[양식 3] 동아리 활동 계획서

암호 동아리 활동 계획서

1. 주제 : 양자내성암호, 양자 알고리즘 연구 및 양자프로그래밍

2. 개요 : 양자 알고리즘과 NIST에서 진행하고 있는 Post Quantum Cryptography 공모전의 후보 알고리즘들에 대하여 학습하고, 양자프로그래밍이 가능한 ProjectQ 를 활용한 양자게이트 설계 및 구현

3. 목적
- 양자 후 시대를 준비하고 있는 암호학계의 연구동향 파악
- 양자관련 암호지식과 양자프로그래밍 연습
- 암호 동아리 스터디, 세미나를 통한 회원들 간의 자발적인 학습 및 즐거운 유대관계 형성
- 기존 암호를 대체할 새로운 양자내성 암호가 필요하다는 흥미로운 주제를 통한 암호 동아리 홍보 및 유치
- 다양한 암호 동아리 외부 활동 (암호경진대회, 설문조사, 한성대학교 학부생 대상 설명회 개최)
- 동아리 활동의 실질적인 결과물 배출 (학술대회 논문, 공모전 수상 등)

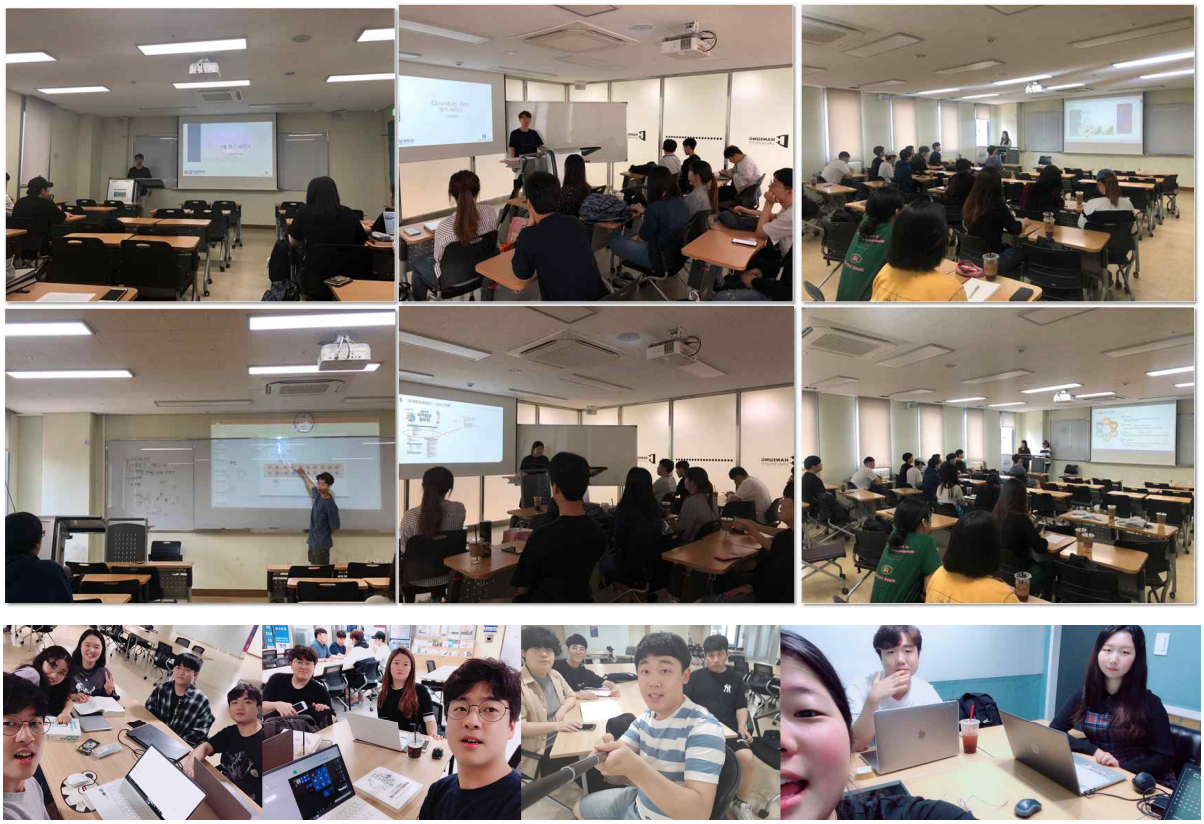
4. 세부 추진사항 및 계획

동아리 학습 계획

NIST PQC Round2 Algorithm
- 현재 Round2를 진행 중인 26개의 암호알고리즘 중 격자와 코드기반 중 몇가지 알고리즘을 중심적으로 학습(ClassicMcEliece, NTRU 등) - 해당 알고리즘의 키 공유, 암호화, 복호화를 이해하고 Reference 코드의 C 코드와 비교 학습
양자 알고리즘
- 해외 논문을 참조하여 양자 알고리즘을 활용한 암호 공격 동향 파악 및 리뷰
양자 프로그래밍
- IBM에서 제공하며, 파이썬을 사용한 양자 프로그래밍이 가능한 툴 ProjectQ 사용 - 양자프로그래밍을 통한 Grover, Shor 알고리즘의 학습 및 구현 (예제코드 활용) - 덧셈, 곱셈, 모듈러와 같은 핵심연산을 설계한 양자게이트 학습 및 프로그래밍
세미나 진행 및 피드백

학습 방법 및 진행사항
- 3~4명으로 구성된 팀 단위의 동아리 활동 진행, 각 팀별 세부주제를 선정하여 연구 및 학습
- 기존 동아리 회원은 양자관련 심층적인 학습, 신입 회원의 경우 보안 관련 기초 학습 병행 또한 가능
- 월별 팀 단위의 정기 세미나를 통한 학습결과 발표 및 피드백, 세미나 발표 자료는 유투브 및 동아리 홈페이지에 업로드 함으로써 결과를 남김

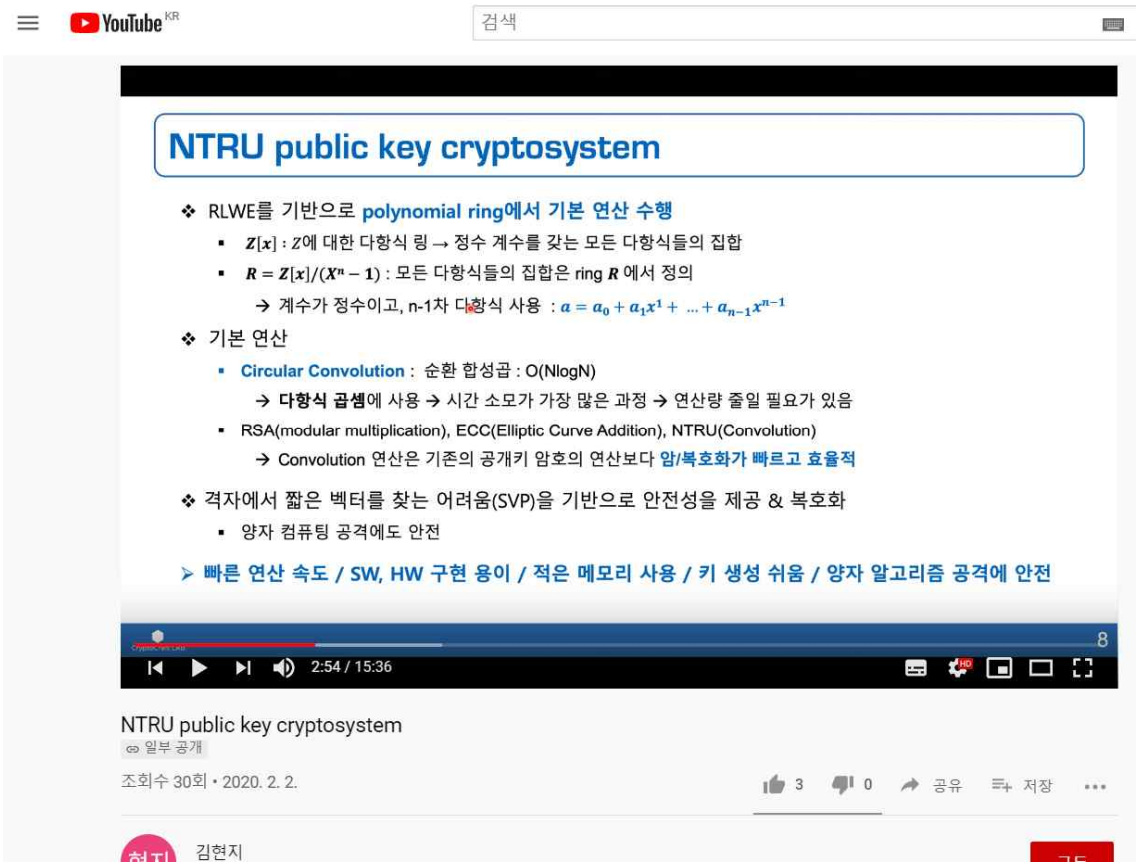
- 정기 세미나 및 스터디

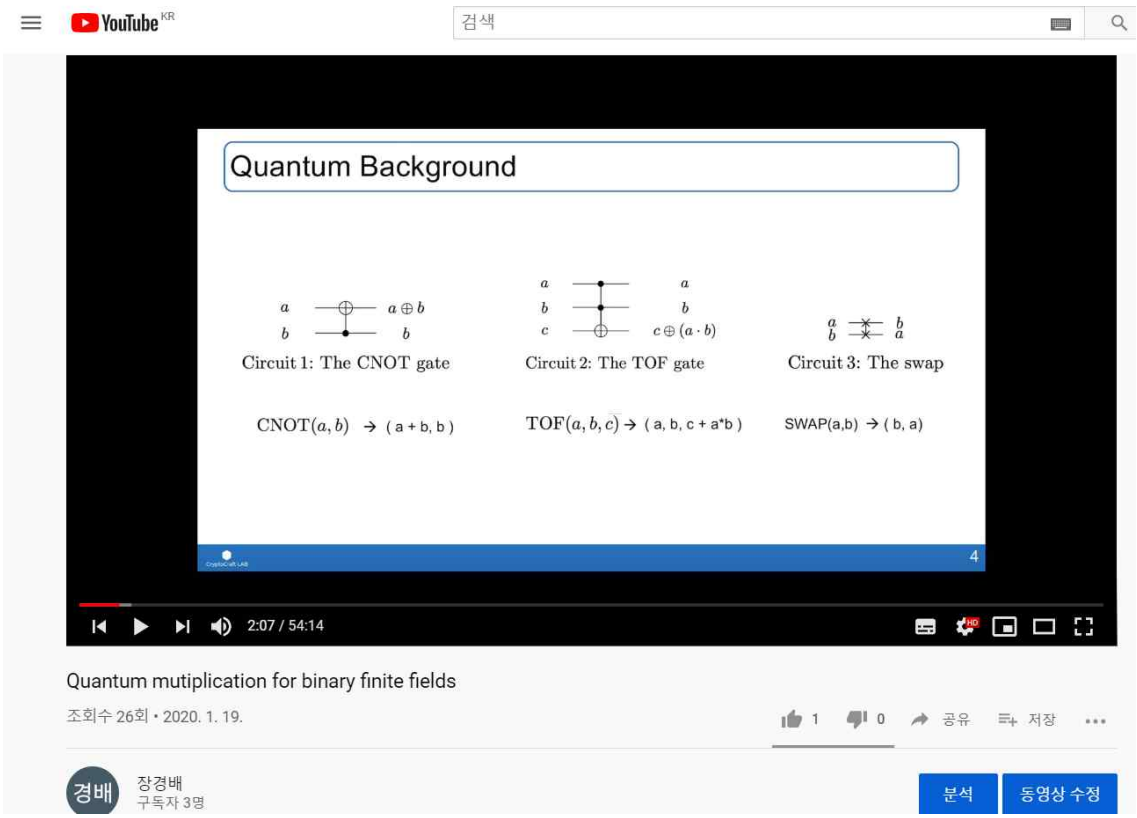


- 감염병 방지 온라인 세미나 진행

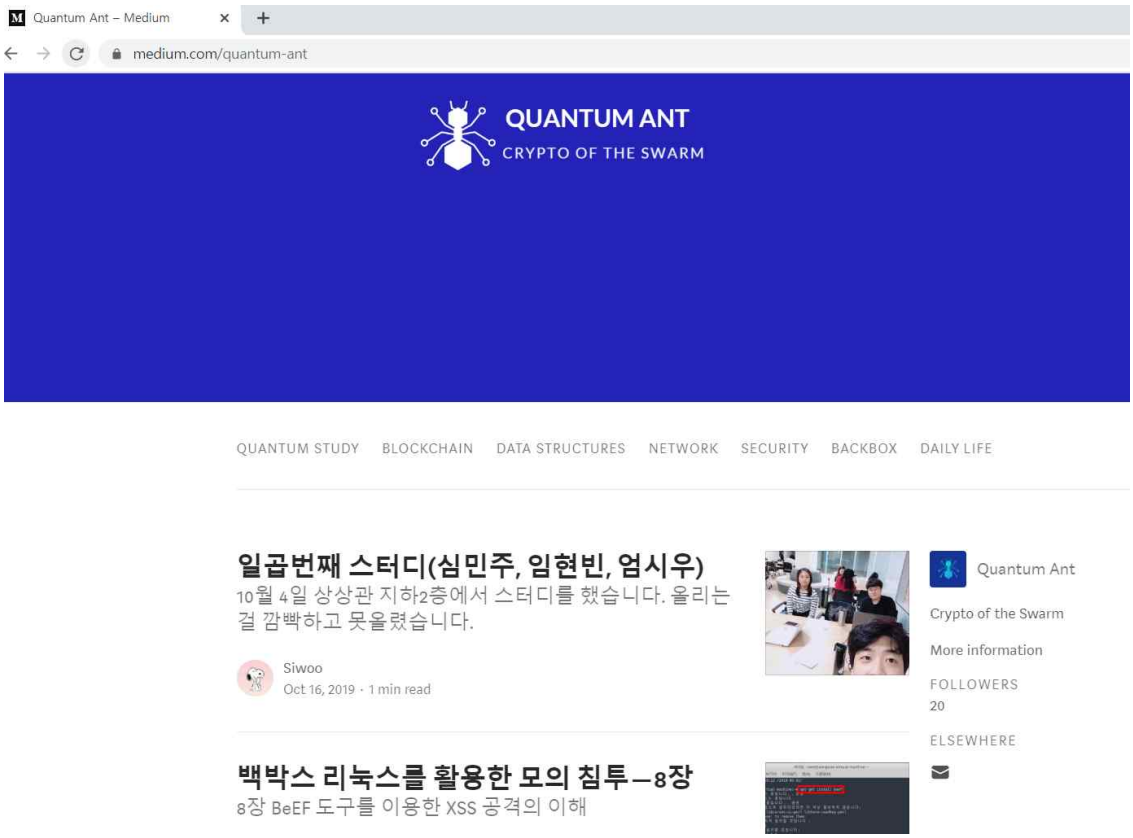
  - 코로나 19로 인해 오프라인 세미나는 잠정 연기, 스카이프 화상 회의를 통한 온라인 세미나 진행 중

- 학습 결과 유투브 업로드


YouTube KR
검색
NTRU public key cryptosystem
❖ RLWE를 기반으로 polynomial ring에서 기본 연산 수행
▪ $Z[x]$: Z에 대한 다항식 링 → 정수 계수를 갖는 모든 다항식들의 집합
▪ $R = Z[x]/(X^n - 1)$: 모든 다항식들의 집합은 ring R 에서 정의
→ 계수가 정수이고, n-1차 다항식 사용 : $a = a_0 + a_1x^1 + \ldots + a_{n-1}x^{n-1}$
❖ 기본 연산
▪ Circular Convolution : 순환 합성곱 : O(NlogN)
→ 다항식 곱셈에 사용 → 시간 소모가 가장 많은 과정 → 연산량 줄일 필요가 있음
▪ RSA(modular multiplication), ECC(Elliptic Curve Addition), NTRU(Convolution)
→ Convolution 연산은 기존의 공개키 암호의 연산보다 암/복호화가 빠르고 효율적
❖ 격자에서 짧은 벡터를 찾는 어려움(SVP)을 기반으로 안전성을 제공 & 복호화
▪ 양자 컴퓨팅 공격에도 안전
➢ 빠른 연산 속도 / SW, HW 구현 용이 / 적은 메모리 사용 / 키 생성 쉬움 / 양자 알고리즘 공격에 안전
8
2:54 / 15:36
NTRU public key cryptosystem
일부 공개
조회수 30회 • 2020. 2. 2.
3
0
공유
저장
김현지

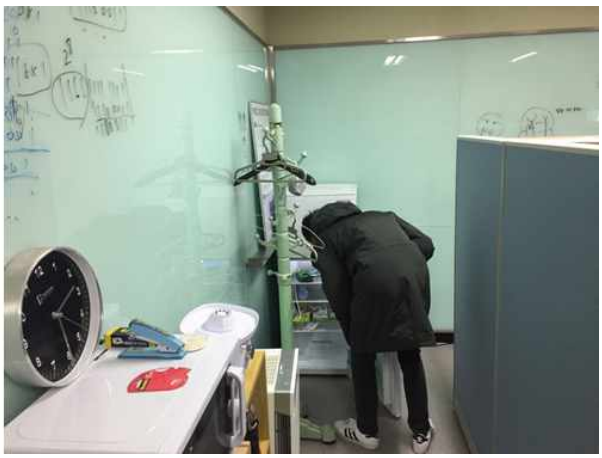

YouTube KR
검색
Quantum Background
Circuit 1: The CNOT gate
Circuit 2: The TOF gate
Circuit 3: The swap
CNOT(a, b) → (a + b, b)
TOF(a, b, c) → (a, b, c + a*b)
SWAP(a,b) → (b, a)
4
2:07 / 54:14
Quantum mutiplication for binary finite fields
조회수 26회 • 2020. 1. 19.
1
0
공유
저장
경배
장경배
구독자 3명
분석
동영상 수정

- 연구실 홈페이지 운영 (https://medium.com/quantum-ant)
  - 스터디, 세미나 결과를 자료로 남김



동아리 암호관련 활동 계획 및 주기적인 신입회원 모집

- 동아리방 확보 : 동아리 회원들이 자유롭게 회의 및 소통이 가능한 동아리방 확보(완료)

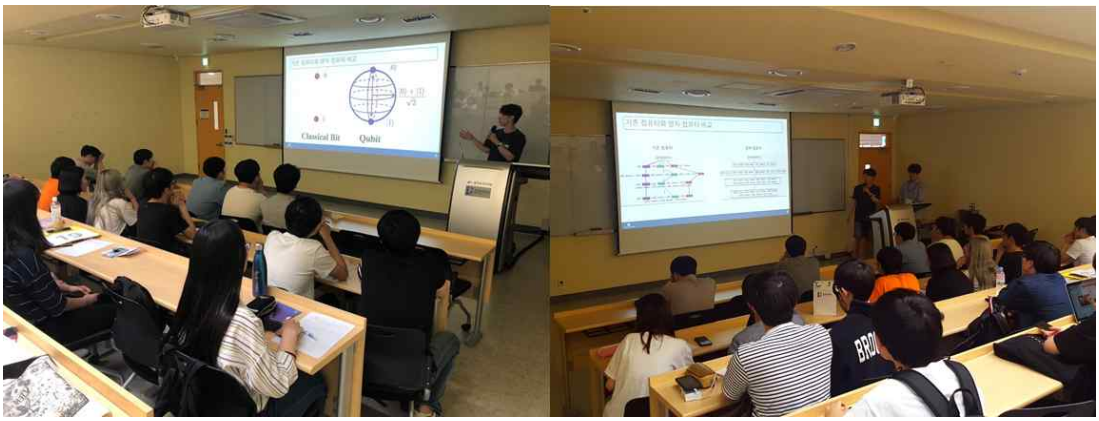


<동아리방>

- 동아리부스 활성화 : 한성대학교 축제기간 내소정의 상품과 함께 작은이벤트 개최,
동아리 홍보 및 신입 회원 모집 또한 진행

<2019년도 주최 사진>

- 교내활동 : 한성대학교 학부생을 대상으로 주기적으로 양자관련 설명회 개최 및 신입회원 모집



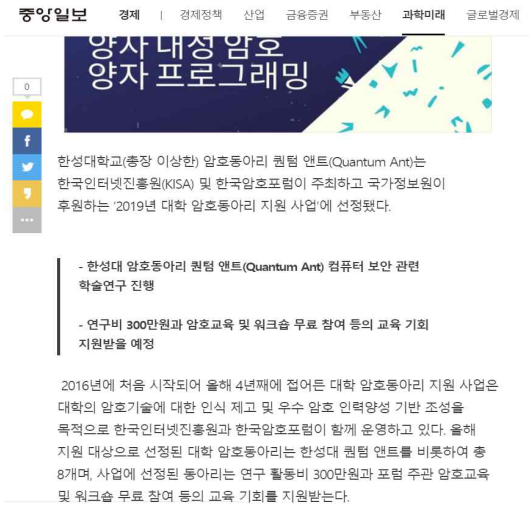
<2019년, 4번의 설명회 개최>

- 교외활동 : 일반 시민들을 대상으로 암호 동아리 홍보 및 양자 관련 지식 공유

<해운대>

<혜화역>

- 언론홍보 : 한성대학교 한성신문, 교내 잡지에 암호동아리 홍보, 대외홍보팀를 활용한 동아리 홍보



중앙일보 경제 | 경제정책 산업 금융증권 부동산 과학미래 글로벌경제

양자 대칭 암호
양자 프로그래밍

한성대학교(총장 이상한) 암호동아리 퀀텀 앤트(Quantum Ant)는 한국인터넷진흥원(KISA) 및 한국암호포럼이 주최하고 국가정보원이 후원하는 '2019년 대학 암호동아리 지원 사업'에 선정됐다.

- 한성대 암호동아리 퀀텀 앤트(Quantum Ant) 컴퓨터 보안 관련 학술연구 진행

- 연구비 300만원과 암호교육 및 워크숍 무료 참여 등의 교육 기회 지원받을 예정

2016년에 처음 시작되어 올해 4년째에 접어든 대학 암호동아리 지원 사업은 대학의 암호기술에 대한 인식 제고 및 우수 암호 인력양성 기반 조성을 목적으로 한국인터넷진흥원과 한국암호포럼이 함께 운영하고 있다. 올해 지원 대상으로 선정된 대학 암호동아리는 한성대 퀀텀 앤트를 비롯하여 총 8개며, 사업에 선정된 동아리는 연구 활동비 300만원과 포럼 주관 암호교육 및 워크숍 무료 참여 등의 교육 기회를 지원받는다.

<중앙일보>

한성이슈

커뮤니티한성 > 한성공지 > 한성이슈

내비게이션

- 공지사항
- 학사공지
- 비교과공지
- 한성이슈
- 입찰/견적 공고
- 취업공지
- 산학협력중점교수멘토링
- 장학공지
- 국내외 교류현황(MOU)
- 장애학생지원

2019년 대학 암호동아리 지원 사업 선정

작성자 | 대외홍보팀 조회수 | 556 등록일 | 2019.05.13

2019년 대학 암호동아리 지원 사업 선정

암호동아리 퀀텀 앤트(Quantum Ant)는 한국인터넷진흥원(KISA) 및 한국암호포럼이 주최하고 국가정보원이 후원하는 '2019년 대학 암호동아리 지원 사업'에 선정됐습니다.

2016년에 처음 시작되어 올해 4년째에 접어든 대학 암호동아리 지원 사업은 대학의 암호기술에 대한 인식 제고 및 우수 암호 인력양성 기반 조성을 목적으로 한국인터넷진흥원과 한국암호포럼이 함께 운영하고 있습니다. 올해 지원 대상으로 선정된 대학 암호동아리는 한성대 퀀텀 앤트를 비롯하여 총 8개며, 사업에 선정된 동아리는 연구 활동비 300만원과 포럼 주관 암호교육 및 워크숍 무료 참여 등의 교육 기회를 지원받습니다.

<한성대학교 대외홍보팀>

- 암호보안 관련 학술대회 및 양자 관련 워크샵 참가

<정보보호학회 동계학술대회>

<양자 워크샵>

- 국가암호공모전 참가 : 2020년 논문 분야 참가 예정

<2019년 우수 동아리>

<2019년 UCC 분야>

<2019년 논문 분야>

<2019년 UCC 분야>

- 동아리 내부 활동 : 동아리 선후배 간 친밀감/소통/협력을 위한 동아리 회식 개최

- 동아리 운영 구조 : 동아리장은 전체적인 운영을 담당하며, 각 팀장들은 동아리 내 특정역할을 담당

동아리장

장경배

신입회원 모집 및 홍보 팀장	학습 및 연구 팀장	동아리 내 친목 팀장
김현준, 김경호	최승주, 박재훈	김현지

동아리 운영 목표

- 보안에서 암호라는 분야를 널리 홍보
- 소외되는 동아리 회원이 없는 운영을 위한 동아리 장 및 팀장들의 관심과 노력
- 대학원생으로 구성된 동아리 장 및 팀장들의 학습 및 연구결과 피드백
- 각 동아리원의 수준에 맞는 부담 없는 팀 단위 학습 및 연구 진행
- 주기적인 소통, 동아리 회원 간 친밀감을 통한 활동적인 동아리 운영
- 회원들이 자부심을 느끼는 동아리로 만들기
- 장수하는 동아리 만들기
- 2020년도 암호 동아리 지원 사업 최우수 동아리

동아리 지원금 활용 계획

	비용	인원 / 횟수	합계
세미나 개최비	75,000	7회	525,000
회의비	7,500	30명 / 5회	1,125,000
분기별 팀 회식비	300,000	4회	1,200,000
상품비(축제,설문조사)	50,000	3회	150,000
			3,000,000

월별 계획

분기 / 활동분야	1분기	2분기			3분기			4분기	가중치 (%)	비고
	3	4	5	6	7	8	9	10		
- 동아리 홍보 및 팀별 인원 및 세부주제 선정									10	
- 양자 내성 암호 알고리즘 동작구조 발표 (키생성, 암호화, 복호화) (1/2)									10	
- 양자 내성 암호 알고리즘 동작구조 발표 (키생성, 암호화, 복호화) (2/2) - 양자 알고리즘을 사용한 공격동향 발표									15	
중간보고서 제출 대표자 회의 및 국가암호공모전 참여									10	
- 양자 게이트 학습 및 양자 프로그래밍 실습									15	
- 연구 진행 발표 및 양자 암호 초청 세미나									15	
최종 보고서 제출 대표자 회의 참석									10	
- 최종 연구 종합 및 교육 영상 제작									15	
분기별 진도(%)	10	35			40			15		