

미래 양자컴퓨터 시대를 대비한 차세대 암호체계 추진 동향

2022. 6. 29.(수)

한국인터넷진흥원 차세대암호융합팀

김기문 팀장





Content

- I 양자 환경의 암호체계 안전성 위협
- II 양자 위협에 대응하는 차세대 암호
- III 국내외 표준화 및 정책 동향
- IV 국내외 상용화 및 시범적용 사례
- V 향후 준비사항 및 결론

KISA 차세대암호융합팀 소개



'22년 사업 소개

- (일반회계) 암호이용활성화
 - 암호기술 역기능 대응
 - 신변종 악성 랜섬웨어에 대한 암호기능 및 복구가능성 심층 분석(매년 4건)
 - 랜섬웨어 복구도구/매뉴얼 개발 및 랜섬웨어사후대응협의회 운영(매년 4회)
 - 암호기술 안전성 시험평가
 - 암호모듈검증 시험평가('22년 6건) 및 통합관리시스템 운영·관리
 - 암호모듈검증 전문가 교육(매년 2회) 및 중소·영세업체 대상 컨설팅 지원(매년 5개사)
 - 암호기술 응용기반 확대
 - 국내·외 암호기술 표준화 관련 제·개정 대응 및 소스코드/가이드 개발·보급
 - 산업분야별 암호이용 현황 및 차세대암호 적용 방안 등 암호이용 동향조사(매년 1회)
- (R&D) 동향암호 기반 동형기계학습 알고리즘 개발 및 라이브러리 구현
 - 동형기계학습 키 관리 통합 시스템 적용 시나리오 개발
 - 응용분야 별 동형기계학습 키 관리 통합 시스템 적용 시나리오 개발

KISA 차세대암호융합팀 소개



암호기술 역기능 대응

- 랜섬웨어 암호기능 심층 분석을 통한 복구 가능성 판단
 - 파일 암호화 시 사용한 암호 알고리즘(블록 암호, 스트림 암호, 공개키 암호) 분석
 - 암호키 생성 및 관리 관련 암호 API, 파일 암호화 방식 분석
 - 시스템 메모리 내 암호키 관련 정보 수집 및 분석
 - ※ 현재까지 신종 및 변종 랜섬웨어 25종 분석 완료 및 6종 복구 성공(복구율 24%)
- 피해 복구 지원을 위한 랜섬웨어 복구도구 개발 및 국내·외 배포
 - 분석 결과 기반 랜섬웨어 복구도구 및 사용 매뉴얼(한/영) 개발 후 배포
 - ※ (국내) KISA 암호이용활성화 홈페이지(<https://www.seed.kisa.or.kr>)
 - ※ (국외) 노모어랜섬 홈페이지(<https://www.nomoreranom.org>)

구분	Magniber	SimpleLocker	LooCipher	Ragnar	Immuni	Hive
국내	완료	완료	완료	완료	'22.7 예정	완료
국외	완료	완료	'22년 하반기 예정			

KISA 차세대암호융합팀 소개



암호기술 역기능 대응

- 분기별 랜섬웨어 동향 보고서 발간
 - 랜섬웨어 공격 및 사고사례, 국가별 랜섬웨어 대응 정책
 - 랜섬웨어 암호기능 분석 사례, 복구도구 개발 현황



Contents	
01. 개요	02
02. 랜섬웨어 사고사례	05
2.1. KISA 랜섬웨어 신고 현황(1Q)	05
2.2. KISA 랜섬웨어 신고사건(1Q)	05
2.3. KISA 랜섬웨어 신고사건(1Q)	05
2.4. Southgate International 한국 랜섬웨어 공격(2Q)	06
2.5. Microsoft의 랜섬웨어 공격(2Q)	06
2.6. BitLocker의 랜섬웨어 공격(2Q)	06
2.7. KISA 랜섬웨어 신고사건(1Q)	06
03. 랜섬웨어 관련 국내·외 대응	07
3.1. 미국, 중국, 영국 등 주요 국가의 랜섬웨어 대응 정책	07
3.2. 미국, 중국, 영국 등 주요 국가의 랜섬웨어 대응 정책	08
3.3. 미국의 랜섬웨어 대응 정책(2Q)	09
3.4. 미국의 랜섬웨어 대응 정책(2Q)	09
3.5. 미국의 랜섬웨어 대응 정책(2Q)	10
04. 1분기 신종·변종 랜섬웨어 동향	11
4.1. BlackCat 랜섬웨어	11
4.2. DoubleLocker 랜섬웨어	16
4.3. DoubleLocker 랜섬웨어	19
05. 랜섬웨어 복구 동향	22
5.1. 1분기 랜섬웨어 복구도구 개발 현황	22
06. 결론	27

- 랜섬웨어 피해 복구 확대를 위한 국내·외 관계 기관 협력
 - (국내) 국정원, 백신社 등과 협력하여 랜섬웨어 암호기능 분석 확대
 - (국외) 美 FBI, 유로폴(노모어랜섬) 등과 협력하여 국외 피해자 복구 지원

KISA 차세대암호융합팀 소개



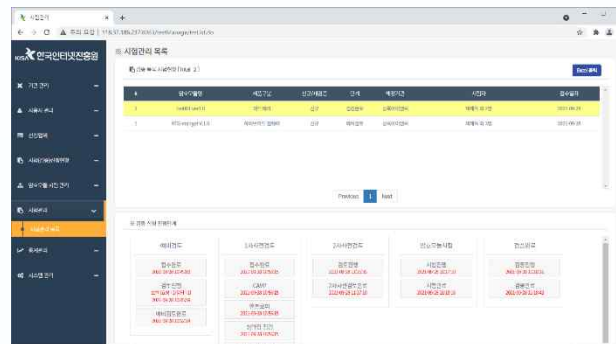
암호기술 안전성 시험평가

· 암호모듈검증 시험평가

구분	'18	'19	'20	'21	'22
검증 완료	2건	3건	4건	5건	6건 중 1건

· 암호모듈검증 통합관리시스템

- 사용자 : 암호모듈 시험 신청 및 진행 현황, 자가검증, 암호모듈 보완요청사항 등 확인
- 시험자 : 검증/재검증 신청, 암호모듈 통계 확인, 신청업체/사용자 등 관리
- 통합관리시스템 환경 구축(~8월), 시범 테스트(9월~12월)



KISA 차세대암호융합팀 소개



암호기술 안전성 시험평가

- 암호모듈검증 컨설팅

- 영세중소업체 대상 암호모듈/제출물 개발 및 요구사항 해석 등 지원
- 암호모듈 개발에 필요한 샘플 모듈/매뉴얼 제공을 통한 암호모듈 컨설팅

구분	'20	'21	'22
지원 업체 수	5개	5개	5개 지원 예정

- 암호모듈검증 전문교육

- 기초과정 : 암호수학/알고리즘, 암호모듈 검증기준 등 이론 중심
- 심화과정 : 암호수학/알고리즘, 암호모듈 개발 방법 등 구현 중심

구분	'20	'21	'22
지원 업체 수	580명	455명	258명

KISA 차세대암호융합팀 소개



암호기술 응용기반 확대

- 국내 암호기술 개발 및 이용 현황 파악을 위한 암호이용 동향조사
 - 기업에서 개발한 암호제품의 유형, 판매 수요처, 사용 암호알고리즘 등 조사
 - 조사된 결과를 분석·재가공하여 암호이용 동향조사 보고서 발간(예정)
- KISA가 개발한 암호기술(4종) 및 KCMVP 관련 암호기술 소스코드 개발·배포

구분			C/C++	Java	ASP	JSP	PHP
1	블록암호	SEED	O	O	O	O	O
2		HIGHT	O	O	-		
3	해시함수	SHA-2	O	O	O	O	O
4		SHA-3	O	O	O	O	O
5	메시지인증	HMAC	O	O	O	O	O
6	난수발생기	CTR_DRBG	O	O	-		
7	전자서명	EC-KCDSA	O	O	-		
8		KCDSA	O	O	-		
9	키 유도 함수	KBKDF	O	O	O	O	O
10		PBKDF	O	O	-		

KISA 차세대암호융합팀 소개



암호기술 응용기반 확대

- 암호알고리즘/키 길이 이용, 양자컴퓨터 환경에서의 암호기술 이용 등 안내서 보급

순번	암호기술 안내서
1	패스워드 선택 및 이용 안내서(2008.01)
2	다양한 보안 프로토콜에서의 SEED 활용 가이드라인(2008.06)
3	개인정보DB 암호화 관리 안내서(2009.10)
4	웹사이트 회원탈퇴 기능 구현 안내서(2009.10)
5	보조기억매체 이용 안내서(2010.01)
6	상용 소프트웨어에서의 암호기능 이용 안내서(2012.12/2013.06)
7	암호정책 수립기준 설명서(2013.12)
8	암호기술 구현 안내서(2013.12)
9	암호이용 안내서(2013.12)
10	암호 키 관리 안내서(2014.12)
11	HTML5 암호기술 이용 안내서(2015.12)
12	사물인터넷(IoT) 환경에서의 암호인증기술 이용 안내서(2017.12)
13	양자컴퓨팅 환경에서의 암호기술 이용 안내서(2017.12)
14	암호 알고리즘 및 키 길이 이용 안내서(2018.12)
15	패스워드 선택 및 이용 안내서(2019.06)

- 국내(TTA, KS) 및 국외(ISO/IEC) 표준화 기구 활동
 - 국내(건), 국외(건) 표준화 제개정 작업
 - ISO/IEC 19790/24759 등 국내·외 표준화 개정 작업 중

KISA 차세대암호융합팀 소개



연구개발 과제

- 격자기반 양자내성 공개키암호 스킴 개발('17~'19)
 - SW·HW 및 응용환경(통신프로토콜)에 대한 양자내성암호 Lizard/Rlizard 최적 구현
 - NIST(국외) 및 TTA(국내) 표준 알고리즘 제안
 - SW 등록 6건, 기술문서 6건, 논문 4건(국외 1건, 국내 3건)
- 경량암호 등의 암호 안전성 분석 자동화 기술 개발('17~'19)
 - 암호 키관리 안전성 분석 도구 개발 및 테스트
 - 기술문서 3건, 논문 9건(국외 3건, 국내 6건)
- 동형암호화된 데이터의 심층신경망 연산을 지원하는 완전 동형암호 알고리즘 개발 및 라이브러리 구현('20~'23)
 - 동형암호 키 관리 정책·기술 동향 분석 및 프레임워크 개발
 - 동형암호 키 관리 프레임워크 관련 TTA 표준화 제안 예정('22.10~)

KISA 차세대암호융합팀 소개



'23년 사업 확대 계획

- 차세대 암호기술 이용환경 조성
 - 차세대암호 전환체계 마련
 - 차세대암호 전환 지원을 위한 플랫폼 운영 및 기준·가이드 마련
 - 차세대 암호기술을 적용한 서비스의 성능 실증·비교·검증 등 시범적용
 - 차세대 암호산업 육성 기반 조성
 - 차세대 암호기업 육성을 위한 인큐베이팅, 개발·테스트 플랫폼 지원 등 기술지원
 - 대학(원)생 및 구직·재직자 대상 차세대암호 전문인력 양성을 위한 아카데미 운영
 - 차세대 암호기술 테스트 환경 구축 및 지원
 - 차세대 암호기술 안전성 기준 개발을 통한 취약성 분석·검증 환경 구축·운영
 - 차세대 암호제품의 성능 실증을 위한 가상화 기반 테스트베드 구축·운영
- AI 기반 랜섬웨어 고속 분류 및 암호기능 자동화 분석
 - 랜섬웨어에서 사용되는 암호 API, 암호키 생성 및 암호화 동작 과정, 볼륨 웨도우 삭제 방법, 네트워크 전송 방법 등을 통한 랜섬웨어 그룹화를 통한 고속 분류
 - 랜섬웨어 동작을 통한 암호 API 후킹, 랜섬웨어 정적 분석을 통한 암호 정보 확인 등의 복구기술 노하우를 통한 암호기능 자동화 분석을 통한 복구가능성 확인

The background features a stylized network diagram with nodes and connecting lines. A prominent blue banner with a diagonal line pattern is positioned across the middle. The bottom left corner contains the KISA logo and the text '한국인터넷진흥원'.

I 양자 환경의 암호체계 안전성 위협

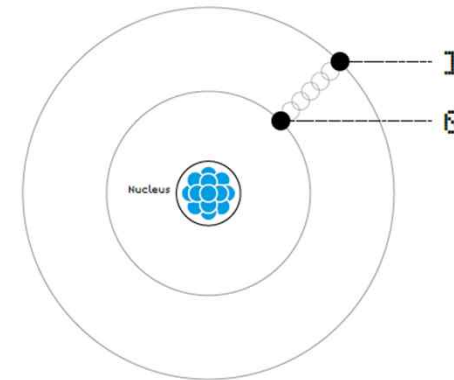
I 양자 환경의 암호체계 안전성 위협



양자 기술이란? (1/3)

- 양자(Quantum)

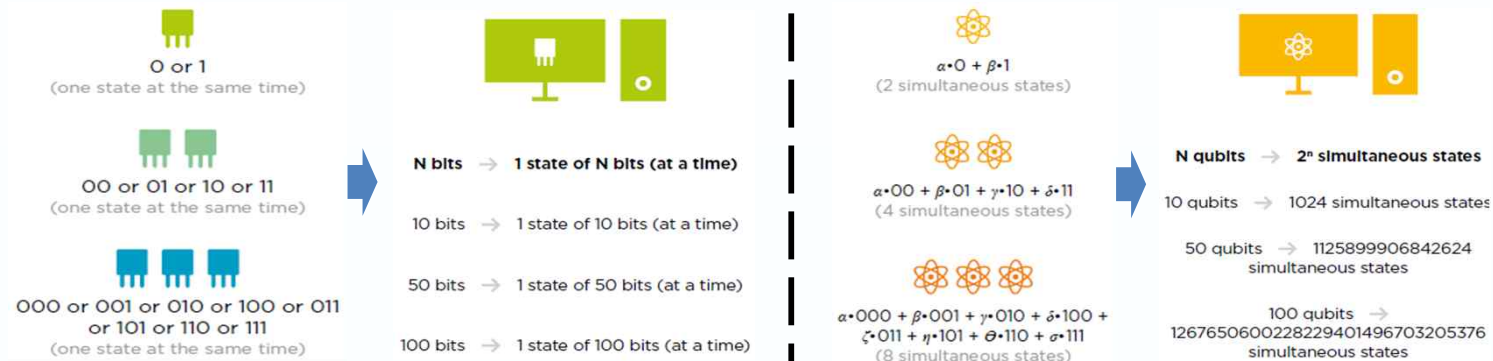
- 더 이상 나눌 수 없는 에너지의 최소 단위
- 광자, 전자 등 미시세계의 물질이 갖는 물리량



- 큐비트(Qubit, Quantum bit)

- 양자를 정보로 나타내기 위한 기본단위
- 고정적인 상태(0 or 1)를 갖는 비트와 달리 하나의 큐비트가 두 상태를 동시에 보유

[고전 비트 vs 큐비트]



I 양자 환경의 암호체계 안전성 위협



양자 기술이란? (2/3)

• 양자의 물리적 특성

- 중첩(Superposition)
 - 양자는 여러 상태를 동시에 보유 가능하며, 측정 시에만 붕괴되어 고정
 - 큐비트를 이용해 여러 정보를 동시에 처리할 수 있도록 함
- 얽힘(Entanglement)
 - 두 개 이상의 양자가 상호작용하여 연관된 상태를 가짐
 - 상호작용된 큐비트를 통해 연산 및 통신 등의 속도 향상
- 불확정성(Uncertainty)
 - 양자 측정 시 두 가지 이상의 물리량을 동시에 측정할 수 없음
 - 큐비트 전송 과정에서 도청자가 정보를 얻을 수 없도록 함
- 복제 불가능(No-cloning)
 - 동일한 상태의 양자를 복제하는 것이 불가능함
 - 불확정성과 같이 도청자의 정보 획득을 방지

I 양자 환경의 암호체계 안전성 위협

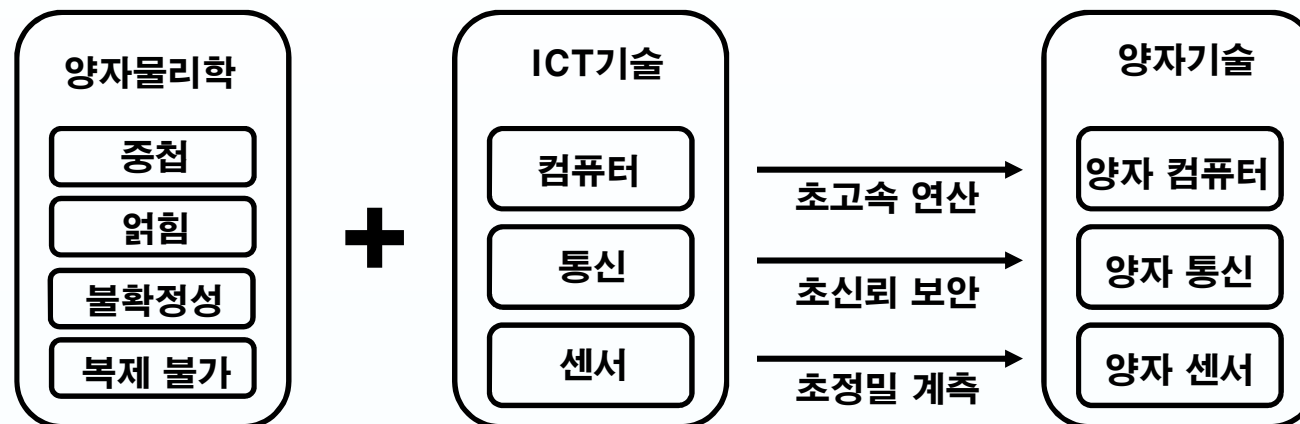


양자 기술이란? (3/3)

- 양자 기술

- 양자의 여러 물리적 성질을 ICT 각 분야에 접목한 기술

- 양자 컴퓨터 : 중첩된 다수 양자의 동시 계산을 통한 초고속 연산
 - 양자 통신 : 양자의 특성을 이용해 도청 및 복제가 불가능한 초신뢰 보안
 - 양자 센서 : 외부 작용 시 양자의 상태 변화를 이용한 정밀 계측



※ 분류 기준 : 양자 기술 연구개발 투자 전략(2021), 과학기술정보통신부

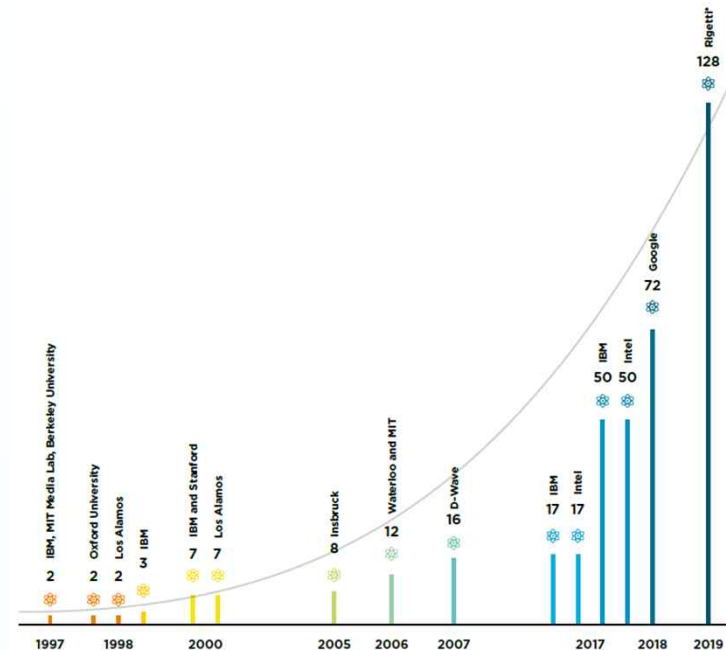
I 양자 환경의 암호체계 안전성 위협



양자 기술 - 양자 컴퓨터(1/2)

- 양자 컴퓨터(Quantum Computer)란?
 - 양자물리학적 현상을 이용하여 정보를 처리하는 장치
 - 양자 컴퓨터를 이용하여 다양한 큐비트 연산을 수행 가능

- 양자 컴퓨터 개발 현황
 - 국외 : IBM, Google 등 글로벌 기업 중심으로 개발 진행(128큐비트 수준)
 - 국내 : 기관(KIST 등) 및 학계 중심 연구개발 진행



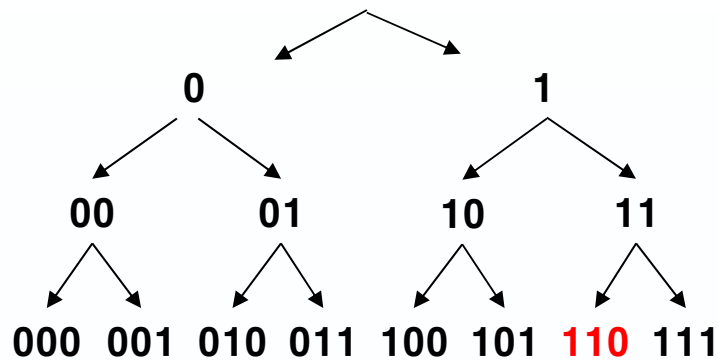
I 양자 환경의 암호체계 안전성 위협



양자 기술 - 양자 컴퓨터(2/2)

- 양자 알고리즘 : 양자 컴퓨터에서만 수행되는 큐비트 연산 알고리즘
- 간단한 예시 - 3비트 탐색 연산
 - 정답 비트 '110'을 찾는 문제를 가정

고전 비트 연산(Brute-force)



→ 최대 7회 연산 필요

→ 비트 수가 증가할수록 기하급수적인 속도 차이 발생

큐비트 연산 (Grover 알고리즘)

상태	확률		상태	확률		상태	확률
000	1		000	0.03		000	0.00
001	0		001	0.03		001	0.01
010	0		010	0.04		010	0.01
011	0		011	0.03		011	0.01
100	0	양자 연산	100	0.03	양자 연산	100	0.01
101	0		101	0.03		101	0.00
110	0		110	0.77		110	0.95
111	0		111	0.04		111	0.01

→ 단 2회 연산으로 정답에 근접

I 양자 환경의 암호체계 안전성 위협



양자 기술 - 양자 통신 및 센서

- 양자 통신(Quantum Communication)
 - 양자의 물리적 특성을 이용한 도·감청 및 해킹을 차단하는 통신 기술
 - 도청자가 존재할 경우 양자의 상태 변화를 통해 감지 가능



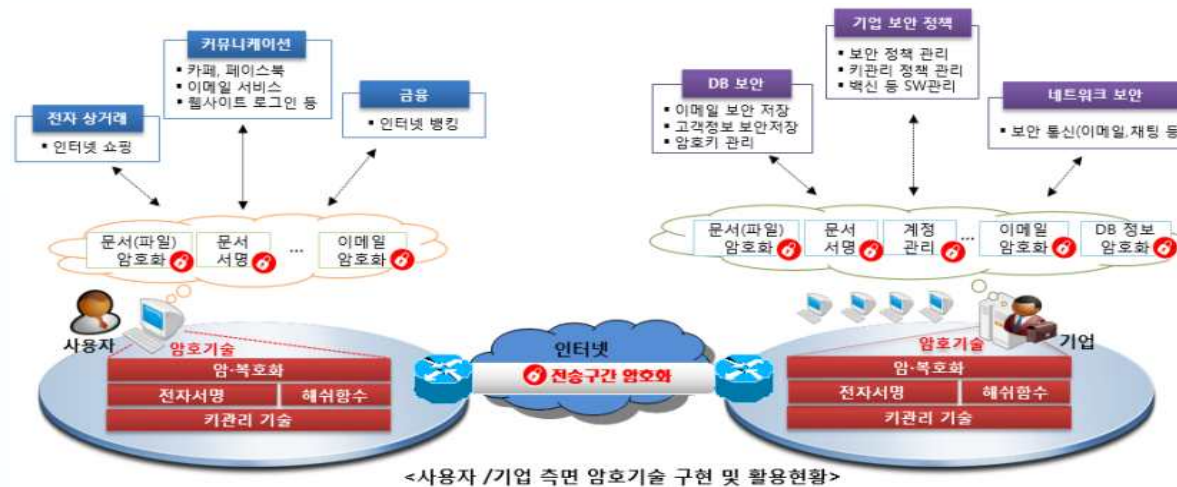
- 양자 센서(Quantum Sensor)
 - 외부 작용에 쉽게 변화하는 양자의 특성을 이용한 초정밀 측정 기술
 - 탐지대상 물체와 양자와의 상호작용에 의한 상태 변화 측정

I 양자 환경의 암호체계 안전성 위협



암호기술 개요(1/2)

- 배경 : 암호기술의 중요성
 - 모든 정보보호제품 및 서비스의 근간을 이루는 정보보호의 기반기술
 - 전자거래, 스마트폰, 웹서비스, 공동·금융인증서 등 일상생활에 필수적



I 양자 환경의 암호체계 안전성 위협



암호기술 개요(2/2)

- 암호기술의 주요기능
 - 대칭키 암호(Symmetric Key Cryptography)
 - 데이터의 기밀성, 무결성 보장 등 기본기능을 제공하는 암호기술
 - 블록암호, 해시함수 프리미티브 및 MAC, 난수발생기 등 포함
 - 암호·복호화를 통한 데이터 보호, 인증 및 무결성 검증, 비밀정보 생성 등
 - 공개키 암호(Public Key Cryptography)
 - 대칭키 암호기술의 키 관리 문제를 해결하기 위해 개발된 암호기술
 - 공개키 암호·복호화(PKE), 키 교환(KEM), 전자서명(Digital Signature) 등 포함
 - 데이터 및 암호키의 안전한 전송/교환, 서명 및 인증 등
- 암호기술이 붕괴된다면?
 - 정보화 시대에 개인 및 기업의 가장 큰 자산인 데이터의 보호 수단이 사라지며, 전자거래 등 모든 ICT 인프라 사용자 간의 신뢰를 더 이상 보장할 수 없음

I 양자 환경의 암호체계 안전성 위협



양자 환경의 위협(1/2)

- 양자 알고리즘(Quantum Algorithm)
 - 양자 컴퓨터에서 양자 중첩, 양자얽힘 등 양자(Quantum)의 성질을 이용하여 빠른 연산 수행 가능
- 쇼어의 알고리즘(1994)
 - 공개키암호를 해독할 수 있는 양자알고리즘
 - 기존 공개키암호 설계방식인 인수분해(RSA), 이산대수(DH) 문제를 빠르게 연산하여 해독
- 그로버의 알고리즘(1996)
 - 대칭키 암호에 대한 암호키 검색 능력 상승

Algorithms for Quantum Computation: Discrete Logarithms and Factoring

Peter W. Shor
AT&T Bell Labs
Room 2D-149
600 Mountain Ave.
Murray Hill, NJ 07974, USA

Abstract

A computer is generally considered to be a universal computational device; i.e., it is believed able to simulate any physical computational device with a cost in computation time of at most a polynomial factor. It is not clear whether this is still true when quantum mechanics is taken into consideration. Several researchers, starting with David Deutsch, have developed models for quantum mechanical computers and have investigated their computational properties. This paper gives Las Vegas algorithms for finding discrete logarithms and factoring integers on a quantum computer that take a number of steps which is polynomial in the input size, e.g., the number of digits of the integer to be factored. These two problems are generally considered hard on a classical computer and have been used as the basis of several proposed cryptosystems. (We thus give the first examples of quantum cryptanalysis.)

1 Introduction

Since the discovery of quantum mechanics, people have found the behavior of the laws of probability in quantum mechanics counterintuitive. Because of this behavior, quantum mechanical phenomena behave quite differently than the phenomena of classical physics that we are used to. Feynman seems to have been the first to ask what effect this has on computation [13, 14]. He gave arguments as

[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give an explicit model of quantum computation. He defined both quantum Turing machines and quantum circuits and investigated some of their properties.

The next part of this paper discusses how quantum computation relates to classical complexity classes. We will thus first give a brief intuitive discussion of complexity classes for those readers who do not have this background. There are generally two resources which limit the ability of computers to solve large problems: time and space (i.e., memory). The field of analysis of algorithms considers the asymptotic demands that algorithms make for these resources as a function of the problem size. Theoretical computer scientists generally classify algorithms as efficient when the number of steps of the algorithms grows as a polynomial in the size of the input. The class of problems which can be solved by efficient algorithms is known as P. This classification has several nice properties. For one thing, it does a reasonable job of reflecting the performance of algorithms in practice (although an algorithm whose running time is the tenth power of the input size, say, is not truly efficient). For another, this classification is nice theoretically, as different reasonable machine models produce the same class P. We will see this behavior reappear in quantum computation, where different models for

< 쇼어 알고리즘을 이용한 RSA 공격 소요시간 >

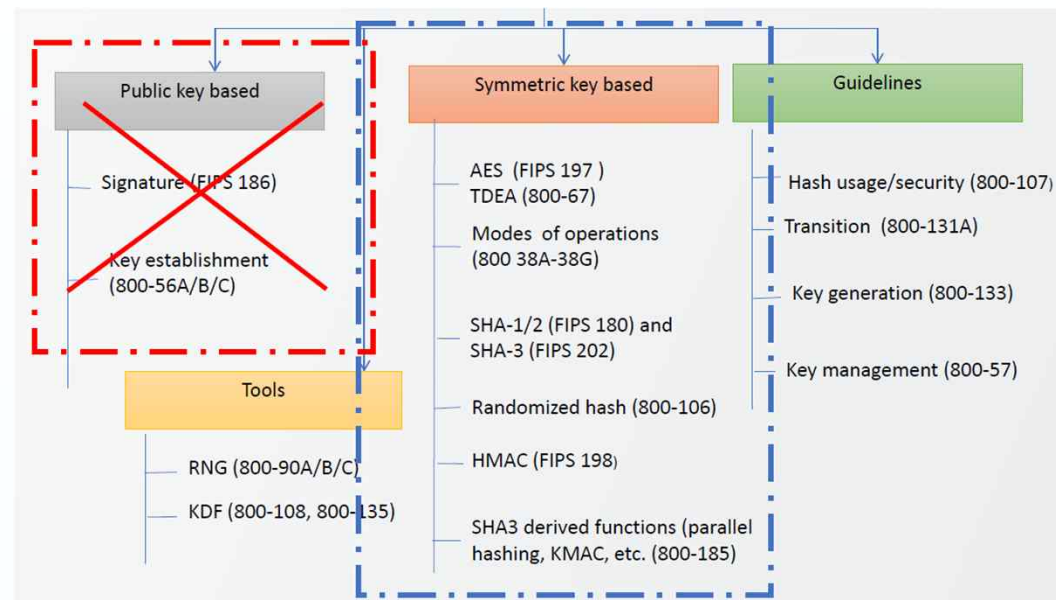
size in bits	1024	2048	4096
number of qubits	5124	10244	20484
number of gates	3×10^9	2×10^{11}	2×10^{12}
factoring time	4.5 min.	36 min.	4.8 hours

I 양자 환경의 암호체계 안전성 위협



양자 환경의 위협(2/2)

- 암호체계의 안전성 위협
 - 모든 ICT·정보보호 서비스 및 시스템에서 사용되는 암호체계에 영향
 - 공개키 암호(RSA, DH 등)는 더 이상 사용이 불가하며(쇼어),
대칭키 암호(AES, ARIA, SHA 등)는 키 길이 등 안전성 강화 필요(그로버)





Ⅱ 양자 위협에 대응하는 차세대 암호

II 양자 위협에 대응하는 차세대 암호



대칭키 암호 고도화

- 대칭키 암호체계(Symmetric Key Cryptosystem)

보안강도	Quantum	56	64	96	112	128
	Classical	112	128	192	224	256

- 블록암호

- SEED, ARIA, LEA, HIGHT, AES, ...
- 암호키 길이 2배 이상 확대(224비트 이상) 필요

- 해시함수

- SHA-2, SHA-3, LSH, ...
- 출력 해시 길이 3배 이상 확대(336비트 이상) 필요

II 양자 위협에 대응하는 차세대 암호



양자내성암호(PQC) (1/2)

- 공개키 암호체계(Public Key Cryptosystem)
 - 공개키 암호(PKE)
 - 키 교환(KEM)
 - 전자서명(Signature)
- 양자내성암호(Post-Quantum Cryptography)로 대체 필요

암호기능	알고리즘
공개키 암호	RSA, ECC, ...
키 교환	DH, ECDH, ...
전자서명	RSA, KCDSA, ECDSA, ...



암호기능	알고리즘
공개키 암호 /키 교환	NTRU, Kyber, ...
전자서명	Dilithium, Falcon, ...

II 양자 위협에 대응하는 차세대 암호



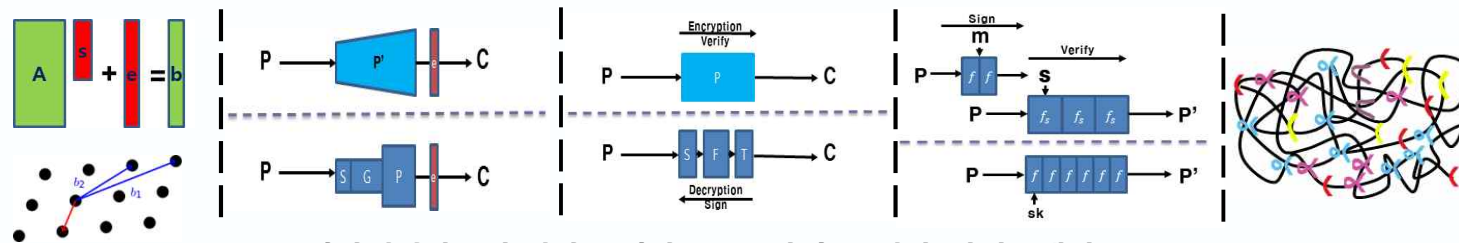
양자내성암호(PQC) (2/2)

· 양자내성암호란?

- 양자 컴퓨터 환경에서도 안전하도록 설계된 공개키 기반 알고리즘
- 양자 컴퓨터로도 해결 불가능한 다양한 수학적 난제에 기반한 안전성

※ 기존 공개키 알고리즘은 양자 컴퓨터로 쉽게 해결되는 인수분해 및 (타원곡선)이산대수 문제 기반

- 격자 기반 : 격자 구조에서 최단거리 벡터 등 비밀 벡터를 찾는 문제
- 코드 기반 : 비밀 행렬로 구성된 선형 코드의 디코딩 문제
- 다변수 기반 : 비밀 성분으로 구성된 다변수 이차식 문제
- 해시함수 기반 : 암호학적 해시함수의 충돌쌍을 찾는 문제
- 아이소제니 기반 : 타원곡선 간의 관계 연산을 찾는 문제



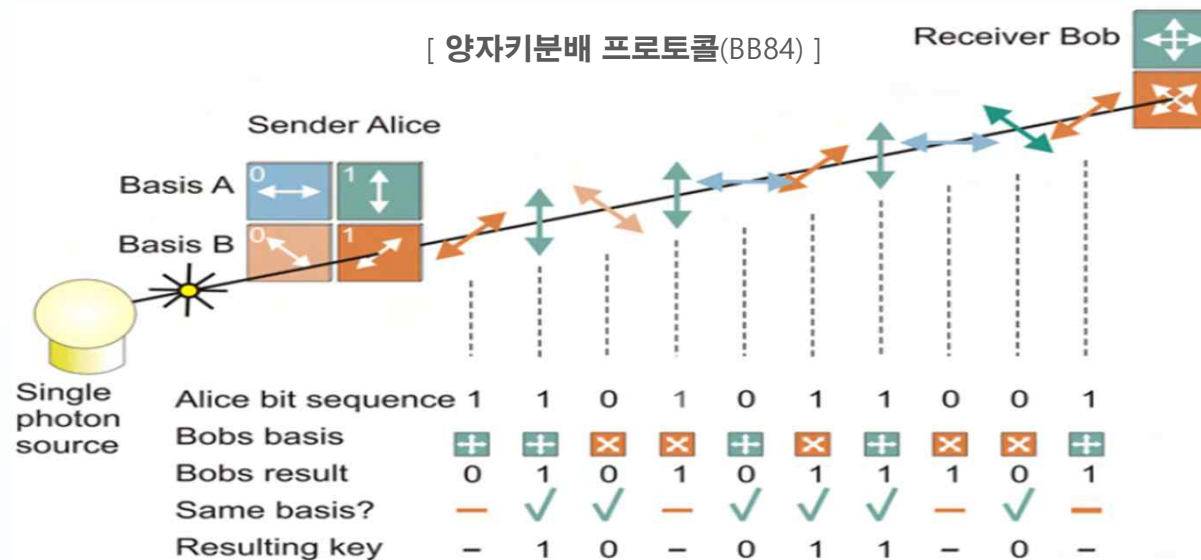
[양자내성암호의 개념도(격자, 코드, 다변수, 해시, 아이소제니)]

II 양자 위협에 대응하는 차세대 암호



양자키분배(QKD)

- 다른 선택지 : 양자키분배(Quantum Key Distribution)
 - 양자물리학적 원리를 통한 암호키 교환 기술
 - 측정 정보 동기화 이후 광자 전송을 통해 암호키를 갱신
 - 기존 공개키 암호체계 중 키 교환(KEM) 대체를 위해 고려 가능



II 양자 위협에 대응하는 차세대 암호



양자내성암호 vs 양자키분배 (1/2)

- 범위 및 용어 정리

양자 환경의 차세대 암호기술

양자내성암호(PQC)

- 수학적 난제를 이용한 차세대 암호기술
- 공개키 암호(PKE), 키 교환(KEM) 및 전자서명(SIG) 대체

양자암호(QC)

- 양자물리학적 원리를 이용한 차세대 암호기술

양자키분배(QKD)

- 양자암호기술 중 현재 알려진 실용화 기술
- 키 교환(KEM) 대체

양자난수발생기(QRNG)

II 양자 위협에 대응하는 차세대 암호



양자내성암호 vs 양자키분배 (2/2)

• 활용 방안

- 양자내성암호와 양자키분배는 상호 보완적인 관계
- 국방·금융 등 국가 최중요 데이터는 양자내성암호/양자키분배 혼용, 보편적인 중요 데이터는 양자내성암호를 활용하여 보호하는 방향성

	양자내성암호(PQC)	양자키분배(QKD)
기반문제	• 수학적 난제 기반	• 양자물리학 원리 기반
주요기능	• 공개키 암호·복호화 • 전자서명 • 암호키 교환	• 암호키 교환
장점	• SW·HW 등 기존 응용환경 적용 가능 • 암호·복호화, 인증 등 모든 암호기능 제공	• 공격자의 연산능력에 관계없는 안전성
단점	• 공격 기법 발전으로 인한 잠재적 위험 가능성	• 전용 HW장비 필요 및 이로 인한 고비용 • 장거리 통신의 어려움 • 전자서명 등 인증기능 부재



Ⅲ 국내외 표준화 및 정책 동향

Ⅲ 국내외 표준화 및 정책 동향



표준화(NIST) (1/4)

- **추진경과**

- 양자내성암호 알고리즘 공모전 및 표준화 일정 공지 (2016)
 - ✓ 2024년까지 표준화 완료
- 1라운드: 82종 알고리즘을 제출받아 69개 선정(2017. 7월)
- 2라운드: 26개의 알고리즘 선정 (2019. 2월)
- 3라운드 후보 15종(Finalists 7종, Alternates 8종) 선정 (2020. 7월)

- **알고리즘 평가기준**

- ◆ 안전성: 고전 공격 및 양자 공격 내성
- ◆ 성능: 다양한 컴퓨팅 플랫폼에서 측정
- ◆ 기타: 대체 용이성, 부채널 공격 내성, 단순함 및 유연성, 오용에 대한 내성 등

Ⅲ 국내외 표준화 및 정책 동향



표준화(NIST) (2/4)

• 3라운드 후보

- 수개월 내 3라운드 결과가 발표될 것으로 예상됨(PKC 2022, 3월)

기능	기반문제	최종후보 (7종)	대체 후보(8종)	특이사항
PKE / KEM	격자	NTRU CRYSTALS-KYBER SABER	FrodoKEM NTRUprime	<ul style="list-style-type: none"> • 범용 환경에 적합 • 1종 표준화 예정 • IPR 이슈
	코드	Classic McEliece	Bike HQC	<ul style="list-style-type: none"> • 특수 환경에 적합 • 0~1종 표준화 예상
	아이소제니	-	SIKE	-
서명	격자	CRYSTALS-Dilithium Falcon	-	<ul style="list-style-type: none"> • 범용 환경에 적합 • 1종 표준화 예정
	다변수	Rainbow	GeMSS	<ul style="list-style-type: none"> • 특수 환경에 적합 • 안전성 문제 발생
	해시	-	Picnic SPHINCS+	<ul style="list-style-type: none"> • 높은 안전성(SPHINCS+) • 0~1종 표준화 예상

III 국내외 표준화 및 정책 동향



표준화(NIST) (3/4)

- 3라운드 주요 이슈
 - IPR(지식재산권) 이슈
 - 표준화가 완료되면 NIST는 선정 알고리즘에 대한 특허권을 양도받을 예정
 - 그러나 일부 알고리즘에 대해서는, NIST가 구현 기법 등 원천기술에 대한 특허권을 확보하지 못할 수 있음
 - NIST는 3라운드에서 알고리즘 선정 시 해당 문제를 적극적으로 고려할 것임
 - 안전성 이슈
 - 다변수 기반 서명 알고리즘(Rainbow, GeMSS) 안전성 이슈 발생
 - 다변수 기반 알고리즘은 3라운드에서 선정되지 못할 가능성이 높음
 - NIST는 (작은 서명 등) 특수 환경에 적합한 알고리즘을 선정하기 위한 새로운 공모를 4라운드에서 추진 예정

Ⅲ 국내외 표준화 및 정책 동향



표준화(NIST) (4/4)

- 해시 기반 서명 알고리즘 표준

- 안전성이 증명된 해시 기반 서명 알고리즘의 경우 별도 표준화가 진행중
 - 상태 저장(Stateful) 해시 기반 서명에 대한 스페셜 가이드(SP 800-208) 발간

문서	주요내용
NIST SP 800-208	<ul style="list-style-type: none">• Recommendation for Stateful Hash-Based Schemes (2020. 10월 완료)<ul style="list-style-type: none">▪ Stateful 해시 기반 서명 알고리즘 (XMSS 및 LMS)▪ FIP186-4 (디지털서명표준) 문서 대체용

III 국내외 표준화 및 정책 동향



표준화(IETF)

· 알고리즘 및 응용환경 표준

- 해시 기반 서명 알고리즘 및 IETF에서 다양한 통신 프로토콜에서의 하이브리드 키교환, 해시 기반 서명 등 양자내성암호 알고리즘 사용 방안에 대한 표준 발간

문서	주요내용
RFC 8391	• XMSS: eXtended Merkle Signature Scheme (2019. 5월) (해시 기반 서명 알고리즘 XMSS)
RFC 8554	• Leighton-Micali Hash-Based Signatures (2019. 4월) (해시 기반 서명 알고리즘 LMS)
RFC 8784	• Post-quantum 안전성을 위한 IKEv2 사전 공유키 혼합 <ul style="list-style-type: none">▪ IKEv2의 사전 공유 키 공격에 대비하기 위한 PQ기법
RFC 8778	• CMS에서의 HSS/LMS 해시 기반 전자서명 사용 <ul style="list-style-type: none">▪ CMS(Cryptographic Message Syntax) 프로토콜에서 해시 기반 PQ 알고리즘 HSS 및 LMS 사용 방법
RFC 8784	• COSE에서의 HSS/LMS 해시 기반 전자서명 사용 <ul style="list-style-type: none">▪ COSE(CBOR Object Signing and Encryption) 프로토콜에서 해시 기반 PQ 알고리즘 HSS 및 LMS 사용 방법
Draft	• TLS 1.2를 위한 하이브리드 양자내성 키교환 <ul style="list-style-type: none">• ECDH와 PQ 알고리즘을 사용하는 하이브리드 키교환 프로토콜
Draft	• IKEv2 사전 공유 키 혼합 방식에 대한 대안적 접근 <ul style="list-style-type: none">▪ RFC 8784의 예외사항인 Initial IKEv2 SA를 포함

Ⅲ 국내외 표준화 및 정책 동향



표준화(ITU-T SG17)

· ITU-T SG17 사이버 보안 표준

- 5G 시스템에 대한 양자내성암호 지침 표준 발간
- X.509 PKI 표준에 양자내성암호 관련 업데이트 진행 중

문서	주요내용
ITU-T X.1811 (X.5GSec-q)	Security guidelines for applying quantum-safe algorithms in 5G systems (5G 환경에서 사용되는 암호알고리즘의 양자 위협 식별 및 PQ 알고리즘 사용 지침 제시)
ITU-T X.509	Information technology – Open Systems Interconnection – The directory: Public-key and attribute certificate frameworks - 공개키 기반(PKI) 표준 X.509에 대한 PQ 알고리즘 업데이트 진행

III 국내외 표준화 및 정책 동향



표준화(ETSI)

· 산업계 표준

- ETSI에서는 알고리즘 자체보다는 산업계 요구사항을 고려한 문서 발간
- 산업계 양자내성암호 전환 및 적용 관련 문서 발간

문서	주요 내용
ETSI GR QSC 001 V1.1.1	양자내성암호 알고리즘 프레임워크
ETSI GR QSC 006 V1.1.1	대칭키 암호에 대한 양자컴퓨팅 한계
ETSI GR QSC 003 V1.1.1	PQC 사례 연구 및 발전 시나리오
ETSI GR QSC 004 V1.1.1	양자내성 위협 분석
ETSI TR 103 570 V1.1.1	양자내성 키교환
ETSI TR 103 617 V1.1.1	양자내성 VPN
ETSI TR 103 618 V1.1.1	양자내성 신원기반 인증
ETSI TR 103 619 V1.1.1	마이그레이션 전략 및 스킴 권고사항
ETSI TS 103 744 V1.1.1	양자내성 하이브리드 키교환

Ⅲ 국내외 표준화 및 정책 동향



표준화(국내)

- TTA 양자내성암호 알고리즘 표준화
 - 격자 기반 공개키 암호 알고리즘 Ring-Lizard(2019)
 - 다변수 기반 공개키 암호 알고리즘 HiMQ(2020)
- KpqC 연구단(2021~)
 - 목적 : 행정기관, 공공용 양자내성암호 공모 및 표준화
 - 주관 : KpqC 연구단
 - 활동기간 : '21년 11월 ~ '24년 9월
 - 선정 알고리즘 : 2~3종
 - 최종목표 : 암호모듈검증(KCMVP) 대상 보호함수 지정



Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(미국) (1/5)

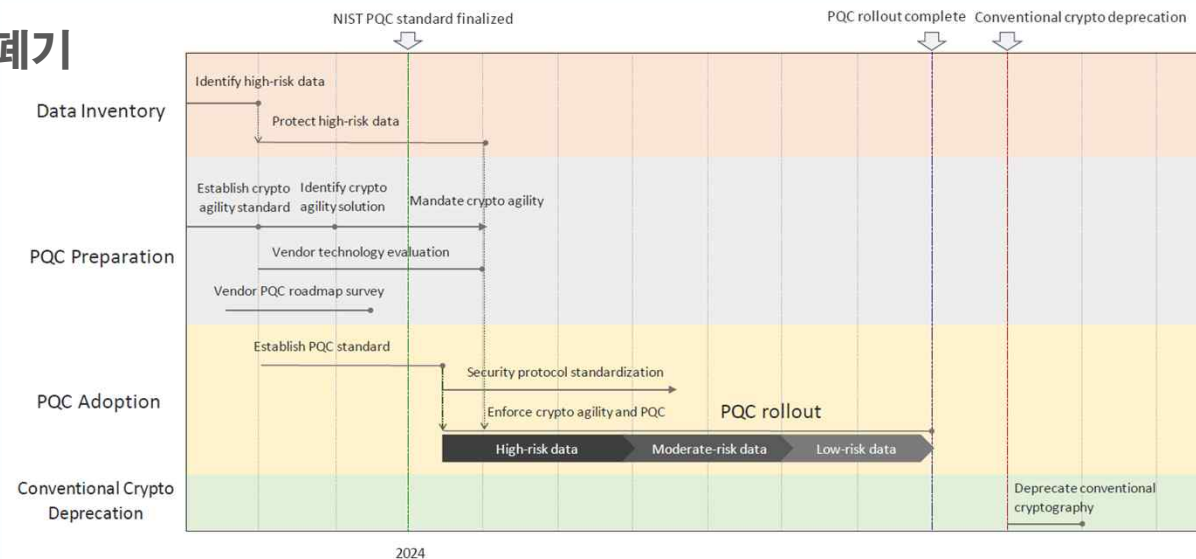
- NIST 양자내성암호 전환 워크숍(2020.10)
 - 목적
 - NIST 알고리즘 표준화와 연계하여, 실용적인 전환 방안 및 대책 등의 수립
 - 현안
 - 양자내성암호는 기존 공개키암호를 바로 대체하지 못할 가능성이 큼
 - 기존 공개키와 양자내성암호의 차이점으로 인해 기존 인프라에 영향
 - 암호키 크기, 서명 크기
 - 오류 처리 속성
 - 복잡한 파라미터 설정 등
 - 이에 따라 전환에 10년 이상이 소요될 수 있어 조기 준비 필요
 - NIST 향후 지원 사항
 - 암호 전환을 위한 백서 및 지침 발간, 구현물 및 사례 개발

Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(미국) (2/5)

- JP모건('20.10, NIST 워크숍 발표)
- **우선순위**에 따른 양자내성암호 전환단계 제시
 - 1) 데이터 자산 목록정리
 - 2) 전환 준비
 - 3) PQC 적용 : 데이터 중요도에 따라 전환 추진
 - 4) 기존 암호 폐기



Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(미국) (3/5)

- NIST 양자내성암호 준비 보고서 발간 (2021.4)
 - 양자내성암호 현황
 - 양자내성암호는 기존 암호에 비해 활용이 어려움
 - 큰 암호키/서명, 복잡한 처리절차 등
 - 안전한 도입을 위한 공개키 검증, 복호화 실패 등 이슈 해결 필요
 - 성능/확장성에 따른 프로토콜, 인프라 업데이트까지 필요할 수 있음
 - 도전과제
 - NIST 표준 시 다양한 응용환경에 적합한 복수 알고리즘을 채택 예정이며, 이에 따라 여러 요소를 고려한 전환 계획 수립 필요
 - 프로토콜 개선 및 신규 애플리케이션 개발 등 양자내성암호에 적합한 응용환경 도입
 - 알고리즘에 따라 표준 및 전환절차 등의 문서 업데이트 및 전환계획 작성
 - 현 공개키 암호의 사용처 목록 작성, 이를 지원하기 위한 도구 개발 등
 - 전환 계획
 - 전환 우선순위 및 요구사항 등 도출 필요

Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(미국) (4/5)

- NIST 양자내성암호 전환 시나리오 발간 (2021.6)
- 양자내성암호로의 체계적 전환을 위한 공개키 암호의 사용처별 시나리오 제안
- 5가지 시나리오에 따른 전환 프로세스 분류
 - 1) FIPS-140 검증받은 하드웨어 및 소프트웨어에 포함된 공개키암호 전환 시나리오
 - 2) 공개키암호가 포함된 암호 라이브러리의 전환 시나리오
 - 3) 공개키암호가 포함된 응용프로그램에 대한 전환 시나리오
 - 4) 컴퓨팅 플랫폼에 내재된 공개키암호에 대한 전환 시나리오
 - 5) 산업분야에 적용된 공개키암호를 사용하는 통신프로토콜에 대한 전환 시나리오

Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(미국) (5/5)

- **바이든 정부 행정명령**
 - “미국 내 IT 인프라 양자내성암호 업그레이드 프로세스 시작”(‘22.5~)
 - NIST 양자내성암호 알고리즘 선정 지원을 위한 WG 운영
 - 양자내성암호 전환 로드맵 및 테스트 지원
 - 암호전환 일정 수립 및 소요예산 산출, 상용 암호제품 호환성 및 성능 등 테스트
 - 양자내성암호 전환 프로젝트 수행
 - 취약암호 탐지 및 데이터변환 등 지원도구 개발, 취약 IT시스템 식별 및 현황 파악, 전환촉진/권장사항 및 전환 상태 등 보고서 발간
 - 국가안보시스템에 대한 대칭키 암호 고도화(~’23)

III 국내외 표준화 및 정책 동향



국가별 정책 동향(EU) (1/3)

• ETSI 양자내성암호 사례 및 적용 시나리오 (2020.7)

- 다양한 ICT 서비스 적용 시 문제점, 고려사항, 해결방안 등
- 주로 표준 프로토콜 위주의 적용사례 연구
 - 네트워크 보안 프로토콜: TLS, IPsec, IKE, SMTP 등
 - ① 단순교체
 - ② 하이브리드
 - ③ 시스템 재구성 (Re-engineering)
 - 오프라인 서비스:
 - 이메일 (S/MIME)
 - X.509
 - IoT : 와이파이, 홈네트워크
 - IoT 기기는 너무나 다양해서 단일 솔루션이 없음
 - 소규모자원에 대한 문제 해결 필요
 - 위성통신
 - 키펰배 시스템: Kerberos, Zigbee, DTLS
 - 인증: 애플리케이션 인증

ETSI GR QSC 003 V1.1.1 (2017-02)



Quantum Safe Cryptography; Case Studies and Deployment Scenarios

5	Network security protocols	10
5.1	Introduction	10
5.2	TLS	10
5.2.1	TLS cryptography	10
5.2.2	Drop-in replacement	11
5.2.3	Hybrid scheme	11
5.2.4	Re-engineering	11
5.3	Discussion	11
5.3.1	Integration into the protocol stack	11
5.3.2	Handling large key sizes	12
5.3.3	Is quantum-safe authentication required today?	13
6	Offline services	13
6.1	Secure e-mail	13
6.2	Credentials for offline services	14
6.3	Discussion	14
7	Internet of Things	14
7.1	Introduction	14
7.2	IoT cryptography	15
7.3	Discussion	15
8	Satellite communications	16
8.1	Requirements	16
8.2	Constraints	16
8.3	Discussion	17
9	Key Distribution Centres	17
9.1	Introduction	17
9.2	Examples	18
9.2.1	Kerberos	18
9.2.2	ZigBee® Trust Centre	18
9.2.3	Datagram Transport Layer Security (DTLS)	18
9.3	Discussion	18
10	Authentication	19
10.1	Introduction	19
10.2	Requirements and use cases	19
10.2.1	Authenticating Internet-based applications	19
10.2.2	Offline file Authentication	19
10.2.3	Authenticating broadcast communications	20
10.3	Symmetric solutions	20
10.4	Discussion	20

III 국내외 표준화 및 정책 동향



국가별 정책 동향(EU) (2/3)

• ETSI 양자내성암호 전환 전략 및 권고사항(2020.7)

• 양자내성암호 전환을 위한 단계적 접근 방식 제시

1단계 - 자산 목록 정리

- 시작 및 전환 상태 (기존 암호체계 → 완전한 양자내성 암호체계)
- 자산 목록 정리
- 1 단계에 대한 비즈니스 프로세스 요구사항

2단계 - 준비 및 전환 계획

- 전환 계획 작성
- 전환 시 이슈
- 하드웨어 기반 보안 환경에 미치는 영향
- 전환과정에서의 키 관리
- 전환과정에서의 신뢰 관리
- 전환과정에서의 시스템 분리 방식
- 전환과정에서 기존 공개키암호로 보호받는 자원에 대한 접근
- 2단계에 대한 비즈니스 프로세스 요구 사항

3단계 - 전환 실행

- 전환 관리
- 위험 완화 관리
- 3단계를 위한 비즈니스 프로세스 요구사항

ETSI TR 103 619 V1.1.1 (2020-07)



CYBER: Migration strategies and recommendations to Quantum Safe schemes

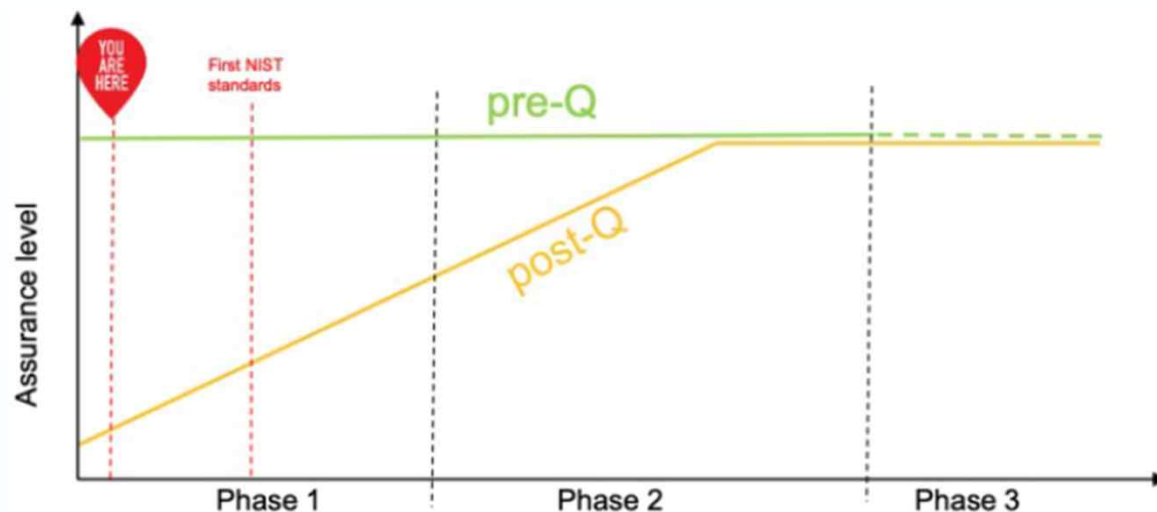
4	Staged approach to QSC migration	7
5	Stage 1 - Inventory compilation	7
5.1	Starting and end states of migration	7
5.2	Inventory compilation	8
5.3	Business process requirements for stage 1	10
6	Stage 2 - Preparation of the migration plan	11
6.1	Creation of the migration plan	11
6.2	Migration issues	13
6.3	Considerations for migration impact on hardware based security environment	13
6.4	Key management during migration	14
6.5	Trust management during migration	14
6.6	Isolation approaches during migration	14
6.7	Access to non-QSC protected resources after migration	14
6.8	Business process requirements for stage 2	15
7	Stage 3 - Migration execution	15
7.1	Migration management	15
7.2	Mitigation management	15
7.3	Business process requirements for stage 3	16

Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(EU) (3/3)

- ANSSI(프랑스 국가사이버보안원) (2021.7)
 - ANSSI(프랑스)에서는 PQCrypto 2021에서 양자내성암호 전환 3단계를 제시
 - 현재 준비단계(1단계)에서, 하이브리드 알고리즘을 적용하는 완충단계 (2단계)
 - 안전한 양자내성암호 알고리즘을 사용하는 전환단계(3단계)을 제시
 - 알고리즘의 성숙도를 고려하여 기반문제를 고려한 대체용 PQC 알고리즘도 필요



Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(일본)

- **일본중앙은행(BOJ): 전환 검토보고서 발간(2021.6)**
 - 암호체계 전환 준비성 강조 및 조기 전환 준비의 필요성 제시
- 1) **암호체계 전환은 최소 10년이상 소요**
 - 시스템 개선, 하드웨어, 소프트웨어 교체
 - 암호 해독이 가능한 양자컴퓨터 개발은 10년 이상 걸리나, 개발 전 모든 암호전환을 완료해야 함
- 2) **수확 공격에 대비하기 위해 반드시 조기에 전환을 시작해야 함**
 - **수확 공격**: 장기간 보호되어야 하는 암호화 데이터를 미리 수집, 저장한 후 양자컴퓨터를 이용한 해독을 통해 정보를 탈취하는 공격
- 3) **기술 발전 속도가 증가하여, 고성능 양자컴퓨터의 개발 속도가 빨라지고 있음**
 - 2014년 5큐비트 양자컴퓨터 개발 이후, 2020년 100 큐비트 이상으로 성능 증가
- 4) **실제 양자내성암호 기술 개발 및 산업계 적용·실증 시 시간이 소요됨**
 - 성능, 보안 등의 문제는 구현방법에 따라 달라지므로 검증에 시간이 소요됨
 - 실제 적용가능 여부 등의 조기 확인을 위해 **신규시스템은 양자내성암호 적용을 권고**

Ⅲ 국내외 표준화 및 정책 동향



국가별 정책 동향(IMF)

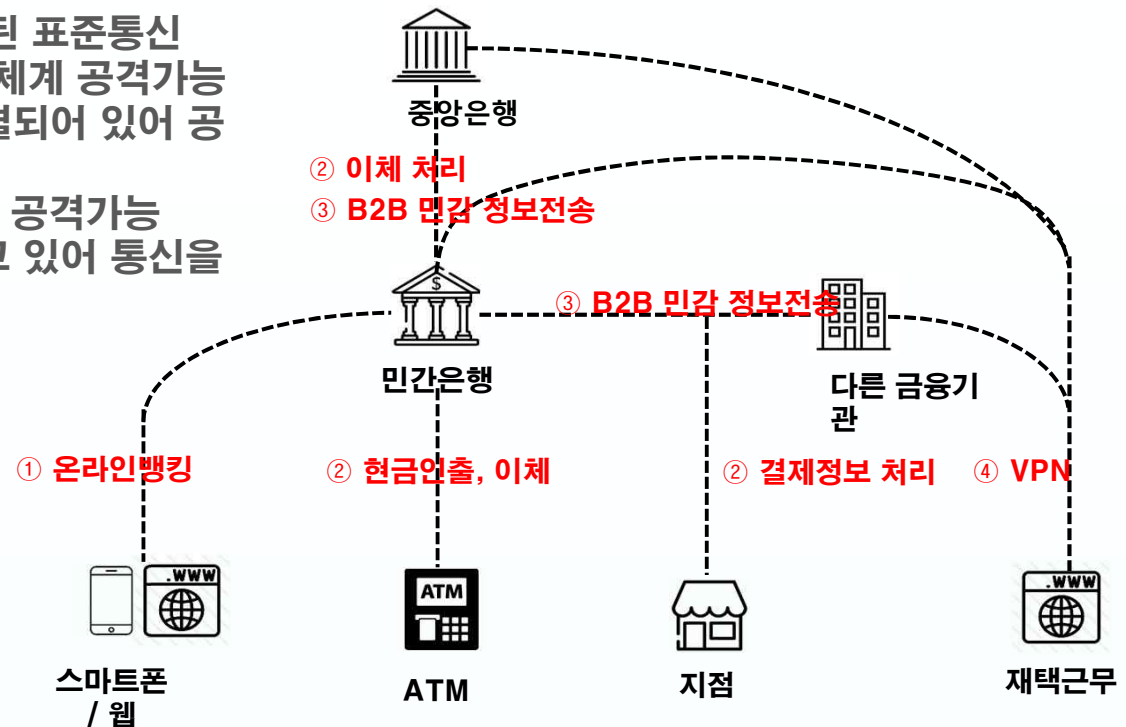
· IMF 양자컴퓨터 위협 보고서(2021.3)

· 양자컴퓨터 위협

- ① 온라인뱅킹: 공개키 적용된 표준통신 또는 사용자-은행간 인증체계 공격가능
- ② ATM기는 내부망으로 연결되어 있어 공개키암호 해킹 가능
- ③ 전송데이터에 대한 MITM 공격가능
- ④ VPN은 공개키를 적용하고 있어 통신을 해킹 시도 가능

· 전환단계

- 1단계 - 자산 목록 정리
- 2단계 - 전환 계획 준비
- 3단계 - 전환 실행



Ⅲ 국내외 표준화 및 정책 동향

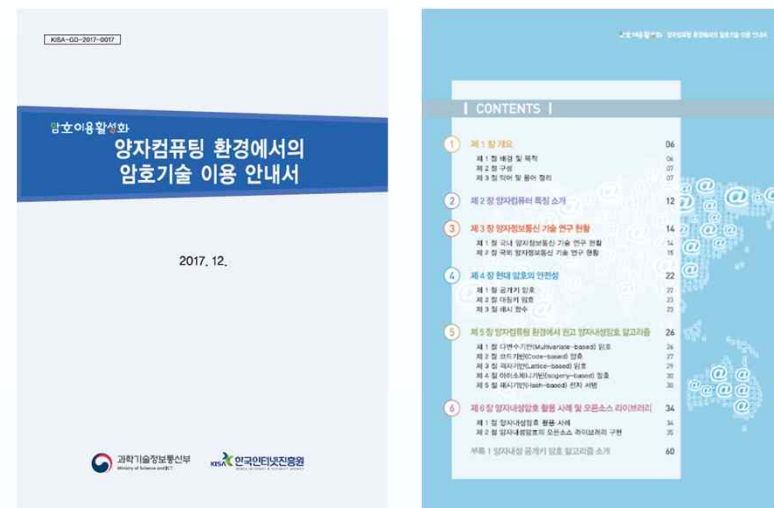


국가별 정책 동향(국내)

· 국내 현황

- 양자컴퓨팅 환경에서의 암호이용 안내서 발간('17, KISA)
- 양자내성암호 알고리즘 2종 표준화('19~'20) 이후 전환에 대한 사업화 노력중

[양자컴퓨팅 환경에서의 암호이용 안내서]



The background features a stylized network diagram with nodes and connecting lines. A prominent blue banner with a diagonal line pattern is positioned across the middle. The bottom left corner contains the KISA logo and the text '한국인터넷진흥원'.


IV 국내외 상용화 및 시범적용 사례

IV 국내외 상용화 및 시범적용 사례



암호제품 상용화

· 인증서, 통신장비, VPN 등 양자내성암호 활용 제품 상용화

기업명	구분	제품명	주요내용
   	상용제품	PQSoC	PQC 하드웨어 칩
		PQSlb	경량 PQC 라이브러리
		PQSDK	API 및 아키텍처 등 지원
		PQE2E	단대단 암호화 지원
		FSP 3000 Connect Guard (PKI 표준 하드웨어 기반 제품)	PQC 탑재 광전송 네트워크 장비
		Radiate Quantum-Safe Toolkit	PQC 소프트웨어 개발 툴킷
		Digicert社 인증서 생성 툴킷 개발	다양한 인증서 서비스 회사

IV 국내외 상용화 및 시범적용 사례



암호전환 시범적용 및 테스트 (1/3)

· 오픈소스 프로젝트

- 구글, MS 등 오픈소스 개발 및 응용환경 적용테스트(TLS/SSH, VPN, 웹 등)

기업명	구분	제품명	주요내용
Microsoft	오픈소스	PQCrypto-VPN	OpenVPN을 양자내성 VPN으로 개발
OQS (프로젝트)		Liboqs	C 기반 라이브러리
		OQS-OpenSSL	OpenSSL 1.1.1
		OQS-OpenSSL Provider	OpenSSL 3.0
		OQS-BoringSSL	BoringSSL
		OQS-OpenSSH	OpenSSH

IV 국내외 상용화 및 시범적용 사례



암호전환 시범적용 및 테스트 (2/3)

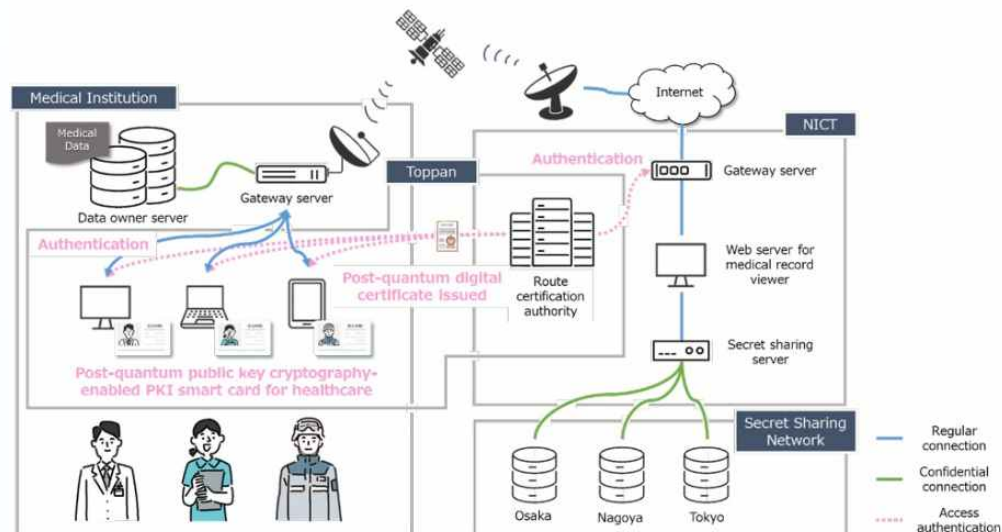
- FLOQI(Full-life-cycle post-quantum PKI) 프로젝트
 - 독일 교육과학부에서 지원하는 연구프로젝트
 - 기존 공개키 및 양자내성암호를 지원하는 PKI 구축하고 인증서를 발급
 - 참여기관
 - Technische Universität (TU) Berlin, Fraunhofer AISEC, BMW, Bosch, Nixdorf, ESCRYPT
- '22년까지 다양한 플랫폼에 맞는 양자내성 기술 개발, 자동차업계 및 금융분야 시험 등 추진

IV 국내외 상용화 및 시범적용 사례



암호전환 시범적용 및 테스트 (3/3)

- 일본 NICT 클라우드시스템 양자내성암호 적용
- NICT, 글로벌 암호기업 등 공동으로 양자내성암호 적용 및 상용화 추진('20~)
 - 클라우드 서비스
: 서비스개발('20~ '21) → 시범테스트 ('22~ '24년) → 서비스적용테스 ('25년 ~) → 상용화 ('30년 ~)
 - 의료정보시스템
: 기술개발('20~ '21) → 적용시험 ('22~ '24년) → 제한적 적용 ('25년 ~) → 서비스 시작 ('30년 ~)

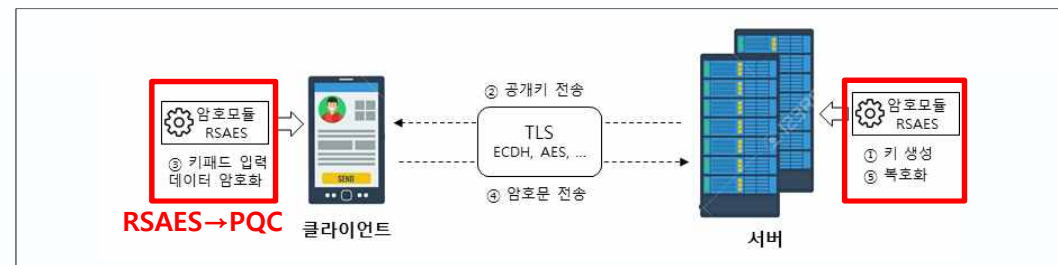


IV 국내외 상용화 및 시범적용 사례



상용화 및 시범적용(국내)

- 산업계 상용화 사례
 - LG 유플러스
 - 자사 통신망에 양자내성암호(Ring-Lizard) 구현 및 적용 ('21.2월)
 - 응용서비스에 양자내성암호 시범적용 ('21년)
- 시범적용 및 테스트 사례
 - KISA 및 국내 3개 업체 (NSHC, 이스트시큐리티, 잉카인터넷)
 - 자사 서비스에 대한 양자내성암호(Ring-Lizard, NTRU 등) 시범적용 ('21 5. ~ 11월)
 - ❖ 적용서비스 : 모바일 앱 내 키패드 보안솔루션(NSHC, 잉카인터넷)
 - ❖ 악성코드 탐지시스템(이스트시큐리티)



[잉카인터넷 양자내성암호(Ring-Lizard) 시범적용 환경]



V 결론

V 결론



향후 준비사항 (1/2)

- 차세대 암호 원천기술 개발 및 확보
 - 양자 컴퓨터 위협에 대응하기 위한 알고리즘은 개발되었으나 현업에 적용을 위한 최적화, 안전성 강화 등 원천기술의 확보 필요
 - 양자내성암호, 양자키분배 등 차세대 암호의 원천기술 선제 확보 및 표준·특허 등 국제화를 통한 글로벌 트렌드 주도
- 차세대 암호의 신뢰 기반 구축 및 운영
 - 양자 컴퓨터 환경에 대응 가능한 기술이 개발되더라도 안전한 구현 및 활용 등 암호기술을 안심하고 사용하기 위한 국가적 기준 필요
 - 차세대 암호의 시험·검증체계의 확립을 통한 신뢰성 확보 및 국가·공공인프라 고도화를 통한 안심국가 기반 마련

V 결론



향후 준비사항 (2/2)

- 차세대 암호기업 및 인력 육성
 - 기존 암호기술에 비해 복잡하고 난해한 차세대 암호기술을 국내기업에서 직접 개발하고 활용하기 위한 산업적 기반 확보 필요
 - 교육·컨퍼런스 등을 통한 차세대 암호인재 육성 및 제품개발·컨설팅 등 암호기업 지원으로 기반산업의 성장동력 확보
- 차세대 암호체계로의 성공적인 전환 지원
 - 국내기업의 차세대 암호체계로의 전환을 위한 국가주도의 가이드라인 및 원활한 암호체계 전환을 위한 각종 지원 필요
 - 암호전환 정책·로드맵 수립 및 전환 지원을 위한 도구 개발 등 민간기업의 암호전환 및 지원을 위한 체계 마련



Internet On, Security In!

감사합니다

