GIST	**지스트(광주과학기술원) 보도자료** http://www.gist.ac.kr	
보도시점	한국시간 2020.7.15.(수) 오후 6시 부터 보도하여 (국제엠바고 영국시간 7.15. 오전 10시) 주시기 바랍니다.	
배포일	2020.07.15.(수)	
보도자료 담당	홍보팀 김효정 팀장	062-715-2061
	홍보팀 이나영 선임행정원	062-715-2062
자료 문의	전기전자컴퓨터공학부 함병승 교수	062-715-3502

지스트 함병승 교수, 새로운 절대 보안 암호통신 기술 확보

- 기존에 불가능한 절대 보안이 담보되는 새로운 방식의 암호키분배 기술 세계 최초 확보
- 향후 국방망, 행정망, 금융망은 물론 의료 데이터 전송이나 원격 강의를 위한 교육망 등 다양한 보안 분야에 적용 기대

□ 지스트(광주과학기술원, 총장 김기선) 전기전자컴퓨터공학부 함병승 교수(지스트 광양자정보처리센터장)가 양자암호키 분배 기술을 전면 대체할 수 있고, 전송 거리에 상관없이 기존 광통신 네트워크와 호환되는 새로운 절대보안 암호통신 프로토콜을 제시하였다.

◦ 함병승 교수는 기존 양자암호통신에서 필수적인 양자화된 신호, 양자채널, 양자검출기의 세 가지 요소를 완전히 배제함은 물론, 전통적 고전 암호통신 방법과 호환되는 수준에서 무조건적 정보통신 보안성을 확보하였다.

□ 양자암호키분배(QKD; Quantum Key Distribution)는 양자 통신을 위해 비밀 키를 분배·관리하는 기술로, 1984년 최초로 제시된 이후 지난 36년 동안 연구되어 온 무조건적으로 안전한 암호통신을 위한 양자기술*이다. 그러나 양자신호, 양자채널, 양자검출기의 불완전성으로 인해 무조건적 보안 확보**는 현실적으로 불가하다. 무엇보다도 절대 보안을

위해 양자키는 재사용이 불가하므로 시내 금융/행정 전산망 적용에도 어려움이 있다.

*양자기술(quantum technology): 더는 쪼갤 수 없는 양자적 특성을 정보통신 분야에 적용해 보안, 초고속 연산 등을 통해 기존의 정보통신에서 한 걸음 나아간 차세대 정보통신기술이다.

**무조건적 보안(unconditional security): 고전암호통신에서는 무조건적 보안이 원천적으로 불가하여 해킹 문제가 빈번한 사회 이슈가 된다. 무조건적 보안을 위해서는 Shannon의 정보이론에 따라 동전 던지기와 같은 무작위성에서만 확보되어야 한다. 문제는 이와 같은 무작위성을 전송/교환할 방법으로는 현재까지는 양자암호키분배가 유일하다.

□ 본 연구는 양자암호키 생성/교환 기술에 기초한 기존 양자암호는 물론 공개키 방식 등 전통적 고전암호를 대체하는 무조건적 보안성을 보장하는 새로운 암호통신 기술에 관한 것으로 기존 고전암호 통신처럼 일반 채널을 통신 선로로 하고 고전적 신호를 열쇠로 사용하되, 양자암호와 같이 절대 보안을 담보하므로 그 파급력은 엄청날 것으로 기대된다.

◦ 기존 양자암호통신에서는 절대보안 원리가 양자화된 신호의 복제불가원리에 있었다면 이번 연구에서는 절대 보안을 신호의 양자화가 아닌 채널의 양자화(양자중첩)*에서 확보하였고, 키분배 과정이 광메모리 원리와 동일하게 확정적이다. 또한 암호키 생성/교환 속도가 광통신 데이터 전송속도와 비슷한 수준이기에 인류의 숙원사업인 일회용 암호(One Time Pad), 즉 정보의 직접 절대 보안 통신을 구현하는 데 적용 가능하다.

*양자중첩은 영(Young)의 이중슬릿 실험에서 나타나는 빛의 간섭으로서 결맞음 특성 중 하나인데, 한쪽 혹은 양쪽 선로에서 데이터 도청은 허용하되 도청된 데이터의 해독은 불허하는 원리에 따라 데이터 전송의 무조건적 보안성은 원리적으로 담보된다.

□ 함병승 교수는 “이번 연구성과는 종래 어떠한 방법으로도 불가능한 절대 보안이 담보되는 새로운 방식의 암호키분배 기술을 세계 최초로 확보하였다는데 가장 큰 의의가 있다”면서, “향후 국방망, 행정망, 금융망은 물론 원격 의료를 위한 의료 데이터 전송이나 원격 강의를 위한 교육망 등 다양한 보안 분야에 적용될 수 있기를 기대한다”고 말했다.

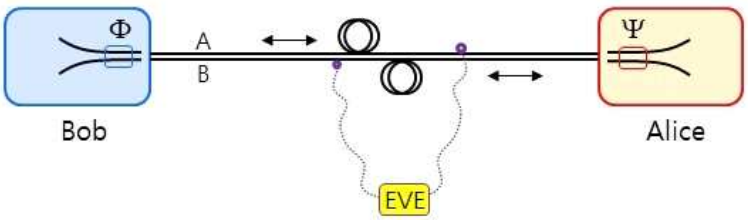
◦ 연구 결과는 네이처(Nature) 자매지인 사이언티픽 리포츠(Scientific Reports)에 2020년 7월 15일 온라인으로 게재됐다. 〈끝〉

논문의 주요 내용

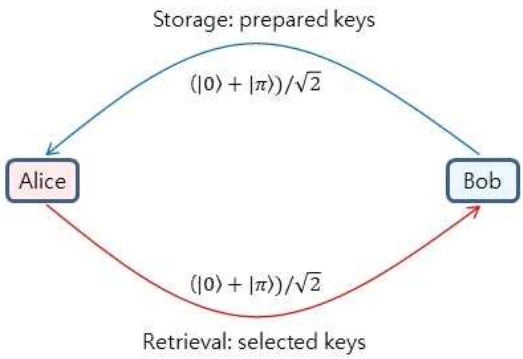
1. 논문명, 저자 정보

- 논문명 : Unconditionally secured classical cryptography using quantum superposition and unitary transformation
- 저널명 : Scientific Reports
- 저자 정보 : 함병승 (Ham, Byoung S.)

그 림 설 명



[그림1] 마하젠더 간섭계를 이중선로로 하는 무조건적으로 안전한 고전암호통신



[그림 2] 무조건적 보안성을 담보하는 그림 1의 양자역학적 해석