-cxr} \cdot a^e \bmod n$을 계산한다.
5. $z \leftarrow K^{cy} \cdot a \bmod n$을 계산한다.

위 계산을 통해 생성된 트랜스크립트 (A,c,z)를 출력한다. 여기서 A와 c는 각각 Z_n^*와 $Z_{2^{l(\lambda)}}$에서 uniform한 분포를 가지며, z는 $z^e \equiv K^c \cdot A \bmod n$을 만족하는 유일한(unique) 값이다. 이는 다음을 통해 확인할 수 있다.

$$\begin{aligned} z^e &\equiv K^{cye} \cdot a^e \bmod n \\ &\equiv K^{c(1-xr)} \cdot a^e \bmod n \\ &\equiv K^c \cdot K^{-cxr} \cdot a^e \bmod n \\ &\equiv K^c \cdot (K^{-cxr} \cdot a^e) \bmod n \\ &\equiv K^c \cdot A \bmod n \end{aligned} \quad (2)$$

따라서, 제안한 PI 기법은 정의 6에 의해 정직한 검증자 영지식을 만족한다.

다음으로 PI 기법이 비밀정보인 k에 대한 지식 증명이 가능함을 보인다. 동일한 커밋먼트 A에 대해 생성된 서로 다른 질의-응답 쌍 (c_1,z_1)과 (c_2,z_2)이 주어지면, 다음 계산을 통해 k를 얻을 수 있다. 여기서 $\gcd(c_1-c_2,e) \neq 1$인 경우 새로운 질의-응답 쌍을 이용한다. 먼저 확장 유클리드 알고리즘을 이용하여 $x(c_1-c_2)+ye=1$을 만족하는 $x,y \in Z$를 계산한다. $z_1/z_2 = k^{c_1-c_2}$이므로 아래 수식을 통해 k를 계산할 수 있다.

$$\begin{aligned} k &\equiv k^{x(c_1-c_2)+ye} \\ &\equiv (z_1/z_2)^x \cdot K^y \bmod n \end{aligned} \quad (3)$$

따라서, 제안한 PI 기법은 정의 7에 의해 비밀정보 k에 대한 지식 증명이 가능하다.

제안한 PI 기법은 정리 4에 의해 수동적 위장 공격에 안전하다. □

V. ID 기반 인증 및 키 교환 프로토콜

본 장에서는 4장에서 제안한 IBS 기법을 기반으로 ID 기반 인증 및 키 교환 프로토콜을 설계하고, 이를 분석한다.

5.1 ID 기반 인증 및 키 교환 프로토콜

ID 기반 인증 및 키 교환 프로토콜에 참여하는 개체는 키 생성기관 KGC(Key Generation Center)와 두 사용자 A와 B이다. 두 사용자는 KGC로부터 서명키를 발급받고 이를 이용하여 인증 및 키 교환을 아래와 같이 수행한다.

• **시스템 셋업 단계:** KGC는 IBS 기법의 Setup 알고리즘을 통해 공개 파라미터 $pp=(n,e,g,H,h,f)$와 마스터 비밀키 $msk=(n,p,q,d)$를 생성한다. 여기서 $f:\{0,1\}^{*}\rightarrow\{0,1\}^{k}$는 추가적으로 사용하는 해시함수를 의미한다.

• **키 발급 단계:** 시스템에 참여하는 모든 개체는 자신의 ID에 대한 서명키 sk_{ID}를 KGC로부터 발급받는다. KGC는 IBS 기법의 KeyGen 알고리즘을 이용하여 sk_{ID}를 생성한다.

서로 다른 두 개체 A와 B의 ID를 각각 ID_A와 ID_B라 하자. A와 B는 KGC로부터 각각 서명키 $sk_A=H(ID_A)^d \bmod n$과 $sk_B=H(ID_B)^d \bmod n$을 안전한 채널을 통해 발급받는다.

• **인증 및 키 교환 단계:** 시스템에 참여하는 두 개체 A와 B는 인증 및 키 교환을 위해 IBS 기법의 Sign/Verify 알고리즘과 질의-응답 프로토콜을 통하여 인증을 수행하고, 키 교환을 위한 요소를 주고받는다.

두 개체 A와 B의 인증 및 키 교환 프로토콜은 다음과 같이 수행된다.

1. A가 먼저 챌린지에 해당하는 난수 $N_A \in \{0,1\}^{*}$를 선택하여 (ID_A, ID_B)와 함께 B에게 전달한다.
2. B는 전송받은 (ID_A, ID_B)를 확인하고 챌린지에 해당하는 난수 $N_B \in \{0,1\}^{*}$를 선택한다. 그리고 $m_B=ID_B\|ID_A\|N_B\|N_A$에 대한 서명 $\sigma_B \leftarrow \mathrm{Sign}(m_B, sk_B, \mathrm{pp})$를 생성하여 m_B와 함께 A에게 전송한다. Sign 알고리즘의 내부 동작 과정은 다음과 같다.

① $r_B \leftarrow Z_n$, $Cmt_B \leftarrow g^{er_B} \bmod n$

② $\sigma_B^1 \leftarrow h(Cmt_B\|m_B)$, $\sigma_B^2 \leftarrow sk_B^{\sigma_B^1} \cdot g^{r_B} \bmod n$

③ $\sigma_B=(\sigma_B^1, \sigma_B^2)$

3. A는 $\mathrm{Verify}(\sigma_B, m_B, ID_B, \mathrm{pp})$ 알고리즘을 통해 전송받은 서명 σ_B를 검증한다. Verify 알고리즘의 내부 동작 과정은 다음과 같다.

① $Cmt_B \leftarrow (\sigma_B^2)^e \cdot H(ID_B)^{-\sigma_B^1} \bmod n$

② $\sigma_B^1 = ?\, h(Cmt_B\|m_B)$에 대해 등식이 성립하면 T를 출력하고, 그렇지 않으면 F를 출력한다.

출력이 F이면 A는 프로토콜을 중단하고, T이면 $m_A=ID_A\|ID_B\|N_A\|N_B$에 대한 서명 $\sigma_A \leftarrow \mathrm{Sign}(m_A, sk_A, \mathrm{pp})$을 생성하여 m_A와 함께 B에게 전송한다. Sign 알고리즘의 내부 동작 과정은 다음과 같다.

① $r_A \leftarrow Z_n$, $Cmt_A \leftarrow g^{er_A} \bmod n$

② $\sigma_A^1 \leftarrow h(Cmt_A\|m_A)$, $\sigma_A^2 \leftarrow sk_A^{\sigma_A^1} \cdot g^{r_A} \bmod n$

③ $\sigma_A=(\sigma_A^1, \sigma_A^2)$

그리고 검증 과정에서 생성한 Cmt_B와 서명 과정에서 생성한 난수 r_A를 이용하여 다음과 같이 세션키(session key) ssk를 계산한다.

① $K_A=(Cmt_B)^{r_A} \bmod n$

② $ssk=f(K_A\|ID_A\|ID_B)$

4. B는 $\mathrm{Verify}(\sigma_A, m_A, ID_A, \mathrm{pp})$ 알고리즘을 통해

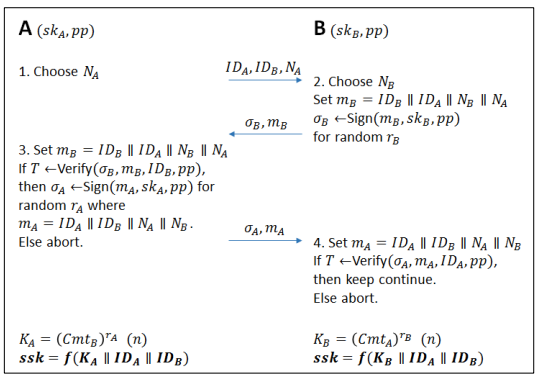

Fig. 3. ID-based authentication and key exchange protocol

Table 1. Comparison of efficiency

Scheme	Sig. size	Sign. costs	Ver. costs	Assumption
[2]	$2Z_n^*$	2exp in Z_n^*	1mexp(2) in Z_n^*	RSA onewayness
[4]	$2Z_n^*$	2exp in Z_n^*	1mexp(2) in Z_n^*	RSA onewayness
[10]	$2G_1$	1exp in G_1+1fexp in G_1	3pair	CDH in G_1
[11]	$2G_1$	2exp in G_1	2pair	CDH in G_1
[6]	$3Z_{p'}+1Z_{q'}$	1exp in $Z_{p'}$	1mexp(2)+1exp in $Z_{p'}$	discrete logarithm
[7]	$2Z_{p'}+1Z_{q'}$	1fexp in $Z_{p'}$	1mexp(2)+1fexp in $Z_{p'}$	discrete logarithm
[8]	$1Z_{p'}+2Z_{q'}$	1fexp in $Z_{p'}$	1mexp(3) in $Z_{p'}$	discrete logarithm
Ours	$1Z_n^*+1h$	1mexp(2)+1fexp in Z_n^*	1mexp(2) in Z_n^*	RSA onewayness

전송받은 서명 σ_A를 검증한다. Verify 알고리즘의 내부 동작 과정은 다음과 같다.

① $Cmt_A \leftarrow (\sigma_A^2)^e \cdot H(ID_A)^{-\sigma_A^1} \bmod n$

② $\sigma_A^1 = ?h(Cmt_A \| m_A)$에 대해 등식이 성립하면 T를 출력하고, 그렇지 않으면 F를 출력한다.

출력이 F이면 A는 프로토콜을 중단하고, T이면 검증과정에서 생성한 Cmt_A와 서명과정에서 생성한 난수 r_B를 이용하여 다음과 같이 세션키 ssk를 계산한다.

① $K_B = (Cmt_A)^{r_B} \bmod n$

② $ssk = f(K_B \| ID_A \| ID_B)$

5.2 분석

제안하는 IBS 기법은 기존 RSA 일방향성을 기반으로 설계된 기법과 비교하여 (i) 서명 크기가 작고, (ii) 고정된 지수 연산(fixed-based exponen-tiation)을 수행하기 때문에 서명 생성이 효율적이며, (iii) 추가적인 디피-헬만 파라미터 정보의 공유 없이 키 교환이 가능하다. 자세한 분석을 위해 [Table 1]에서 기존의 IBS 기법과 제안하는 IBS 기법의 서명 크기와 서명 생성 및 검증 연산에 따른 효율성을 비교한다.

표에서 Z_p와 Z_q는 각각 소수 p와 소수 q를 위수로 하는 군을 의미하고, $q < p$를 만족한다. Z_n은 합성수 n을 위수로 하는 군을 의미하고, G_1은 겹선형 함수를 구성하는 군을 의미한다. exp는 지수 연산(exponentiation)을, fexp는 고정된 원소에 대한 지수 연산을, mul은 곱셈 연산(multiplica-tion)을, 그리고 pair는 페어링 연산(pairing)을 의미한다.

[Table 1]에 따르면 본 논문에서 제안하는 IBS 기법은 기존의 RSA 일방향성에 기반하여 설계된 기법과 비교하여 서명 생성 및 검증 연산량은 동일하지만 서명 크기가 작다. 보안강도 112bit를 기준으로 n은 2048bit, 해시함수 h의 출력 길이는 224bit이기 때문에 기존 기법의 서명 크기는 2048+2048=4096bit이고, 제안하는 기법의 서명 크기는 2048+224=2272bit이다. 따라서 제안한 IBS 기법의 서명 크기가 기존 기법보다 작고, 이를 기반으로 설계한 ID 기반 인증 및 키 교환 프로토콜에서 각 개체의 전송 효율성이 높다.

또한 기존 RSA 일방향성에 기반하여 설계된 IBS 기법을 이용하여 인증 및 키 교환 프로토콜을 수행할 경우, 인증 단계 이후에 키 교환 단계에서 추가적인 디피-헬만 파라미터 공유가 필요하다. 이를 위해 각 개체는 임의의 군 원소를 선택하고 이에 대한 지수 연산을 수행해야 한다. 그러나 제안하는 기법에서는 각 개체가 동일하게 사용할 수 있는 군 원소가 공개 파라미터에 포함되어 추가적인 군 정보에 대한 공유 없이 키 교환이 가능하며, 고정된 군 원소에 대한 지수 연산을 수행하므로 연산 측면에서도 효율적이다.

이산 로그(discrete logarithm) 문제에 기반하여 설계된 기법의 경우 p′은 2048bit이고, q′은 224bit이기 때문에 Bellare 등의 기법, Galindo 등의 기법, 그리고 Hwang 등의 기법은 서명 크기가 각각 3×2048+224=6368bit, 2×2048+224=4320bit, 2048+2×224=2496bit이나 타원 곡선군을 이용하면 훨씬 작은 크기의 서명을 생성할 수 있다.

CDH(Computational Diffie-Hellman) 문제의 안전성에 기반하여 설계된 기법의 경우, G_1의 위

수가 1024bit인 겹선형 함수를 이용했을 때, 서명 크기는 1024+1024 =2048bit로 제안하는 IBS 기법의 서명 크기보다 작다. 그러나 검증 단계에서 비용이 높은 페어링 연산이 2번 또는 3번 이상 수행되며, 표에는 포함되지 않은 맵 투 포인트(map-to-point) 해시 연산(임의의 ID를 겹선형 군 G_1으로 대응시키는 연산)이 추가로 수행되어야 하므로 연산 측면에서 매우 비효율적이다.

VI. 결 론

본 논문에서는 새로운 ID 기반 서명 기법을 기반으로 효율적인 ID 기반 인증 및 키 교환 프로토콜을 설계하였다. RSA 일방향성에 기반하여 안전성을 증명하고, 기존 IBS 기법들과의 효율성을 비교·분석하였다.

제안한 ID 기반 서명 기법은 기존에 RSA 일방향성에 기반하여 설계된 기법과 비교하여 서명 크기가 작기 때문에 이를 이용하여 설계된 ID 기반 인증 및 키 교환 프로토콜은 전송량 측면에서 기존의 프로토콜에 비해 효율적이다. 또한 인증을 위한 세션과 키 교환을 위한 세션이 동시에 수행되기 때문에 연산량 측면에서도 효율적이다.

제안한 ID 기반 인증 및 키 교환 프로토콜은 기존 기법들에 비해 연산량 및 전송량 측면에서 효율적이기 때문에 다양한 종류의 기기로 구성된 사물인터넷 환경에 유용하게 활용될 수 있다.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, Nov. 1976.

[2] A. Shamir, "Identity-based cryptosystems and signature schemes," Advances in Cryptology, CRYPT0'84, LNCS 196, pp. 47-53, 1985.

[3] A. Fiat and A. Shamir, "How to prove yourself: practical solutions to identification and signature problems," Advances in Cryptology, CRYPT0'86, LNCS 263, pp. 186-194, 1987.

[4] L.C. Guillou and J.J. Quisquater, "A 'paradoxical' identity-based signature scheme resulting from zero-knowledge," Advances in Cryptology, CRYPT0'88, LNCS 403, pp. 216-231, 1990.

[5] Y. Dodis, J. Katz, S. Xu, and M. Yung, "Strong key-insulated signature schemes," Proc. of the PKC'03, LNCS 2567, pp. 130 - 144, 2003.

[6] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes," Journal of Cryptology, vol. 22, no.1, pp. 1-61, Jan. 2009.

[7] D. Galindo and F.D. Garcia, "A schnorr-like lightweight identity- based signature scheme," Proc. of the AFRICACRYPT'09, LNCS 5580, pp. 135 - 148, 2009.

[8] J.Y. Hwang, S.H. Kim, D. Choi, S.H. Jin, and B. Song, "Robust authenticated key exchange using passwords and identity-based signatures," Proc. of the SSR'15, LNCS 9497, pp. 43 - 69, 2015.

[9] D. Boneh and M.K. Franklin, "Identity-based encryption from the Weil pairing," Advances in Cryptology, CRYPTO'01, LNCS 2139, pp. 213 - 229, 2001

[10] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing," Proceedings of Symposium on Cryptography and Information Security, Jan. 2000.

[11] J.C. Cha and J.H. Cheon, "An identity-based signature from gap diffie-hellman groups," Proc. of the PKC'03, LNCS 2567, pp. 18 - 30, 2003.

[12] C. Gentry and Z. Ramzan, "Identity-based aggregate signatures," Proc. of the PKC'06, LNCS 3958, pp. 257 - 273, 2006.

[13] Y.M. Tseng, and T.T. Tsai. "Efficient revocable id-based encryption with a public channel," The Computer Journal, vol. 55,

no. 4, pp. 475-486, Apr. 2012.
〔14〕 T.Y. Wu, T.T. Tsai, and Y.M. Tseng, "A revocable id-based signcryption scheme," Journal of Information Hiding and Multimedia Signal Processing, vol. 3, no. 3, pp. 240-251, Jul. 2012.
〔15〕 T.T. Tsai, Y.M. Tseng, and T.Y. Wu, "Provably secure revocable id based signature in the standard model," Security and Communication Networks, vol. 6, no. 10, pp. 1250-1260, Oct. 2013.
〔16〕 J.Y. Hwang, D.H. Choi, H. Cho, and B Song, "New efficient batch verification for an identity based signature scheme," Security and Communication Networks, vol. 8, no. 15, pp. 2524-2535, Oct. 2015.
〔17〕 N.P. Smart, "Identity-based authenticated key agreement protocol based on Weil pairing," Electronics Letters, vol. 38, no. 13, pp. 630-632, Jun. 2002.
〔18〕 K. Shim, "Efficient id-based authenticated key agreement protocol based on weil pairing," Electronics Letters, vol. 39, no. 8, pp. 653-654, Apr. 2003.
〔19〕 K.Y. Choi, J.Y. Hwang, D.H. Lee, and I.S. Seo, "Id-based authenticated key agreement for low-power mobile devices," Proc. of the ACISP'05, LNCS 3574, pp. 494 - 505, 2005.
〔20〕 L. Chen, Z. Cheng, and N.P. Smart, "Identity-based key agreement protocols from pairings," International Journal of Information Security, vol. 6, no. 4, pp. 213-241, Jul. 2007.

〈저자소개〉

엄 지 은 (Jieun Eom) 학생회원
2010년 2월: 고려대학교 수학과 졸업
2012년 2월: 고려대학교 정보보호대학원 석사 졸업
2013년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 암호 프로토콜, 함수 암호, 클라우드 보안

서 민 혜 (Minhye Seo) 학생회원
2012년 2월: 고려대학교 수학과 졸업
2012년 3월~현재: 고려대학교 정보보호대학원 석박사 통합과정
〈관심분야〉 암호 프로토콜, 인증 및 키 교환, 함수 암호

박 종 환 (Jong Hwan Park) 정회원
1999년 2월: 고려대학교 수학과 졸업
2004년 2월: 고려대학교 정보보호대학원 석사 졸업
2008년 8월: 고려대학교 정보보호대학원 박사 졸업
2013년 9월~현재: 상명대학교 컴퓨터과학과 조교수
〈관심분야〉 함수 암호, 브로드캐스트 암호, 암호 프로토콜

이 동 훈 (Dong Hoon Lee) 종신회원
1983년 8월: 고려대학교 경제학과 학사 졸업
1987년 12월: Oklahoma University 전산학과 석사 졸업
1992년 5월: Oklahoma University 전산학과 박사 졸업
1993년 3월~1997년 2월: 고려대학교 전산학과 조교수
1997년 3월~2001년 2월: 고려대학교 전산학과 부교수
2001년 3월~현재: 고려대학교 정보보호대학원 교수
2015년 3월~현재: 고려대학교 정보보호대학원 원장
〈관심분야〉 암호 프로토콜, 암호이론, 함수 암호, SW 보안, 모바일 보안, 자동차 보안, USN이론