논문 20-45-05-23 The Journal of Korean Institute of Communications and Information Sciences '20-05 Vol.45 No.05
https://doi.org/10.7840/kics.2020.45.5.933

제3자 없이 수행할 수 있는 상호 양자개체인증

강 민 성◆, 최 지 웅*, 김 용 수**, 김 일 영**, 문 성 욱**, 한 상 욱°

Mutual Quantum Entity Authentication without a Third Party

Min-Sung Kang◆, Ji-Woong Choi*, Yong-Su Kim**, Il-Young Kim**,
Sung Moon**, Sang-Wook Han°

요 약

본 논문은 제3자 없이 통신구성원들이 상호간에 인증할 있는 양자개체인증 프로토콜을 제안한다. 기존 인증 프로토콜들은 안전성과 효율성을 이유로 신뢰할 수 있는 제3자(trusted third party)의 제어를 받아서 상호 개체인증을 수행한다. 하지만, 신뢰할 수 있는 제3자를 구현하는 것은 매우 어려운 일이며, 이러한 제3자가 구현되었다 하더라도 프로토콜 수행 중에 악의적인 노드가 되어 통신구성원들의 인증키를 탈취하는 문제가 발생할 위험이 항상 존재한다. 본 논문에서 제안하는 프로토콜은 remote Bell state preparation 기법을 이용함으로 제3자 없이 통신구성원들 간의 상호인증이 가능하기 때문에 제3자에 의한 내부자 공격으로부터 완전히 안전하다. 또한, 제안하는 프로토콜은 선형광학으로 생성하고 측정할 수 있는 두 Bell 상태(states) $|\Phi^{\pm}>_{AB}$만 사용하기 때문에 실제 하드웨어로 쉽게 구현이 가능하다는 장점을 갖는다.

Key Words : Quantum Cryptography, Quantum Entity Authentication, Trusted Third Party, Remote Bell State Remote Preparation, Bel State Measurement

ABSTRACT

We propose a quantum entity authentication protocol that allows communication members to authenticate each other without third parties. Existing authentication protocols perform mutual object authentication under the control of a trusted third party for security and efficiency reasons. However, it is challenging to implement a trusted third party, and even if such a third party is implemented, there is always a risk that the trusted third party becomes a malicious node during the protocol execution and steals authentication keys of communication members. The protocol proposed in this paper is entirely safe from insider attacks by third parties because it allows mutual authentication between communication members without a third party by using remote Bell state preparation scheme. In addition, because the proposed protocol uses only two Bell states $|\Phi^{\pm}>_{AB}$ that can be generated and measured by linear optics, the advantage is that it can be easily implemented in real hardware.

※ 본 연구는 한국연구재단 중견연구자과제(No. 2019R1A2C2006381) 및 KIST 기관 고유 과제(Grant No. 2E29580) 지원으로 수행되었습니다.

◆ First Author : 1. Center for Quantum Information, Korea Institute of Science and Technology (KIST). 2. Artificial intelligence & Big Data Examination Division, Korean Intellectual Property Office, ykhmss@gmail.com, 심사관, 정회원

° Corresponding Author : Center for Quantum Information, Korea Institute of Science and Technology (KIST), swhan@kist.re.kr, 책임 연구원(양자정보연구단장), 정회원

* 1. Center for Quantum Information, Korea Institute of Science and Technology (KIST). 2. Department of Physics, Korea University, jodol007@kist.re.kr, 학생(석박사 통합), 학생회원

** Center for Quantum Information, Korea Institute of Science and Technology (KIST), {yong-su.kim, iykim, s.moon}@kist.re.kr, {선임 연구원, 전문 연구원, 책임 연구원}, 정회원

논문번호 : 021910-247-A-RN, Received October 21, 2019; Revised October 28, 2019; Accepted October 28, 2019

Ⅰ. 서 론

양자 원격전송(quantum teleportation)[1-4], 양자 중계기(quantum repeater)[5-9], 양자 직접통신(quantum direct communication)[10-12], 중재자 양자 서명(arbitrated quantum sig- nature)[13-15]과 같은 다양한 양자정보처리 또는 양자 통신 프로토콜은 얽힘(entanglement) 기반 양자 네트워크에서 구현된다. 이러한 얽힘 기반 양자 네트워크는 일반적으로 신뢰할 수 있는 제3자(trusted third party)에 의해서 구성되며, 얽힘 기반 양자 네트워크에 접속하는 사용자들은 안전한 통신을 위해서 사전 인증(pre-authentication)을 수행한다[16]. 그러나, 현대암호에서 신뢰할 수 있는 제3자를 구현하는 것은 아주 어려우며, 설사 신뢰할 수 있는 제3자를 구현했다고 하더라도 쉽게 악의적인 노드로 변절한다[17,18]. 이러한 문제를 해결하기 위해서는 제3자의 권한을 제한하거나 제3자 없이 수행할 수 있는 개체 인증이 필요하다.

위에서 언급한 제3자를 신뢰할 수 없는 문제점은 현대암호에서 뿐만 아니라 양자개체인증 프로토콜에서도 똑같이 제기되고 있다[19,20]. 2015년에 제안된 양방향 양자개체인증 프로토콜에서는 Green-berger-Horne-Zeilinger(GHZ)-like상태를 이용하여 구성한 양자네트워크 상에서 신뢰할 수 있는 제3자 Charlie의 통제 하에 통신구성원 Alice와 Bob이 unitary operation과 entanglement swapping을 연속적으로 수행하여 상호간에 정당함을 확인한다[21]. 그러나, 이 프로토콜의 신뢰할 수 있는 제3자인 Charlie를 구현하는 것은 아주 어렵다. 특히, G. Gao가 문제점을 제기한 것처럼 Charlie가 신뢰할 수 없는 상황이 된다면 그에 의해서 인증키(authentication key)가 유출되는 보안 허점(security loophole)이 발생할 수 있다[20]. 최근 이러한 내부자 공격의 대응책으로 통신구성원들이 공유하는 얽힘 상태의 상관관계를 검증하는 entanglement correlation checking기법과 난수(random number)를 이용하여 인증키(authentication key)를 난독화(obfuscation)하는 인증키 난독화(authenti- cation key obfuscation) 기법이 제안되었지만, 이는 근본적인 해결책은 아니다[19].

본 논문에서는 remote Bell state prepa- ration[22,23]을 이용하여 제3자 없이도 통신구성원들이 상호 양자개체인증이 가능한 프로토콜을 제안한다. 제안하는 프로토콜에서는 제3자 없이도 정보적으로 대칭성 있게 Bell 상태(state)를 공유할 수 있는 remote Bell state preparation 기법의 특성을 이용하여 Alice와 Bob 상호간에 정당한 사용자임을 검증할 수 있다 [22,23].

본 논문은 다음과 같이 구성되어 있다. 2장에서는 remote Bell state preparation 기법을 소개하고, 3장에서는 제3자가 없는 양방향 양자개체인증 프로토콜을 제안한다. 4장에서는 제안하는 프로토콜의 안전성을 분석한 후 5장에서는 내용을 요약하고 결론을 도출한다.

Ⅱ. Remote Bell State Preparation Scheme

그림 1은 remote Bell state preparation의 개념도이다. 그림 1의 개념도를 간략하게 설명하면 광자 A와 B의 수평 편광상태 $|H>$와 수직 편광상태 $|V>$의 probability amplitudes는 polari- zation beam splitter(PBS)1 에 의해서 나눠진다 (경로: a → c & d / 경로: b → e & f). 그리고 Alice와 Bob은 $|H>$의 probability amplitudes는 유지하며, $|V>$의 probability amplitudes는 교환한다 (경로: d → e' / 경로: e → d'). 각각의 광자들은 PBS2를 통과하게 된다 (경로: c & d' → g / 경로: e' & f → h).

위에서 설명한 remote state preparation 기법을 이용하여 Alice와 Bob이 Bell state $|\Phi^{\pm}>_{AB}=\frac{1}{2}(|HH>\pm|VV>)_{AB}$를 공유하기 위해서 각각 광자

$$A:\ \frac{1}{\sqrt{2}}(|H>_A+|V>_A), \tag{1}$$

$$B:\ \frac{1}{\sqrt{2}}(|H>_B\pm|V>_B) \tag{2}$$

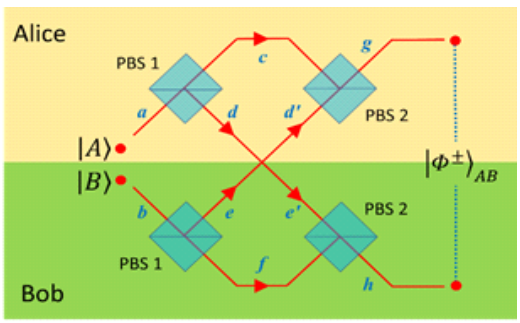


그림 1. Remote Bell state preparation의 광학 도식[22].
Fig. 1. The optical scheme of remote Bell state preparation[22].

를 준비한다. 그림1의 광학장치에 입력된 식 (1)과 (2)의 광자 $|A>=\frac{1}{\sqrt{2}}(|H>_A+|V>_A)$와 $|B>=\frac{1}{\sqrt{2}}(|H>_B\pm|V>_B)$는 (경로: a / 경로: b)

$$\frac{1}{2}(a_H^\dagger+a_V^\dagger)(b_H^\dagger\pm b_V^\dagger)|0>_{AB}. \quad (3)$$

여기서, $a^\dagger$와 $b^\dagger$는 경로 a와 b의 creation operators이다. 그리고 식 (3)을 전개하면 다음과 같다.

$$\frac{1}{2}(a_H^\dagger b_H^\dagger\pm a_H^\dagger b_V^\dagger+a_V^\dagger b_H^\dagger\pm a_V^\dagger b_V^\dagger)|0>_{AB}. \quad (4)$$

이어서 식 (4)의 광자 $a_D^\dagger b_D^\dagger|0>_{AB}$는 PBS1을 지나면 (경로: a → c & d / 경로: b → e & f)

$$\frac{1}{2}(c_H^\dagger f_H^\dagger\mp c_H^\dagger e_V^\dagger-d_V^\dagger f_H^\dagger\pm d_V^\dagger e_V^\dagger)|0>_{AB} \quad (5)$$

이 된다. 여기서, relative phase의 변화 (± → ∓)는 광자가 PBS에서 reflecting경로로 진행하면서 발생된 것이다. 이어서 식 (5)의 광자는 Alice와 Bob에 의해 $d_V^\dagger\rightarrow e'^\dagger_V$와 $e_V^\dagger\rightarrow d'^\dagger_V$의 probability amplitudes는 교환된다 (경로: d → e' / 경로: e → d'):

$$\frac{1}{2}(c_H^\dagger f_H^\dagger\mp c_H^\dagger d'^\dagger_V-e'^\dagger_V f_H^\dagger\pm e'^\dagger_V d'^\dagger_V)|0>_{AB} \quad (6)$$

그리고 이 상태들은 PBS2를 지나면 (경로: c & d' → g / 경로: e' & f → h)

$$\frac{1}{2}(g_H^\dagger h_H^\dagger\pm g_H^\dagger g_V^\dagger+h_V^\dagger h_H^\dagger\pm g_V^\dagger h_V^\dagger)|0>_{AB} \quad (7)$$

로 변화된다. 결과적으로 경로 g와 h를 거친 각각 단일 광자는

$$\frac{1}{\sqrt{2}}(g_H^\dagger h_H^\dagger\pm g_V^\dagger h_V^\dagger)|0>_{AB} \quad (8)$$

이 되며, Alice와 Bob은 Bell state $|\Phi^\pm>_{AB}=\frac{1}{2}(|HH>\pm|VV>)_{AB}$ 를 공유한다. 다만, 경로 g 또는 h 한쪽으로만 각각의 단일 광자가 지나면 remote Bell state preparation은 실패한 것이며, 이 기법의 성공확률은 50%이다.

Ⅲ. Mutual Quantum Entity Authentication Protocol

제안하는 프로토콜은 준비단계, 인증단계, 검증단계로 구성된다. 준비단계에서는 Alice와 Bob은 인증키를 사전에 공유한다. 인증단계에서 Alice와 Bob은 인증키에 대응하는 양자상태를 준비하며, 이것을 remote Bell state preparation 기법에 입력한다. 검증단계에서 그들은 공유한 Bell state를 측정하여 서로의 정당한 사용자임을 검증한다.

3.1 준비단계(preparation step)

P1. Alice와 Bob은 최초 대면을 통해 인증키 $K=(k_1,k_2,k_3,\ ...,k_{2N})$를 공유한다. 여기서, $k_i=\alpha_i\|\beta_i\in\{00,01,10,11\}$, $|K|=4N$이다.

3.2 인증단계(authentication phase)

A1. Alice와 Bob은 사전에 공유한 인증 키 $k_i=\alpha_i\|\beta_i$에 대응하는 초기 양자상태를 생성한다:

$$|A>=\otimes_{i=1}^{2N}\frac{1}{\sqrt{2}}\left(|H>_{A_i}+(-1)^\alpha|V>_{A_i}\right), \quad (9)$$

$$|B>=\otimes_{i=1}^{2N}\frac{1}{\sqrt{2}}\left(|H>_{B_i}+(-1)^\beta|V>_{B_i}\right). \quad (10)$$

예를 들어, 만약 $k_i=10$라면, Alice와 Bob은 각각 $\frac{1}{\sqrt{2}}(|H>_{A_i}-|V>_{A_i})$, $\frac{1}{\sqrt{2}}(|H>_{B_i}+|V>_{B_i})$를 생성한다. 표 1은 인증키에 대응하는 Alice와 Bob이 생성하는 모든 초기 양자상태를 나타낸다.

A2. Alice와 Bob은 각각 식 (9)과 (10)의 초기 양자상태를 그림 1과 같은 remote Bell state preparation을 위한 광학장치에 입력하여

$$|AB>=\otimes_{i=1}^{2N}\frac{1}{2}(g_H^\dagger h_H^\dagger+(-1)^{\alpha_i}(-1)^{\beta_i}g_H^\dagger g_V^\dagger +(-1)^{\alpha_i}g_H^\dagger g_V^\dagger+(-1)^{\beta_i}h_V^\dagger h_H^\dagger)|0>_{A_iB_i} \quad (11)$$

를 획득한다. 결과적으로 경로 g와 h를 동시에 지나는 각각의 단일 광자는

표 1. 인증키 $k_i=\alpha_i\|\beta_i\in\{00,01,10,11\}$에 따라 Alice와 Bob이 생성하는 두 광자 $|A>$와 $|B>$.
Table 1. Two photons $|A>$ and $|B>$ generated by Alice and Bob according to the authentication key $k_i=\alpha_i\|\beta_i\in\{00,01,10,11\}$.

$k_i=\alpha_i\|\beta_i$	$\|A>$	$\|B>$
00	$\frac{1}{\sqrt{2}}(\|H>_{A_i}+\|V>_{A_i})$	$\frac{1}{\sqrt{2}}(\|H>_{B_i}+\|V>_{B_i})$
01	$\frac{1}{\sqrt{2}}(\|H>_{A_i}+\|V>_{A_i})$	$\frac{1}{\sqrt{2}}(\|H>_{B_i}-\|V>_{B_i})$
10	$\frac{1}{\sqrt{2}}(\|H>_{A_i}-\|V>_{A_i})$	$\frac{1}{\sqrt{2}}(\|H>_{B_i}+\|V>_{B_i})$
11	$\frac{1}{\sqrt{2}}(\|H>_{A_i}-\|V>_{A_i})$	$\frac{1}{\sqrt{2}}(\|H>_{B_i}-\|V>_{B_i})$

$$|A'B'>=\otimes_{i=1}^{N}\frac{1}{\sqrt{2}}(g_H^{\dagger}h_H^{\dagger} +(-1)^{\alpha_i}(-1)^{\beta_i}g_H^{\dagger}g_V^{\dagger})|0>_{A_iB_i} \quad (12)$$

이다. 여기서, remote Bell state preparation의 성공확률이 50%이기 때문에 전체 양자상태는 N 개가 되며, Alice와 Bob은 최종적으로 Bell states $\otimes_{i=1}^{N}|\Phi^{\pm}>_{A_iB_i}=\frac{1}{2}(|HH>+(-1)^{\alpha_i}(-1)^{\beta_i}|VV>)_{A_iB_i}$를 공유하게 된다.

3.3 검증단계(Verification phase)

V1. Alice와 Bob은 식 (12)의 Bell states $|A'B'>$를 그림 2와 같은 Bell state measurement를 수행한다. 만약, 이 장치에 Bell state $|\Phi^{+}>_{A_iB_i}$가 입력되면,

$$\frac{1}{\sqrt{2}}(g'^{\dagger}_H h'^{\dagger}_H+g'^{\dagger}_H h'^{\dagger}_V)|0>_{A_iB_i} \quad (13)$$

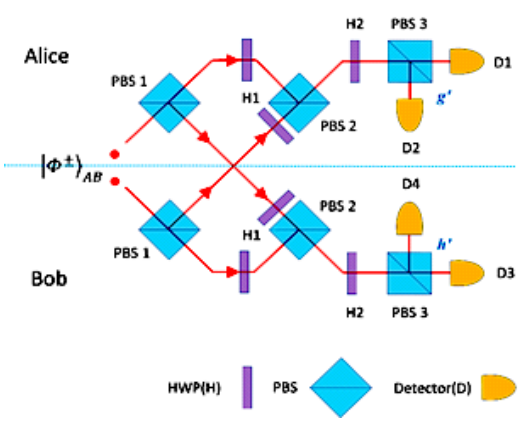


그림 2. 입자들의 간섭이 없는 벨 상태 측정의 광학 도식[22].
Fig. 2. The optical scheme of Bell state measurement without interfering particles[22].

가 출력된다. 반대로 Bell state $|\Phi^{-}>_{A_iB_i}$가 입력되면,

$$\frac{1}{\sqrt{2}}(g'^{\dagger}_H h'^{\dagger}_V+g'^{\dagger}_V h'^{\dagger}_H)|0>_{A_iB_i} \quad (14)$$

가 출력된다[22]. 그러므로 식 (13)의 $|\Phi^{+}>_{A_iB_i}$는 D13 또는 D24에 coincidences가 발생하며, 식 (14)의 $|\Phi^{-}>_{A_iB_i}$는 D14 또는 D23에 coincidences가 발생한다[22].

V2. 인증키 $k_i=\alpha_i\|\beta_i$에서 $\alpha_i\oplus\beta_i=0$ 또는 1이다. 만약 $\alpha_i\oplus\beta_i=0$이면, Alice와 Bob의 Bell measurement결과는 $|\Phi^{+}>_{A_iB_i}$이 되어야 한다. 그리고 $\alpha_i\oplus\beta_i=1$이면, Alice와 Bob의 Bell measurement결과는 $|\Phi^{-}>_{A_iB_i}$이 되어야 한다. 이외의 경우에는 Alice 또는 Bob이 정당한 사용자가 아님을 의미하며, 인증이 실패한 것이다.

Ⅳ. Cryptoanalysis

제안하는 프로토콜에서 제3자가 존재하지 않으며, Alice와 Bob은 자체적으로 Bell state를 공유하고 측정한다. 그러므로 제3자에 의한 내부자 공격에 제안하는 프로토콜은 완전히 자유로우며, 공격자 Eve는 Alice 또는 Bob인 척하는 위장공격(impersonation attack)[21]과 intercept and resend 공격을 시도할 수 있다.

4.1 위장공격

Eve는 인증키 $k_i=\alpha_i\|\beta_i$를 모르기 때문에 α_i 또는 β_i를 추측하여 식 (8)의 초기 양자상태 $\otimes_{i=1}^{2N}\frac{1}{\sqrt{2}}\left(|H>_{A_i}+(-1)^{\alpha_i}|V>_{A_i}\right)$ 또는 식 (9)의 초기 양자상태 $\otimes_{i=1}^{2N}\frac{1}{\sqrt{2}}\left(|H>_{B_i}+(-1)^{\beta_i}|V>_{B_i}\right)$를 생성해야 한다. 예를 들어 Eve가 인증정보 e_i를 준비하고 Bob으로 위장한다면, 초기 양자상태는

$$|E>=\otimes_{i=1}^{2N}\frac{1}{\sqrt{2}}\left(|H>_{E_i}+(-1)^{e_i}|V>_{E_i}\right) \quad (15)$$

이다. 이후에 3장에서 설명한 그림 1의 remote Bell state preparation가 수행되면, Alice와 Eve는

$$|A'E'>=\otimes_{i=1}^{N}\frac{1}{\sqrt{2}}(g_H^{\dagger}h_H^{\dagger} +(-1)^{\alpha_i}(-1)^{e_i}g_H^{\dagger}g_V^{\dagger})|0>_{A_iE_i} \quad (16)$$

를 공유하게 된다. 이어서 Alice와 Eve는 그림 2의 Bell state measurement를 수행하여 측정결과 α_i와 e_i를 얻는다. Alice와 Eve의 $\alpha_i \oplus e_i$가 Alice와 Bob의 $\alpha_i \oplus \beta_i$와 일치한다면, Eve는 정당한 사용자임이 인증된다. 그러나, Eve가 공격에 성공할 확률은 $1/2^N$이며, N이 아주 크다면 사실상 Eve의 위장공격은 불가능하다.

4.2 Intercept and resend 공격

Eve는 Alice와 Bob이 교환하는 광자를 탈취할 수 있고, 탈취한 광자로부터 인증키를 획득하려는 시도를 할 수 있다. 좀 더 구체적으로 설명하면, Eve는 경로 d → e 그리고 경로 e'→ d로 교환되는 식 (6)의 광자를 탈취하여 측정한다. 그리고 Eve는 측정결과를 가지고 Alice와 Bob의 인증키를 추측할 수 있다. 예를 들어, 인증키 $k_i = 01$이면, Alice와 Bob은 광자 $\frac{1}{\sqrt{2}}(|H>_{A_i} - |V>_{A_i})$와 $\frac{1}{\sqrt{2}}(|H>_{B_i} + |V>_{B_i})$를 각각 생성한다. 이어서 경로 c, d, e, f를 통과한 두 광자는

$$\frac{1}{2}(c_H^{\dagger}f_H^{\dagger} + c_H^{\dagger}e_V^{\dagger} - d_V^{\dagger}f_H^{\dagger} - d_V^{\dagger}e_V^{\dagger})|0>_{A_iB_i} \quad (17)$$

이다. 이때, Eve는 식 (9)의 경로 e와 d를 통과하는 광자 $e_V^{\dagger}|0>_{B_i}$와 $d_V^{\dagger}|0>_{B_i}$를 탈취하고 측정한다. 이러한 측정결과를 통해 Eve는 Alice와 Bob의 인증키에 관한 정보를 획득하려고 한다. 그러나 Eve는 단지 측정결과로부터 전송된 광자가 수직(vertical) 편광을 광자가 전송되었다는 사실만 알 수 있으며, 그 외에 아무런 정보를 획득할 수 없다. 왜냐하면, 표 2에서 알 수 있듯이, 인증키에 관한 정보는 광자의 상대적 위상(relative phase)에 의해서 구별되기 때문이다. 게다가, 이러한 Eve의 부정행위로 인해서, 경로 (c, d) 그리고 경로 (e, f)를 통과하는 두 광자의 중첩(superposition)이 사라지게 된다. 그러므로, 경로 g와 h상의 양자상태는 얽힘 상태가 아닌 product 상태가 된다. 결과적으로 Alice와 Bob은 product 상태를 측정한 결과를 통해서 Eve의 침입이 있었다는 사실을 감지할 수 있다.

표 2. 인증키 $k_i \in \{00, 01, 10, 11\}$에 대응하는 경로 c, d, e, f를 지나는 두 광자.
Table 2. Two photons passing the path c, d, e, and f corresponding to the authentication key $k_i \in \{00, 01, 10, 11\}$.

k_i	경로: c, d, e, f
$00: \|\Phi^+>_{A_iB_i}$	$\frac{1}{2}(c_H^{\dagger}f_H^{\dagger} - c_H^{\dagger}e_V^{\dagger} - d_V^{\dagger}f_H^{\dagger} + d_V^{\dagger}e_V^{\dagger})\|0>_{A_iB_i}$
$01: \|\Phi^->_{A_iB_i}$	$\frac{1}{2}(c_H^{\dagger}f_H^{\dagger} + c_H^{\dagger}e_V^{\dagger} - d_V^{\dagger}f_H^{\dagger} - d_V^{\dagger}e_V^{\dagger})\|0>_{A_iB_i}$
$10: \|\Phi^->_{A_iB_i}$	$\frac{1}{2}(c_H^{\dagger}f_H^{\dagger} - c_H^{\dagger}e_V^{\dagger} + d_V^{\dagger}f_H^{\dagger} - d_V^{\dagger}e_V^{\dagger})\|0>_{A_iB_i}$
$11: \|\Phi^+>_{A_iB_i}$	$\frac{1}{2}(c_H^{\dagger}f_H^{\dagger} + c_H^{\dagger}e_V^{\dagger} + d_V^{\dagger}f_H^{\dagger} + d_V^{\dagger}e_V^{\dagger})\|0>_{A_iB_i}$

V. 결 론

본 논문에서는 remote Bell state preparation기법을 이용하여 제3자 없이도 통신구성원인 Alice와 Bob이 서로를 상호 인증할 수 있는 프로토콜을 제안했다. 기존의 인증 프로토콜의 경우 신뢰할 수 있는 제3자의 도움과 제어를 받아서 쉽게 상호인증 할 수 있는 장점이 존재한다. 하지만, 실제로 신뢰할 수 있는 제3자를 구현하는 것은 매우 어려우며, 신뢰할 수 있는 제3자가 구현이 되더라도 쉽게 악의적인 노드로 변절한다. 이로 인해서 제3자를 포함하는 인증 프로토콜은 의한 내부자공격에 취약한 문제점이 있었다. 본 논문에서 제안하는 프로토콜은 remote Bell state preparation and measurement 기법을 이용하기 때문에 인증을 위한 Bell state를 제3자 없이도 Alice와 Bob이 정보적으로 대칭성 있게 준비하고 측정할 수 있으며, 이를 기반으로 Alice와 Bob은 제3자의 도움 없이도 서로의 정당함을 검증할 수 있다. 결과적으로, 제안하는 프로토콜에서 제3자가 없이도 존재하지 않으므로 제3자에 의한 내부자 공격을 원천적으로 차단할 수 있다. 이를 확인하기 위해서 제안하는 프로토콜에서 Eve가 위장공격과 intercept and resend 공격을 실행할 경우 안전성을 분석했다. 첫번째, Eve가 위장공격을 수행할 경우에는 인증키에 관한 정보없이 Eve가 검증에 통과할 수 있는 확률은 $1/2^N$임을 확인했다. 두번째, Eve가 intercept and resend 공격을 수행할 경우에는 경로 e와 d를 지나는 광자로부터 인증키에 대응하는 상대적 위상에 관한 정보를 얻어내는 것이 불가능함을 확인했다.

마지막으로 구현의 관점에서 선형광학으로 완전히 구별하기 어려운 Bell state $|\Phi^{\pm}>_{AB}$와 $|\Psi^{\pm}>_{AB}$를 사용하는 기존의 프로토콜과 달리 제안하는 기법은

Bell state $|\Phi^{\pm}>_{AB}$만을 사용하기 때문에 쉽게 구현할 수 있다.

References

[1] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Phys. Rev. Lett.*, vol. 70, no. 13, p. 1895, 1993.

[2] A. Karlsson and M. Bourennane, "Quantum teleportation using three-particle entanglement," *Phys. Rev. A*, vol. 58, no. 6, p. 4394, 1998.

[3] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, p. 575, 1997.

[4] J. Heo, et al., "Implementation of controlled quantum teleportation with an arbitrator for secure quantum channels via quantum dots inside optical cavities," *Scientific Reports*, vol. 7, no. 1, p. 14905, 2017.

[5] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, ""Event-ready-detectors" Bell experiment via entanglement swapping," *Phys. Rev. Lett.*, vol. 71, no. 26, p. 4287, 1993.

[6] J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, "Experimental entanglement swapping: entangling photons that never interacted," *Phys. Rev. Lett.*, vol. 80, no. 18, p. 3891, 1998.

[7] J. Jin, et al., "Entanglement swapping with quantum-memory-compatible photons," *Phys. Rev. A*, vol. 92, no. 1, p. 012329, 2015.

[8] J. Heo, M.-S. Kang, C.-H. Hong, S.-G. Choi, and J.-P. Hong, "Scheme for secure swapping two unknown states of a photonic qubit and an electron-spin qubit using simultaneous quantum transmission and teleportation via quantum dots inside single-sided optical cavities," *Phys. Lett. A*, vol. 381, no. 22, pp. 1845-1852, 2017.

[9] J. Heo, M.-S. Kang, C.-H. Hong, H. Yang, and S.-G. Choi, "Schemes generating entangled states and entanglement swapping between photons and three-level atoms inside optical cavities for quantum communication," *Quantum Inf. Process.*, vol. 16, no. 1, p. 24, 2017.

[10] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block," *Phys. Rev. A*, vol. 68, no. 4, p. 042317, 2003.

[11] H. Lee, J. Lim, and H. Yang, "Quantum direct communication with authentication," *Phys. Rev. A*, vol. 73, no. 4, p. 042305, 2006.

[12] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Sci. Bulletin*, vol. 62, no. 22, pp. 1519-1524, 2017.

[13] G. Zeng and C. H. Keitel, "Arbitrated quantum-signature scheme," *Physical Rev. A*, vol. 65, no. 4, p. 042312, 2002.

[14] H. Lee, C. Hong, H. Kim, J. Lim, and H. J. Yang, "Arbitrated quantum signature scheme with message recovery," *Phys. Lett. A*, vol. 321, no. 5-6, pp. 295-300, 2004.

[15] Q. Li, W. H. Chan, and D.-Y. Long, "Arbitrated quantum signature scheme using Bell states," *Phys. Rev. A*, vol. 79, no. 5, p. 054307, 2009.

[16] A. Farouk, et al., "Robust general N user authentication scheme in a centralized quantum communication network via generalized GHZ states," *Frontiers of Phys.*, vol. 13, no. 2, p. 130306, 2018.

[17] I. Ingemarsson and G. J. Simmons, "A protocol to set up shared secret schemes without the assistance of a mutually trusted party," in *Workshop on the Theory and Appl. Cryptographic Techniques*, pp. 266-282, Springer, 1990.

[18] B. A. Forouzan, *Cryptography & network security,* McGraw-Hill Inc., 2007.

[19] M.-S. Kang, J. Heo, C.-H. Hong, H.-J. Yang, S.-W. Han, and S. Moon, "Controlled mutual

quantum entity authentication with an untrusted third party," *Quantum Inf. Process.*, vol. 17, no. 7, p. 159, 2018.

[20] G. Gao and Y. Wang, "Cryptanalysis of controlled mutual quantum entity authentication using entanglement swapping," *Commun. in Theoretical Phys.*, vol. 67, no. 1, p. 33, 2017.

[21] M.-S. Kang, C.-H. Hong, J. Heo, J.-I. Lim, and H.-J. Yang, "Controlled mutual quantum entity authentication using entanglement swapping," *Chinese Phys. B*, vol. 24, no. 9, p. 090306, 2015.

[22] Y.-S. Kim, et al., "Informationally symmetrical Bell state preparation and measurement," *Optics express*, vol. 26, no. 22, pp. 29539-29549, 2018.

[23] Y.-S. Kim, et al., "Symmetrical Bell state preparation and measurement without a third party," in *CLEO,* San Jose, CA, USA, May 2019.

강 민 성 (Min-Sung Kang)

2005년 : 고려대학교 물리학사
2013년 : 고려대학교 정보보호대학원 석사
2016년 : 고려대학교 정보보호대학원 박사
2016년~2019년 : 한국과학기술연구원 박사후연구원
2019년~현재 : 특허청 심사관
<관심분야> 양자정보, 양자암호, 양자 컴퓨팅

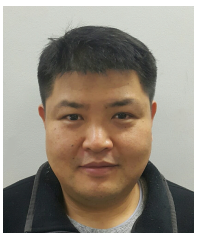
최 지 웅 (Ji-Woong Choi)

2016년 : 고려대학교 물리학사
2016년~현재 : 고려대학교 응용물리학과 석·박사통합과정
<관심분야> 양자정보, 양자암호, 양자인증, 양자서명
[ORCID:0000-0001-8354-3497]

김 용 수 (Yong-Su Kim)

2006년 : 연세대학교 물리학사
2007년 : POSTECH 물리학석사
2012년 : POSTECH 물리학박사
2012년~2013년 : 미 Gaithersburg 국립표준기술연구소 초빙연구원
2013년~현재 : 한국과학기술연구원 선임연구원
<관심분야> 양자 광학, 양자 정보
[ORCID:0000-0001-5763-1522]

김 일 영 (Il-Young Kim)



1999년 : 서울과학기술대학교 제어계측 공학사
2004년 : 서울과학기술대학원 메카트로닉스 공학석사
2004년~2009년 : 컨벡스(주)
2009년~2010년 : LG전자(주)
2010년~2011년 : ㈜유메카
2011년~현재 : 한국과학기술연구원 전문원
<관심분야> 양자암호, 양자정보, 전자제어시스템

문 성 욱 (Sung Moon)

1986년 : 연세대학교 금속공학사
1988년 : 연세대학교 금속공학석사
1994년 : 연세대학교 반도체공학박사
1995년 : 영 MMT 초빙연구원
1996년 : 영 CMF 초빙연구원
1989년~현재 : 한국과학기술연구원 책임연구원
<관심분야> 양자 암호, 양자 디바이스
[ORCID:0000-0002-2127-9173]

한 상 욱 (Sang-Wook Han)

1999년 : KAIST 전기 및 전자공학사
2001년 : KAIST 전기 및 전자공학석사
2006년 : KAIST 전기 및 전자공학박사
2006년~2009년 : ㈜퓔셀플러스 선임연구원
2009년~2012년 : 삼성종합기술원 전문연구원
2012년~현재 : 한국과학기술연구원 책임연구원 (양자정보연구단장)
<관심분야> 양자정보, 양자키분배, 난수 생성기, 양자 서명, 단일 광자 검출기, 양자 컴퓨팅
[ORCID:0000-0002-4098-3326]