

양자통신상의 가용성침해공격

An Availability Invasion Attacks on a Quantum Communications



정보시스템공학과
권혁동



CONTENTS

01 보안의 3요소

02 양자

03 양자통신

04 제안기법

05 결론



01 보안의 3요소

01 기밀성 | Confidentiality

인가되지 않은 제 3자는 정보에 접근할 수 없어야 한다.

02 무결성 | Integrity

전송된 데이터가 원본과 동일하며 수정되지 않았을 보장한다.

03 가용성 | Availability

인가된 사용자는 항상 손쉽게 정보 접근이 가능하다.



01 보안의 3요소

01 기밀성 | Confidentiality

Sniffing, Scamming, Traffic analysis

02 무결성 | Integrity

Spoofing, Modification, Fabrication, Masquerading, Replaying, Repudiation

03 가용성 | Availability

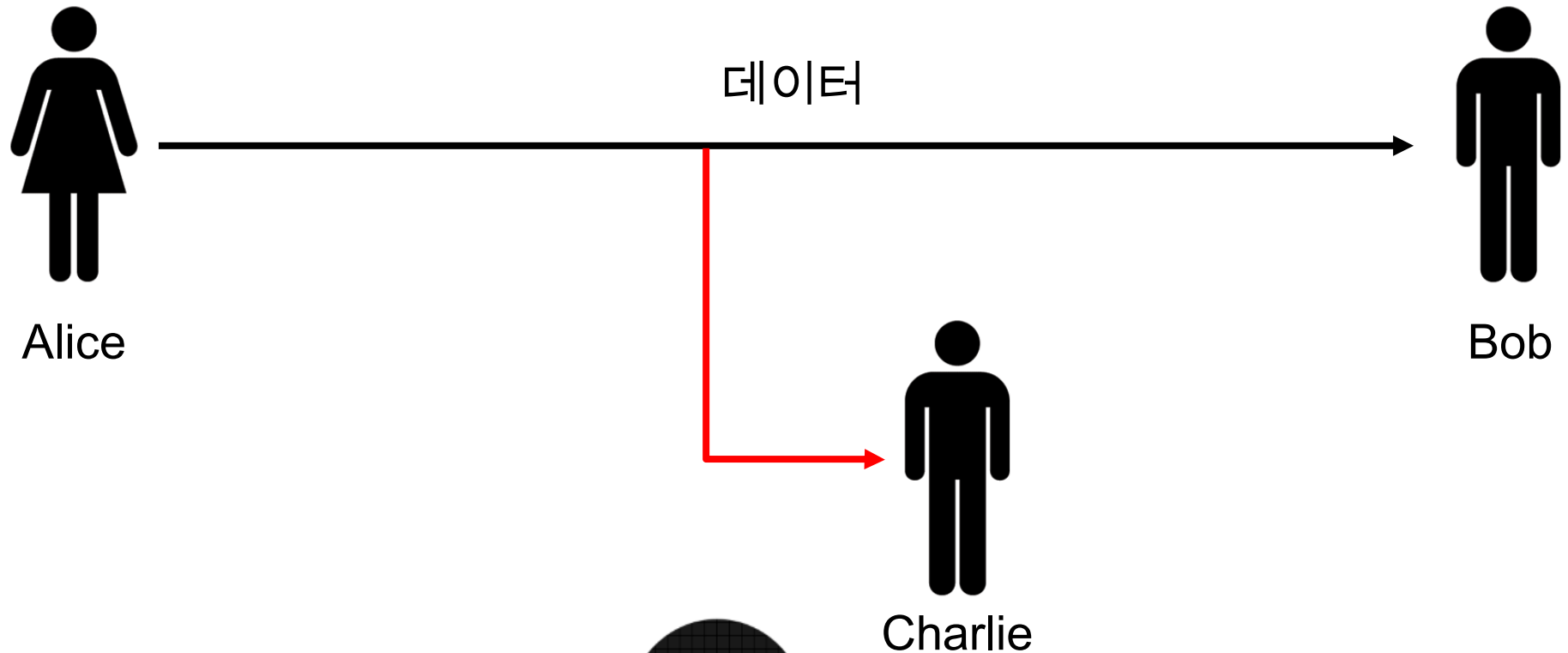
Denial of Service, Interruption



01 보안의 3요소

스니핑 공격 | Sniffing attacks

통신의 주체가 아닌 제 3자가 통신 채널을 감청하여 데이터를 관찰하는 공격

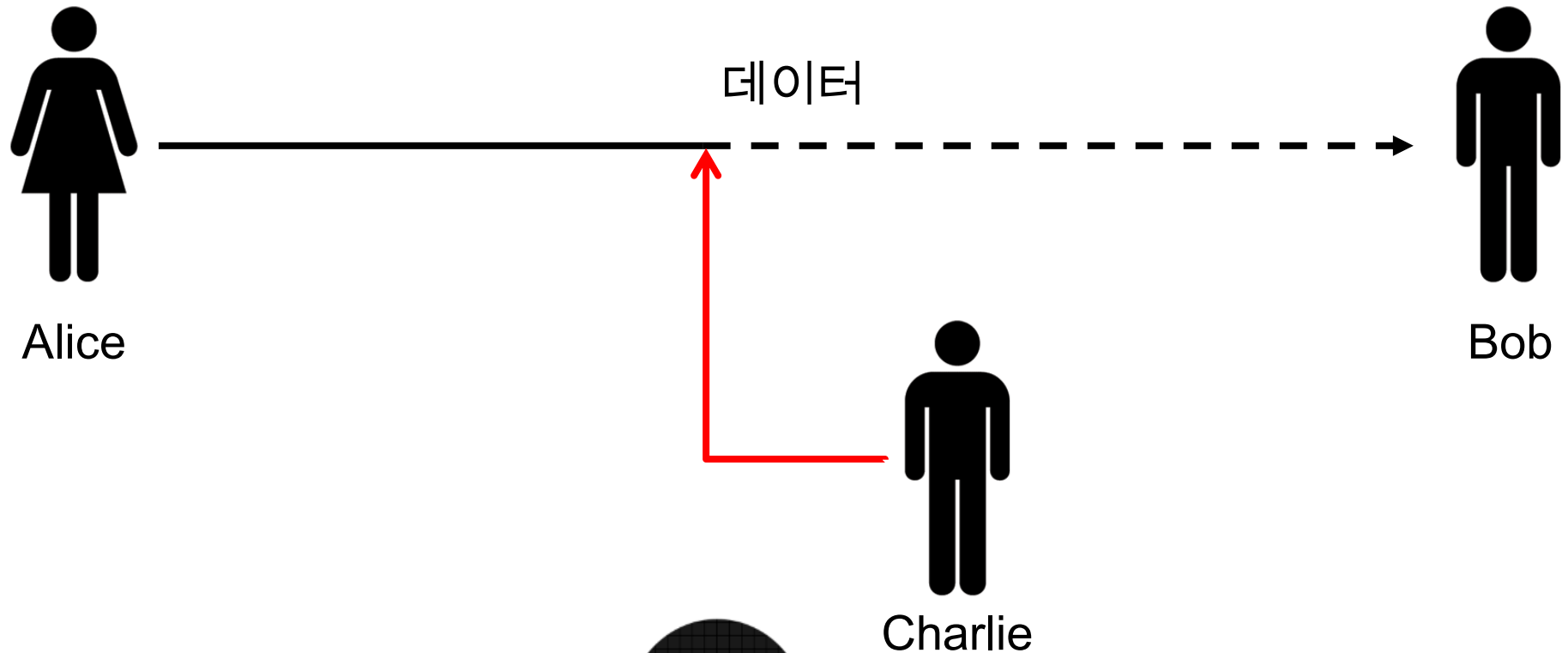




01 보안의 3요소

서비스 거부 공격 | Sniffing attacks

통신 자체가 이루어지지 않도록 방해하는 공격





02 양자

양자 | Quantum

1899년 독일의 물리학자 막스 플랑크가 제시

더 이상 나눌 수 없는 에너지 최소량의 단위

고전역학이 적용되지 않는 일부 특이한 성질 보유



02 양자

01 양자 중첩 | Superposition

02 양자 얽힘 | Entanglement

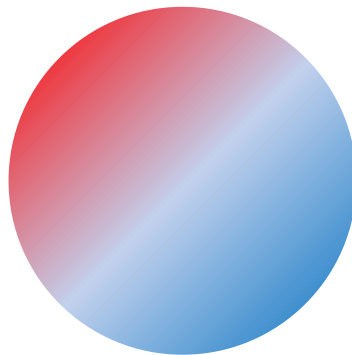
03 양자 붕괴 | Collapse



02 양자

01 양자 중첩 | Superposition

모든 양자는 일정한 확률을 가지고 상태 구성에 기여함
관측되기 전 까지는 가능성에 따라 여러가지 상태로 동시에 존재 가능



1/2 - 빨간색

1/2 - 파란색

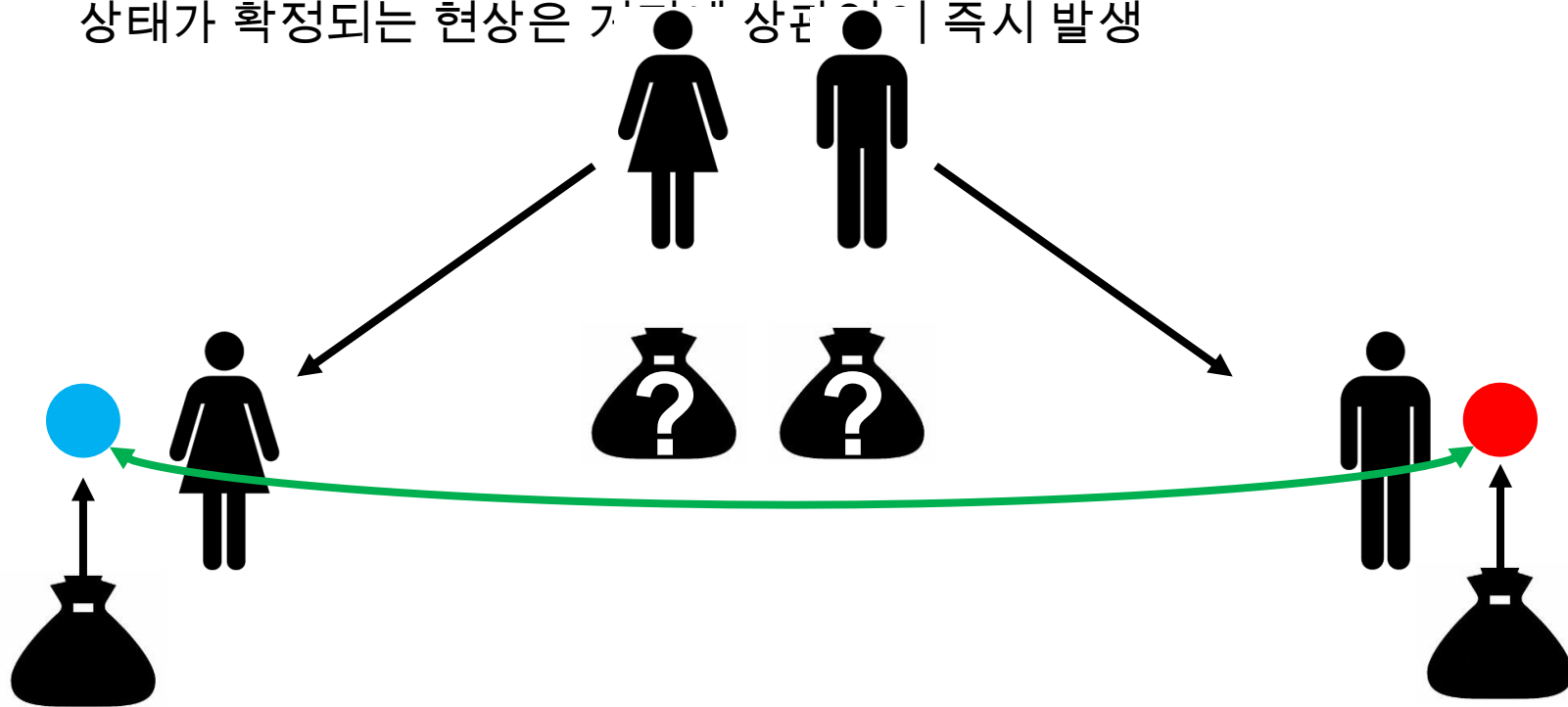


02 양자

02 양자 얽힘 | Entanglement

서로 연관이 있는 양자는 한쪽의 상태를 관측하는 순간 다른 쪽의 상태도 결정됨

상태가 확정되는 현상은 기묘한 상관관계 | 즉시 발생



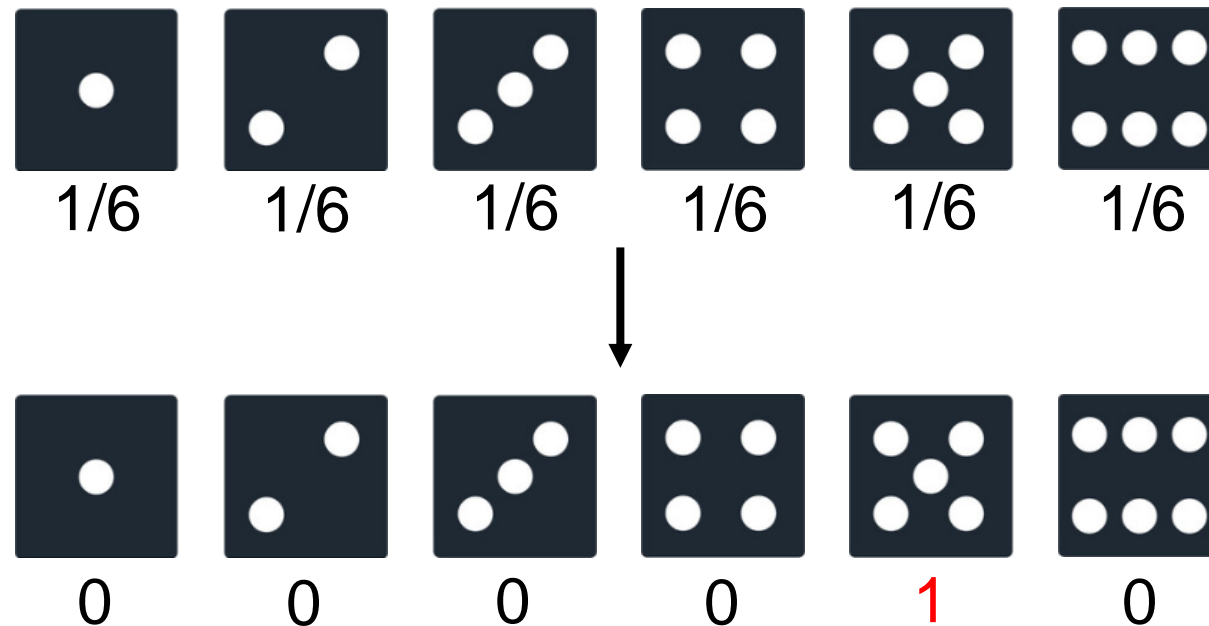


02 양자

03 양자 붕괴 | Collapse

양자를 관측하는 순간 중첩상태에서 벗어나는 현상

다른 상태가 될 확률은 전부 제거되며 한 가지의 상태가 될 확률만 존재





03 양자통신

01 통신 프로토콜 BB84

1984년 C. H. 베넷, G 브라사드가 제안

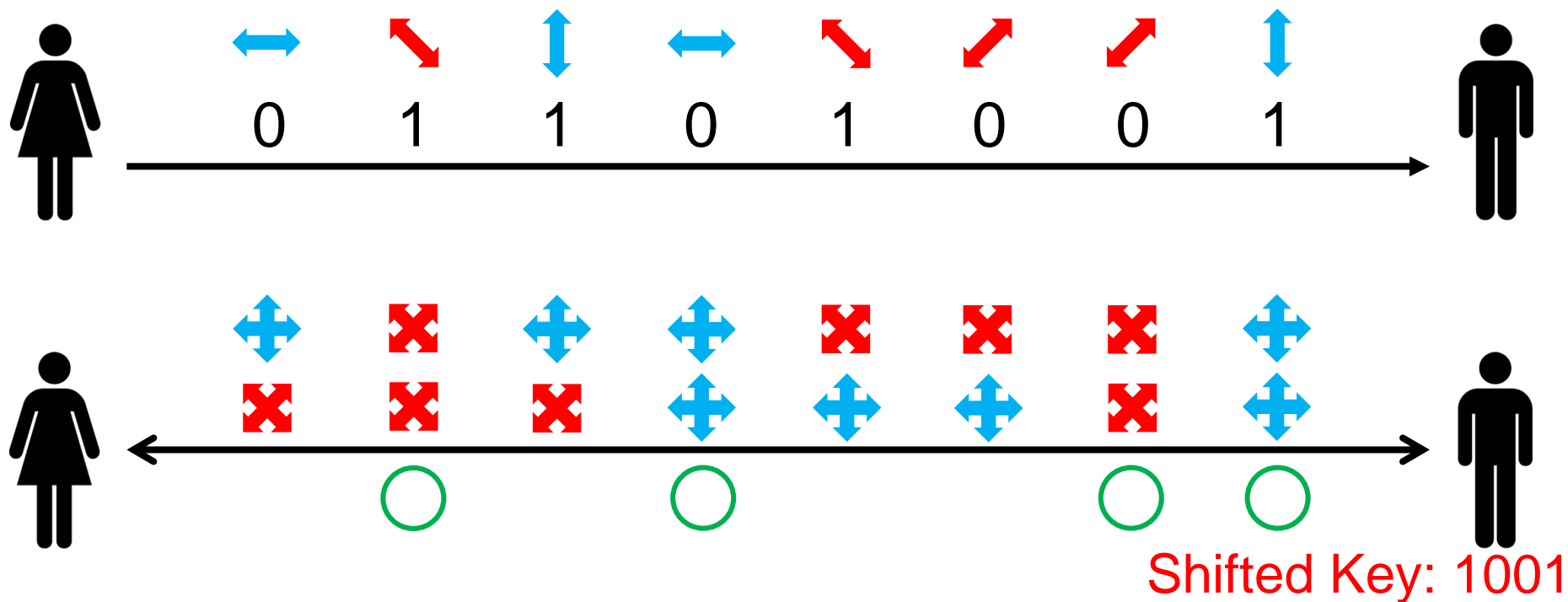
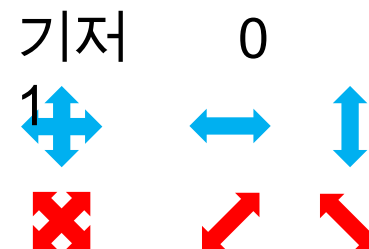
송신자와 수신자간 OTP를 생성하는 프로토콜

양자 키 분배: Quantum Key Distribution (QKD)



03 양자통신

01 통신 프로토콜 BB84

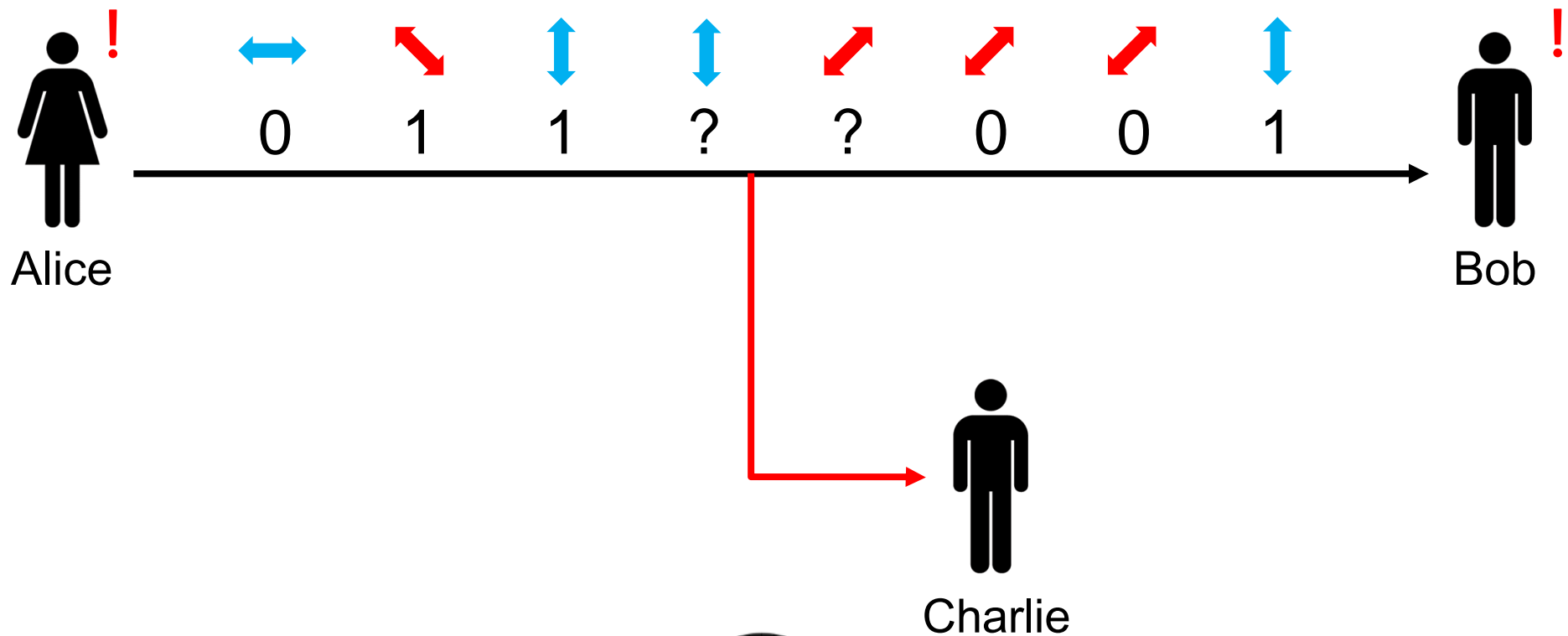




03 양자통신

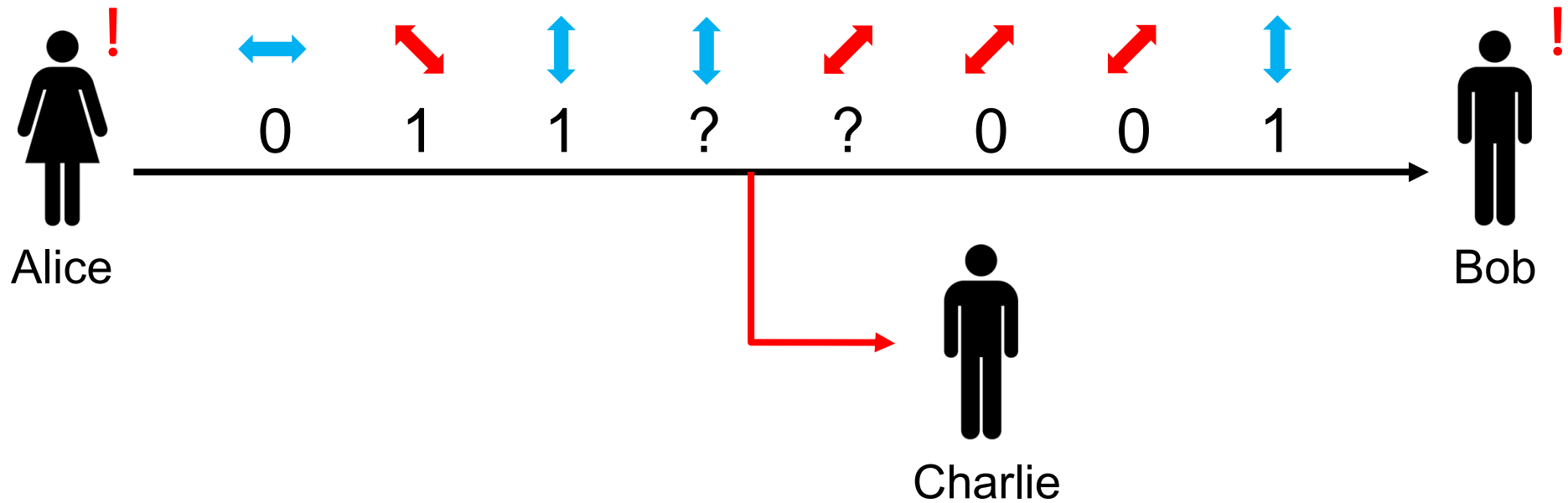
01 통신 프로토콜 BB84

양자 에러 비트율 | Quantum Error Bits Rate (QBER)





04 제안기법



지속적인 양자채널 관측을 통해 QBER를 상승
본디 통신을 의도한 사용자들은 QKD의 진행이 불가능
공격자가 관측을 중단하기 전 까지 통신 개시가 어려움



05 결론

01 고전 채널 상에서의 스니핑 공격은 기밀성 침해 공격

공격자가 수동적이며 데이터를 훔쳐보는 선의 공격

02 양자 채널 상에서의 스니핑 공격은 가용성 침해 공격

통신 주체간 정상적인 통신 진행을 방해함

03 통신 채널 자체를 보호할 수 있는 수단이 필요함

Journal of the Korea Institute of Information and
Communication Engineering

한국정보통신학회誌 Vol. 17, No. 2: 399~406, Mar. 2013

【五】【五】

양자 통신 환경 상에서의 가용성 침해 공격.

/// 저자정보 제공 전에 삭제 ///

An Availability Invasion Attacks on a Quantum Communications

※역기도 학제※ Hyeok-Dong Kwon¹⁾, Hun-jeong Seo^{1*)}

*Department of Information System Engineering, Hansung University, Seoul 02876, Korea. lee@hansung.ac.kr

³Department of IT Engineering, Hansung University, Seoul 02876, Korea.

이 두 노래

요약

[illegible]

ABSTRACT 4

The confidentiality, integrity and availability are known as the "three goals" of security. Among them, packet sniffing attack is classified as confidentiality invasion attacks. The sniffing attack can't understand contents of communications, but a third person who is unauthorized can eavesdropping the contents. In general, a confidentiality attack is less likely to be directly impacted by the victim, and even if the information is exposed to the attacker, it is usually encrypted so that the attacker difficult obtain original message. The quantum communications are expected to show "store" than current communications method by using quantum which has superposition. The quantum collapsed when they are observed, even if the communication contents are exposed, the original can be hidden. In this paper, we concentrate on quantum characteristics, and examine the types of packet sniffing attack change to availability invasion attacks. 4

키워드: "알파 통신", "픽셋", "스니컬", "공보", "서비스", "저본", "가용성."

Key word: Quantum communication, Packet scheduling, Delay of service, Availability

Received 29 November 2014; Revised 29 December 2014; Accepted 21 January 2015
(Received 29 November 2014; Received 29 December 2014; Received 21 January 2015)

*Carrozzeria Asfalter Bros - via Sordani 10 - 20121 Milano - Tel. 02/40.00.00

Department of IT Engineering, Bannag University, Bangkok 10260, Thailand

Open Access <http://dx.doi.org/10.6109/jalice.2018.17.2.399>

9 1534 221

[illegible]

한국정토문화재단논문지 Vol. 17, No. 2, 399~406, Mar. 2013.

1. 서론

[의리할(복수형)] [의리할(복수형)] [복원호 위치]

臣等謹將所擬章程繕具清單
 呈請 聖鑒訓示謹奏

이제부터 사의의 '보안'은 각종 '보안'의 원인으로 부각될
 보름 '보안'하기 위해 기밀성(confidentiality), 무결성
 (integrity), 가용성(availability)의 각 가리목 '보안'으로
 보게 시(의)하게 되었으며 각각의 의미는 다음과 같다. 1

기원점은 인공의 작용을 제3자가 조여진 면에서
자나 불인자나 없다든가 하는 것이 아니라, 무엇이든
불이든가 타물이든가 인의 작용이든가 불의 작용이든가
그것을 불인자나 타물인 것이 아니다.

[illegible][illegible]

동선이 새롭게 꾸며져 있다. 4

▶ 말장독인은 빛의 속도인 위광속자(photon)를 사용함으로써 기존의 통신 환경은 0과 1의 이진 정보만을 전달했지만 말장독인은 이진 정보뿐만 아니라 무한정된 양의 정보를 보낼 수 있다.

말과 정신의 가장 큰 정점은 스니핑 공격(sniffing attacks)에 감하는 것이다. 누군가가 제본을 감시하면, 경보가 울리는 것이다. 감을 하도록 할 수 있다. 나. 이러한 공격이 가능한 이유는 말자의 특성에 기인하는 데, 말자는 권유를 하는 순간까지도, 인간이 알지 못하며, 감을 하도록 할 수 없게 되어 있다. 이러한 공격은 말자의 특성에 기인한다. 나

[illegible]

佛敎의 眞實性을 證明할 爲한 佛敎의 眞實性을 證明할 爲한
 佛敎의 眞實性을 證明할 爲한 佛敎의 眞實性을 證明할 爲한
 佛敎의 眞實性을 證明할 爲한 佛敎의 眞實性을 證明할 爲한
 佛敎의 眞實性을 證明할 爲한 佛敎의 眞實性을 證明할 爲한
 佛敎의 眞實性을 證明할 爲한 佛敎의 眞實性을 證明할 爲한

D. 관별·연구·동향+

본정의 서는 양자통신과 관련된 연구와 기법이 "이는 양자역학의 원리를 이용하여 양자통신을 위해 제시된 프로토콜을 확인한다."

2.1'말자

[illegible]

중국어의 어휘는 한자어, 외래어, 신조어, 속어로 나뉘는데, 한자어는 중국에서 유래한 어휘로, 외래어는 외국에서 유래한 어휘로, 신조어는 최근에 만들어진 어휘로, 속어는 일상에서 사용되는 어휘로 분류된다.

Attack type	Attack type
Confidentiality protection	<ul style="list-style-type: none"> Sniffing Spawning Trickle analysis
Integrity protection	<ul style="list-style-type: none"> Spoofting Modification Falsification Manipulating Replaying Republishing
Availability protection	<ul style="list-style-type: none"> Denial of Service Information

지금까지의 통신 내용은 전기·신호를 이용한 것으로
전기·신호의 유무만 파악하여 1의 이진 값을 사용하여
통신이 이루어진다. 하지만, 많은 통신을 할수록 많은

18



Thank You