

암호 동아리 Quantum Ant 최종보고서

1. 작성자

| 소 속 | 한성대학교 | 직 | 그 | 동아리장 |
|-----|-------|-----|---|-------|
| 성 명 | 최 승 주 | 작 성 | 일 | 10.23 |

2. 목표 활동내용

| 기간 | 활동 내용 | 달성률(%) |
|-------|--|--------|
| 3월 | 동아리 홍보 및 팀별 세부 주제 선정 | 100 |
| 4월 | 양자 컴퓨터 개념 및 양자 내성 알고리즘 동향 발표 | 100 |
| 5월~6월 | 기존 대칭키 암호 알고리즘의 양자 알고리즘에 대한 내성 및 취약점 분석 | 100 |
| 7월 | 중간 보고서 제출 | 100 |
| 8월 | 부호 기반 양자 내성 알고리즘 분석 | 100 |
| 9월 | 연구 진행 발표 및 양자 암호 워크샵 참석 최종 연구 종합 및 교육 영상 제작 | 100 |
| 10월 | 최종 결과보고서 제출 | 100 |

2.1 활동 세부 내용

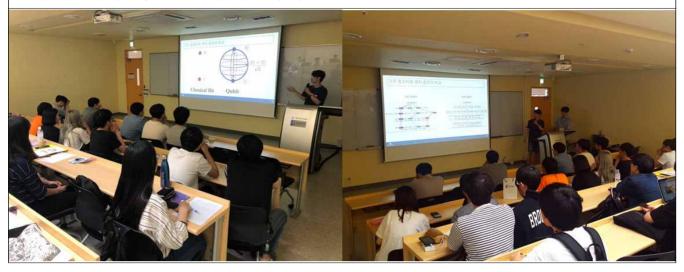
2.1.1 암호 동아리 및 양자 내성 암호 홍보

• 학교 축제 기간 활용하여 동아리 부스 설치 및 암호 동아리 홍보





· 양자 내성 암호 설명회 개최(6.3/6.10/7.30/8.31)



- 해운대에서 시민들을 대상으로 양자 관련 설문조사 실행
- -총 참여:16



- 혜화역에서 시민들을 대상으로 양자 관련 설문조사 실행
- -총 참여:21





2.1.2 부호 기반 양자 내성 알고리즘 분석

- ・2019 국가암호공모전 논문 제출
- 최승주, 장경배, 서화정: NIST 양자 내성 암호 공모전 Rom2 코드기반암호 성능 비교 분석

NIST 양자내성암호 공모전 Round2 코드기반암호 성능 비교 분석

Comparison of Round 2 Code-Based Cryptography for NIST Post-Quantum Cryptography Standardization

9.9

양자합류되의 개발이 빠르게 전쟁되고 있는 지금 다가오는 영자 후 시대에 안전한 입호체계 구축이 불요한 상황이다. 마루 국립표준기술연구소 NIST National Institute of Standards and Technology)에서는 양자내성암호 보조한 공간원을 개최하였고 국제적으로 많은 현물이 환가하여 자신들의 명차 내성 영호 달고리즘들을 제출하였다. 고려고 현재 Round1을 따지 그 높은 공가를 받은 2차에의 영호들이 Round2 참가에 중입하였다. 영호 안전성은 NIST의 보안가운을 거지에 차자 결중이 되겠지만 양자내성암호들이 공통적으로 가지고 있는 매우은 키 목은 세명 그가나 느린 양 복호화 속도는 지명적인 단점이다. 이에 본 논문에서는 후 또 영호들에 대한 성능을 살펴보기 위해 크로기반 영호들에 대한 성능 연기를 2가지 대표 적인 점등의 환경에서 진행한다. 이오의 영호의 독등들에 대해 본식하고 다 나아가 어떤 본야에 표준학되면 적합했지 배고 문서한다. 성능 경가 환경은 고성을 때수고를 포로 세세인 Insel 프로세서와 자전력 모바일 프로세서인 ARM에서 진행하였다. 해당 Round2 호 토기반암호를 예상에 할 수 있음과 동시에 현재 코드기반암호들이 개선하여 할 무분에 대해 선 중 본세하도록 한다.

- · 2019 국가암호 공모전 UCC 참가
- 3팀(총 9명)



2.1.3 양자 컴퓨터 개념 및 양자 내성 알고리즘 동향 발표

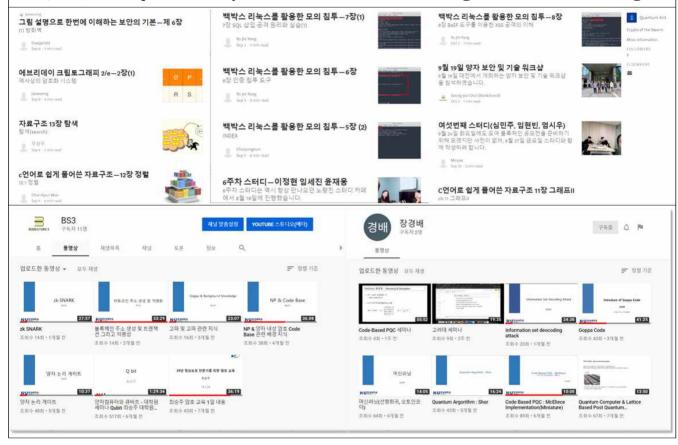
- 2019 한국정보보호학회 학술대회 논문 제출
- 장경배, 서화정: 양자 컴퓨터와 NIST 양자 내성 암호 표준화 동향
- 최승주, 권혁동, 서화정: 부호 기반 양자 내성 암호 NIST 표준화 동향

2010년 존개학술발로대회 논문집 제26년 제1호 (010, S 부호 기반 양자 내성 암호 NIST 표준화 동향 최승주' 권력봉' 서화경" 양자컴퓨터와 NIST 양자내성암호 표준화 동향 *林·传统中卫 打车管路 성장에', 서화성' '현성대학교 대학원 ET용성공학자 Post Quantum Algorithm and Standardization trend of NIST Seung-Ju Choi" Hyeok-Dong Kwon" Hwe-Jeong Seo" Quantum Computer and Standardization trend of NIST *Division of IT Convergence Engineering, Hensung University, Post-Quantum Cryptography Kyoung Bar Jung', Hwo Joong Seo' 'Dept. of Applied IT Engineering, Han-sung University 최근 양과 원폭터 시대에 대비한 양과 내성 장초에 대한 많은 연구가 원했지고 있다. 이러한 음식당에 당취 미국 국월로증기술 연구소에서는 2016년 10월 20일부터 당자 내성 방호에 대한 표종화 사업을 진행하였고, 이미 표종화 1학문도는 분조가 되었고 데, 2019년 1월 30일부터 표준화 2차운도가 전했지고 있다. 본 논문에서는 양과 행류 더와 무호 기반의 양자 내성 암호 중심으로 PEST 표준화 연구의 회신 동향을 살펴본



2.1.4 최종 연구 종합 및 교육 영상 제작

- 홈페이지 및 유튜브 체널에 부호 기반 양자 내성 알고리즘 연구 내용 정리
- 홈페이지: https://medium.com/quantum-ant
- 장경배: https://www.youtube.com/channel/UCHXfXZtUSBDOoui_JPS_xwQ
- 최승주: https://www.youtube.com/channel/UCMgDb1vPsWCXmhSJMnRgGEA



2.1.5 연구 진행 발표 및 양자 암호 초청 세미나

- · 2019 NetSec-KR 워크샵 참석
- · 2019 Quantum Security and its related Technologies 워크샵 참석





2.1.6 기타 활동

- · 동아리 정기 세미나 및 스터디
- 연구 내용 발표(양자, 보안, 해킹, 자료구조, 블록체인, 네트워크)
- 동아리 회식





3. 활동 결과

3.1 동아리 인원 증가

| 비 | 고 | 성 명 | 인원(명) |
|-------|-----------|-------------------------|-------|
| | 대학원생 | 최승주, 권용빈, 장경배, 김경호 | 4 |
| | | 박재현 심민주 양유진 유원상 | |
| 기존 인원 | I H 서 그 개 | 윤재웅 이정현 임세진 최정은 | 1.0 |
| | 학부연구생 | 엄시우 김은혜 정진우 안성민 | 16 |
| | | 이승재 선지민 선서영 이기정 | |
| | 대학원생 | 최승주, 권용빈, 장경배, 김경호, 김현준 | 5 |
| | | 박재현 심민주 양유진 유원상 윤재웅 이정현 | |
| 현재 인원 | 첫 보 서 그 계 | 임세진 최정은 엄시우 김은혜 정진우 안성민 | 10 |
| | 학부연구생 | 이승재 선지민 선서영 이기정 김현지 이윤경 | 19 |
| | | 황필규 | |

3.2 양자 컴퓨터 및 양자 내성 암호 홍보

- ·학교 축제 및 설명회를 통해 학생들에게 양자 내성 암호 홍보
- ·해운대 및 혜화역 설문조사를 통한 일반인들의 양자 컴퓨팅 인지도 조사
- ·학생 및 시민들에게 양자 컴퓨터 및 양자 내성 암호 설명을 통한 인식 향상

3. 지원 예산 집행률

| 내용 | 단위(원) |
|-------|-----------|
| 전체 예산 | 3,065,131 |
| 총 지출액 | 3,064,520 |
| 남은 예산 | 611 |

5월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|---------|------------|------|---------|-----------|-----------|-------|----|
| 2019.05.31 18:41:51 | 체크카드 | (주)커피빈코리아한 | | 62,100 | 0 | 1,076,100 | KB∍ŀ⊆ | |
| 2019.05.31 18:32:48 | 체크카드 | 더(The)스시하루 | | 204,000 | 0 | 1,138,200 | KB₹F⊑ | |
| 2019.05.27 23:14:19 | 인터넷출금이체 | G마켓최승주 | | 35,700 | 0 | 1,342,200 | KC점 | |
| 2019.05.27 15:18:49 | 체크카드 | 주)스타벅스커피코리 | | 100,000 | 0 | 1,377,900 | KB카⊆ | |
| 2019.05.26 18:52:37 | 체크카드 | 주식회사아성다이소 | | 32,100 | 0 | 1,477,900 | KB₹F⊆ | |
| 2019.05.23 01:18:59 | 전자금융 | 2019암호동아리 | | o | 1,500,000 | 1,510,000 | 하나은행 | |
| 2019.04.05 11:37:06 | 현금입금 | | | О | 10,000 | 10,000 | KC점 | |
| | | | 합계 | 433,900 | 1,510,000 | | | |



6월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|---------|-------------|------|---------|--------|-----------|------|----|
| 2019.06.24 13:13:46 | 체크카드 | (주)미고당바이팥고당 | | 45,500 | 0 | 754,580 | KB카드 | |
| 2019.06.24 00:21:53 | 인터넷출금이체 | 카뱅윤재웅 | | 120,000 | 0 | 800,080 | KC점 | |
| 2019.06.20 15:07:48 | 체크카드 | 주)스타벅스커피코리 | | 10,000 | 0 | 920,080 | KB카드 | |
| 2019.06.20 15:02:48 | 체크카드 | 싸유해운대팔레드시 | | 29,020 | 0 | 930,080 | KB카드 | |
| 2019.06.19 22:49:12 | 인터넷출금이체 | 최승주 | | 72,000 | 0 | 959,100 | KC점 | |
| 2019.06.05 23:04:32 | 인터넷입금이체 | 최승주 | | 0 | 55,000 | 1,031,100 | 신논현 | |
| 2019.06.05 22:47:05 | 인터넷출금이체 | 사)한국정보보호학회 | | 55,000 | 0 | 976,100 | KC점 | |
| 2019.06.04 12:18:53 | 체크카드 | 주)스타벅스커피코리 | | 15,000 | 0 | 1,031,100 | KB카드 | |
| 2019.06.03 12:57:01 | 체크카드 | 주)스타벅스커피코리 | | 30,000 | 0 | 1,046,100 | KB카드 | |
| | | | 합계 | 376,520 | 55,000 | | | |

7월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|---------|-------------------|------|---------|-----|---------|------|----|
| 2019.07.30 15:53:24 | 체크카드 | DigitalPublishing | | 14,000 | 0 | 93,080 | KB카드 | |
| 2019.07.30 15:09:15 | 체크카드 | (주)미고당바이팥고당 | | 50,000 | 0 | 107,080 | KB카드 | |
| 2019.07.16 10:26:13 | 인터넷출금이체 | 카뱅이승재 | | 60,000 | 0 | 157,080 | KC점 | |
| 2019.07.16 10:25:25 | 인터넷출금이체 | 장원준 | | 60,000 | 0 | 217,080 | KC점 | |
| 2019.07.16 10:24:31 | 인터넷출금이체 | 신한임지우 | | 60,000 | 0 | 277,080 | KC점 | |
| 2019.07.04 14:25:03 | 인터넷출금이체 | 농협정진우 | | 19,800 | 0 | 337,080 | KC점 | |
| 2019.07.04 14:24:11 | 인터넷출금이체 | 안성민 | | 19,800 | 0 | 356,880 | KC점 | |
| 2019.07.04 11:14:23 | 인터넷출금이체 | 카뱅김정민 | | 13,500 | 0 | 376,680 | KC점 | |
| 2019.07.04 11:12:04 | 인터넷출금이체 | 카뱅김은혜 | | 27,000 | 0 | 390,180 | KC점 | |
| 2019.07.04 10:50:13 | 인터넷출금이체 | 카뱅이승재 | | 30,000 | 0 | 417,180 | KC점 | |
| 2019.07.04 10:33:04 | 인터넷출금이체 | 카뱅신서영 | | 15,000 | 0 | 447,180 | KC점 | |
| 2019.07.04 10:29:41 | 인터넷출금이체 | 하나임현빈 | | 27,000 | 0 | 462,180 | KC점 | |
| 2019.07.02 22:48:58 | 인터넷출금이체 | 케미양유진 | | 45,000 | 0 | 489,180 | KC점 | |
| 2019.07.02 22:34:28 | 인터넷출금이체 | 윤재웅 | | 15,300 | 0 | 534,180 | KC점 | |
| 2019.07.02 22:33:44 | 인터넷출금이체 | 임세진 | | 15,300 | 0 | 549,480 | KC점 | |
| 2019.07.02 22:32:58 | 인터넷출금이체 | 기업이정현 | | 22,500 | 0 | 564,780 | KC점 | |
| 2019.07.02 18:17:55 | 인터넷출금이체 | 신한주상우 | | 29,000 | 0 | 587,280 | KC점 | |
| 2019.07.02 18:17:00 | 인터넷출금이체 | 윤상열 | | 29,000 | 0 | 616,280 | KC점 | |
| 2019.07.02 18:15:39 | 인터넷출금이체 | 기업최현우 | | 29,000 | 0 | 645,280 | KC점 | |
| 2019.07.02 18:14:32 | 인터넷출금이체 | 이영훈 | | 29,000 | 0 | 674,280 | KC점 | |
| 2019.07.01 22:18:37 | 인터넷출금이체 | 기업심민주 | | 24,300 | 0 | 703,280 | KC점 | |
| 2019.07.01 11:54:45 | 인터넷출금이체 | 엄시우 | | 27,000 | 0 | 727,580 | KC점 | |
| | | | 합계 | 661,500 | | | | |

8월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|---------|-----------|------|---------|-----------|-----------|------|----|
| 2019.08.10 03:55:37 | 결산이자 | 이자세금:20원 | | 0 | 131 | 1,279,711 | KC점 | |
| 2019.08.08 22:27:37 | 인터넷출금이체 | 최승주 | | 300,000 | 0 | 1,279,580 | KC점 | |
| 2019.08.06 22:27:28 | 전자금융 | 암호동아리 | | 0 | 1,500,000 | 1,579,580 | 하나은행 | |
| 2019.08.01 11:40:12 | 체크카드 | 세븐일레븐마로니에 | | 7,500 | 0 | 79,580 | KB카드 | |
| 2019.08.01 10:59:14 | 체크카드 | GS25서초제일 | | 6,000 | 0 | 87,080 | KB카드 | |
| | | | 합계 | 313,500 | 1,500,131 | | | |



9월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|------|-------------|------|---------|-----|-----------|------|----|
| 2019.09.04 20:51:12 | 체크카드 | 무한리필고기굼터 | | 186,000 | 0 | 1,051,611 | KB카드 | |
| 2019.09.04 16:14:01 | 체크카드 | (주)미고당바이팥고당 | | 42,100 | 0 | 1,237,611 | KB카드 | |
| | | | 합계 | 228,100 | | | | |

10월 예산 사용 내역

| 거래일시 | 적요 | 보낸분/받는분 | 송금메모 | 출금액 | 입금액 | 잔액 | 거래점 | 구분 |
|---------------------|---------|---------|------|-----------|-----|-----------|------|----|
| 2019.10.23 19:44:58 | 인터넷출금이체 | 하나임현빈 | | 40,000 | 0 | 611 | KC점 | |
| 2019.10.23 19:41:00 | 인터넷출금이체 | 신한주상우 | | 51,000 | 0 | 40,611 | KC점 | |
| 2019.10.23 19:36:54 | 인터넷출금이체 | 하나김경호 | | 51,000 | 0 | 91,611 | KC점 | |
| 2019.10.23 10:25:48 | 인터넷출금이체 | 기업최현우 | | 45,000 | 0 | 142,611 | KC점 | |
| 2019.10.23 10:25:01 | 인터넷출금이체 | 안성민 | | 45,000 | 0 | 187,611 | KC점 | |
| 2019.10.23 10:24:03 | 인터넷출금이체 | 카뱅이승재 | | 45,000 | 0 | 232,611 | KC점 | |
| 2019.10.22 19:32:57 | 인터넷출금이체 | 임세진 | | 45,000 | 0 | 277,611 | KC점 | |
| 2019.10.22 16:02:51 | 인터넷출금이체 | 카뱅이기정 | | 45,000 | 0 | 322,611 | KC점 | |
| 2019.10.22 15:55:52 | 인터넷출금이체 | 카뱅심민주 | | 45,000 | 0 | 367,611 | KC점 | |
| 2019.10.22 15:54:53 | 인터넷출금이체 | 카뱅김정민 | | 51,000 | 0 | 412,611 | KC점 | |
| 2019.10.22 15:19:02 | 인터넷출금이체 | 케미양유진 | | 45,000 | 0 | 463,611 | KC점 | |
| 2019.10.22 15:17:58 | 인터넷출금이체 | 기업최정은 | | 45,000 | 0 | 508,611 | KC점 | |
| 2019.10.20 21:46:51 | 인터넷출금이체 | 기업이정현 | | 45,000 | 0 | 553,611 | KC점 | |
| 2019.10.20 21:40:20 | 인터넷출금이체 | 농협정진우 | | 45,000 | 0 | 598,611 | KC점 | |
| 2019.10.15 19:59:38 | 체크카드 | 램브로양꼬치 | | 180,000 | 0 | 643,611 | KB카드 | |
| 2019.10.07 12:55:50 | 인터넷출금이체 | 카뱅이기정 | | 22,000 | 0 | 823,611 | KC점 | |
| 2019.10.05 22:33:00 | 인터넷출금이체 | 신한선지민 | | 90,000 | 0 | 845,611 | KC점 | |
| 2019.10.05 22:28:45 | 인터넷출금이체 | 카뻥윤재웅 | | 51,000 | 0 | 935,611 | KC점 | |
| 2019.10.05 22:27:41 | 인터넷출금이체 | 엄시우 | | 45,000 | 0 | 986,611 | KC점 | |
| 2019.10.05 22:06:16 | 인터넷출금이체 | 케미양유진 | | 20,000 | 0 | 1,031,611 | KC점 | |
| | | | 합계 | 1,051,000 | | | | |