	지스트(광주과학기술원) 보도자료 http://www.gist.ac.kr	
보도시점	배포 즉시 보도 부탁드립니다.	
배포일	2021.02.22.(월)	
보도자료 담당	홍보팀 조동선 팀장	062-715-2061
	홍보팀 이나영 선임행정원	062-715-2062
자료 문의	전기전자컴퓨터공학부 함병승 교수	062-715-3502

지스트, 차세대 절대 보안통신기술 순수 국내기술로 최초 선점

- 2020년 제안된 무조건적 보안을 담보하는 고전암호통신(USCKD) 기초 최초로 실험검증 수행

- 미래 자동 주행 및 비행에 필수적인 절대보안 유무선 통신기술에 적용 기대

□ 지스트(광주과학기술원, 총장 김기선) 전기전자컴퓨터공학부 함병승 교수(지스트 광양자정보처리센터장)는 통신에 있어 무조건적 보안을 담보할 차세대 고전암호통신* 프로토콜에 대한 최초의 기초실험을 수행하여 검증했다.

* **고전암호키분배(USCKD)**: QKD수준의 무조건적 보안을 보장하는 2020년 국내기술진에 의해 제안된 방식으로써 기존 통신장비 및 선로와 온전히 호환되고, 양자화된 키나 양자선로가 불필요하여 QKD의 양자함정으로부터 자유롭고, 무엇보다도 고전적 선로해킹을 이중 선로의 양자중첩원리에 의해 도청은 허용하되 암호해독은 원천적으로 차단되는 차세대 암호통신 프로토콜.

◦ 이로써 기존 복제불가 원리에 기초하는 양자키분배* 방식과는 달리 기존 통신장비 및 시설과 온전히 호환되며 무조건 보안을 담보하는 차세대 보안통신기술을 순수 국내기술로 선점하였다.

* **양자키분배(QKD)**: 양자역학의 복제불가원리에 기초하여 양자화된 키(큐빗)에 대한 보안을 양자선로에서만 담보하나, 기존 통신선로 및 장비와 호환되지 않고 무조건

적 보안은 양자함정(quantum loophole)으로 인해 조건부로 달성.

□ 함병승 교수는 2020년 자체개발한 무조건적 보안 고전암호키분배 프로토콜을 최초로 실험적으로 증명하여 고전통신 장비 및 시설을 이용한 무조건적 보안통신 실용화에 중요한 초석을 마련하였다.

◦ 본 연구에서 검증한 USCKD 고전암호통신 기술은 무엇보다도 현재 상용시스템과 호환되며, 무조건적 보안성을 단일광자가 아닌 고전광원 즉 레이저로 달성하고 현재까지 유일한 절대보안 방식인 QKD 양자키분배를 이중 선로중첩에서 확보한 차세대 보안통신에 관한 것으로 그 기대효과가 크다.

□ 기존 양자암호통신에서는 절대보안 원리가 양자화된 신호의 복제불가 원리에 있었다면 이번 연구에서는 절대 보안을 신호의 양자화가 아닌 채널의 양자화(양자중첩)에서 확보하였고, 키분배 과정이 양자메모리 원리와 동일하게 확정적이며 암호키 생성/교환 속도가 원리적으로 기존 통신데이터 전송속도와 비슷한 수준이기에 인류의 염원인 원타임 패드(One-Time-Pad, OTP)를 실현할 절대보안 통신방법으로 평가된다.

◦ 무엇보다도 본 연구에서 제안한 절대보안 암호통신기술은 기존 광통신은 물론 무선통신 기기·시설과도 호환적이기에 기존 통신선로를 그대로 이용하여 QKD수준의 무조건적 보안성을 확보하고, QKD와는 달리 복제/스위칭/라우팅에서 자유로워 고전컴퓨터가 주축인 현재 인터넷에 그대로 적용가능하다.

□ 함병승 교수는 “종래 어떠한 방법으로도 불가능한 고전적 절대보안통신을 담보할 새로운 방식의 고전암호키분배 기술을 세계 최초로 선행 검증하였다”면서, “향후 국방망, 행정망, 금융망은 물론 원격 의료를 위한 의료 데이터 전송이나 원격 강의를 위한 교육망, 그리고 미래 자동 주행 및 비행에 필수적인 절대보안 유무선 통신기술이 적용되기를 기대한다”고 말했다.

◦ 이번 연구결과는 네이처(Nature) 자매지인 사이언티픽 리포츠(Scientific Reports)에 2021년 2월 18일(목) 온라인으로 게재됐다.

논문의 주요 내용

1. 논문명, 저자 정보

- 논문명 : Experimental demonstrations of unconditional security in a purely classical regime
- 저널명 : Scientific Reports
- 저자 정보 : 함병승 (Ham, Byoung S.)

용 어 설 명

1. 무조건적 보안

○ 고전(암호)통신에서는 무조건적 보안이 원천적으로 불가하여, 해킹으로 인한 정보유출은 피할 수 없는 한계이다. 무조건적 보안을 위해서는 Shannon의 정보이론에 따라 동전 던지기와 같은 무작위성이 확보되어야 하는데, 이와 같은 무작위성을 무조건적으로 안전하게 전송/교환할 방법은 양자암호키분배가 유일하다. 현 고전 보안체계에서는 컴퓨터가 해결하기 어려운 복잡성, 예를 들면, 소인수분해 계산원리를 차용한 공개키방식 등으로 조건적 보안성을 충족한다.

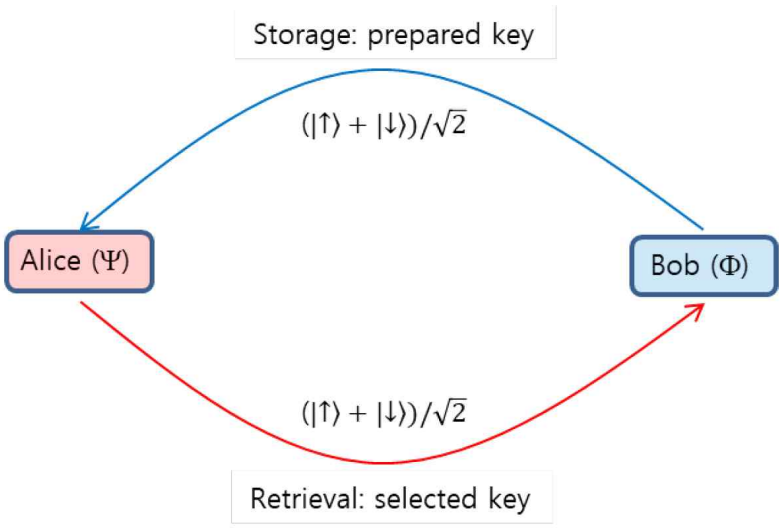
2. 양자암호키분배(QKD)

○ 양자암호는 양자신호의 복제불가원리에 기초하여 원리적으로 무조건적으로 안전한 키분배 방식이다. 그러나 양자암호 구현에 있어 양자함정으로 인해 완벽한 무조건적 보안은 현실적으로 불가하기에 키 전송속도를 조절하여 조건적 무조건성을 추구한다. 또한, 양자키 전송거리는 양자함정으로 인해 극히 제한적이고, 장거리 통신을 위한 양자반복기는 없으며, 다자간 키분배는 고난도 다자간 얽힘광원이 필요하기에, 사실상 장거리 양자인터넷은 요원하다.

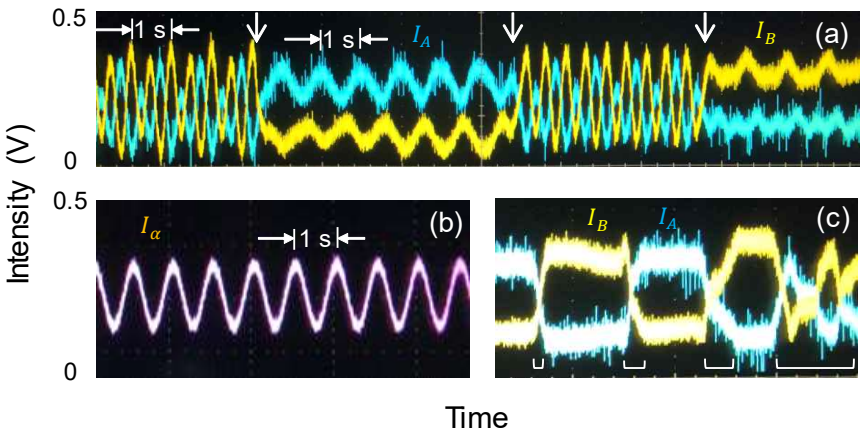
3. 무조건적 보안 고전암호키분배(USCKD)

○ 본 고전양자키분배 기술은 양자신호가 아닌 고전신호를 기반으로 이중 선로를 사용하며 무조건적 보안은 선로중첩으로부터 확보하는데, 이는 통상적으로 마하젠거 간섭계의 거시양자중첩에 해당한다. 따라서, USCKD는 무엇보다도 현재 통신장비 및 시설과 호환되기에, 장거리 통신을 위한 별도의 양자반복기나 인터넷을 위한 다자간 얽힘광원쌍도 필요하지 않으며 양자함정도 없다.

그 림 설 명



[그림1] 마하젠더 간섭계를 자유공간으로 구성하는 무조건적으로 안전한 무선 고전암호통신



[그림 2] 무조건적 보안 고전암호통신(USCKD) 실험증명. (a) 그림 1에 있어 USCKD와 CBW(양자드브로이파)를 이중 마하젠더 위상통제로 증명. (b) 고전적 마하젠더 간섭계 출력신호주기 한계로써 (a)의 CBW에서는 그 주기가 반으로 줄어들어 양자성을 증명함. (c) 암호키(0/1) 선택으로 인한 키분배 확정성 실험. 양자간 동일 암호키면 출력이 +1, 반대 암호키면 -1이 되어 QKD에서 필수불가결한 요소인 sifting없이도 키분배가 양자간 자동확정됨.