

## [양식 3] 동아리 활동 계획서

### 암호 동아리 활동 계획서

#### 1. 주제

양자 컴퓨터 및 양자 내성 암호 연구

#### 2. 개요

양자 컴퓨터의 개념 및 원리를 이해하고 양자 내성 암호의 동향 및 특성들에 대한 학습

##### 양자 컴퓨팅 동향

국제적 대기업, 양자 컴퓨터 개발의 중요성을 파악하여 지속적인 연구 및 개발 중

##### 1. 마이크로 소프트

- 양자 컴퓨팅용 프로그래밍 언어 Q# 출시
- 통상적인 프로그래밍 개념을 양자 컴퓨팅 분야에 도입하는 것을 목적
- 양자 컴퓨팅 분야에서의 개발 환경 제공 중

##### 2. 구글

- 양자 컴퓨터 프로세서 72 큐비트 프로세서 개발
- 양자 우위를 실현하기 위한 개발

##### 3. IBM

- 50 큐비트 프로세서 개발 성공
- 양자 컴퓨터 'IBM Q' 개발하여 클라우드에 개방 중

##### 4. Intel

- 49 큐비트 프로세서 개발

##### 학습 내용

##### 1. 쇼어 알고리즘

- 소인수 분해 처리가 매우 효과적인 양자 알고리즘
- 현존하는 많은 공개키 암호 알고리즘을 뚫을 수 있음

##### 2. Grover 알고리즘

- 양자 알고리즘에 기반을 둔 알고리즘
- 주어진 함수의 특정 출력 값에 대응하는 입력 값 찾기 매우 용이

##### 3. 양자 프로그래밍

- 마이크로 소프트 Q# 학습
- 마이크로 소프트 양자 개발 키트 학습

##### 4. 양자내성암호

- NIST에서 다루고 있는 양자 내성 암호 알고리즘 연구
- Lattice, Code, Multivariate, Hash, etc

#### 3. 목적

- 양자 내성 암호 알고리즘 분석 및 연구를 통한 양자 컴퓨팅 시대에 대비
- 양자 프로그래밍에 대한 이해
- 기존 대칭키 암호 알고리즘의 한계점 파악

#### 4. 세부 추진사항 및 계획

##### 홍보 방안

- 학교 내 홍보 커뮤니티를 통한 동아리 홍보
- 동아리 홈페이지 운영을 통한 홍보 및 활동 기록
- 연구 내용 교육 영상 제작 및 공유를 통한 참여 유도
- 동아리 연구 기여도에 대한 투표 우승팀 소량의 회식비 지원

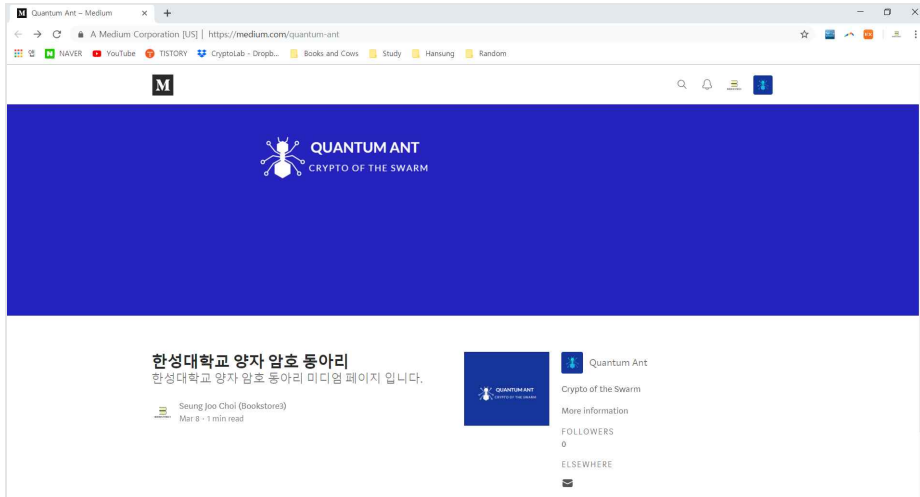
##### 동아리 운영

- 소규모 팀 단위 운영으로 동아리 회원 소외 방지
- 대학원생이 팀장이 되어 학부 연구생의 관리 및 소규모 연구 진행 후 결과 정리 및 발표
- 정보 보호 학회 저널을 통한 양자 컴퓨터 및 양자 알고리즘에 대한 자료 수집
- 월별 정기 세미나를 통한 연구 결과 및 진행 상황 발표

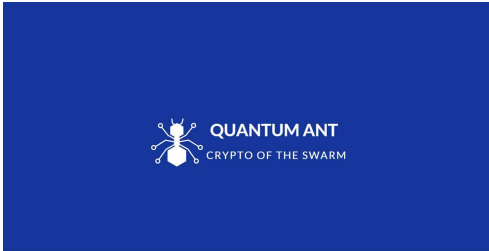
##### 예산 회비

비고	비용	인원 / 횟수	합계
정보보호학회			
회의비			
분기별 팀 회식비			
양자 암호 서적 및 강의			

## 연구실 홈페이지



## 연구실 로고



- 동아리 이름: Quantum Ant
- 동아리 로고 의미:  
개미는 양자와 같이 가장 작은 형태를 갖추고 있는 생명체이지만 다 같이 성실히 노력하여 큰일을 이루는 것과 같이 꾸준한 노력으로 동아리 인원 모두 함께 성과를 이뤄낼 수 있기를 바란다는 뜻
- 매월 세미나 후 각 팀별 연구 결과 종합 및 정리하여 연구실 홈페이지에 게시
- 동아리장이 홈페이지 운영 및 질의응답 관리

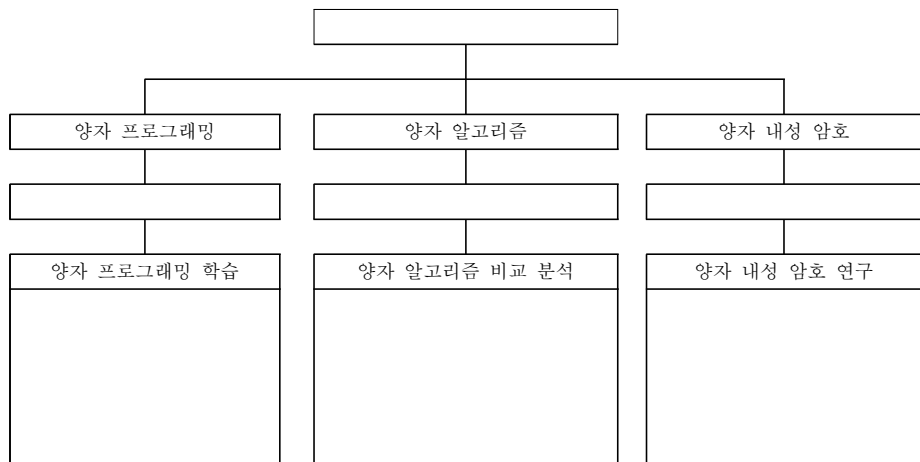
## 동아리 참여 인원

담당분야	성명	소속기관 (현 소속부서)	직위 (직급 분류)	최종학위 및 전공			활동 기간 (개월)	전문성
				학교	취득 년도	학위 (전공)		
동아리장				한성대 학교				블록체인
참여연구원				한성대 학교				양자알고리즘
참여연구원				한성대 학교				양자알고리즘
참여연구원				한성대 학교				어셈블리
학부연구생				한성대 학교				경량암호
학부연구생				한성대 학교				대칭키 암호
학부연구생				한성대 학교				형태보존암호
학부연구생				한성대 학교				VR 보안
학부연구생				한성대 학교				대칭키 암호
학부연구생				한성대 학교				대칭키 암호
학부연구생				한성대 학교				대칭키 암호
학부연구생				한성대 학교				대칭키 암호

### 연구원 수상실적 및 논문

- 2019년 정보보호학술논문발표회, 권용빈, 안규황, 권혁동, 서화정
- 2019년 한국정보통신학회, 권용빈, "Flexible Keypad를 활용한 보안 구현"
- 2019년 정보보호 전문가를 위한 암호 교육 수료 권용빈, 최승주
- 2018년 국가암호공모전 (특별상) 권용빈, 이정현, 임세진, 2-B 분야, "CCTV Cooperation System"
- 2018년 국가암호공모전 (특별상) 최승주, 이현우, 임지훈, 2-B 분야, "스마트 컨트랙트를 활용한 투명하고 신뢰받는 주유소 만들기"
- 2017년 국가암호공모전 (장려상) 양유진, 공승화, 전다형, 2-B 분야, "형태보존암호소개"

### 참여자 역할 분담



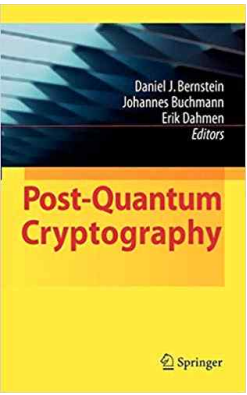
### 추진 전략

<b>양자 컴퓨팅 및 양자 알고리즘 연구</b>	
- 양자 관련 논문들 분석을 통한 양자 컴퓨팅 및 양자 알고리즘에 대한 학습	
- 각 팀별로 논문 정리해 발표 후 정리	
<b>양자 프로그래밍 학습</b>	
- 마이크로 소프트 Q# 문서 및 영상을 통한 양자 프로그래밍 학습	
- 양자 개발 키트를 사용한 양자 개발 환경 구축	
<b>양자 내성 알고리즘 분석</b>	
- Lattice, code, hash 등의 양자 내성 암호 알고리즘 분석	
- 해외 논문 연구 및 양자 내성 알고리즘 세미나 참석	
<b>보고서 작성</b>	

### 연구 결과물

비고	내용
보고서	중간보고서(양자 컴퓨터 최신 동향 및 양자 내성 암호)
	최종보고서(양자 내성 알고리즘 분석 및 양자 프로그래밍 실습)
연구실 홈페이지	매월 연구 결과 정리 후 게시
교육 영상	양자 내성 암호 알고리즘 교육 영상

학습 주요 교재

	제목	Post-Quantum Cryptography
	저자	Bernstein, Daniel J., Buchmann, Johannes, Dahmen, Erik
	가격	\$79.99
	출판사	Springer
	선정 이유	- 양자 세대의 알고리즘에 대한 상세한 설명 - 양자 내성 공개키 암호화 및 서명 시스템 설명 - Hash, Code, Lattice, Multi-variate 기반 암호학 설명

주요 연구기자재

품 명	규 격	수 량	용 도	보유 여부		소요금액 (단가×수량)	비 고
				유	무		
PC		10	연구 및 자료 분석용	10		1,300 x 10	한성대학교
프린트		2	프린트	2		500 x 2	한성대학교

월별 계획

활동분야	분기	1분기				2분기			3분기			4분기		가중치 (%)	비고
		3	4	5	6	7	8	9	10						
- 동아리 홍보 및 팀별 인원 및 세부주제 선정														10	
- 양자 컴퓨터 개념 및 양자 내성 알고리즘 동향 발표														10	
- 기존 대칭키 암호 알고리즘의 양자 알고리즘에 대한 내성 및 취약점 분석														15	
중간보고서 제출														10	
- 양자 내성 알고리즘 분석 및 양자 프로그래밍 실습														15	
- 연구 진행 발표 및 양자 암호 초청 세미나														15	
- 최종 연구 종합 및 교육 영상 제작														10	
최종결과보고서 제출														15	
분기별 진도(%)		10	25			40			25						
분기소요예산(천원)			1,000			1,000			1,000						