2018년 하반기 보고

정보시스템공학과 권혁동

한성대학교
HANSUNG UNIVERSITY

CONTENTS

01 양자채널 상 공격 가능성 분석

한성대학교 HANSUNG UNIVERSITY

01

양자

한성대학교
HANSUNG UNIVERSITY

01. 양자

- 양자: 더 이상 나눌 수 없는 에너지 최소량 단위
- 양자통신: 양자의 특성을 이용한 통신 기법

한성대학교
HANSUNG UNIVERSITY

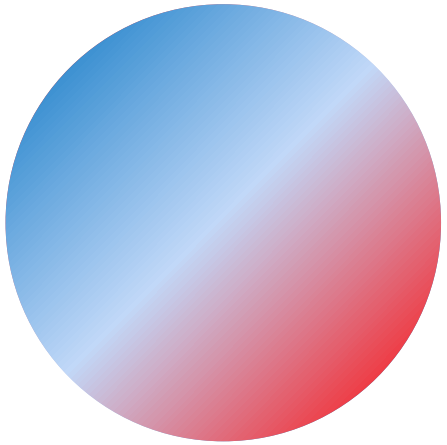
01. 양자

- 양자 중첩
- 양자 얽힘
- 양자 붕괴

한성대학교
HANSUNG UNIVERSITY

01. 양자 - 양자중첩

- 양자는 일정한 확률을 가지고 상태 구성에 기여
- 관측되기 전 까지는 가능성에 따라 여러 상태로 존재 가능



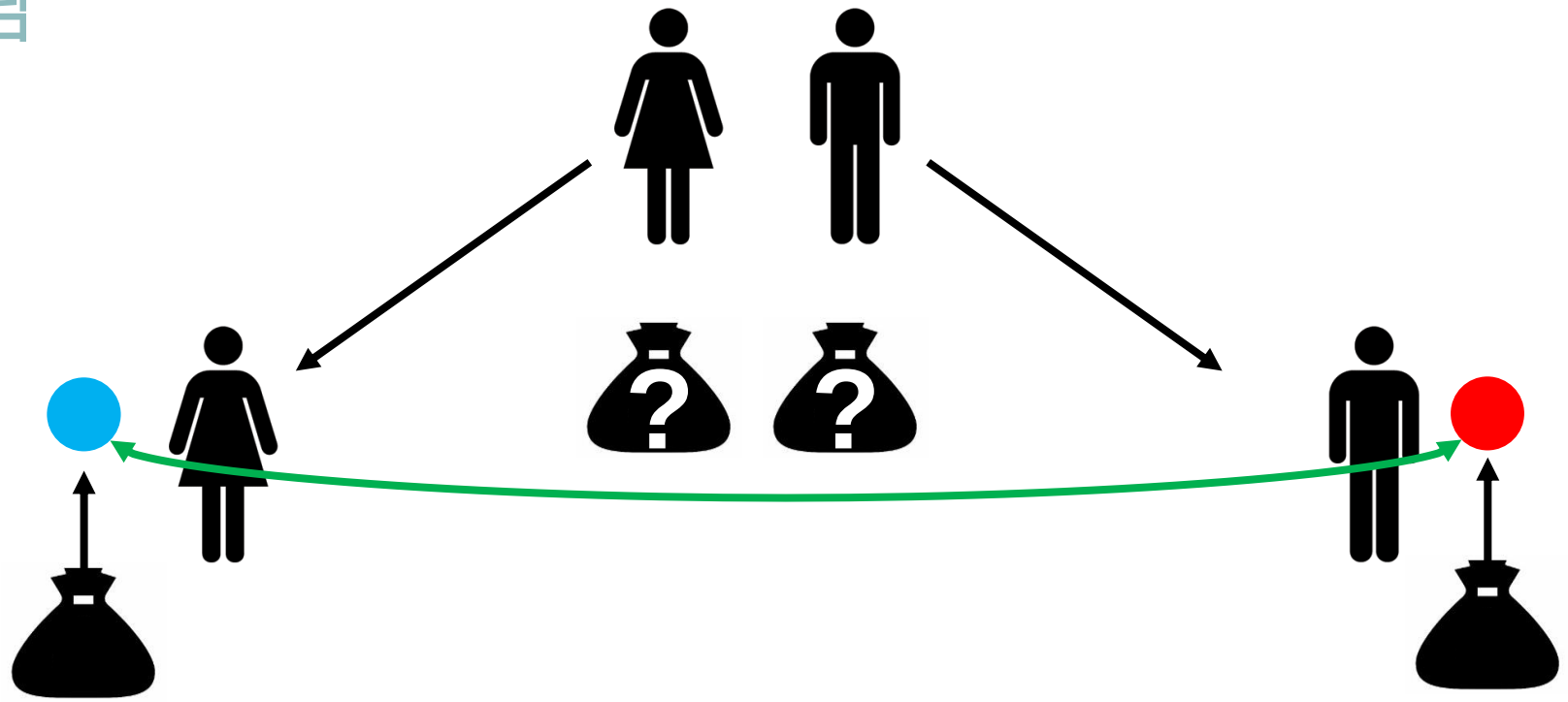
1/2 - 빨간색

1/2 - 파란색

한성대학교 HANSUNG UNIVERSITY

01. 양자 - 양자얽힘

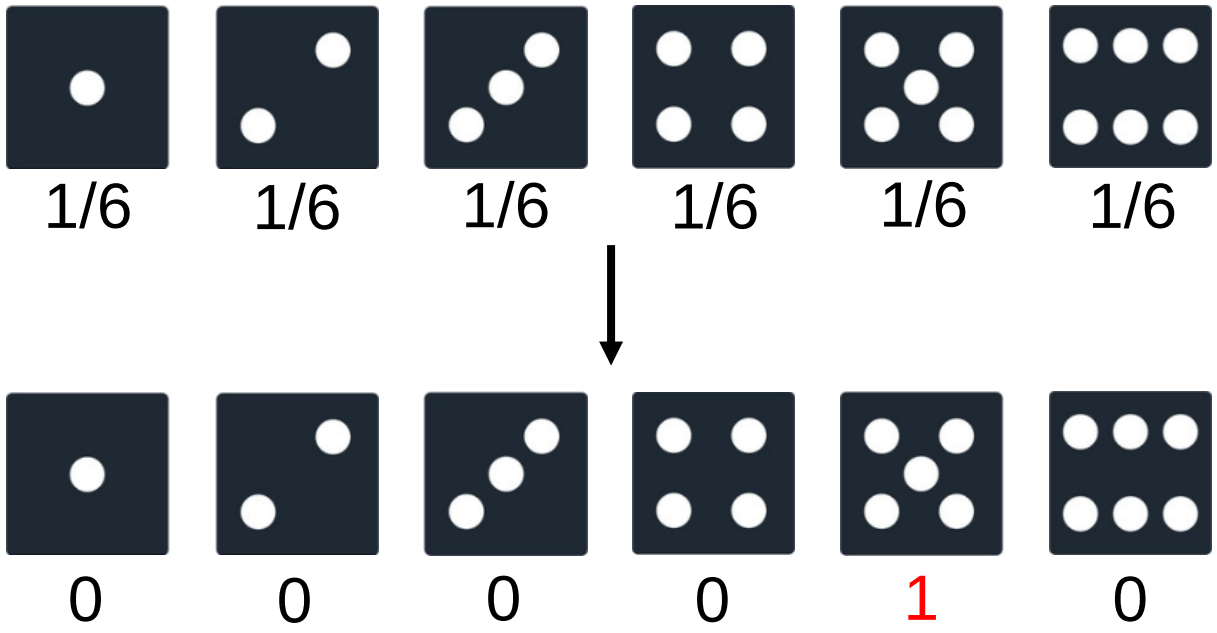
- 서로 연관 있는 양자는 한 쪽을 관측하는 순간 다른 쪽 상태가 결정됨



한성대학교
HANSUNG UNIVERSITY

01. 양자 - 양자붕괴

- 양자를 관측하는 순간 중첩상태에서 벗어나는 현상
- 한 가지의 상태가 될 확률만 남고 다른 확률은 제거됨



한성대학교 HANSUNG UNIVERSITY

02

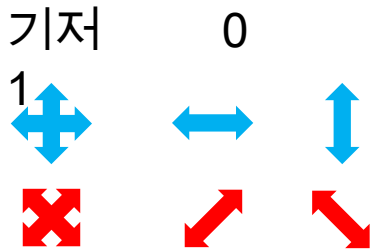
양자통신 프로토콜

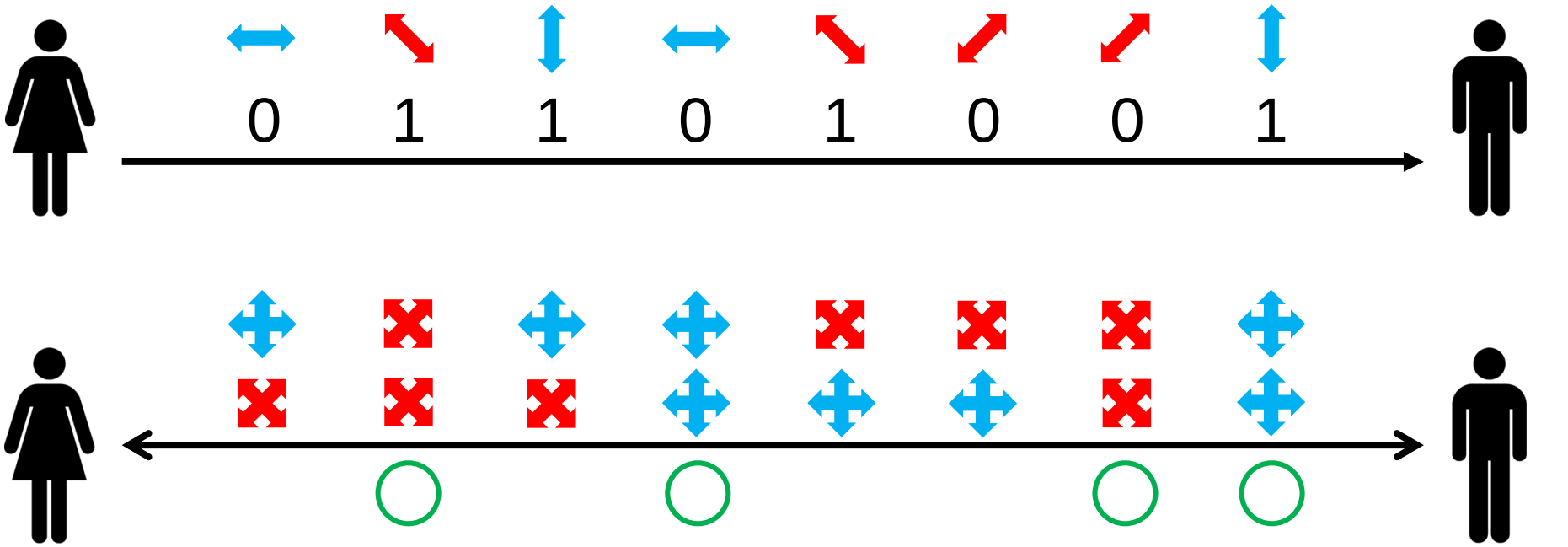
한성대학교
HANSUNG UNIVERSITY

01. 양자통신 프로토콜

- 통신 프로토콜 BB84
- 1984년 C. H. 베넷, G 브라사드
- 송신자와 수신자간 OTP를 생성하는 프로토콜

02. 동작 원리



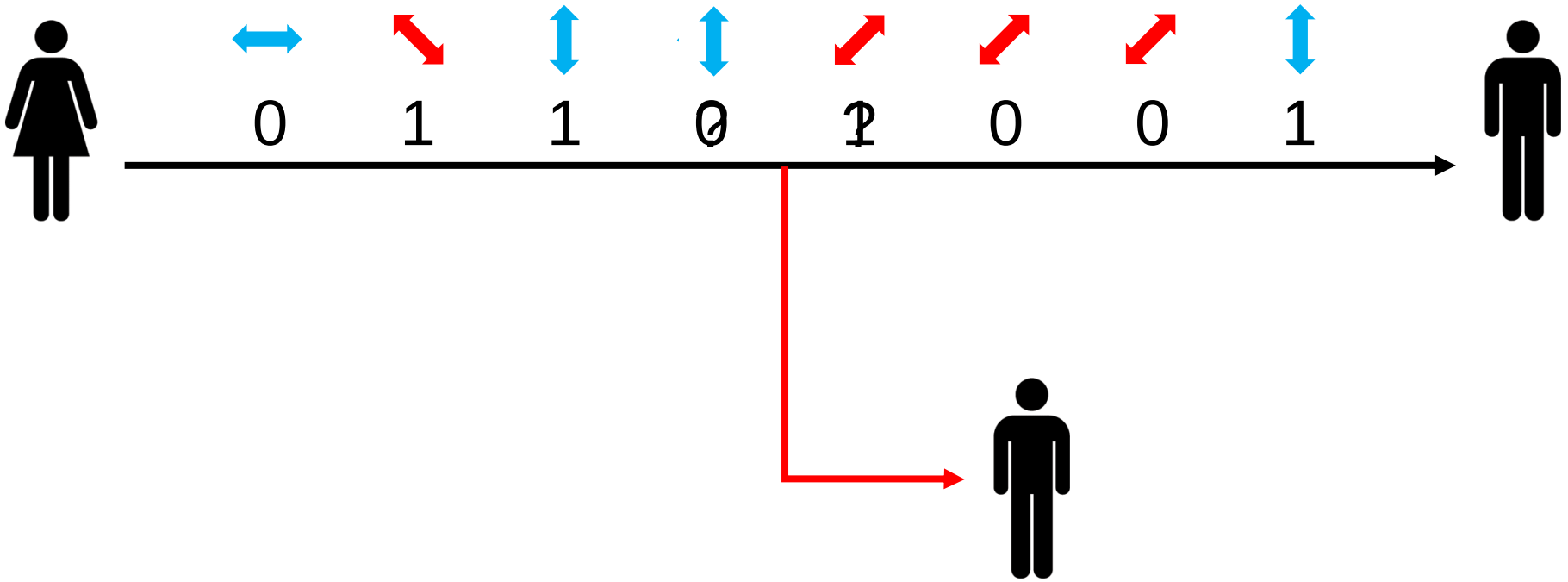


Shifted Key: 1001

한성대학교
HANSUNG UNIVERSITY

03. 방어 기법

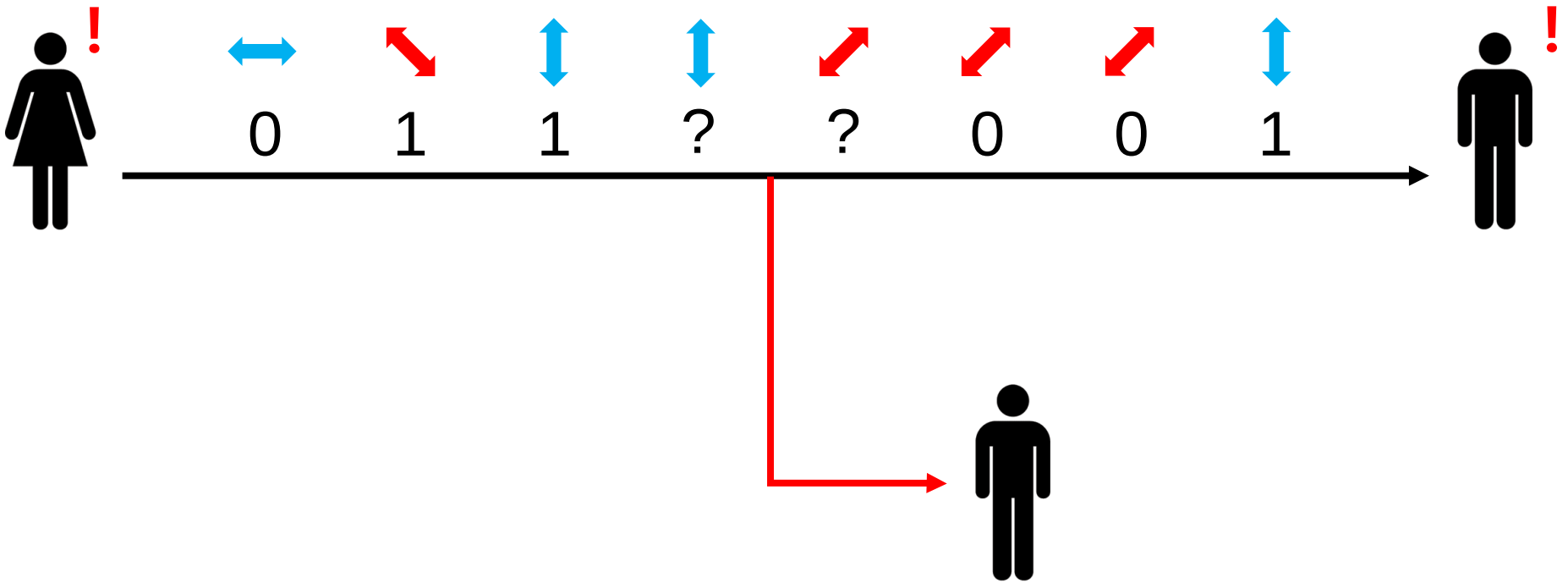
- 양자 에러 비트율이 급격하게 상승하면 도청된 것으로 판단



한성대학교 HANSUNG UNIVERSITY

04. 제안 공격 기법

- 지속적인 양자채널 관측을 통해 QBER를 상승
- 사용자간 키 분배가 정상적으로 이루어질 수 없음



03

결론

한성대학교
HANSUNG UNIVERSITY

01. 결론

- 양자 채널 상에서 스니핑 공격은 가용성 침해로 분류될 수 있음
- 통신 채널 자체를 보호할 수 있는 수단이 필요함

한성대학교
HANSUNG UNIVERSITY

Thank you

한성대학교
HANSUNG UNIVERSITY