양자암호통신의 이해 및 산학연 협력방안

함병승 교수
(bham@gist.ac.kr)

광주과학기술원
전기전자컴퓨터공학부/광양자정보처리센터

2018 양자정보통신기술 국제컨퍼런스
광주 이노비즈센터 대강당
2018.12.12(수)

통신보안

'5G 화웨이 딜레마'...통신 3사 "가성비 따지면 쓰긴 써야 하는데"

조선비즈 안별 기자

입력 2018.09.04 08:03

SK텔레콤, KT, LG유플러스 같은 통신 3사가 9월 5세대(G) 통신 장비 선정 발표를 앞두고 고민이 한창이다. 기술력도 괜찮고 값도 [illegible] 싶지만 공식 발표할 경우 후폭풍이 만만찮다. '보안' 이슈도 있고, 중국산 장비를 기간 통신망에 쓴다는 부담도 크다.

"나라 팔아 먹은 LG유플러스 불매 운동을 해야 한다"는 주장이 나왔을 정도다.

SK텔레콤 직원들이 서울 강남구 테헤란로의 한 건물에서 5G 중계기 성능을 테스트하는 모습. /SK텔레콤 제공

양자암호의 목적은?

- 무조건적 보안이 담보된 정보통신을 위해서!

무조건적 보안은?

- 양자역학의 복제불가원리에 기초!

복제불가 원리란?

- 구분불가성 (무작위성)!

? ? ?

- 통신의 기본원리:
  - 구분성 ('0' or '1')

Internet

디지털
(결정적)

'0'; '1'

중첩/얽힘
(확률적)

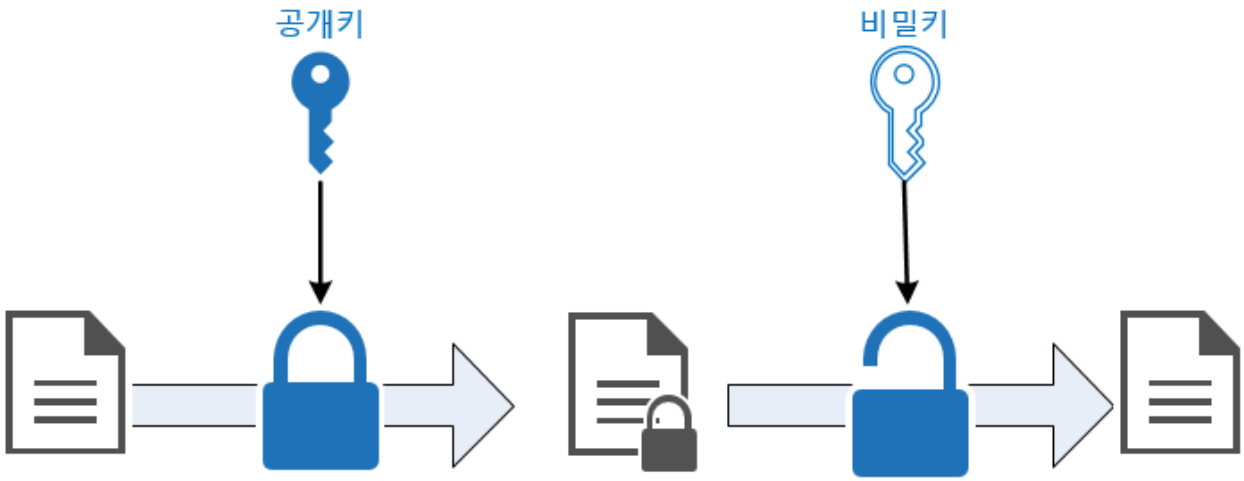
$$\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |1\rangle_B - |1\rangle_A \otimes |0\rangle_B)$$

- 인터넷: 컴퓨터+ 통신
- 양자인터넷: [양자컴퓨터+ 양자통신] → 양자얽힘쌍 필수!

양자암호키분배(QKD)

현대암호체계: Symmetric vs. Asymmetric

RSA: $\exp\left(\left(\sqrt[3]{\frac{64}{9}}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)$ ← 효율적 해킹 알고리즘 존재

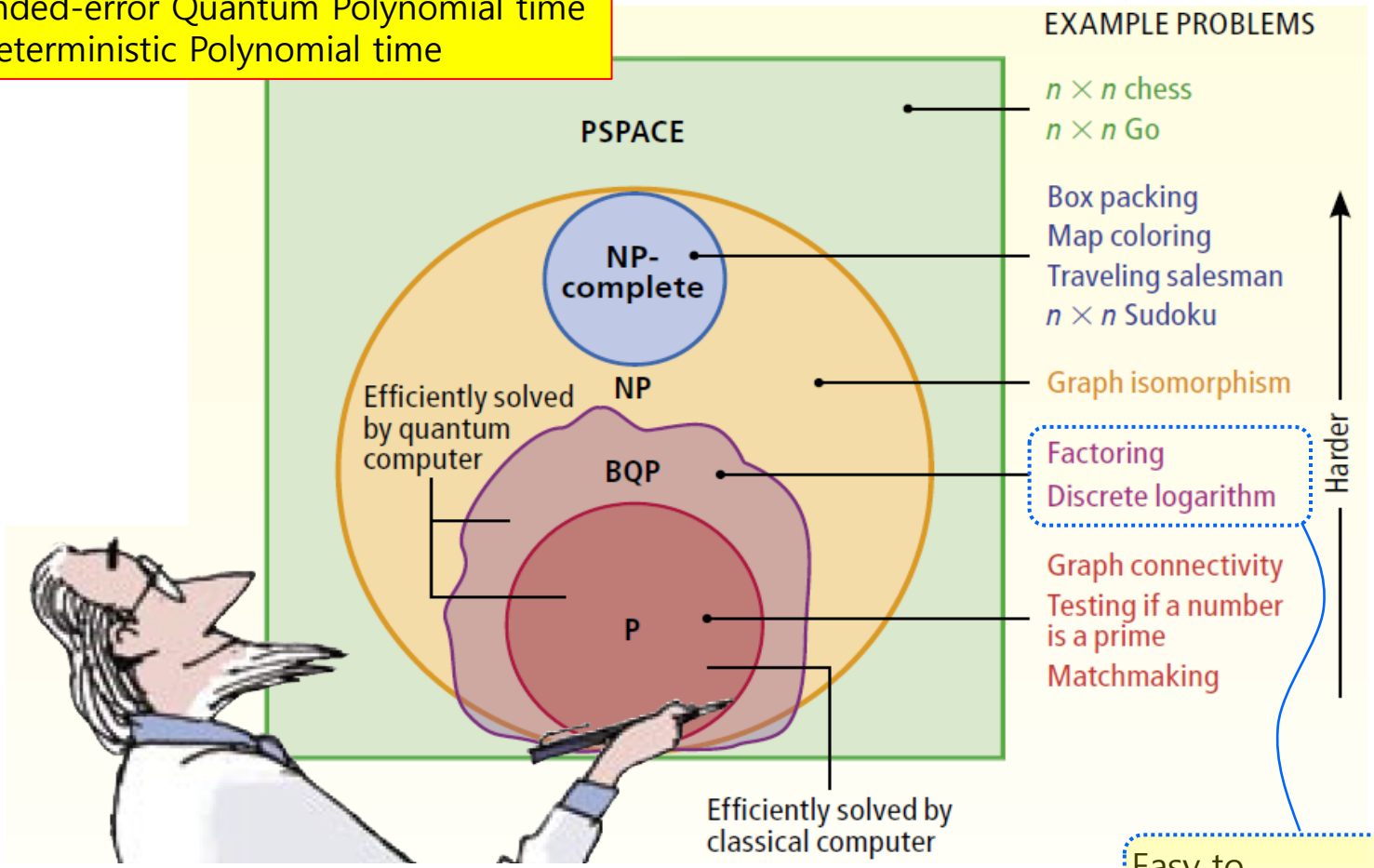


- RSA1024/2048:
  - If you can solve RSA1024 in 10 seconds, it takes 1200 years to solve RSA2048.

- 무조건적 보안? No!

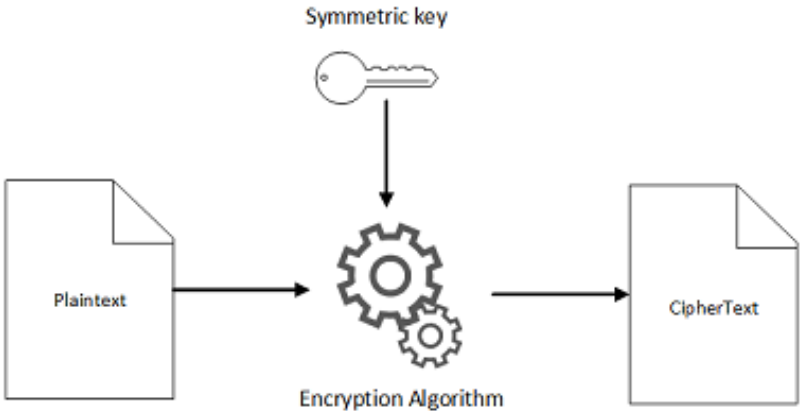
공개키암호 보안: NP complexity

BQP: Bounded-error Quantum Polynomial time
NP: Nondeterministic Polynomial time

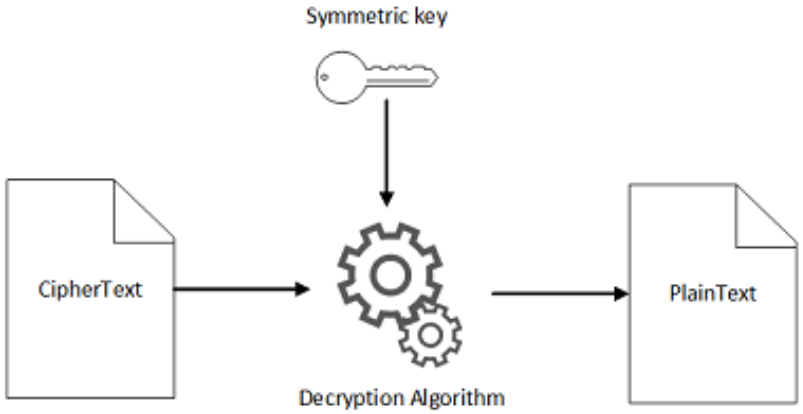


Easy to Quantum Computer

현대암호체계: Symmetric vs. Asymmetric



[암호]



[복호]

```
    H      E      L      L      O  message
 7 (H)  4 (E) 11 (L) 11 (L) 14 (O) message
+23 (X) 12 (M)  2 (C) 10 (K) 11 (L) key
=30     16     13     21     25     message + key
= 4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) (message + key) mod 26
    E      Q      N      V      Z  → ciphertext
```

```
    E      Q      N      V      Z  ciphertext
 4 (E) 16 (Q) 13 (N) 21 (V) 25 (Z) ciphertext
-23 (X) 12 (M)  2 (C) 10 (K) 11 (L) key
=-19    4      11     11     14     ciphertext - key
= 7 (H) 4 (E) 11 (L) 11 (L) 14 (O) ciphertext - key (mod 26)
    H      E      L      L      O  → message
```

- One-Time-Pad (**OTP**)
  - 암호키 길이는 최소한 데이터와 같아야 한다.
  - 암호키는 딱 한번만 사용해야 한다.

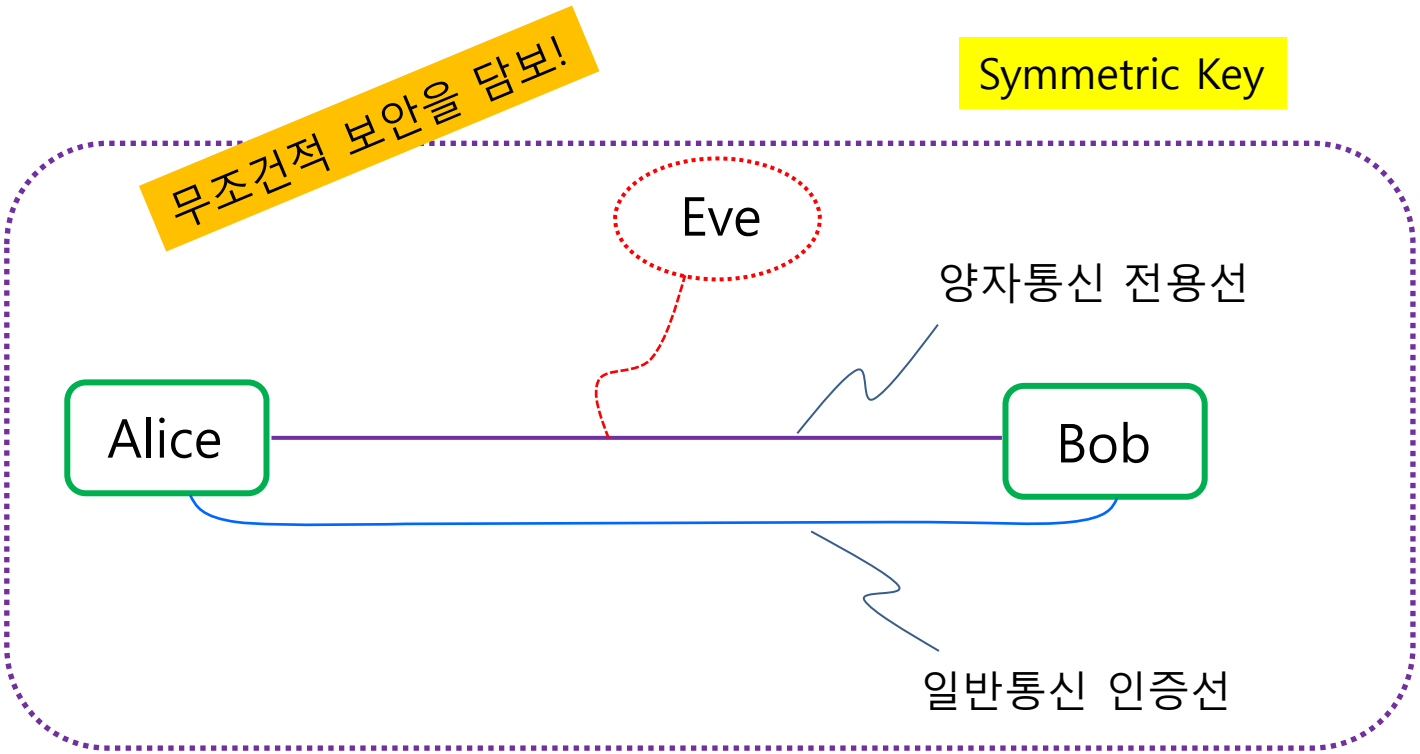
- **암호키 분배는 어떻게 할 것인가?**

⇩

양자암호키분배

양자암호키분배(QKD) 개요

- 양자암호(QKD)
  1. BB84
  2. B92
  3. E91
  4. cv
  5. …



- **양자암호의 무조건적 보안**: 양자역학의 **복제불가(no cloning) 원리**

복제불가원리: Wootters and Zurek, "A single photon cannot be cloned," *Nature* **299**, 802-803 (1982).

복제불가 원리: no cloning theorem

- 복제불가 원리:
  - 임의의 양자상태는 복제할 수 없다.

  → Unknown **nonorthogonal** quantum states satisfying commutation relationship

- 측정:
  - 고전(디지털/아날로그): 결정적
  - 양자(quantum): 확률적 ← 불확정성 원리: $[x, p_x] = i\hbar$ (Non commuting)

    1. Quantum: nonorthogonal(비직교) states
    2. Classical: orthogonal(직교) states

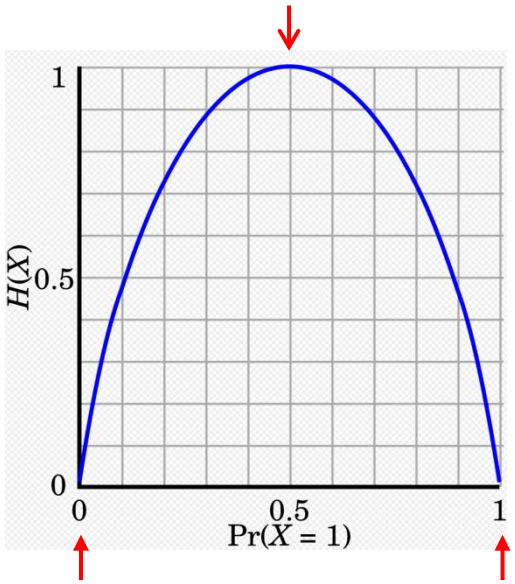
양자정보는 복사가 불가하다!

정보이론과 불확정성 이론 개요

- **불확정성 이론**: canonical commutation 관계를 만족하는 물리상수 두 개중 하나를 정확하게 측정하려 하면 다른 하나는 더 부정확하게 측정됨

  ex: $(\Delta x)(\Delta p) \geq \frac{\hbar}{2}$

- **엔트로피**: Shannon의 확률에 기초한 정보이론
  - $H(X) = -\sum_{i=1}^{n} P(x_i)\log[P(x_i)]$
  - **Perfect randomness**: No information

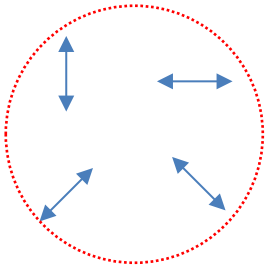


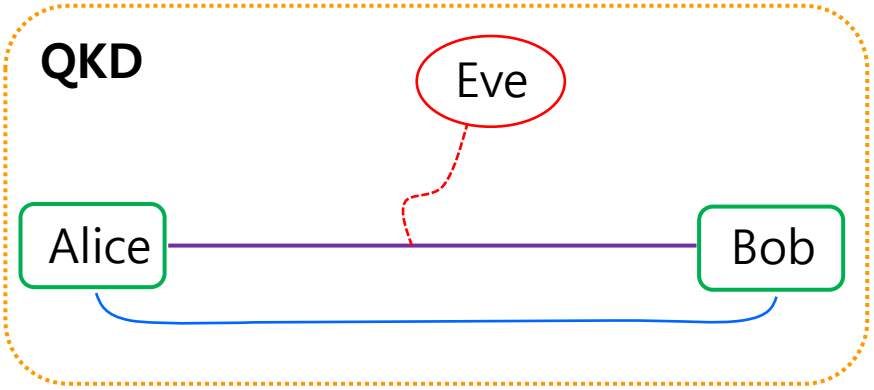
구분불가성

- 해석:
  - 확률(H)이 높다는 것은 정보가 적다는 뜻으로써, **확률 0.5**는 더 이상의 정보가 없다는 뜻.
  - 확률 0의 의미는 최대정보를 뜻한다. 즉 양자역학의 pure state.

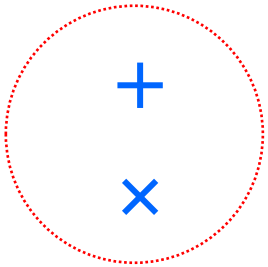
불확정성 원리와 기저쌍 선택

빛의 편광





편광필터: (측정 기저)



Alice (송신자)		Eve (도청자)			
		Basis(기저): +		Basis(기저): ×	
bit	편광	측정확률			
		↑	→	↗	↖
0	↑	1	0	0.5	0.5
1	→	0	1	0.5	0.5
0	↗	0.5	0.5	1	0
1	↖	0.5	0.5	0	1

Q. 동일한 정보를 반복측정한다면 도청가능한가?
A. 그렇다! → 메모리 도청

↓

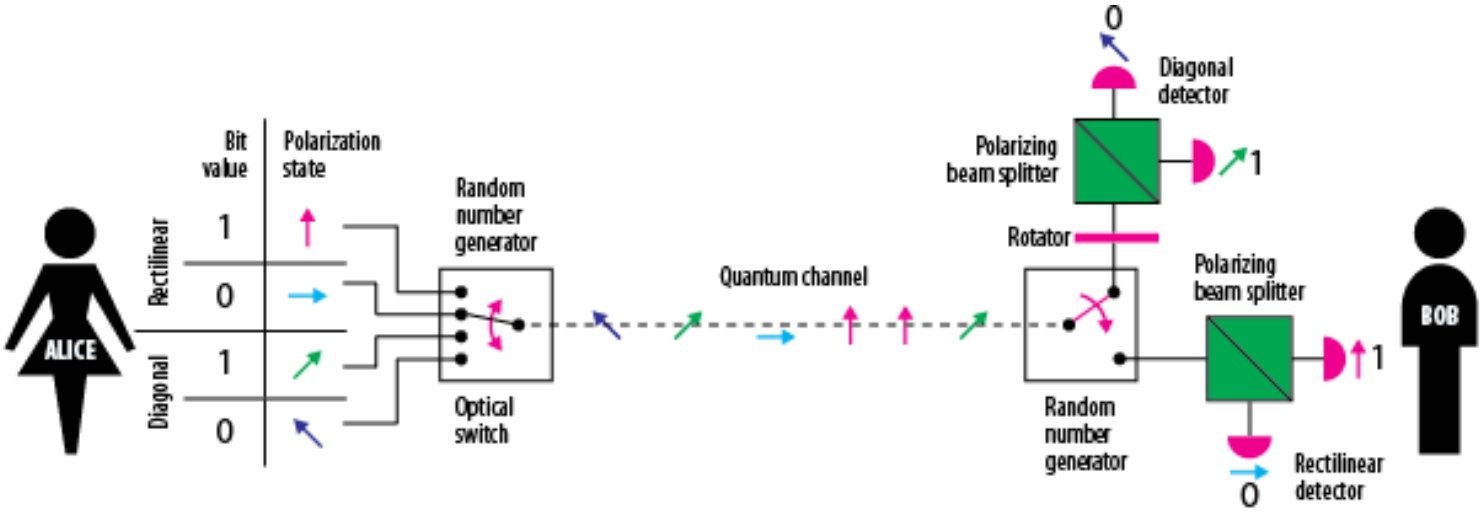
복제불가원리에 의해 원천차단

불확정성 원리 — QKD (BB84)

(Δx) ---------- +

(Δp) ---------- ×

BB84



Quantum transmission & detection	ALICE sends photons	↖	↗	→	↑	↑	↗	↖	↑
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events	↑	↗	↖	↑	↗	↗	↖	↖
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made	Rect	Diag	Diag	Rect	Diag	Diag	Diag	Diag
	ALICE tells BOB which bits to keep		✔		✔		✔	✔	
	ALICE and BOB's shared sifted key	–	1	–	1	–	1	0	–

비직교성 vs. 구분불가성

[양자버전]

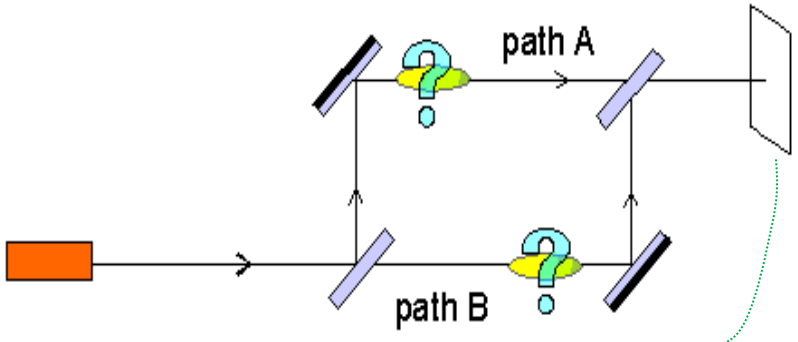
- QKD (BB84)

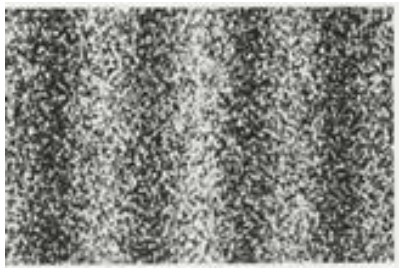
불확정성 원리	QKD (BB84)
(Δx)	+
(Δp)	×

[비직교성]

[고전버전]

- 동전던지기
- 경로중첩: 구분불가성(indistinguishability)





[경로구분 불가성]

무조건적 보안 = 구분불가성(무작위성)

무조건적 보안과 양자상태

- 양자역학의 복제불가원리는 불확정성 원리에 기초한다.
- 불확정성 원리는 서로 비직교상태를 나타내는 변수쌍에 적용된다.
- 비직교상태를 QKD에서는 편광/위상 기저쌍으로 구현

Q. 고전적 빛을 사용해서 복제불가원리를 구현할 수 있는가?

A. 그렇다. 이미 가우시안 연속변수 QKD가 증명되어 있다.

Q. 현재 광통신과 동일한 신호로 무조건적 보안암호를 구현할 수 있는가?

A. 그렇다. 복제불가원리 대신 측정무작위성을 이용 고전적 무조건적 보안을 제시했다:
(BS Ham, arXiv:1807.04233; 1807.08126)

- **고전적 복제불가 원리의 예**:
  - 동전 던지기: 두 번째 동전은 첫번째 동전결과를 복제할 수 없다.
  - 영(Young)의 이중슬릿 실험: 한 경로상태를 정확하게 측정하면 다른 경로상태는 무작위적이다.

- 따라서, 무조건적 보안암호통신은 비고전적 광원에 있는 것이 아니라, 불확정성 원리를 만족하는 복제불가원리 즉 무작위성에 있다.

양자암호키분배의 현실적 한계

- 현재 양자암호의 한계
  1. 불완전한 검출기 → 검출기 함정 → **무조건적 보안은 불가!**
  2. 양자리피터 부재로 장거리 전송 불가
  3. 매우 낮은 키분배율(QBR): <Mbps (10 km 전송거리); OTP 불가
  4. 다중 네트워킹 한계: 다중얽힘 광자쌍 필요

- BB84 양자암호의 적용가능성

  - 기존 RSA보다 보안강화된 단거리 일대일 보안시스템 적용

향후전망:

- 현재 광통신/무선통신 네트워크와 호환가능하며 장거리 전송과 초고속 키분배가 가능한 암호체계 추구

⇩

산학연 연구협력의 당위성

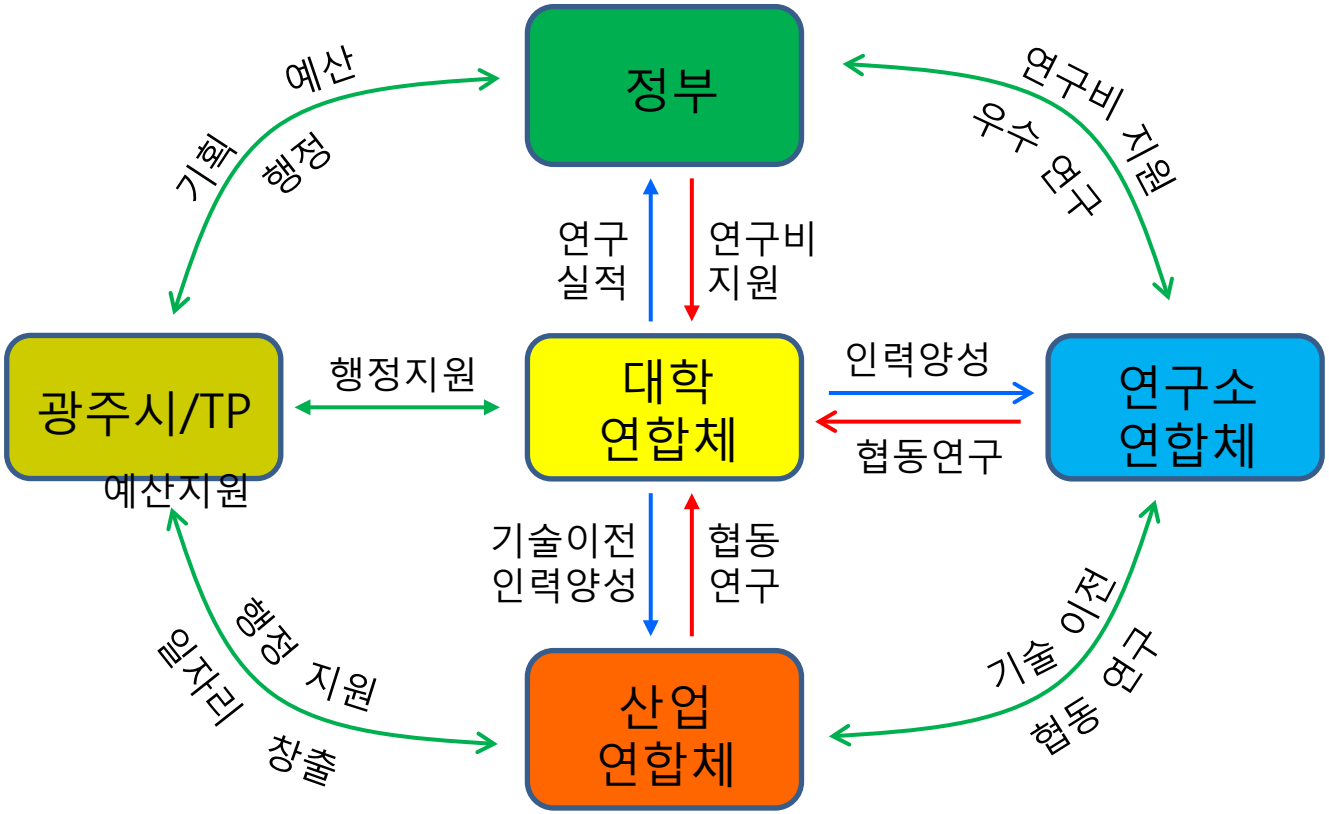
- 광통신
- 무선통신
- 광소자
- 인공지능
- IoT
- 무인자동차
- 국방

양자정보분야 지원: 선진국사례

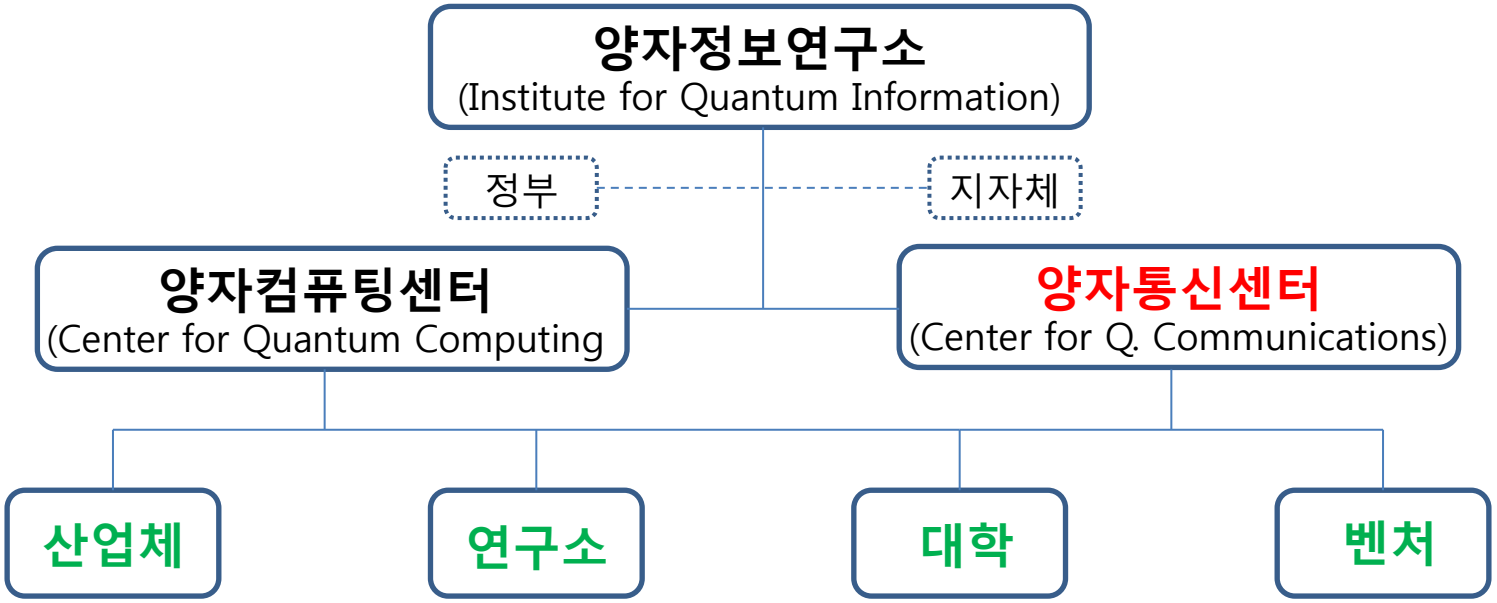
- 중국: Quantum Information Center (10조원)
- 유럽: Quantum flagship (10년 1.2조원/10년)
- 미국: DARPA(2012); IRAPA (2017), → 10Gbps for >1,000km
  IBM/NASA/Google/MS 등 (산업체) → 1 logic qubit
- 캐나다: 워털루대학(Inst. Quantum Computing, 2002년 발족, 30명 교수진, 50명 포닥, 125명 학생)
- 싱가포르: 싱가폴대학 (Center for Quantum Tech, 100명 연구진, 200억원/연)
- 네덜란드: Delft대학(QuTech; Quantum internet 목표)
- 영국: Q. Tech. Hub(350억원/5년; quantum comm.)

한국:
- 연구재단, 개인과제 다수
- 과기부(2차관), SKT 컨소시엄(2015~2019, 150억원/4년)
- 과기부(1차관), 양자컴퓨팅/양자소자(2019~, 950억원 예상)
- 과기부(2차관), 양자통신(예타준비중)

산학연 컨소시엄: 제안(구성)



산학연 컨소시엄: 제안(조직)



연구구제(안):

1. 양자컴퓨터
2. 양자인터페이스(양자리피터: 10G/1,000km)
3. 양자암호(유선: 10G/1000km), 무선, 공중, 우주, 바다)

산학연 컨소시엄: 제안(중소/벤처산업)

산업분야 (IDQ 제품 외):

- ps pulsed laser
- Quantum correlation analysis software
- MZI phase stabilizer (MZI: Mach Zehnder Interferometer)
- MZI phase controller
- MZI channel analysis software
- Photon counter
- Random number generator
- Optical switch/MUX/DeMUX etc.
- AWG
- Fiber connectors, splitters, etc.
- Fiber, multicore single mode
- Laser controller
- QKD simulation software
- Network analyzer
- 광학설비/부품 일체
- Transponders
- Fast photodiodes
- etc.

결론

- 양자암호통신의 핵심은 불확정성 원리에 기초한 복제불가원리에 있다.
  양자암호키분배 프로토콜은 불확정성 원리를 만족하는 기저상태 쌍을 이용한다.
  현재 양자암호(BB84)는 단일광자의 편광이나 위상기저쌍을 이용한다.
- 양자암호키분배의 현실적 문제는 측정기의 불완전성으로 인한 정보누설에 있다.
  따라서, 양자암호의 현실적 의미는 고전암호에 비해 **강화된 보안통신**이다.
- 그러나, 복제불가원리는 비고전적 양자상태에 한정되지 않는다.
  즉, 양자암호통신에 사용되는 키가 비고전적(양자)일 필요는 없다.

⇩

양자암호통신은 현재진행형이며, OTP를 만족하는 새로운 QKD 개발은 복제불가원리를 만족하면서도 기존 통신시스템과 호환가능해야 한다.

⇩

양자정보분야의 국가적인 연구인프라 구축은 이미 세계적인 대세이다. 지난 20여년간의 국가연구개발사업을 경험삼아, 먹튀방지와 더불어 우수연구 선발 및 지원을 위한 정책은 세계적 스펙(현재 기술로 불가능) 이상을 조건으로 하는 Top down 방식이어야 할 것이다.