양자통신상의 가용성침해공격

An Availability Invasion Attacks on a Quantum Communications

정보시스템공학과
권혁동

CONTENTS

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

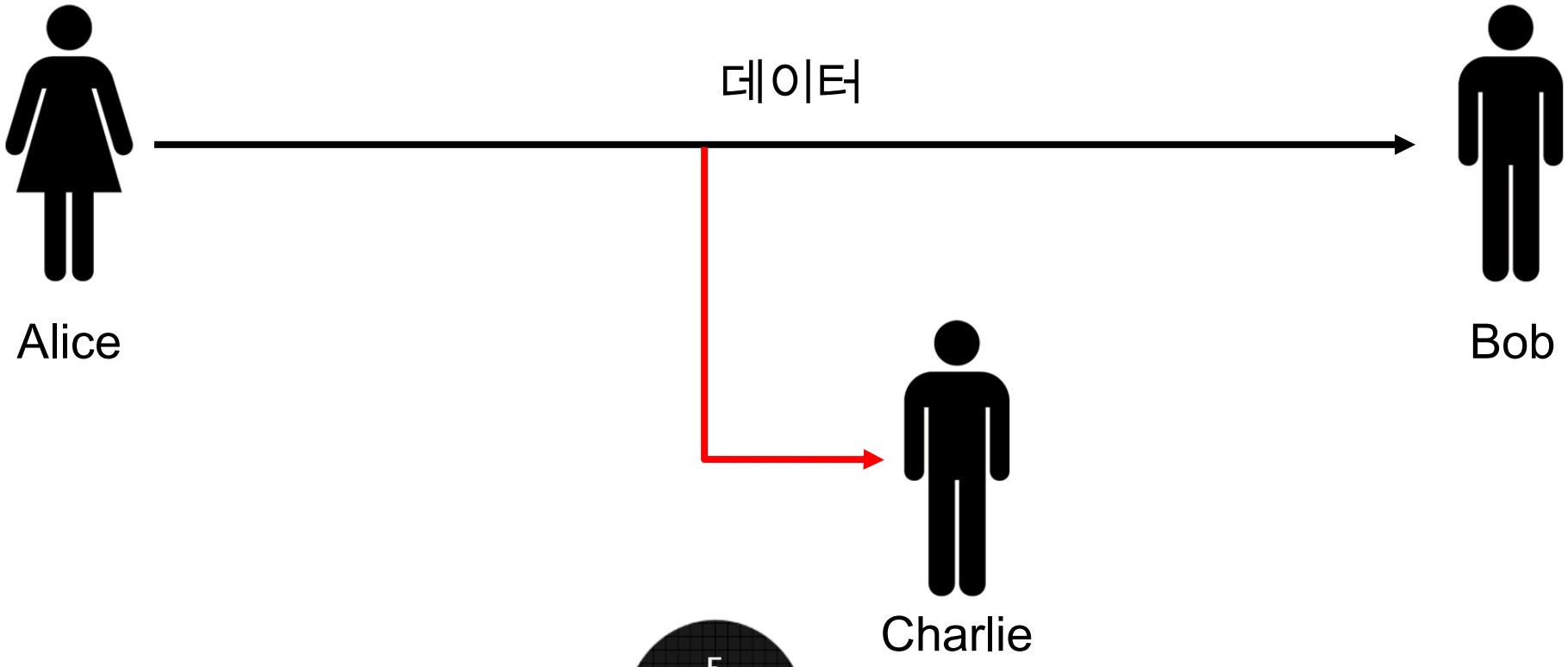
03 가용성 | Availability

Denial of Service, Interruption

01 보안의 3요소

스니핑 공격 | Sniffing attacks

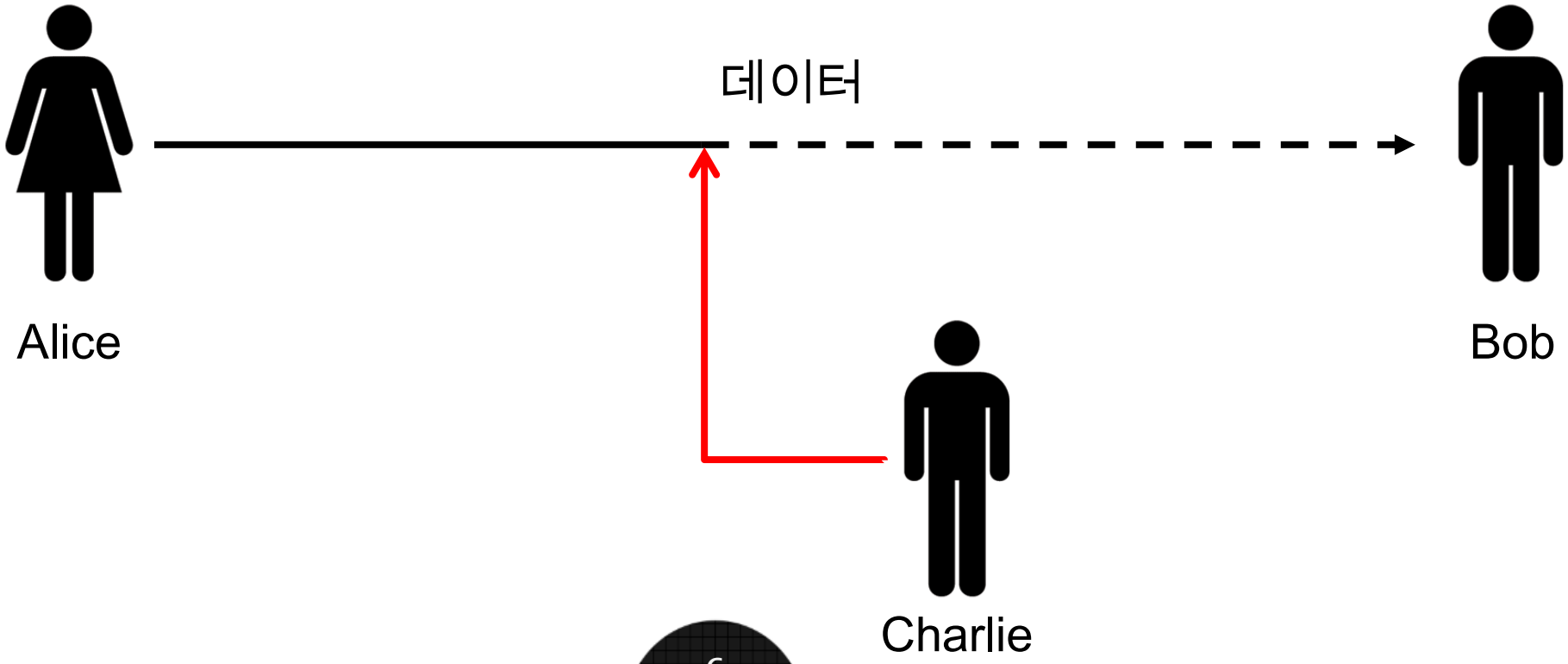
통신의 주체가 아닌 제 3자가 통신 채널을 감청하여 데이터를 관찰하는 공격



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

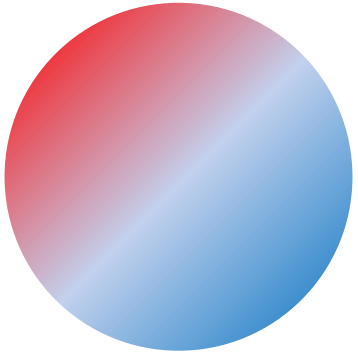
03 양자 붕괴 | Collapse

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

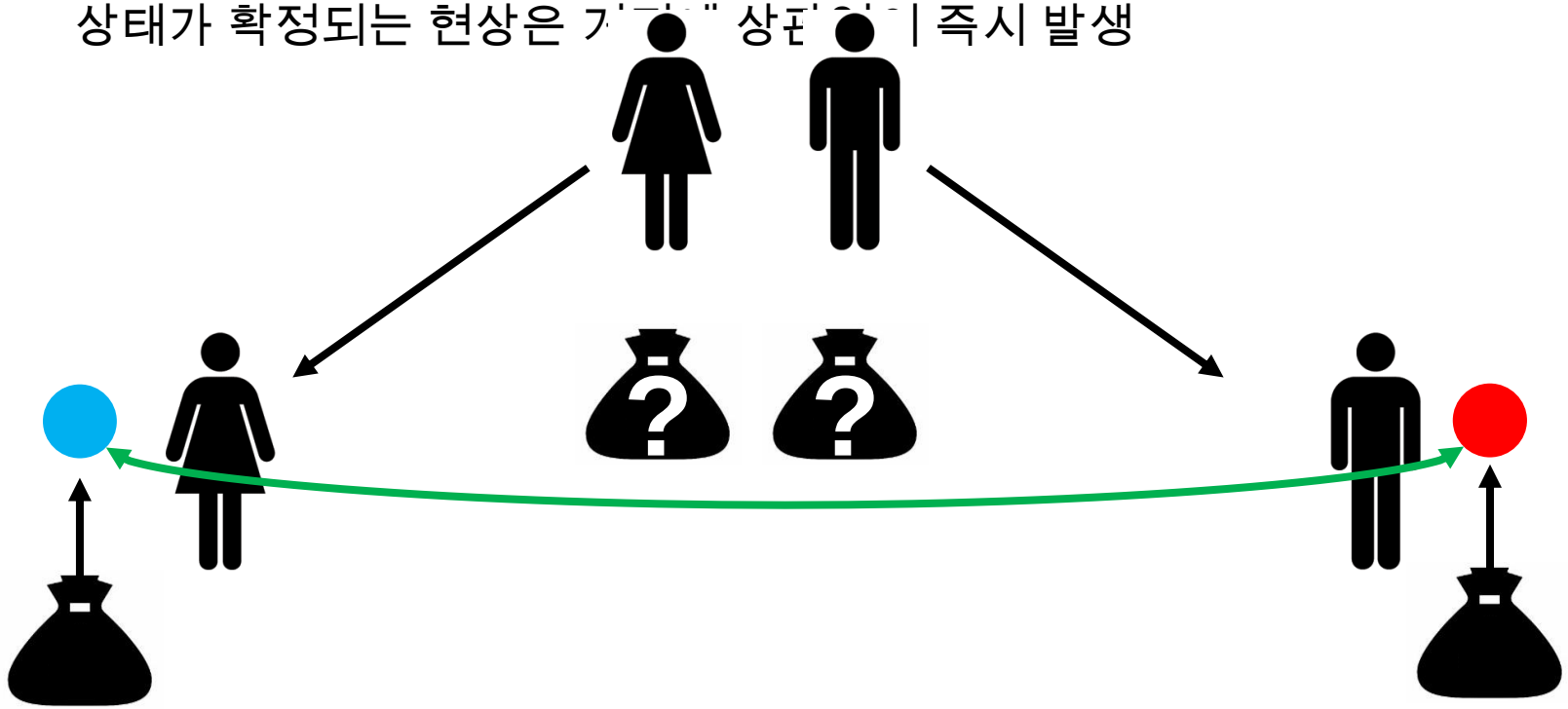
1/2 - 파란색

02 양자

02 양자 얽힘 | Entanglement

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

상태가 확정되는 현상은 거리에 상관없이 즉시 발생

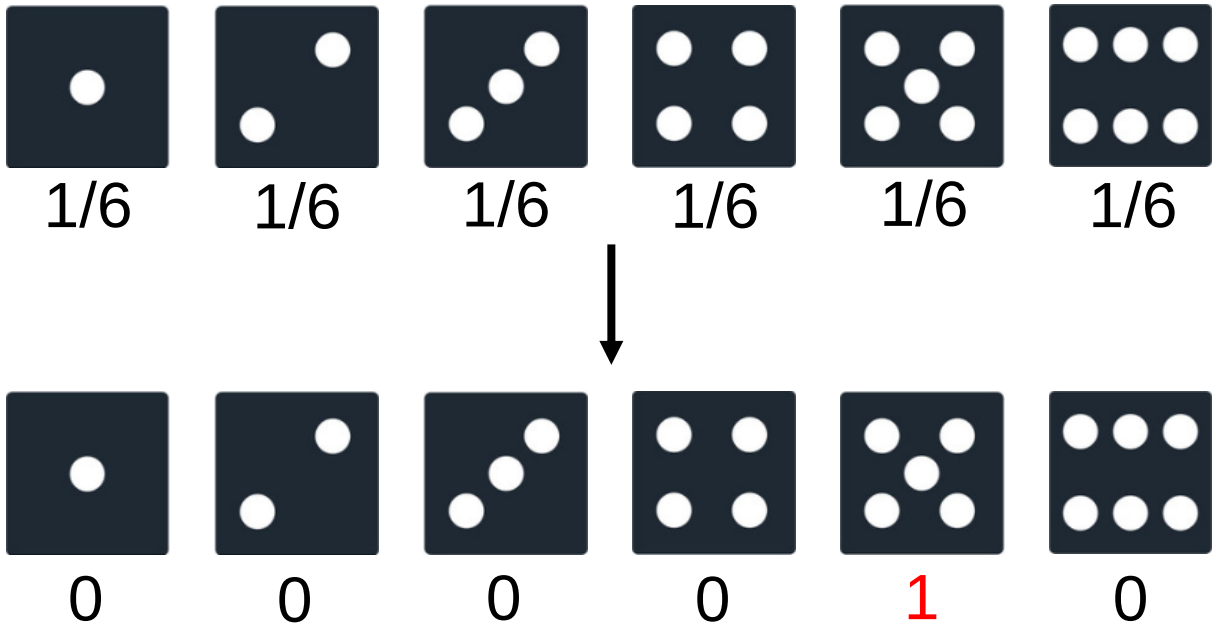


02 양자

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

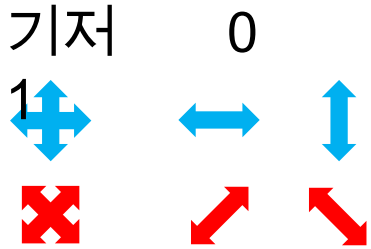
1984년 C. H. 베넷, G 브라사드가 제안

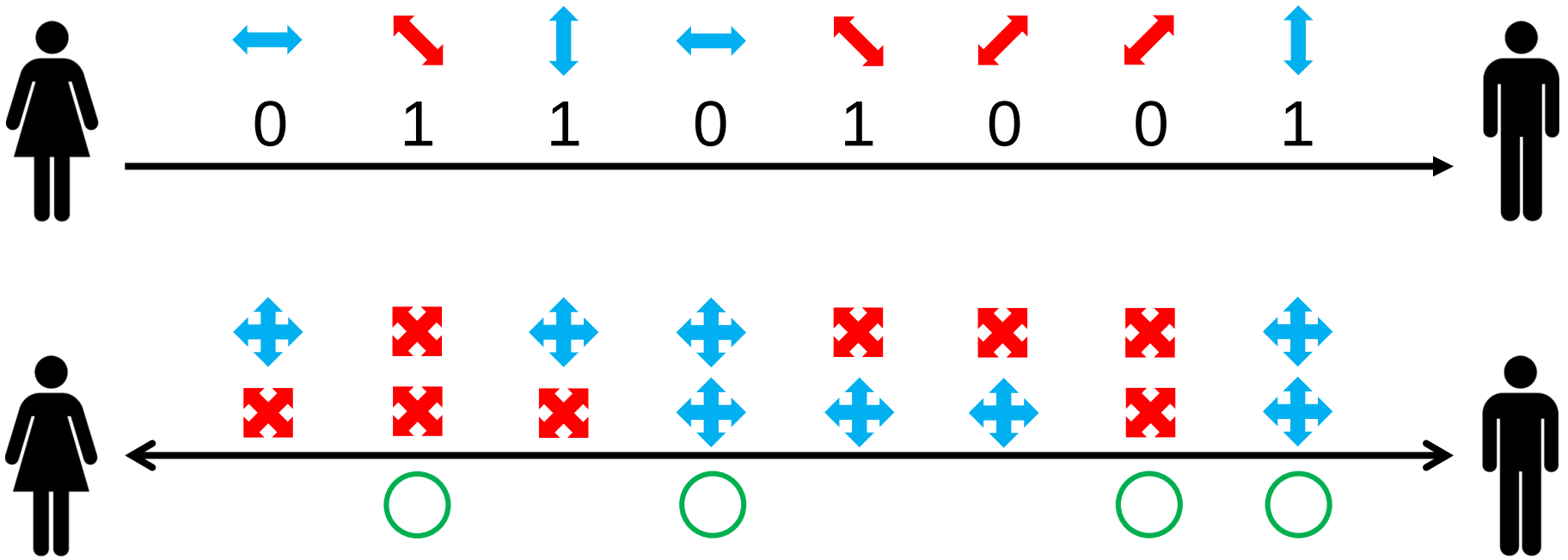
송신자와 수신자간 OTP를 생성하는 프로토콜

양자 키 분배: Quantum Key Distribution (QKD)

03 양자통신

01 통신 프로토콜 BB84

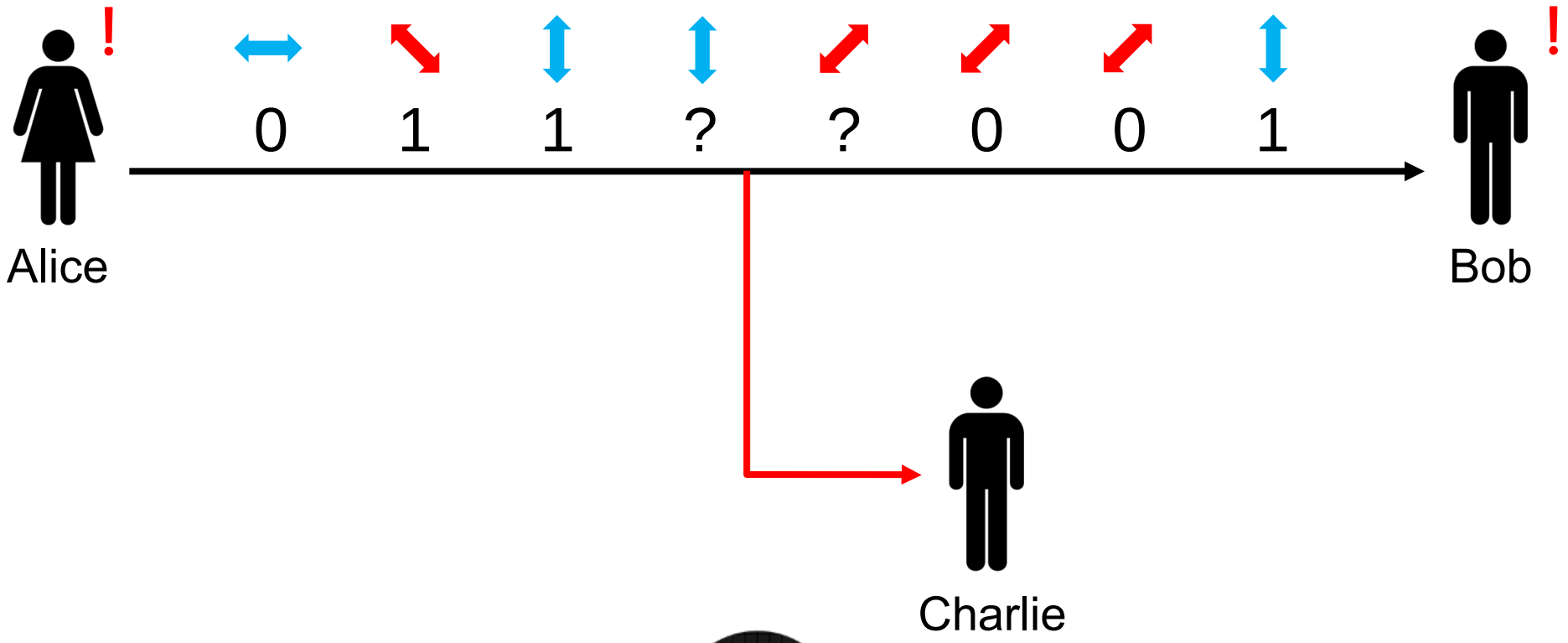




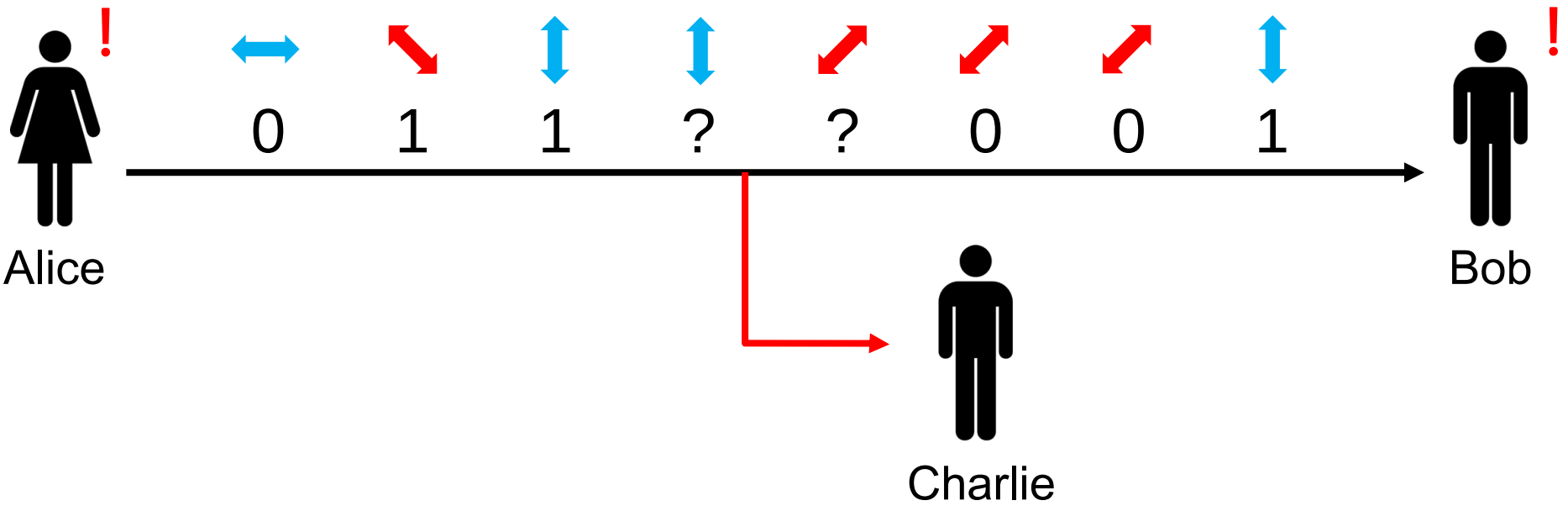
03 양자통신

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

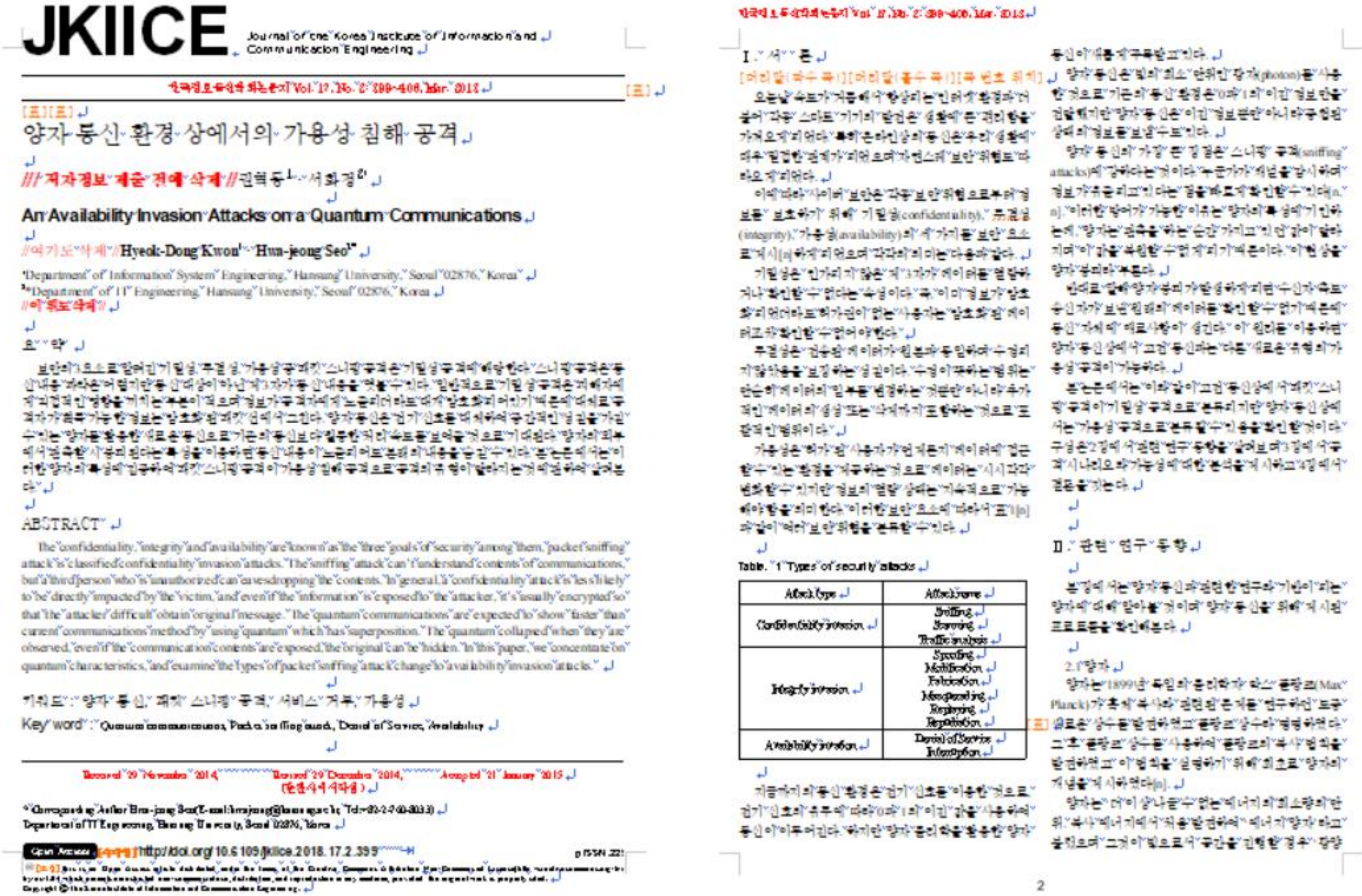
공격자가 수동적이며 데이터를 훔쳐보는 선의 공격

02 양자 채널 상에서의 스니핑 공격은 가용성 침해 공격

통신 주체간 정상적인 통신 진행을 방해함

03 통신 채널 자체를 보호할 수 있는 수단이 필요함

05 결론



JKIICE Journal of the Korea Institute of Information and Communication Engineering

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

양자 통신 환경 상에서의 가용성 침해 공격

An Availability Invasion Attacks on a Quantum Communications

Hyeok-Dong Kwon[1] · Hwa-jeong Seo[2*]

[1]Department of Information System Engineering, Hansung University, Seoul 02876, Korea

[2*]Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

ABSTRACT

The confidentiality, integrity and availability are known as the three goals of security among them, packet sniffing attack is classified 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's usually encrypted so that the attacker difficult obtain original message. The quantum communications are expected to show faster than current communications method by using quantum which has superposition. The quantum collaped 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.

키워드 : 양자 통신, 패킷 스니핑 공격, 서비스 거부, 가용성

Key word : Quantum communications, Packet sniffing attack, Denial of Service, Availability

Ⅰ. 서 론

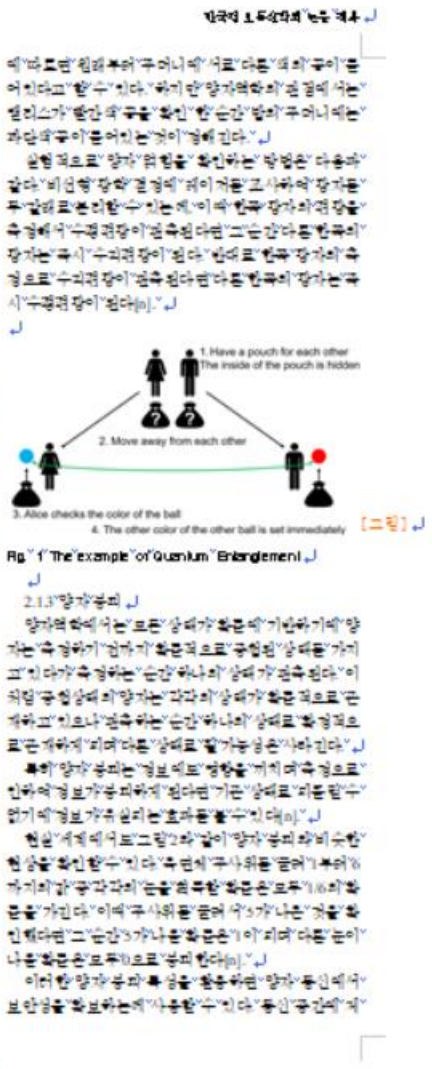
Table. 1 Types of security attacks

Attack type	Attack name
Confidentiality invasion	Sniffing Snooping Traffic analysis
Integrity invasion	Spoofing Modification Fabrication Masquerading Replaying Repudiation
Availability invasion	Denial of Service Interruption

Ⅱ. 관련 연구 동향

2.1 양자

05 결론



Thank You