Quantum Ant : 최종 발표

발표자 : 한성대학교 장경배

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

Qunatum Ant

- 다가오는 양자 컴퓨터 시대에 초점을 맞춘 암호 관련 학술 동아리
- 양자 프로그래밍 및 양자내성암호에 대해 학습
- 다양한 보안관련 기술 : 블록체인, 사용자 인증 등도 학술
- 5명의 동아리 팀장이 중요 역할을 맡음

QUANTUM ANT
CRYPTO OF THE SWARM

Quantum Ant : 최종보고

- **동아리 학습 커리큘럼**
  - 암호 기초학
  - 양자내성암호
  - 양자 알고리즘
  - 양자 프로그래밍

기초 베이스 및 다양한 분야

- 대칭키, 공유키, 키 생성, 암호화, 복호화 등, 암호학에 대한 기초 개념 학습 (전문서적 활용)
- 반드시 암호만 해야 되는 것이 아니라 프로그래밍, 블록체인, AI, 사이버보안에 대해 관심이 있는 학생들은 다양하게 학습 가능

NIST PQC Round3 Algorithm

- 현재 Round2에서 Round3로 진행됨에 따라 추려진 양자내성암호 알고리즘에 대해 학습 중심적으로 학습 (ClassicMcEliece)
- 해당 알고리즘의 키 생성, 암호화, 복호화를 이해하고 Reference 코드의 C 코드와 비교 학습

양자 알고리즘

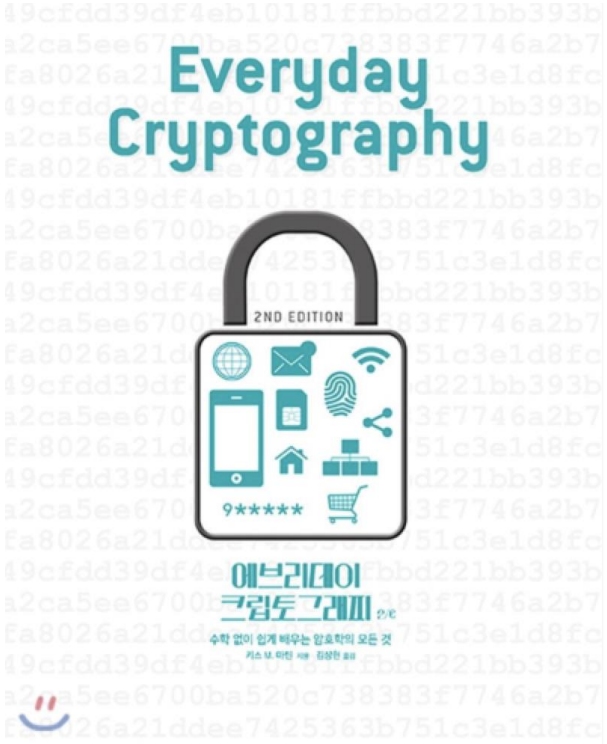
- Grover 알고리즘, Shor 알고리즘 학습으로 동작 메커니즘 파악
- 해외 논문을 참조하여 양자 알고리즘을 활용한 암호 공격 동향 파악 및 리뷰

양자 프로그래밍

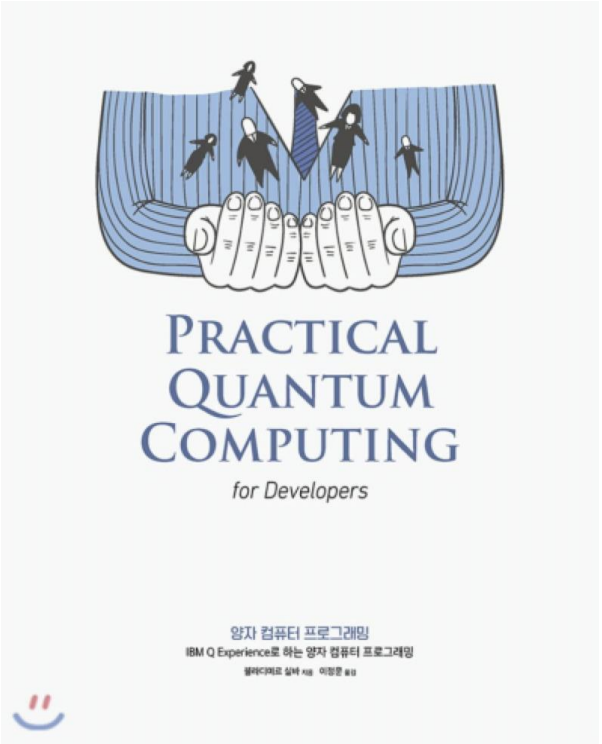
- IBM에서 제공하며, 파이썬을 사용한 양자 프로그래밍이 가능한 툴 ProjectQ 사용
- 양자프로그래밍을 통한 Grover, Shor 알고리즘의 학습 및 구현 (예제코드 및 전문서적 활용)
- 덧셈, 곱셈, 모듈러와 같은 핵심연산을 설계한 양자게이트 학습 및 프로그래밍
- 경량 블록암호를 양자 회로로 구현하여 Grover 알고리즘 공격에 대한 자원 측정 및 안전성 분석

Quantum Ant : 최종보고

- 신입 회원들을 위한 기초 암호 교재 18권, 숙련자를 위한 양자 프로그래밍 교재 5권 구비



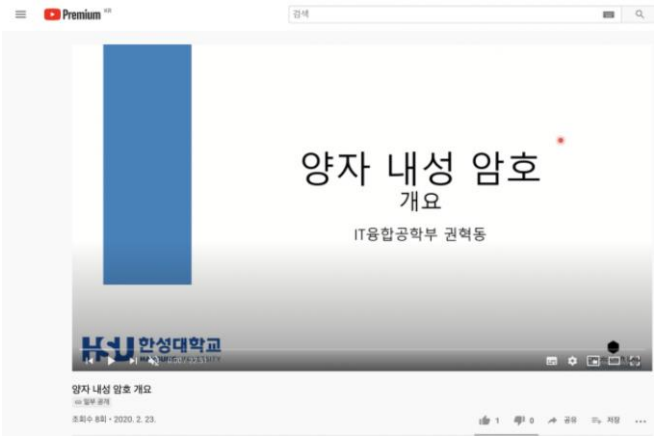
< 기초 암호학 >

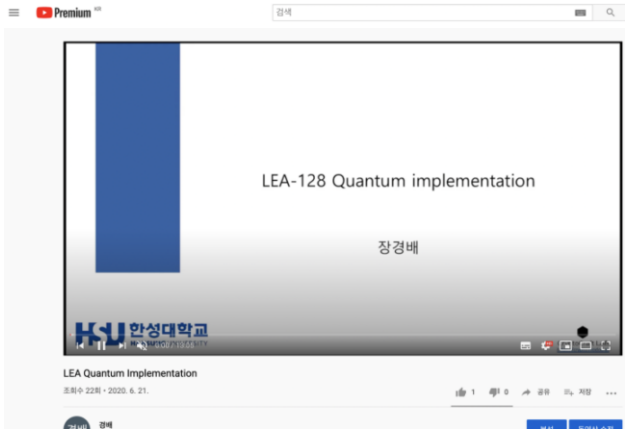


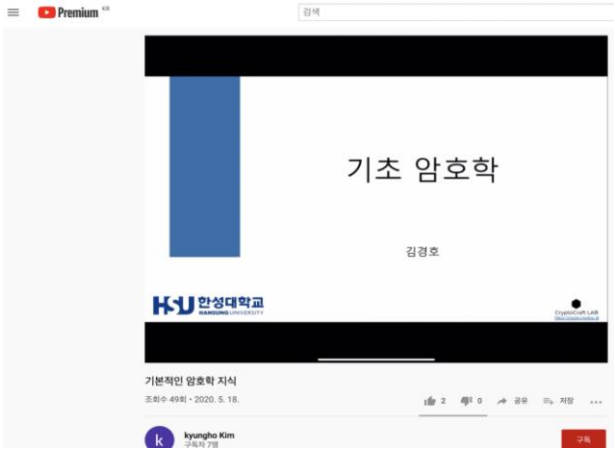
< 양자 프로그래밍 >

Quantum Ant : 최종보고

- 동아리 유투브 채널 운용 : https://www.youtube.com/playlist?list=PLDEpR6c2CcpISXAWZJjMnjKB_a80hHhe6
  - 서적뿐만이 아니라, 동아리 유투브 채널에서 각자 자신에게 맞는 교육 영상을 시청하며 학습이 가능
    - 기초 암호학, 양자내성암호, 양자 컴퓨터







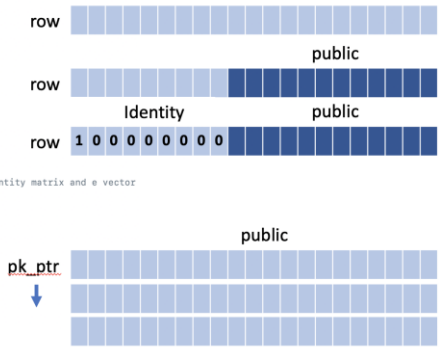
- 동아리 원들의 세미나 공유 영상도 유용한 학습자료
  - 자료구조, 암호 알고리즘

Quantum Ant : 최종보고

- 양자내성암호
  - NIST PQC 공모전 Round 3의 Classic McEliece 레퍼런스 코드와 비교하며 키 생성, 인캡슐, 디캡슐 학습

Classic McEliece : Encapsulation

```
void syndrome(unsigned char *s, const unsigned char *pk, unsigned char *e)
{
    unsigned char b, row[SYS_N/8];
    const unsigned char *pk_ptr = pk;

    int i, j;

    for (i = 0; i < SYND_BYTES; i++)
        s[i] = 0;

    for (i = 0; i < PK_NROWS; i++)
    {
        for (j = 0; j < SYS_N/8; j++)
            row[j] = 0;  // Reset 0 for multiplication

        for (j = 0; j < PK_ROW_BYTES; j++)
            row[ SYS_N/8 - PK_ROW_BYTES + j ] = pk_ptr[j];

        row[i/8] |= 1 << (i%8); //The part composed of the identity matrix

        b = 0;
        for (j = 0; j < SYS_N/8; j++)
            b ^= row[j] & e[j]; //Multiplying the public key formed by attaching the identity matrix and e vector

        b ^= b >> 4;  // ex 00001101 -> 1, 00000011 ->0
        b ^= b >> 2;
        b ^= b >> 1;
        b &= 1;

        s[ i/8 ] |= (b << (i%8));   //--> save syndrome value

        pk_ptr += PK_ROW_BYTES;
    }
}
```



<Classic McEliece : 인캡슐레이션 >

Classic McEliece : Decapsulation

LFSR Synthesis Algorithm (Berlekamp Iterative Algorithm):

1) $1 \rightarrow C(D) \quad 1 \rightarrow B(D) \quad 1 \rightarrow x$
   $0 \rightarrow L \quad 1 \rightarrow b \quad 0 \rightarrow N$
2) If $N = n$, stop. Otherwise compute
$$d = s_N + \sum_{i=1}^{L} c_i s_{N-i}.$$
3) If $d = 0$, then $x + 1 \rightarrow x$, and go to 6).
4) If $d \neq 0$ and $2L > N$, then
   $C(D) - d\,b^{-1} D^x B(D) \rightarrow C(D)$
   $x + 1 \rightarrow x$
   and go to 6).
5) If $d \neq 0$ and $2L \leqq N$, then
   $C(D) \rightarrow T(D)$ [temporary storage of $C(D)$]
   $C(D) - d\,b^{-1} D^x B(D) \rightarrow C(D)$
   $N + 1 - L \rightarrow L$
   $T(D) \rightarrow B(D)$
   $d \rightarrow b$
   $1 \rightarrow x$.
6) $N + 1 \rightarrow N$ and return to 2).

```
for (N = 0; N < 2 * SYS_T; N++)
{
    d = 0;

    for (i = 0; i <= min(N, SYS_T); i++)
        d ^= gf_mul(C[i], s[ N-i]);

    mne = d; mne -= 1;    mne >>= 15; mne -= 1;
    mle = N; mle -= 2*L; mle >>= 15; mle -= 1;
    mle &= mne; //mle = 1111 1111 1111 1111 아니면 0

    for (i = 0; i <= SYS_T; i++)
        T[i] = C[i];

    f = gf_frac(b, d);

    for (i = 0; i <= SYS_T; i++)
        C[i] ^= gf_mul(f, B[i]) & mne;

    L = (L & ~mle) | ((N+1-L) & mle);

    for (i = 0; i <= SYS_T; i++)
        B[i] = (B[i] & ~mle) | (T[i] & mle);

    b = (b & ~mle) | (d & mle);

    for (i = SYS_T; i >= 1; i--) B[i] = B[i-1];
    B[0] = 0;
}

for (i = 0; i <= SYS_T; i++)
    out[i] = C[ SYS_T-i ];
```

(4) (5)

* B[1] = C[0] = 1;

* B[1] = C[0] = 1;

→ End

<Classic McEliece : 디캡슐레이션 >

Quantum Ant : 최종보고

- 국산 경량암호 HIGHT, LEA, CHAM을 양자회로로 구현
  - Grover 알고리즘 적용을 위한 자원 추정

Block Cipher	Plaintext (bit)	Key (bit)	Qubit	Toffoli gate	CNOT gate	X gate
CHAM	64	128	196	2,400	12,285	240
	128	128	268	4,960	26,885	240
	128	256	396	5,952	32,277	304
HIGHT	64	128	201	6,272	20,523	4
LEA	128	128	385	10,416	28,080	68
	128	192	513	15,624	39,816	100
	128	256	641	17,856	45,504	130

< 국산 경량 블록암호 양자 회로 자원 >

Quantum Ant : 최종보고

- NSA에서 만든 경량 블록암호 SIMON을 양자 회로로 구현하여 Grover 알고리즘 자원 추정한 논문
  - Ravi Anand, Arpita Maitra, and Sourav Mukhopadhyay. Grover on SIMON, 04 2020.

- SPECK, 그리고 SIMECK 을 추가로 양자 회로로 구현하여 기존 SIMON 논문의 결과와 비교

Block Cipher	Qubits	Toffoli gates	CNOT gates	X gates
SPECK-32/64	97	1,290	3,706	42
SIMON-32/64	96	512	2,816	448
SIMECK-32/64	96	9,60	1,472	407
SPECK-48/96	145	2,074	5,866	45
SIMON-48/96	144	864	4,800	768
SIMECK-48/96	144	1,632	2,496	721
SPECK-64/128	193	3,286	9,238	57
SIMON-64/128	192	1,408	7,396	1,216
SIMECK-64/128	192	2,688	4,096	1,219

< SIMON, SPECK, SIMECK 추정 자원 비교 >

Quantum resources	SIMECK 32/64	SIMECK 48/96	SIMECK 64/128
Qubits	193	289	385
Toffoli gates	3,840	6,528	10,752
CNOT gates	6,016	10,176	16,640
X gate	1,628	2,884	4,876

< Grover 알고리즘 적용 자원 (SIMECK) >

Quantum Ant : 최종보고 (중간보고 성과)

- 학술대회 참가
  - 한국정보처리학회 춘계학술발표대회, 2020 → 9편 발표
    - 코드기반암호를 활용한 IoT 환경 보안 프로토콜 설계
    - 비콘과 홍채인식 기반의 의료진 신분확인 시스템 제안
    - 블록체인 기반의 디지털 신원증명 동향
  - 한국정보보호학회 하계학술발표대회, 2020 → 12편 발표
    - NIST 양자내성암호 공모전 부호 기반 암호 구현 동향
    - 카라추바 곱셈 양자회로 구현 동향
    - 안면인식을 통한 USB 파일 복호화 시스템
- 학회지 논문 게재
  - 한국정보통신학회, 2020
    -부호 기반 양자내성암호의 이진 필드상의 곱셈 연산 양자 게이트 구현

Quantum Ant : 최종보고

- 학술대회 WISA, 2020
  - Impact of Optimized Operations AB, AC for Binary Field Inversion on Quantum Computers
- 국내 논문지 1편 게재
  - 양자내성암호를 활용한 경량 보안 프로토콜 설계, 한국정보처리학회. 2020.
- 해외 논문지 1편 게재
  - Grover on Korean Block Ciphers, Applied Sciences, 2020.

Quantum Ant : 최종보고

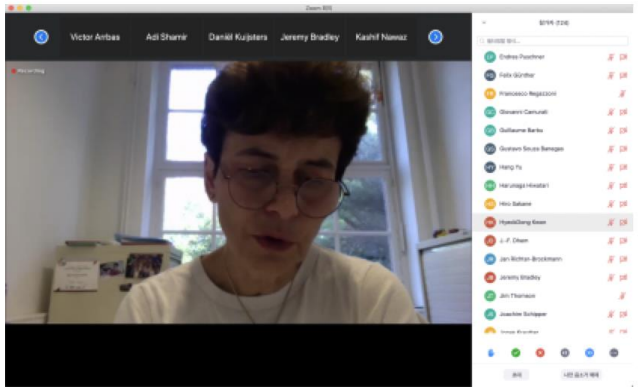
- 국가암호공모전 13편 참가

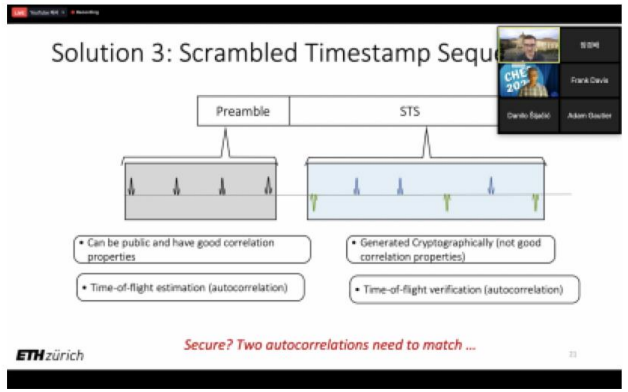
- ICISC 3편 참가
  - Grover on SIMECK
  - Format Preserving Encryption for Steganography
  - Generative Adversarial Networks based Pseudo-Random Number Generator for Embedded Processors

Quantum Ant : 최종보고

- 다양한 보안 워크숍 참가
  - CPS 보안 워크숍
  - NetSec-KR (온라인)
  - IoT 보안 워크숍

- 국제 학술대회 CHES 참가





< CHES 온라인 >

Quantum Ant : 최종보고

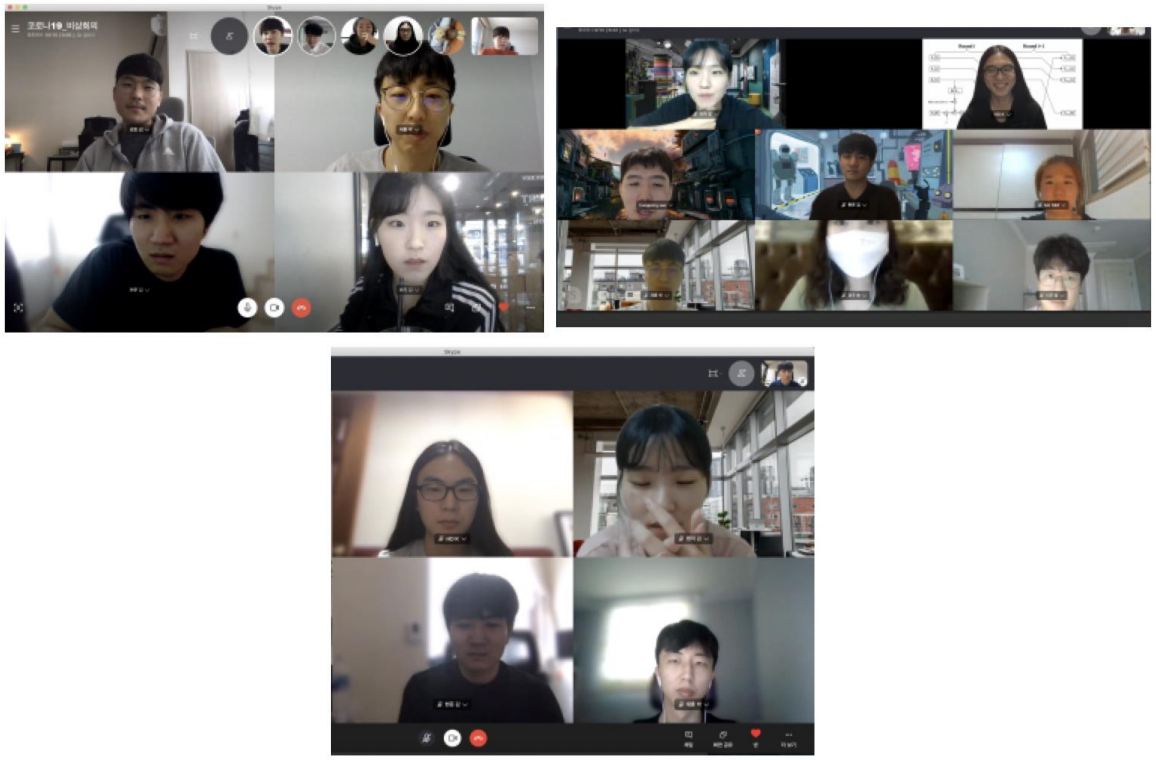
- 초청 강연
  - 지도교수님이 전문가 초청 해주신 기회를 통해, 소수의 동아리 원은 직접 참석하여 수강

< KCMVP >

< 블록체인, 스타트 업 >

Quantum Ant : 최종보고

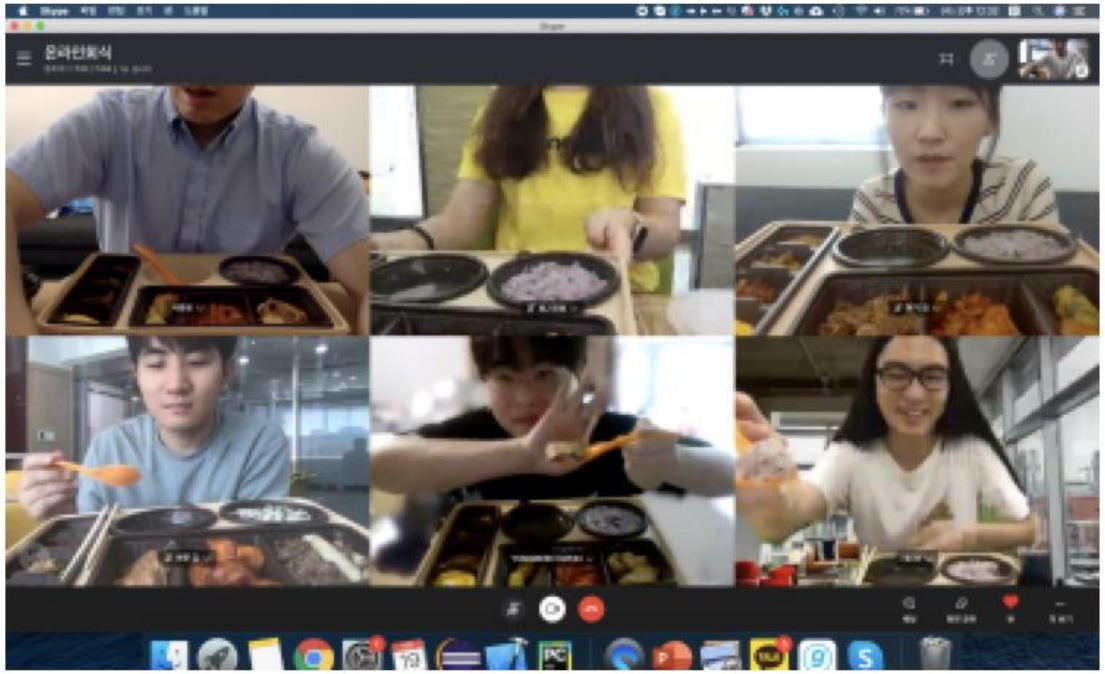
- 감염병 방지 온라인 세미나 진행
  - 나아지지 않는 코로나 19 상황으로 인해 오프라인 세미나는 연기, 스카이프 화상 회의를 통한 온라인 세미나 진행 중



< Skype 온라인 세미나 >

Quantum Ant : 최종보고

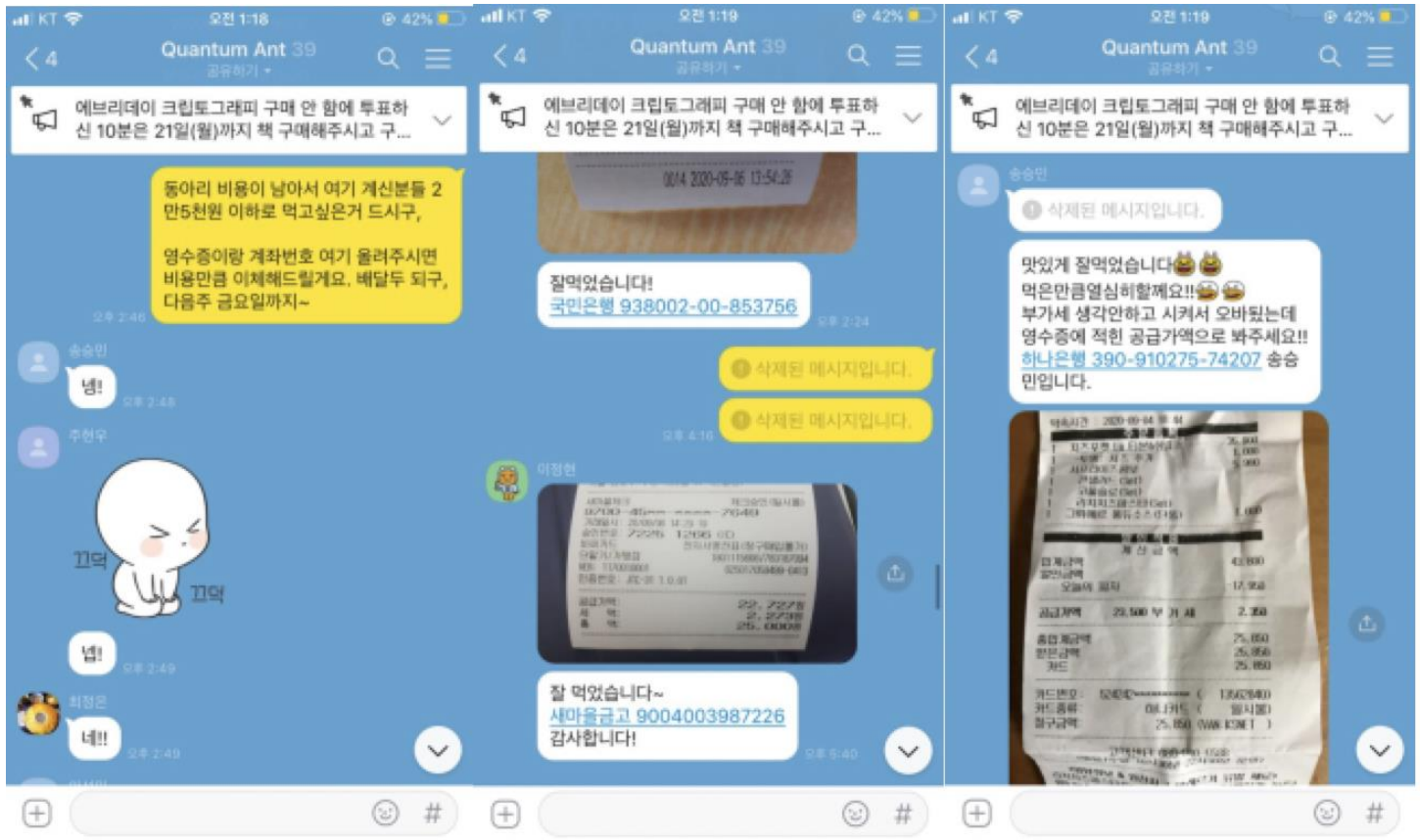
- 온라인 랜선 회식
  - 사회적 거리두기 강도가 높아짐에 따라 스카이프에 접속하여 온라인 회식 진행



< 온라인 랜선 회식 >

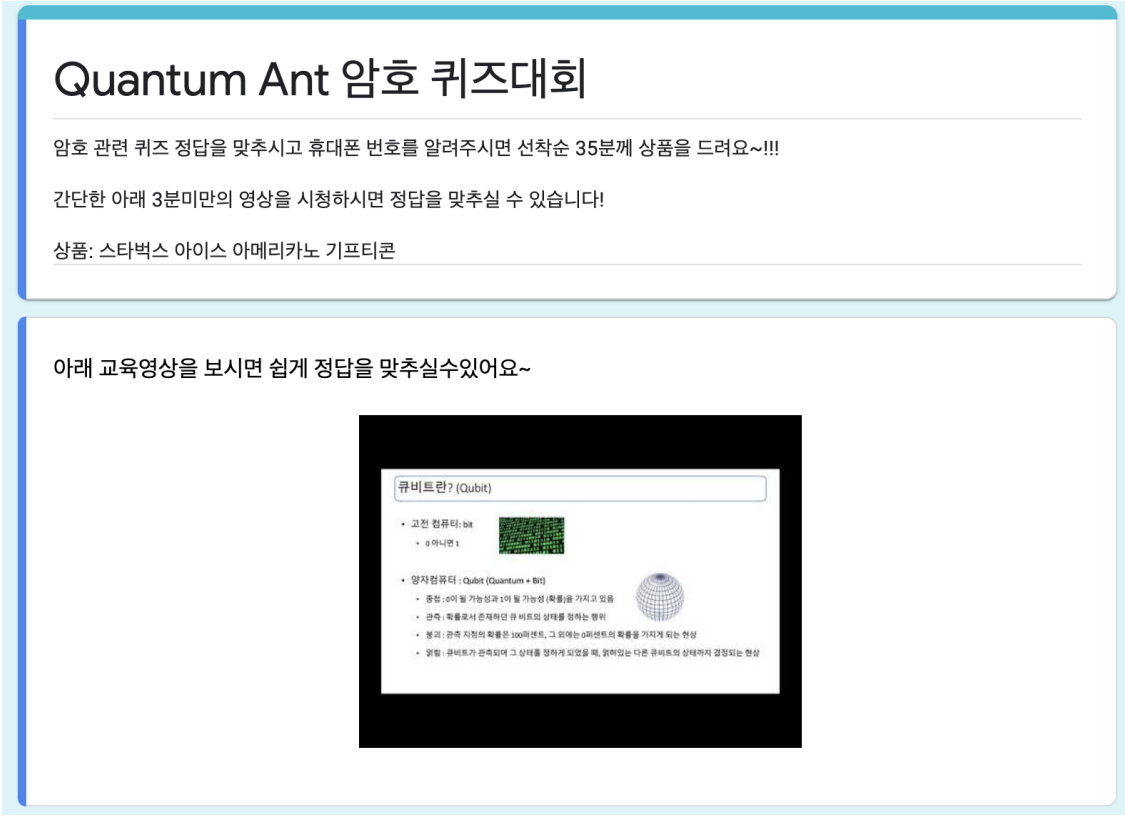
Quantum Ant : 최종보고

- 개인별 회식
  - 거리두기 2.5 단계까지 진행됨에 따라 단체 회식을 진행하지 못하여, 동아리 원들에게 각2,5000원 이하의 배달음식으로 회식을 대체



Quantum Ant : 최종보고

- 1차로 개최한 퀴즈대회의 반응이 좋아 2차를 개최
  - 2차로 열린 퀴즈 대회에서는 직접 제작한 교육영상을 시청해야 맞출 수 있는 난이도의 문제를 출시,
  - 정답자에게는 소정의 상품(스타벅스 기프티콘)을 증정



Quantum Ant : 최종보고

다음중 큐비트(양자비트)의 성질이 아닌 것은? *

- 중첩
- 얽힘
- 붕괴
- 의존

양자 컴퓨터의 계산능력에 안전한 암호 표준화를 위해 미국 국립표준기술연구소 (National Institute of Standards and Technology) 에서 진행중인 표준화 공모전은? *

- 경량암호 공모전
- 해시함수 공모전
- 양자내성암호 공모전
- 일자리 창출 아이디어 공모전

Quantum Ant : 최종보고

다음 중 2번 문제의 정답 공모전의 후보가 아닌 것은? *

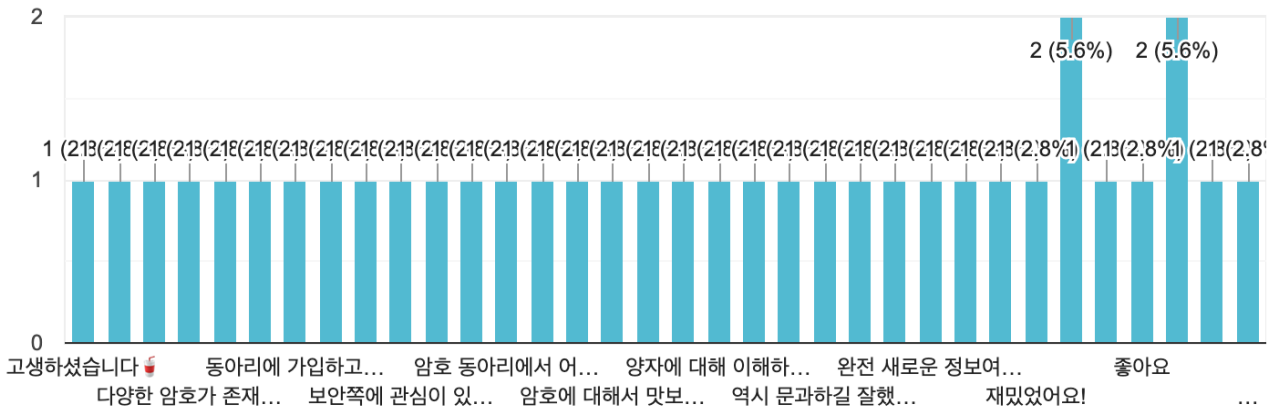
- 격자기반암호
- 코드기반암호
- 다변수기반암호
- 인공지능기반암호

퀴즈를 풀면서 느꼈던 점이나 동아리에 관심이 있으시다면 후기를 적어주세요~!

단답형 텍스트

퀴즈를 풀면서 느꼈던 점이나 동아리에 관심이 있으시다면 후기를 적어주세요~!

응답 36개

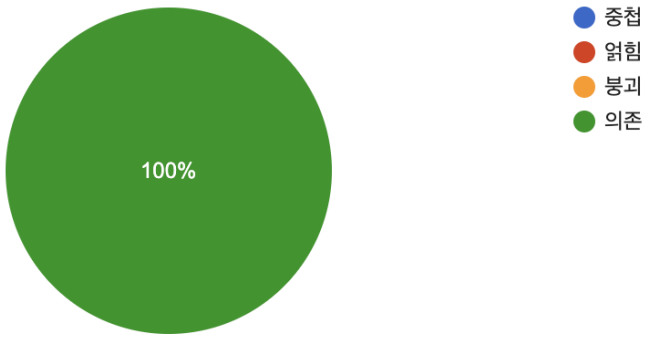


Quantum Ant : 최종보고

- 높은 정답률

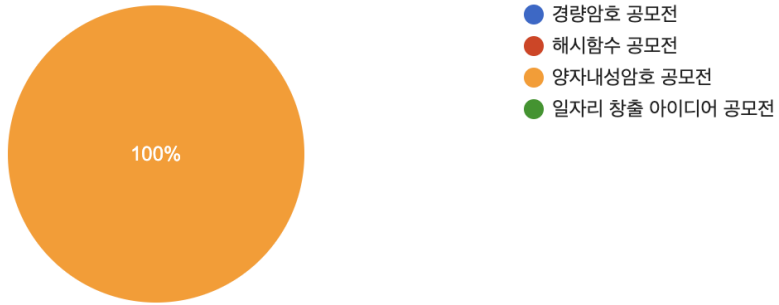
다음중 큐비트(양자비트)의 성질이 아닌 것은?

응답 50개



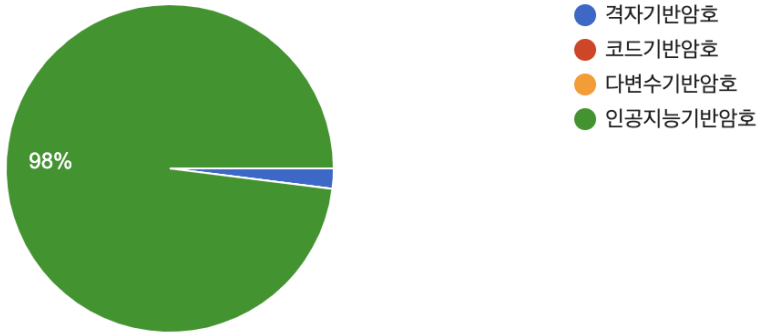
양자 컴퓨터의 계산능력에 안전한 암호 표준화를 위해 미국 국립표준기술연구소 (National Institute of Standards and Technology) 에서 진행중인 표준화 공모전은?

응답 50개



다음 중 2번 문제의 정답 공모전의 후보가 아닌 것은?

응답 50개



Quantum Ant : 최종보고

- 많은 학생들이 퀴즈 대회에 참여, 효과적인 동아리 홍보 및 신입회원 모집 성공

번호	제목	작성자	등록일	조회수
2	한성대학교 암호동아리 Quantum Ant 퀴즈 이벤트(기프티콘...	장경배	2020.08.19	163
1	한성대학교 암호동아리 Quantum Ant 설문조사 이벤트!!	최승주	2020.06.10	227

- 추천 제도를 진행 : 이미 동아리 활동하고 있는 동아리 원들의 친구들이 Quamtum Ant 동아리에 지원

Quantum Ant : 최종보고

분기 / 활동분야	1분기	2분기			3분기			4분기	가중치 (%)	달성률 (%)
	3	4	5	6	7	8	9	10		
- 동아리 홍보 및 팀별 인원 및 세부주제 선정									10	10
- 양자 내성 암호 알고리즘 동작구조 발표 (키생성, 암호화, 복호화) (1/2)									10	10
- 양자 내성 암호 알고리즘 동작구조 발표 (키생성, 암호화, 복호화) (2/2) - 양자 알고리즘을 사용한 공격동향 발표									15	10
중간보고서 제출 대표자 회의 및 국가암호공모전 참여									10	10
- 양자 게이트 학습 및 양자 프로그래밍 실습									15	15
- 연구 진행 발표 및 양자 암호 초청 세미나									15	15
최종 보고서 제출 대표자 회의 참석									10	10
- 최종 연구 종합 및 교육 영상 제작									15	15
분기별 진도 달성률(%)	10	30			40			15		95

Quantum Ant : 최종보고

동아리 지원금 활용 보고 (중간보고 후)

	비용	비고	합계
논문지 게재비(정보보호학회)	100,000	1회	100,000
초청강연 커피	39,000	1회	39,000
상품비(축제, 퀴즈대회)	143,440	1회	143,440
동아리 보안관련 서적 구매	258,800	8권	258,800
학술대회(CHES) 등록	151,140	5명	151,140
동아리원 개인별 회식비	557,740	23명	557,740
인터넷 강의	298,000	3개	298,000
온라인 회식 음식 구매	96,200		96,200
WISA 항공권 취소 수수료	25,000	3명	25,000
			1,669,320

동아리 지원금 잔여금 : 3,000,000 - 2,462,320 = 537,680원

신한할인 캐쉬백(6,490)이 입금되어 현재 통장잔액 = 544,170원

Q & A

감사합니다