연수 제안서

연구 분야	양자인증 시스템 구현
연구 과제명	양자암호 네트워킹 핵심기술 개발
연수 제안 업무	1. QKD 시스템 기반 양자인증 프로토콜 설계 2. 양자암호 네트워크 가입자를 검증하기 위한 양자개체인증 구현

○ 연구 필요성
- 양자 키 분배(Quantum key distribution, QKD) 프로토콜로 대표되는 양자암호는 기밀성만 제공하기 때문에 중간자 공격(Man in the middle attack)에 취약함
- 이러한 양자암호의 취약점을 보완하는 것이 양자인증 기법이나 아직까지 이론 연구에 머물러 있는 실정임
- 그러므로 양자암호 시스템에 실제 적용 가능한 양자인증 프로토콜의 개발은 관련 연구에서 중요한 주제임
- 특히, 양자암호가 네트워크로 확장 되었을 때 다수의 가입자들을 검증하는 양자인증 프로토콜은 필수적임

○ 연구 주요 내용
- Time-bin encoding과 phase encoding을 이용하는 양자인증 프로토콜 개발
- 1xN 양자암호 네트워크 가입자망을 검증하는 다자간 양자개체인증 프로토콜 구현
- 양자 랜덤 오라클을 이용한 양자인증 프로토콜의 안전성 분석

○ 지원자격 및 혜택
- 전자, 전산, 제어, 통신, 수학, 물리 전공자
- 양자광학 시스템 경험자
- 국내외 논문 발표 및 워크숍 참여지원
- 각종 연구 및 교육 프로그램 지원

소속 부 서 : 양자정보연구단

연수 책임자 : 한상욱