PQC(양자내성암호) 최신 연구 개발 동향

국가수리과학연구소 심경아
(kashim@nims.re.kr)

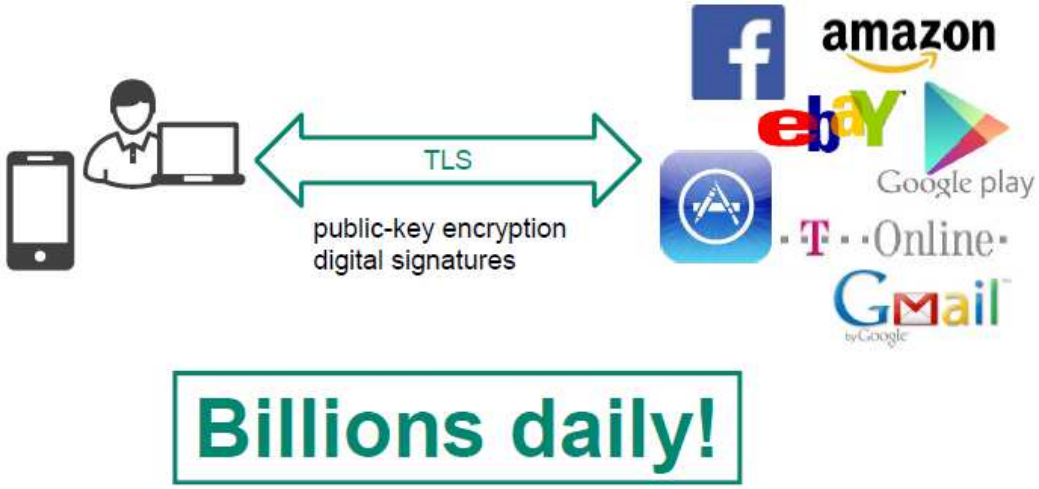
내용

I. 공개키 암호, 양자알고리즘, 양자컴퓨터

II. 양자내성암호 연구 개발 동향

공개키 암호 분류

- 공개키 암호
  - 암호화 알고리즘: 기밀성, 키 전송
  - 전자서명 알고리즘 (사이버 인감) : 인증, 무결성, 위/변조 방지, 부인 방지
  - 키분배 알고리즘: 비밀키 공유



공개키 암호-Trapdoor one-way function

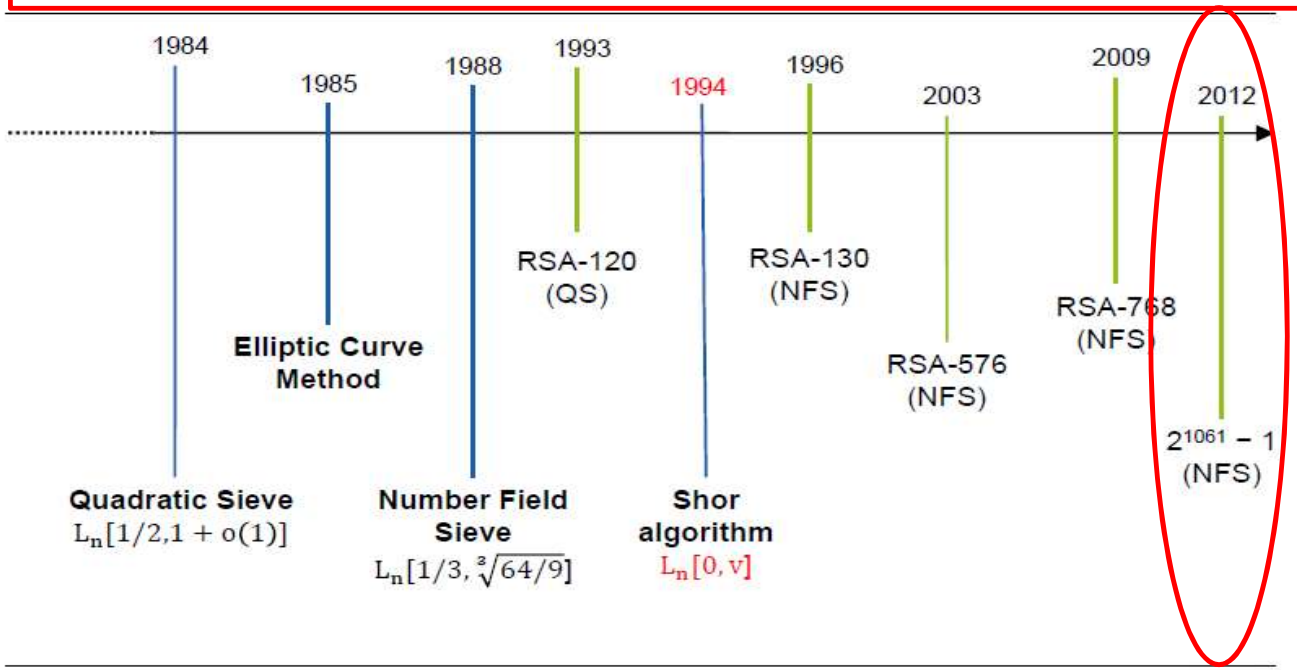
- One-way function (일방향 함수): 해시 함수
  - f: X -> Y : f(x) 계산은 쉬우나 f(x)로 부터 preimage x를 계산하는 것은 어려운 함수
- Trapdoor one-way function
  - One-way function으로 적당한 trapdoor를 가지고 있으면 f(x)로 부터 preimage x를 계산하는 것이 쉬워지는 함수
  - 공개키 암호를 설계하기 위해서는 Trapdoor one-way function을 찾아야 함
- Computational hard problems
  - 소인수분해 문제, 이산대수문제, Diffie-Hellman 문제 …

국제 표준 공개키 암호

- 국제 표준 vs 계산적 난제 (Computational hard problems)
  - RSA 암호화/전자서명 알고리즘
    - ✓ 소인수분해 문제: 주어진 합성수 n=pq, n의 소인수 p, q를 구하는 문제
  - DSA 전자서명 알고리즘 (국내 표준 KCDSA)
    - ✓ 이산대수문제: 유한체에서 주어진 g^x 로 부터 주어진 이산대수 x을 구하는 문제
  - ECDSA 전자서명 알고리즘 (국내 표준 EC-KCDSA)
    - ✓ 타원곡선 이산대수문제: 타원곡선에서 Q=xP 로 부터 이산대수 x을 구하는 문제
  - Diffie-Hellman 키교환
    - ✓ Diffie-Hellman 문제: 주어진 xP와 yP 로부터 xyP를 구하는 문제

공개키 암호-공격에 대한 대응

- [기본 구조] 공개키 암호알고리즘의 안전성은 기본 논리로 사용되는 수학적 난제에 의존, 사용된 수학적 난제가 해결되면 암호알고리즘도 깨지게 되는 구조
- [계산적으로 어려운 문제] 소인수분해 문제
  - 주어진 합성수 n=pq, n의 소인수 p, q를 구하는 문제
  - 공격 대응 : 키길이를 2배 씩 늘여서 사용 1024 비트 -> 2048 비트



양자알고리즘-Shor 알고리즘

- Shor 알고리즘 (1994)
  - ➢ 소인수분해 , 이산대수문제 다항식 시간 안에 해결

Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*

Peter W. Shor†

RSA and ElGamal insecure

A digital computer is g
device; that is, it is believ
an increase in computatio
true when quantum mechanics is taken into consideration. This paper considers factoring integers and finding discrete logarithms, two problems which are generally thought to be hard on a classical computer and which have been used as the basis of several proposed cryptosystems. Efficient randomized algorithms are given for these two problems on a hypothetical quantum computer. These algorithms take a number of steps polynomial in the input size, e.g., the number of digits of the integer to be factored.

Keywords: algorithmic number theory, prime factorization, discrete logarithms, Church's thesis, quantum computers, foundations of quantum mechanics, spin systems, Fourier transforms

AMS subject classifications: 81P10, 11Y05, 68Q10, 03D10

- ➢ 공개키 암호 붕괴 예고: RSA, ECDSA 실시간에 해독, 안전성 붕괴

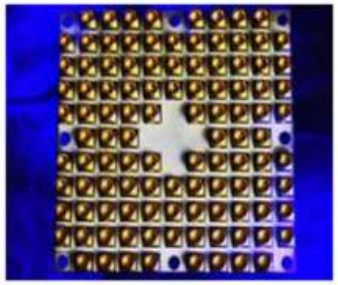
양자알고리즘

- Grover 알고리즘
  - 검색 문제, 전수조사 복잡도 N -> $\sqrt{N}$
  - 대칭키 암호, 해시 함수 키길이를 두 배로 늘이면 대응 가능

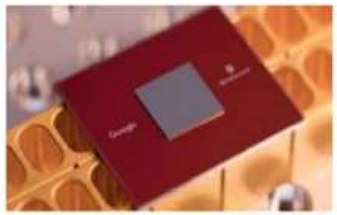
Cryptographic Algorithm	Scheme	Type	Pre-quantum Security Level	Post-quantum Security Level
Symmetric-Key Cryptographic Algorithm	AES-128	Block cipher	128	64 (Grover)
	AES-256	Block cipher	256	128 (Grover)
	Salsa20	Stream cipher	256	128 (Grover)
	GMAC	MAC	128	128 (No impact)
	Poly 1305	MAC	128	128 (No impact)
Hash Function	SHA-256	Hash function	256	128 (Grover)
	SHA-3	Hash function	256	128 (Grover)
Public-Key Cryptographic Algorithm	RSA-3072 [27]	Encryption	128	Broken
	RSA-3072 [27]	Signature	128	
	DSA-3072 [27]	Signature	128	
	ECDSA-256	Signature	128	
	DH-3072 [27]	Key exchange	128	
	ECDH-256 [27]	Key exchange	128	

- 격자문제 PIP (Principal Ideal Problem)를 풀어주는 다항식 기반 양자알고리즘

양자컴퓨터의 발전

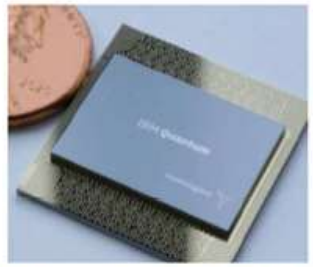


Intel Tangle Lake (Q49, '18)

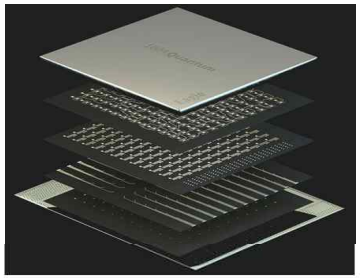


Google Bristlecone (Q72, '18)

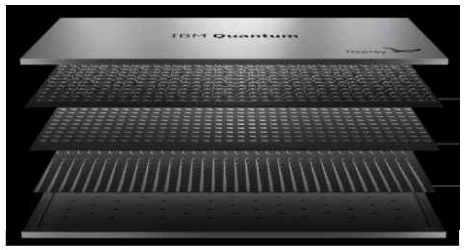
IBM Q System One (Q20, '19)



IBM Hummingbird (Q65, '20)



IBM Eagle (Q127, '21)



IBM Osprey (Q433, '22)

- IBM Condor (Q1121, '23) 예고
- 세계 정보기술(IT)·가전 전시회 'CES 2021'
  - ➢ 2030년까지 100만 큐빗 달성 선언

IonQ (Q32, '20)

Rigetti Aspen-8 (Q31, '20)

D-wave (Q5000+, '20)

Harvard & MIT (Q256, '21)

양자 컴퓨팅: 이론과 실제

How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits

Craig Gidney[1] and Martin Ekerå[2,3]

[1]Google Inc., Santa Barbara, California 93117, USA

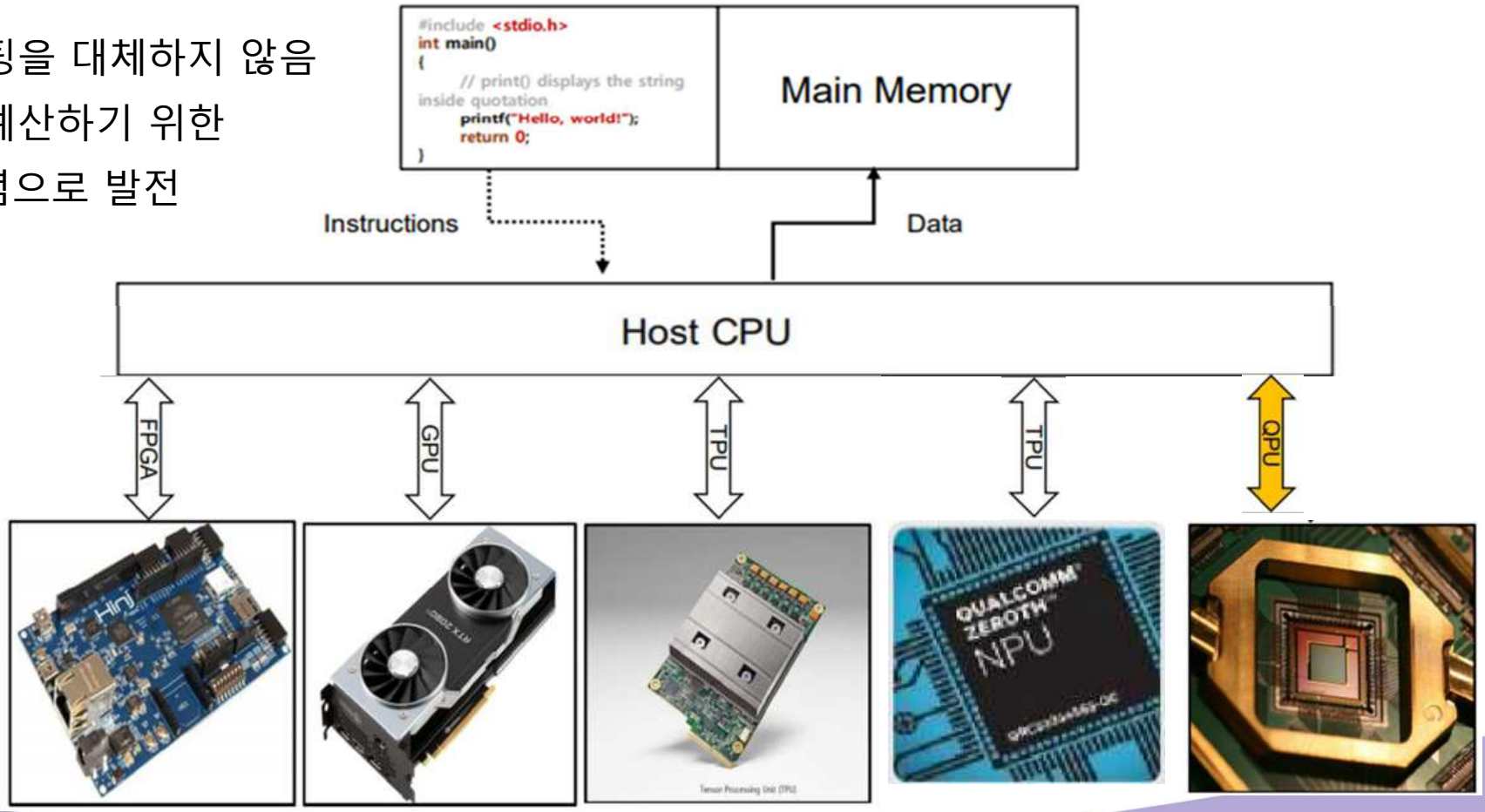
Quantum 5, 433 (2021).

Abstract

We significantly reduce the cost of factoring integers and computing discrete logarithms in finite fields on a quantum computer by combining techniques from Shor 1994, Griffiths-Niu 1996, Zalka 2006, Fowler 2012, Ekerå-Håstad 2017, Ekerå 2017, Ekerå 2018, Gidney-Fowler 2019, Gidney 2019. We estimate the approximate cost of our construction using plausible physical assumptions for large-scale superconducting qubit platforms: a planar grid of qubits with nearest-neighbor connectivity, a characteristic physical gate error rate of 10^{-3}, a surface code cycle time of 1 microsecond, and a reaction time of 10 microseconds. We account for factors that are normally ignored such as noise, the need to make repeated attempts, and the spacetime layout of the computation. When factoring 2048 bit RSA integers, our construction's spacetime volume is a hundredfold less than comparable estimates from earlier works (Van Meter et al. 2009, Jones et al. 2010, Fowler et al. 2012, Gheorghiu et al. 2019). In the abstract circuit model (which ignores overheads from distillation, routing, and error correction) our construction uses $3n + 0.002n \lg n$ logical qubits, $0.3n^3 + 0.0005n^3 \lg n$ Toffolis, and $500n^2 + n^2 \lg n$ measurement depth to factor n-bit RSA integers. We quantify the cryptographic implications of our work, both for RSA and for schemes based on the DLP in finite fields.

양자 컴퓨팅-양자 가속기

- QPU
  - ➢ 기존 고전 컴퓨팅을 대체하지 않음
  - ➢ 특정 고속으로 계산하기 위한 accelerator 개념으로 발전



양자내성암호

Q. 보편적인 양자컴퓨터가 개발되지 않는다면 전통적인 공개키 암호를 계속 사용해도 좋은가?

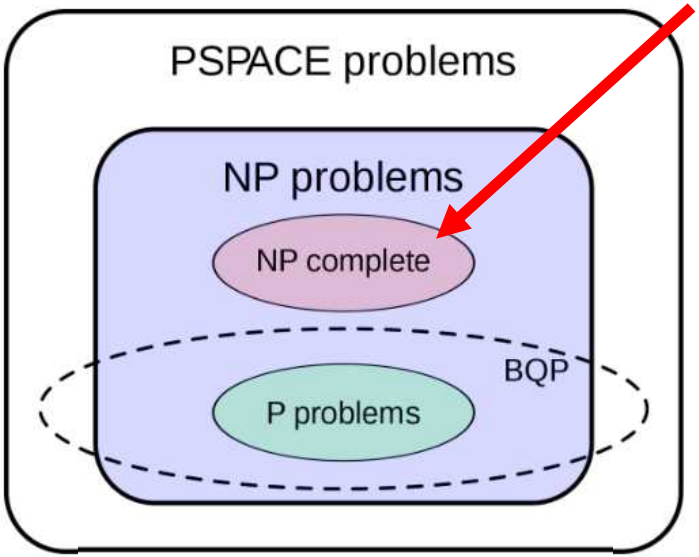
- 소인수분해 문제: 전통적인 방법으로 풀 수 있는가?
  - ✓ RSA 합성수 크기 교체: RSA 2048-비트 합성수 (112-비트 안전도) 사용 -> 3072-비트 합성수 (128-비트 안전도)로 교체 시기 도래
- 인수분해 전용 양자 가속기 개발 가능성

II. 양자내성암호 연구 개발 동향

양자내성암호 정의

- 현재의 컴퓨터와 양자컴퓨터를 이용한 공격에 모두 안전한 공개키 암호알고리즘
  - 양자컴퓨터에 안전한 수학적 난제
  - 양자 컴퓨터가 효율적으로 풀 수 있는 문제들의 집합

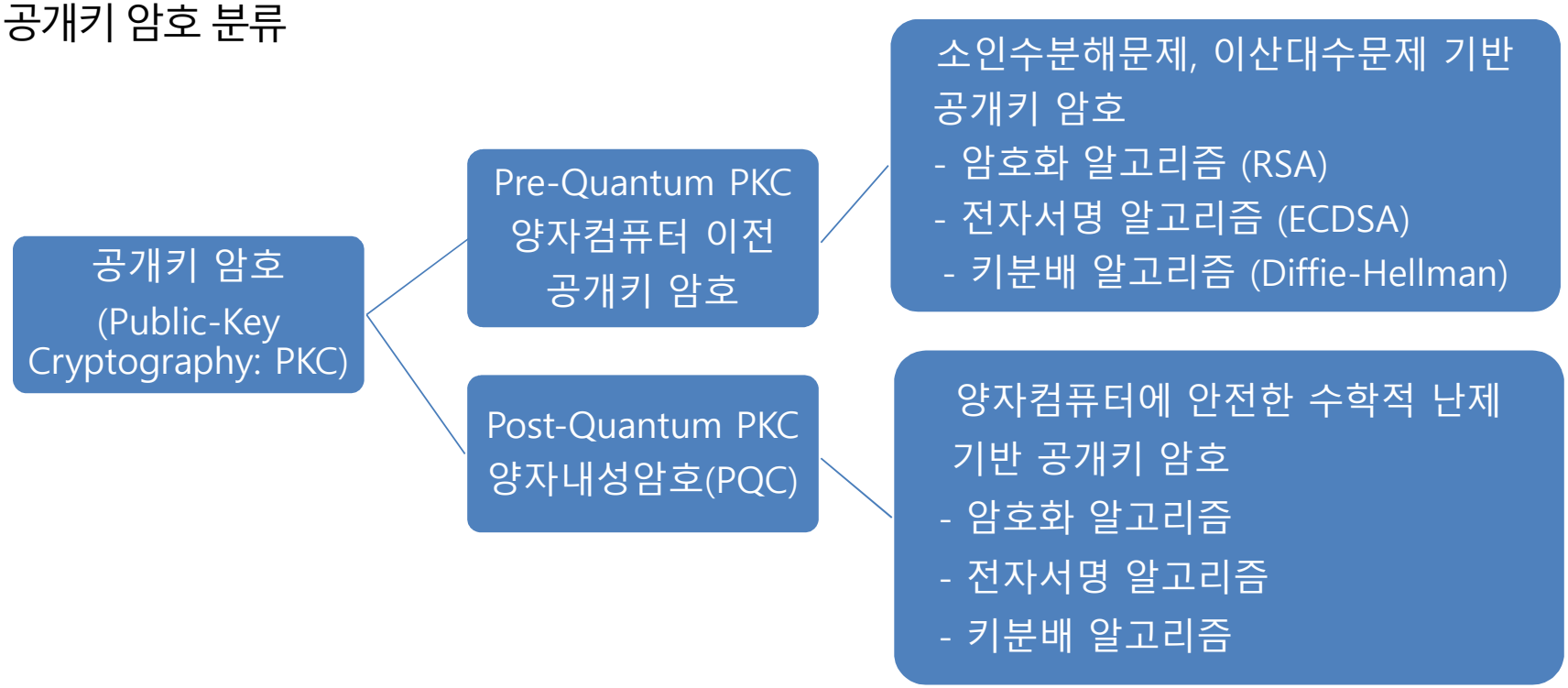
    BQP(Bounded error, Quantum, Polynomial time)



<출처: 위키피디아>

공개키 암호 분류

- 공개키 암호 분류



양자내성암호-양자컴퓨터에 안전한 난제

- 다변수 이차식 문제 기반
  - 다변수 이차식 시스템의 해를 구하는 문제 (Multivariate-Quadratic problem)
- 해시 함수 기반
  - 해시 함수 H, H(x)=H(x′)를 만족하는 값 x, x′을 찾는 문제 (Collision resistance problem)
- 격자 문제 기반
  - 가장 짧은 길이의 벡터를 찾는 문제 (Shortest vector problem)
- 코드 문제 기반
  - Syndrome Decoding problem
- Supersingular isogeny 문제 기반
  - Supersingular 타원곡선에서 isogeny 를 찾는 문제

양자내성암호 국내/국제 표준화 현황

- 국내 표준화
  - ➢ 다변수 이차식 기반 양자내성 전자서명 알고리즘/격자 기반 키설정 알고리즘
    - ✓ 2020년 6월 정보통신 단체표준 TTA 표준 제정 완료
- 국제 표준화
  - ➢ 미국 NIST 표준: Round 4 최종 알고리즘 선정
    - ✓ 키설정 (KEM) 알고리즘: kyber
    - ✓ 전자서명 알고리즘: Dilithium, Falcon, SPHINCS+
  - ➢ IETF 표준: 해시 함수 기반 stateful 전자서명 알고리즘 XMSS, XMSS^MT, LMS 표준 제정
    - ✓ 서명 생성 후 비밀키 업데이트가 필요, 이를 위한 별도의 보안 장치 필요
    - ✓ state의 안전한 관리를 요구하고 서명 개수의 제한이 있는 전자서명
    - ✓ NIST도 표준 추진 중에 있음.

양자내성암호 국내/국제 표준화 현황

- 미국 NIST 양자내성암호 표준화 알고리즘 선정 발표
  - 4 라운드 최종 알고리즘 암호화/키설정 알고리즘 1종, 전자서명 3종 선정
  - 후보알고리즘 코드기반 3종, supersingular-isogeny 기반 키설정 알고리즘 1종 선정
  - 4 라운드 최종 알고리즘 중 3종이 구조화된 격자 이용
- 미국 NIST 전자서명 알고리즘 재공모 계획 발표
  - 구조화된 격자의 잠재적 위협 고려, 다양성 확보, 서명 길이 짧고, 서명 검증이 빠른 전자서명 공모
  - 2023년 6월 1일 마감
- 진화된 공격 등장
  - 3 라운드 후보 Rainbow 공격, 격자 기반 암호에 대한 향상된 dual lattice 공격 발표
  - 4 라운드 후보 알고리즘 SIKE에 대한 공격: 수시간 안에 비밀키 복구 성공
- 우수한 국산암호 기술의 개발과 면밀한 검증 필요
  - 미국 NIST의 양자내성암호 공모, 중국 등 독자 표준 준비
  - 잠재적 위협 고려와 다양성 확보를 위한 양자내성암호 개발 및 면밀한 검증 필요

양자내성암호 성능

- NIST PQC 표준화 4 라운드 최종 전자서명 알고리즘
  - ➢ Dilithium, Falcon: 격자 기반
- AVX2 지원 PC, 128-비트 안전도

전자서명 알고리즘		키 생성		서명 생성		서명 검증	
		시간 (ms)	cycle	시간 (ms)	cycle	시간 (ms)	cycle
양자내성암호	Dilithium	0.024 ms	87,757	0.069 ms	256,532	0.026 ms	94,930
	Falcon	7.408 ms	27,668,945	0.228 ms	847,094	0.040 ms	147,256
현 국제 표준	ECDSA-256	0.009 ms	31,908	0.021 ms	76,038	0.063 ms	230,999
	RSA-2048	72.131 ms	271,097,593	0.547 ms	2,019,834	0.017 ms	63,856

전자서명 알고리즘		공개키 길이 (Byte)	비밀키 길이 (Byte)	서명 길이 (Byte)
양자내성암호	Dilithium	1,312 B	2,528 B	2,420 B
	Falcon	897 B	1,281 B	666 B
현 국제 표준	ECDSA-256	72 B	72 B	72 B
	RSA-2048	256 B	256 B	256 B

양자내성암호 적용

- Google
  - **CECPQ1** (**Combined Elliptic-Curve and Post-Quantum 1**): 웹 브라우저 Transport Layer Security (TLS) 양자내성 키분배 프로토콜
    - ✓ X25519+NewHope, hybrid 사용 둘 중 하나가 안전하지 않더라도 전체 안전성 보장
    - ✓ Google Chrome 54 beta
  - **CECPQ2** (**Combined Elliptic-Curve and Post-Quantum 2**)
    - ✓ X25519+NTRU-HRSS
    - ✓ *CECPQ2b:* X25519+SIKE
- WireGuard (VPN protocol): long-term key로는 Classic McEliece, ephemeral key로는 Saber 적용
- OpenSSLNTRU, OpenSSH: Streamlined NTRU 적용
- 상용화 사례: 통신 3사 위주, QRNG, QKD, PQC 시범 적용/상용화
  - QKD, QRNG, PQC는 안전한 통신을 위한 단위 요소 기술에 불과
  - 단일 기술의 사용으로 마치 양자 보안의 전부라고 생각하거나 양자 보안을 달성했다는....

양자내성암호 개발 성과

- 다변수 이차식 기반 전자서명 알고리즘
  - 서명의 길이가 가장 짧고 성능이 우수
  - 공개키 빈번한 전송 없이 서명만 생성하는 기기에 적합, CA, Root CA의 전자서명으로 적합
- 격자 기반 전자서명 알고리즘
  - 효율성을 고려한 cyclotomic 격자 기반 전자서명 알고리즘
  - 잠재적 공격에 안전한 non-cyclotomic 격자 기반 전자서명 알고리즘
  - 구조화된 격자가 아닌 standard 격자를 기반 전자서명 알고리즘

  => Standard 격자 >> non-cyclotomic 격자 >> cyclotomic 격자 (안전성 강도)
- 격자 기반 암호화/키설정 알고리즘
  - 검증된 격자 난제 효율적인 격자 기반 암호화/키설정 알고리즘

⇒ **인증/기밀성/키분배 위한 전자서명/암호화/키설정 알고리즘으로 구성된 양자내성암호 원천 기술 풀세트 확보**

감사합니다.