*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.25, NO.5, Oct. 2015 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2015.25.5.993

# HB+ 프로토콜 기반의 스마트 OTP 인증*

신 지 선†‡
세종대학교

# HB+ protocol-based Smart OTP Authentication*

Ji Sun Shin†‡
Sejong University

요 약

OTP(One time password)는 금융거래 등 보안이 중요한 작업에 인증 수단의 하나로 널리 사용된다. 일반 비밀번호(password) 기반의 인증과 달리 비밀번호를 한번만 사용한다는 점에서 강력한 보안을 제공하지만, OTP 카드 혹은 생성기를 가지고 있어야한다는 점에서 사용성에 제약이 있다. 이를 극복하기 위하여 스마트폰이 OTP 카드를 대체하여 코드 값을 생성하는 스마트 OTP(smart OTP)가 사용되기 시작하였다. 스마트폰에 NFC 통신 기능을 더하여 근거리통신을 통해 코드 값을 전달할 수도 있다. 이러한 스마트 OTP는 기존 OTP의 단점을 극복하여 OTP의 사용성을 향상시킨다. 하지만, 스마트폰이 지니는 보안 취약점으로 인해 OTP 코드 값 유출 등의 보안 문제가 발생할 수 있다. 따라서, 본 논문에서는 초경량 인증 프로토콜인 HB+ 프로토콜을 이용하여 OTP 코드를 인증하는 방안을 제안한다. 이를 통해 유출 등으로 남용되는 코드를 구별하도록 한다. 본 논문에서는 제안하는 방안의 효율성과 안전성에 대해서 논의하고 스마트 OTP의 안전한 사용에 기여하고자 한다.

ABSTRACT

OTP(One time password) is widely used as an authentication method for financial and other security-sensitive transactions. OTP provides strong security since each password is used only one time while normal password-based authentications use passwords as long term secrets. However, OTP-based authentications relatively lack usability since they require users to hold an OTP card or generator. To overcome such a problem, smartphones start replacing OTP cards and such a method is called smart OTP. However, smart OTP inherits security vulnerabilities that smartphones have.

In this paper, we propose a smart OTP authentication based on an extremely light authentication protocol called HB+. HB+ protocol is developed for low-cost devices and has small communication and computation costs. We present our solution and discuss its security, efficiency and practicality. Our contribution is providing a method to securely use smart OTP without losing its efficiency and usability.

**Keywords:** OTP, Smartphones, Security, Authentication

## I. 서 론

OTP(One Time Password)는 대표적인 인증 방법의 하나로 현재 금융 결제시 다중(multi)인증의 한 방법으로 널리 사용된다. OTP의 원리는 일반 비밀번호(password) 인증 방식과 유사하다: 사용자와 인증서버가 비밀번호를 공유하고, 외부에 노출하지 않도록 비밀을 유지한다. 일반 비밀번호 인증과

접수일(2015년 9월 11일), 수정일(1차: 2015년 9월 11일, 2차: 2015년 9월 23일), 게재확정일(2015년 9월 23일)
* 본 연구는 2015년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임 (NRF- 2013R1A1A3009163).
† 주저자, jsshin@sejong.ac.kr
‡ 교신저자, jsshin@sejong.ac.kr(Corresponding author)

Fig. 1. NFC-based Mobile Payments

OTP 인증방식의 다른 점은 비밀번호가 한번만 사용된다는 점이다. 따라서 OTP 인증방식을 위해서 사용자와 서버는 많은 비밀번호를 공유해야하고, 비밀번호 동기화 구축이 필요하다. 이러한 부담(overhead)에도 불구하고 비밀번호를 한번만 사용하는 강한 보안성 때문에 OTP는 금융 등 높은 보안이 요구되는 작업에 널리 사용되고 있다.

### 1.1 스마트 OTP

금융보안에 OTP가 널리 사용됨에 따라서 OTP의 사용성을 개선하고자하는 노력이 계속되어왔다. 특히, OTP의 사용에 있어 가장 큰 장애는 OTP 카드나 OTP 생성기를 사용자가 가지고 있어야한다는 점(what you have based authentication)이다. 이러한 문제를 개선하기 위하여 제안된 방안이 스마트 OTP이다. 스마트 OTP는 스마트폰이 OTP 카드와 생성기를 대체하여 스마트폰에서 OTP코드를 생성받고, 필요한 경우에 스마트폰에 내장된 NFC(near field communication) 등의 근거리 통신 기능을 통해 코드를 전달하는 방법이다. 스마트 OTP는 두 가지 측면에서 OTP의 활용성을 증진시킨다:

(1) 사용자가 추가로 OTP 카드를 가지고 있지 않아도 된다.

(2) 사용자가 OTP 코드 값을 입력하는 대신 스마트폰이 NFC 통신 등을 통해 코드 값을 전송할 수 있으므로 OTP 코드 값이 길어져도 사용성과 효율성을 크게 떨어뜨리지 않는다.

사용성 측면에서 크게 발전한 스마트 OTP는 Fig. 1와 같이 스마트폰을 이용한 결제의 인증에 활용될 수 있다. 스마트폰 결제 환경을 좀 더 살펴보면, 스마트폰과 결제기(reader)의 통신거리는 10cm 이내로 매우 가깝다(Fig. 2). 접촉을 요구하지 않을 뿐 사용자의 스마트폰과 결제기는 가까이 위치한다.

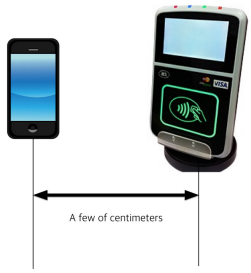


Fig. 2. A few centimeters distance between mobile phones and reader

연구 결과에 따르면 NFC와 같은 수 센티미터 이내의 근거리 통신의 중간자 공격(man-in-the-middle attack)은 수행하기 쉽지 않다[1]. 더불어 위와 같은 결제 상황에서는 사용자 혹은 사용자와 결제담당자와 같이 1인 이상의 사람이 물리적으로 함께 존재하여 이러한 공격을 더 어렵게 할 수 있다.

근거리 통신에 있어서 보다 실현성이 있는 위협은 도청 공격(eavesdropping)이다[1]. 다만, 일반적인 OTP를 사용하는 경우에는 비밀값이 일회성이므로 사용후 코드값이 노출되어도 보안의 문제가 없다. 하지만, OTP 코드 값을 인증하는 우리의 문제에 있어서 근거리 통신 도청 공격은 고려의 대상이 되므로 뒤에서 좀 더 자세히 다루기로 한다.

한편, 스마트 OTP의 활용에 있어서 보안의 위협은 근거리 통신에만 국한되지 않는다. 스마트폰 내의 보안 위협도 고려할 대상이 된다. 스마트 OTP는 OTP를 스마트폰에서 생성/보관하기 때문에 기존의 OTP 방식과 다르게 스마트폰이 갖는 보안 취약점을 그대로 갖게 된다. 예를 들어, 악성코드로 인한 OTP생성 앱에 대한 해킹 등으로 인해 OTP코드가 전달 및 유출될 수 있고, 스마프폰 기기의 시간을 조작하여 시간동기화를 앞당겨 원하는 시간의 OTP코드를 알아낼 수도 있다.

이러한 보안 취약점에도 불구하고 OTP카드 및 생성기를 스마트폰이 대체하는 스마트 OTP는 사용자가 가진 것을 바탕으로 한 인증방식(what you have based authentication)의 단점을 극복하는 매우 유용한 방법이다. 따라서, 스마트 OTP의 안전한 활용을 위하여 보안 취약점을 해결하는 것이 시급하다. 그리고 해결방안은 OTP인증이 지닌 가볍고 효율적인 장점을 유지하여야 한다.

본 논문에서, 우리는 스마트 OTP 인증을 통하여

스마트 OTP의 취약점을 극복하는 방안을 제시한다. 우리의 방안은 OTP가 갖는 효율성을 그대로 유지하면서 공격자가 다른 사용자의 OTP 코드를 유출 및 남용하는 것을 막는다. 이를 통해 안전한 스마트 OTP 사용을 보장하도록 한다.

## II. 배 경

우리의 솔루션은 가벼운 인증 프로토콜인 HB+ 프로토콜을 기반으로 한다. 여기서 간단히 HB+ 프로토콜과 그의 기초가 되는 HB 프로토콜을 소개한다.

### 2.1 HB/HB+ 프로토콜

2005년 Juels와 Weis는 Hopper-Blum 프로토콜(HB 프로토콜)을 확장하여 HB+프로토콜을 설계하였다[2,3]. HB 프로토콜은 긴 자료를 다루거나 복잡한 계산을 하기 어려운 '사람(human)'을 인증하는 방법으로 개발되었는데, 이러한 특징 때문에 사람처럼 저장능력과 계산능력에 한계가 있는 passive RFID-tag 인증에도 적합하다고 판단되었다[3].

HB 및 HB+ 프로토콜의 기본원리는 다음과 같다(Fig. 3):

- 기본 설정: 인증 대상인 태그(tag)와 이를 인증하고자 하는 리더(reader)는 n-bit 비밀키 x를 공유한다.
- 한 라운드의 기본 구성:

1. 태그 인증을 위하여 리더는 랜덤한 n-bit 챌린지(challenge) a를 보낸다.
2. 태그는 a와 x의 내적(inner product)값인 z을 계산하여 보내고, 리더는 이 값이 맞는지 확인한다. z값이 a·x값이 아니면 인증 실패가 된다.

그러나, 기본구성에서 z값은 1bit으로 공격자가 비밀키 x를 몰라도 z값을 맞출 확률이 1/2가 된다. 따라서, 기본 구성 라운드를 k번 반복하여 인증의 보안성을 높인다. 즉, k개의 챌린지 a에 대해서 모두 맞는 값을 답하면 인증성공으로 결정한다. 이렇게 비밀키를 모르는 공격자가 인증성공이 될 확률을 $(1/2)^k$으로 낮출 수 있다.

하지만 k번의 라운드에 걸친 메시지 통신은 k개의 (a, z) 값들을 생성하게 되어 태그와 리더의 대화를 듣고 내용을 수집한 공격자(eavesdropper)는 가우시안 알고리즘(Gaussian Elimination)으로 쉽게 비밀값 x를 얻을 수 있다[3].

#### 2.1.1 HB 프로토콜

HB 프로토콜[2,3]은 이러한 도청 공격으로부터 안전하도록 수정한 프로토콜이다. Fig. 4에서 보듯이 HB 프로토콜에서는 태그와 리더가 추가로 소음 매개변수(noise parameter) η를 공유한다. 또한, 각 기본 구성 라운드에서 태그는 1-η의 확률로 맞는 답을 하고 η의 확률로 틀린 답을 한다. 리더는 k번의 라운드 실행 후에 태그로부터 온 답 중에서 맞는 답의 개수가 k*(1-η)이상이면 인증성공으로 판단한다.

HB 프로토콜의 실행결과로 도청 공격자는 여전히 k개의 (a, z)값들을 얻게 되는데, 여기서 k*η 개의 짝은 틀린 짝으로 구성되어있다. 이렇게 잘못된 값이 섞여있는 자료에서 비밀키 값 x를 알아내는 것은 Learning Parity in the Presence of Noise 혹은 LPN 문제를 푸는 것과 연관성이 있다. 다음에 LPN 문제의 정의를 명시한다.

정의 1. [LPN Problem] A는 q×n 이진값(binary)의 행렬이고, x는 랜덤함 n-bit 벡터이며, η는 0보다 크고 1/2보다 작은 상수 소음 매개변수라고 하자. 그리고 v는 해밍무게(Hamming weight)가 ηq이하인 랜덤한 q-bit 백터이다. 이들 중 A, η, z=(A·x)⊕v 가 주어졌을 때, |(A·x)⊕v|≤ηq인

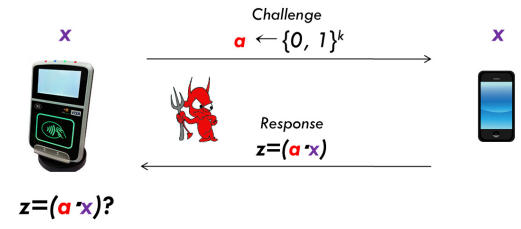


Fig. 3. The basic principle of HB/HB+ protocols

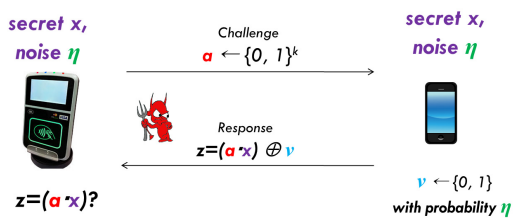


Fig. 4. HB protocol

n-bit 벡터 x′을 찾으시오.

LPN problem은 NP-hard 문제로 알려져있다[4]. Juels와 Weis는 LPN 난제(hardness of LPN problem)를 바탕으로 하여 HB 프로토콜이 도청 공격으로부터 안전함을 증명하였다[3].

그러나 HB 프로토콜은 능동적 공격자(active adversary)에게 안전하지 않다. 가짜 리더로서 프로토콜 실행에 직접 참여하는 공격자는 챌린지인 a값을 같은 값으로 반복하여 태그가 답하는 값을 수집하고, 그 중에서 더 빈도수가 높은 값을 맞는 z값으로 취할 수 있다. 이렇게 여러 챌린지 a에 대해서 맞는 (a, z)값들을 얻음으로써 비밀키 x값을 얻어낼 수 있다[3].

### 2.1.2 HB+ 프로토콜

Juels와 Weis는 HB 프로토콜을 수정하여 직접 프로토콜 실행에 참여하는 능동적 공격자들로부터 안전한 프로토콜인 HB+ 프로토콜을 제안하였다. Fig. 5에서 보듯이 HB+ 프로토콜에서는 태그도 challege 값을 선택하여 보내도록 수정하였다. 이를 통해, 리더를 가장한 공격자가 의도적으로 반복하거나 특정한 값으로 선택한 챌린지 a값이 주는 영향이 태그가 선택한 챌린지 b값에 의해 중화되도록 하였다.

마찬가지로, Juels과 Weis는 LPN 난제를 바탕으로 능동적으로 참여하는 공격자에 대한 HB+프로토콜의 안전성을 증명하였다. Juels와 Weis는 k번의 라운드를 순차적(sequential) 실행하였을 때(즉, 3k번의 통신) 그 안전성을 증명하고, 병렬적(parallel) 실행하였을 때(즉, 3번의 통신)의 안전성을 오픈 문제로 제시하였는데, 후에 Katz와 Shin이 병렬적 실행에서도 안전함을 증명하였다[5]. 따라서, 그림 3에서처럼 여러 라운드의 메시지를 병렬적으로 주고받음으로써 3번만의 통신으로 HB+프로토콜을 실행할 수 있게 되었다(Fig. 6).

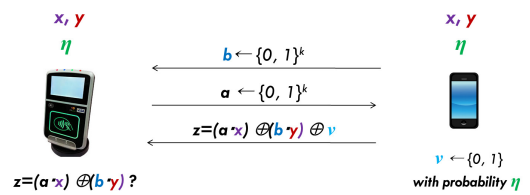


Fig. 5. HB+ protocol

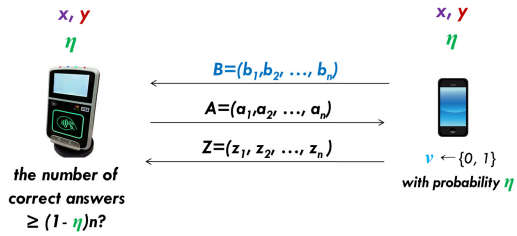


Fig. 6. Parallel composition of HB+

### 2.1.3 중간자 공격(Man-in-the-middle attack)

앞서 설명하였듯이 태그 혹은 리더를 가장하여 프로토콜 실행에 능동적으로 참여하는 공격자에 대한 HB+프로토콜의 안전성은 Juels와 Weis에 의해 증명되었으나, 합법적 태그(honest tag)와 합법적 리더(honest reader) 사이에서 수행하는 중간자 공격(man-in-the-middle attack)에는 HB+프로토콜이 안전하지 않다는 것이 Gilbert 등에 의하여 발표되었다[5].

우리의 솔루션의 적용 환경인 근거리 통신에서는 중간자 공격 어렵기 때문에(2.2절 참조) 본 논문에서는 중간자 공격은 고려대상에서 제외한다.

## 2.2 근거리 통신 보안

NFC와 같은 근거리 통신의 공격은 도청할 수 있는 거리를 연장하는 등의 통신 내용에 직접 영향을 주지 않는 도청(eavesdropping) 목적의 수동적 공격(passive adversary)에 집중된다[1].

그 밖에 통신의 내용에 직접 영향을 주는 능동적인 공격(active attack)으로는 통신을 방해하는 Dos(denial of service) 형태의 공격이 있고, 통신 내용을 변조(modification)하는 공격이나 중간자 공격(man-in-the-middle attack)이 있으나 이러한 공격들은 근거리 통신에서 어렵고, 특히 NFC처럼 수 센티미터 내의 접촉에 가까운 근거리에 통신에서 중간자 공격은 거의 불가능한 것으로 나타났다[1].

따라서, 본 논문에서는 문제의 적용환경인 NFC 통신환경에의 성격에 따라 통신 내용을 수집하여 비밀키를 알아내려는 도청 공격(eavedropping)과 가짜 태그나 가짜 리더의 위장공격(impersonation)에 집중하고, 중간자 공격 및 DoS 공격 등은 고려대상에서 제외하기로 한다.

## III. 공격 모델

### 3.1 통신 능력

통신과 관련되어 고려하는 공격의 모델은 다음과 같다:

- 도청 공격자: 공격자가 직접 프로토콜 메시지를 보내거나, 바꾸거나, 삭제하지 않는 한 도청에 관련된 모든 공격을 포함한다. 즉, 통신 거리를 확대하여 도청 효과를 높이는 공격도 모두 포함한다.
- 능동적 공격자: 합법적인 사용자가 아닌데 사용자 태그를 가장하여 시도하거나 가짜 리더로 가장하여 프로토콜 실행에 능동적으로 참여하는 공격을 포함한다.[1)]

### 3.2 스마트폰 해킹 능력

공격자는 스마트폰 앱 해킹등을 통하여 미래 특정 시점의 OTP 코드 값을 미리 알아낼 수 있다라고 가정한다. 이러한 가정은 공격자의 통신 능력에 무관하게 적용된다고 가정한다.

## IV. HB+ 기반의 OTP 인증

### 4.1 가정 및 기본 설정

- 각 OTP 코드 W의 길이는 짝수인 2k-bit이다.[2)]
- 태그와 리더가 OTP 코드 값을 동기화 하는 방법은 제공된다고 가정한다.
- 각 태그는 OTP 코드 인증을 위한 비밀키(long term secret) K를 갖는다. HB+ 프로토콜 사용 편의상 이 키의 길이는 짝수인 2k-bit으로 설정한다.
- 인증서버는 각 태그의 비밀키와 OTP 코드를 모두 저장하고 있고, 리더의 요청이 있을 때 안전하게 값을 전달해준다.
- 이 절에서는 리더가 비밀키 K를 안전하게 보관한다고 가정한다. 리더의 비밀키 관리에 대한 보안성 강화방안은 뒤에 5.2절에서 논의한다.
- 소음 매개변수 η값은 HB/HB+ 프로토콜에 따라서 0과 1/2 사이의 값으로 한다.[3)]

### 4.2 프로토콜 동작 소개

HB+기반 smart OTP 인증은 HB+프로토콜을 이용하여 간단하게 동작할 수 있다 (Fig. 7). 구체적으로, OTP 코드값 W를 다음과 같이 인증한다:

(1) 태그와 리더는 K⊕W 를 계산하여 앞의 k-bit을 x값으로 뒤에 k-bit을 y값으로 취한다.
(2) HB+ 프로토콜의 두 비밀키로 x와 y을 사용하여 HB+ 프로토콜을 수행한다.
(3) 리더가 프로토콜의 결과로 인증 성공을 얻으면 W값에 인증이 성공한 것으로 판단한다.

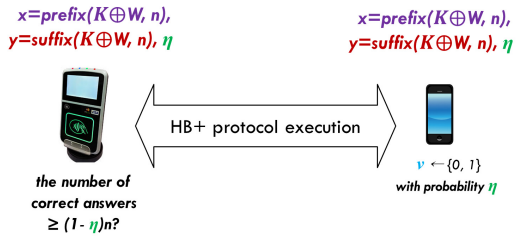


Fig. 7. HB+based OTP Authentication

즉, 제안방식에서는 OTP 코드값을 인증하기 위하여 비밀키와 OTP 코드값을 xor한 값을 기존의 HB+ 프로토콜의 비밀값으로 사용한다. 합법적인 태그와 리더만이 K 값을 알기 때문에, 공격자가 W를 미리 유출한 경우에도 K⊕W값을 계산할 수 없고, 따라서 인증에 성공할 수 없다. 그러므로 리더는 프로토콜 인증결과를 통해서 합법적 태그와 OTP 코드값을 도용한 공격자를 구별함으로써 W값을 인증할 수 있다.

## V. 제안 방식의 보안성과 비밀키 관리 방안

### 5.1 보안성

앞서 간단히 설명하였듯이 본 논문의 제안 방식을

1) 본 논문에서는 신호 전달 방해 등의 도스(denial of service) 타입의 공격은 비밀키를 알아내는데 크게 위협이 되지 않으므로 고려대상에서 제외한다. 또한, 중간자 공격은 앞서 이야기하였듯이 두 개체 중에 적어도 한명이 참가하는 10cm이내의 근거리 통신에서 실현 가능성이 적으므로[1] 고려대상에서 제외한다.

2) 바이트(byte) 코드값이 이진값으로 전환되므로 짝수가 된다.

3) 구체적인 소음 매개변수값, 비밀키값 등은 후속 연구에서 제안 방식의 구현과 실험 분석을 통해 구하고자한다.

적용하면 OTP 남용을 막을 수 있다. 즉, 공격자가 OTP 코드값 W을 미리 알게 되더라도 인증 비밀키 K를 모르기 때문에 OTP 코드 인증에 성공할 수 없기 때문이다.[4] 공격자의 통신 공격 능력에 따른 보안성을 표 1에서 간단히 정리한다.

HB+ 기반의 OTP 인증(HB+based OTP authentication)의 보안 수준은 HB+ 프로토콜의 보안수준을 따른다.[5] 그러므로 결국 제안 방식의 보안 강도는 비밀키의 길이에 의존한다고 볼 수 있다.

앞서 이야기 하였듯이 기존의 OTP와 달리 스마트 OTP에서는 코드값을 스마트폰이 근거리 통신을 이용하여 전달하므로 코드값의 길이를 길게 하여도 사용성이 떨어지지 않는다. 따라서 코드값의 길이를 길게 하고, 이를 통해 코드값과 같은 길이를 갖는 비밀키의 길이를 길게하여 HB+ 기반 OTP 인증(HB+based OTP authentication)의 보안성을 강화할 수 있다.

Table 1. The security of HB+-based OTP authentication

| | |
|---|---|
| Security against passive adversaries | By the security of HB+ protocol, HB+-based OTP authentication is secure against eavesdroppers who collected samples from execution transcripts. |
| Security against active adversaries | By the security of HB+ protocol, HB+-based OTP authentication is secure against active attackers impersonating either tag or reader. |

### 5.2 비밀키 관리

OTP 코드 값을 인증하기 위하여 추가로 요구되는 것이 비밀키(long term secret) K값이다. 비밀키를 사전에 공유하는 것은 NFC 기반뿐만 아니라 신용카드 결제 등 모든 원격(remote) 인증 기반의 결제에서 큰 제약이 되지는 않는다. 결제를 위하여 사용자는 이미 인증정보 등록절차를 거치기 때문이다.

보다 관심을 두어야할 문제는 비밀키 관리방법이다. 우선 태그 즉 스마트폰이 비밀키를 저장하고 사용하는 방법으로는 소프트웨어적인 방법과 하드웨어적인 방법이 있다. 소프트웨어적인 방법은 비밀키 변경등이 용이한 장점이 있으나 스마트폰 보안 취약점에 따라서 비밀키가 유출될 가능성도 있는 단점도 있다. 더 바람직한 방법은 TPM과 같은 하드웨어적 방식인데 이 방법은 비밀키의 안전성이 보장된다는 장점이 있으나 비밀키 값의 변경이 어렵다는 단점이 있다. 하지만 OTP 코드 및 비밀키의 길이를 길게 함으로써 비밀키에 대한 보안성을 강화하여 이를 극복할 수 있다. 그 밖에도 하드웨어의 모듈화 및 블록화(removable block) 발전에 따라서 다양한 방법으로 이를 극복할 수 있다고 기대한다.

리더의 비밀키 관리 방식은 하드웨어적으로 불가능하기 때문에 보안에 대한 관심이 더 요구된다. 리더는 사용자의 비밀키를 인증서버로부터 받아서 사용하므로 리더가 보관하는 비밀키에 대한 보안이 요구된다. 이를 극복하는 방안을 두 가지로 제안한다:

(1) 암호화 자료 계산: 준동형(homomorphic) 암호화 기술 등을 이용하여 암호화된 값을 리더가 계산하도록 하여 리더를 통한 비밀키 유출을 막을 수 있다. 준동형 암호화 기술은 계산 효율이 낮아 일반적으로 많이 적용되지 못하였으나 본 논문에서는 bit단위의 자료에 간단한 연산만을 요구하기 때문에 적용가능성이 높다. 특히 리더는 높은 계산 능력을 가정할 수 있어 암호화 자료 계산을 통한 보안강화는 실현 가능한 방안이 될 수 있다.

(2) 클라우드: 리더는 태그와 서버 사이에서 단순히 메시지를 전달하는 역할만 하고, 서버가 직접 인증 역할을 맡아서 할 수 있다. 따라서, 리더기는 사용자의 비밀키 값이 필요하지 않게 된다. 이렇게 클라우드 서버가 대신 계산을 하는 것은 클라우드 보안기술의 강화에 따라서 사용자(태그)의 역할에도 적용될 수 있겠다.

## VI. 제안 방식의 효율성

최근 발표된 사물인터넷을 위한 경량 알고리즘의 구현결과에 의하면 경량 알고리즘들의 효율성은 128bit AES에 준하거나 그 보다 낮다. 128bit AES 알고리즘 보다 높은 성능의 경량 알고리즘과 그 차이가 크지 않다[7].

4) W값을 알고 K값을 모르는 공격자 A가 HB+ 기반 OTP 인증에 성공할 수 있다면 이 공격자에게 랜덤한 W값을 줌으로써 HB+ 프로토콜 공격에 성공할 수 있다.

5) 제안방식의 보안성과 HB+ 프로토콜 보안성의 귀납적 관계는 비교적 명확하므로 security parameter를 이용한 구체적 증명과 비교는 생략한다.

한편 HB+ 프로토콜은 그들과 비교하였을 때 초경량 알고리즘으로 분류될 수 있다. HB+ 프로토콜이 요구하는 통신량은 n-bit 비밀키로 O(n)라운드를 병렬적 실행할 경우 $O(n^2)$ bit의 양이다. 또한, AES 구현을 위해 요구되는 게이트 수는 대략 5,000정도 인데 반하여 HB+ 프로토콜은 200-2000개의 게이트 수 이하로 구현 가능하다 [2].

## VII. 논의사항(Discussion)

본 논문에서는 HB/HB+의 증명된 안정성(provably security)에 따라서 HB+을 바탕으로 OTP 인증을 제안하였다. 하지만 HB+ 대신 더 가벼운 HB 프로토콜을 OTP 인증에 적용해도 충분한 적용환경(application)이 있다고 본다.

본 논문의 예인 스마트폰을 이용한 NFC 결제에 OTP 인증으로 HB 프로토콜을 적용한다고 가정하자. 여기서, 태그의 역할을 하는 스마트폰이 리더기가 보내는 챌린지 a값이 반복되는지 검증한다면 앞서 설명된 공격인 챌린지 a값을 반복하여 HB 프로토콜의 키를 알아내는 공격은 어렵게 된다.

특히, 병렬적 실행에서는 전체 챌린지 값들이 함께 전송되기 때문에 챌린지 값의 반복여부를 확인하여 프로토콜 진행 여부를 바로 결정할 수 있어 답변을 주는 상황을 미리 막을 수 있다.

## VIII. 결 론

스마트 OTP는 기존 OTP방식의 한계를 극복한 활용가치가 높은 인증 방식이다. 하지만 스마트폰이 갖는 보안 취약점으로 인한 보안 문제를 가지고 있다. 본 논문에서는 초경량 인증 기법인 HB+ 프로토콜을 적용하여 OTP를 인증하는 방안을 제안한다.

제시하는 방안은 적은 오버헤드로 스마트 OTP가 갖는 실용성과 효율성을 그대로 유지하면서 보안성을 강화한다. 이를 통해 본 논문은 스마트 OTP 활용에 공헌하고자 한다.

## References


[1] E. Haselsteiner and K. Breitfuß, "Security in near field communication, strengths and weaknesses," Workshop on RFID Security Security RFIDSec, Jul. 2006.

[2] A. Juels and S.A. Weis, "Authenticating pervasive devices with human protocols," Crypto, LNCS, vol.3621, pp. 293-308, Aug. 2005.

[3] N.J. Hopper and M. Blum, "Secure human identification protocols," Asiacrypt, LNCS, vol.2248, p.52, Dec. 2001.

[4] A. Blum, A. Kalai, and H. Wasserman, "Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model," Journal of the ACM 50, 4, pp.506-519, 2003.

[5] J. Katz and J.S. Shin, "Parallel and concurrent security of the HB and HB+ protocols," Eurocrypt, LNCS, vol. 4004, pp.73-87, May. 2006.

[6] H. Gilbert, M. Robshaw and Y. Seurin, "An active attack against HB+- a probably secure lightweight authentication protocol," Electronics letters, vol. 41, pp.1169-1170, 2005.

[7] H. Seo and H. Kim, "Lightweight cryptographic algorithm implementations for Internet of Things," Review of The Korea Institute of information Security & Cryptology, 25(2), pp.12-17, 2015.


## 〈저자소개〉


**사 진**

신 지 선 (Ji Sun Shin) 정회원
2001년 2월: 서울대학교 컴퓨터공학과 졸업
2009년 5월: 메릴랜드 주립대학(University of Maryland at College Park) 컴퓨터과학과 박사
2009년 9월~2012년 2월: 삼성 SDS 책임연구원
2012년 3월~현재: 세종대학교 조교수
〈관심분야〉 정보보호, 암호학, 컴퓨터 보안