양자컴퓨터에 안전한 암호기술

2020. 6. 12.

뉴스 검색 결과

Google 양자컴퓨터

전체 이미지 뉴스 동영상 쇼핑 더보기 설정 도구

검색결과 약 53,400개 (0.14초)

양자 컴퓨터 구현과 실용 알고리즘 개발 모멘텀

사이언스모니터 - 2020. 6. 1.

이 기술은 **양자** 물리학 분야의 알버트 아인슈타인 (Albert Einstein)이 '먼 거리의 괴이한 작동'에 기반해 전례없는 컴퓨팅이 가능하다. **양자** 컴퓨팅은 ...

"4000 큐비트 **양자컴퓨터**, 비트코인 블록체인 해킹 가능"

사이언스모니터 - 2020. 5. 13.

양자 컴퓨터는 양자 역학 현상인 양자 얽힘(quantum entanglement) 및 중첩(superposition)을 활용한다. 이론적으로 양자 트랜지스터는 1과 0을 ...

文대통령 '**양자컴퓨터**' 언급에 관련주 급등

조선비즈 - 2020. 5. 26.

문재인 대통령이 **양자컴퓨터**를 유망 기술로 지목하며 관련 종목이 강세를 보이고 있다. **양자컴퓨터**는 0과 1을 하나만 담을 수 있는 기존 컴퓨터와는 ...

[특징주]文대통령 '**양자컴퓨터**' 언급에 우리넷 등 강세

뉴스 검색 결과

[특징주] 아이에이네트웍스, 정부 **양자컴퓨터** 기술 투자 소식에↑ 2020.05.28 | 아시아경제 | 다음뉴스

[아시아경제 장효원 기자] 정부가 **양자컴퓨터** 개발을 포함한 국가 연구개발 예산에 24조원을 투자한다는 소식에 아이에이네트웍스가 강세다. 28일 오전 10시13분 현재...

└ [특징주]아이에이네트웍스, 정부 **양자컴퓨터** 기술 ... 2020.05.28 | 이데일리 | 다음뉴스

[특징주]드림시큐리티, **양자컴퓨터** 개발 소식에 21% 급등

2020.05.28 | 머니S | 다음뉴스

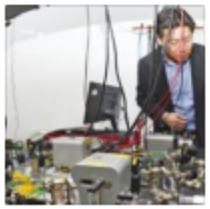
정부가 **양자컴퓨터** 개발에 투자한다는 소식에 드림시큐리티 주가가 강세다. 28일 오전 9시14분 드림시큐리티는 전일대비 735원(21.46%) 오른 4160원에 거래 중이다. 드림...

└ 드림시큐리티, 세계 9조 **양자컴퓨터** 정부 24조 투... 2020.05.27 | 서울경제TV

└ 드림시큐리티 주가, **양자 컴퓨터** 개발 소식으로 급... 2020.05.28 | 동양뉴스통신

모바일금융 해킹 피해 위험성..'**양자**보안'으로 이중 보안 7시간전 | 매일경제 | 다음뉴스

정보 해킹, 모바일 인증 및 결제 사기가 급증하면서 보안에 대한 관심이 높아진 가운데 **양자컴퓨터** 시대가 열리며 보안의 중요성은 한층 더 부각될 전망이다. 9일 관련 업계...

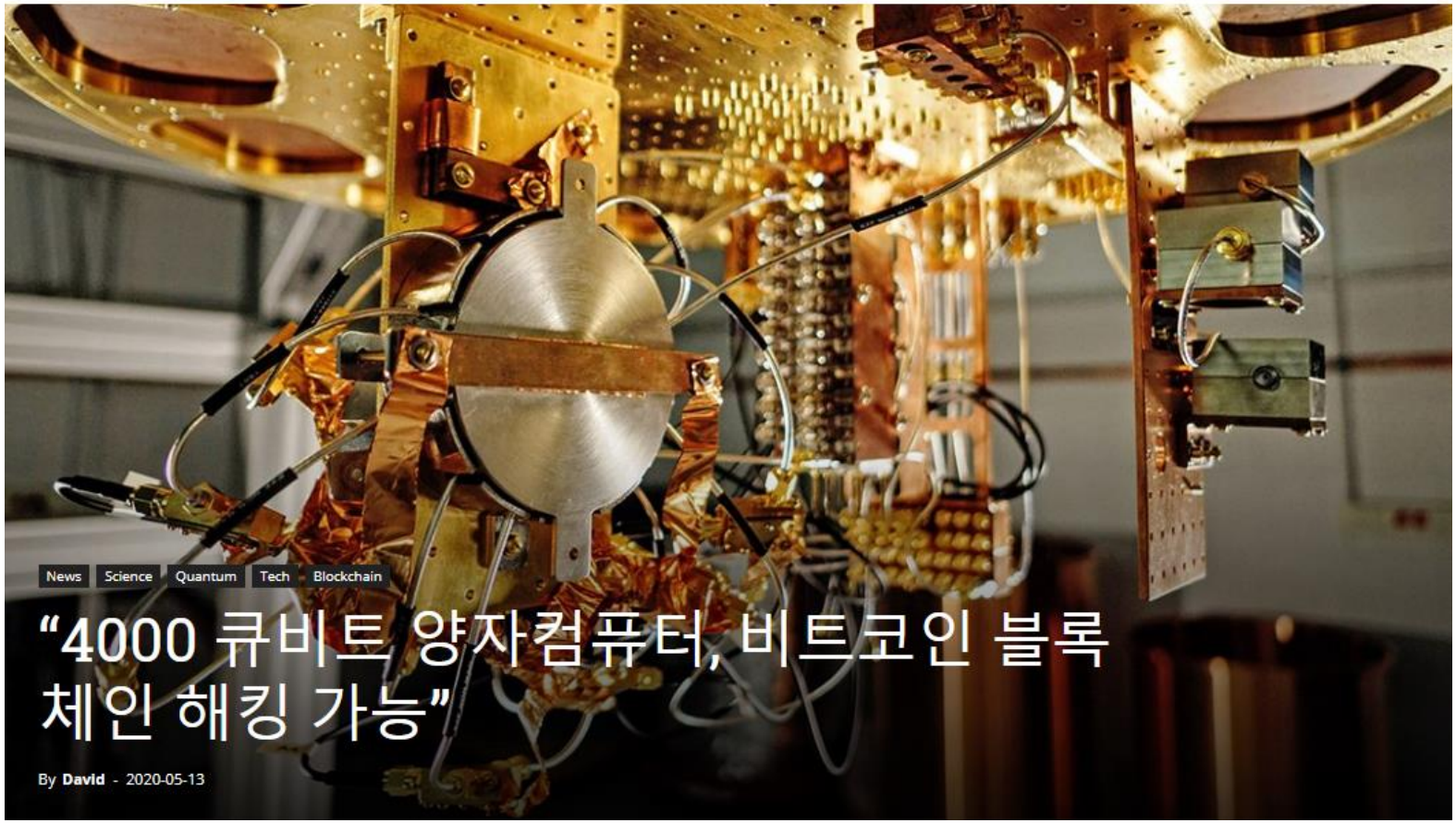


양자컴퓨터가 뭐길래..구글·MS·삼성전자도 개발 참여 2020.05.18 | 한국경제 | 다음뉴스

왼쪽)가 서울대 자동화시스템공동연구소 내 실험실에서 디지털 방식으로 작동하는 **양자컴퓨터** 개발 장비를 살펴보고 있다. 신경훈 한국경제신문 기자 khshin@hankyung.com...

뉴스 검색 결과

the Science Monitor



뉴스 검색 결과

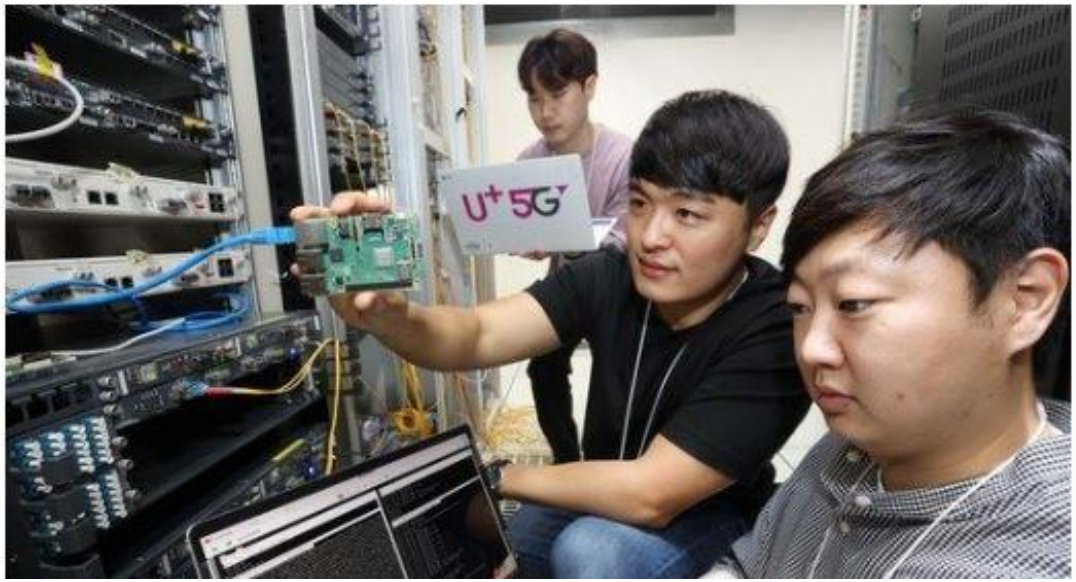
양자컴퓨터도 못 뚫는 '양자내성암호' LGU+ 전송장비에 적용

순수 국내 기술로 개발...상용장비 적용은 세계 최초

유무선 모든 영역에 종단간 보안 확대 기대

(서울=뉴스1) 이창규 기자 | 2020-06-10 09:15 송고

기사보기 | 네티즌의견 | 좋아요 0개 | 공유하기 | 트윗 | 인쇄 | + 확대 | - 축소



강연 목적

- 앞선 기사들의 내용을 제대로 이해하기
  - 양자컴퓨터와 암호 안전성과의 관계 이해
  - 양자컴퓨터에 안전한 암호(PQC) 개발동향 파악
  - PQC 도입을 위해 남은 일들 논의

목 차

1. 양자 컴퓨팅

2. 양자 컴퓨터를 이용한 암호 분석

3. 포스트 퀀텀 암호(PQC)

4. PQC 적용 관련 주요 이슈

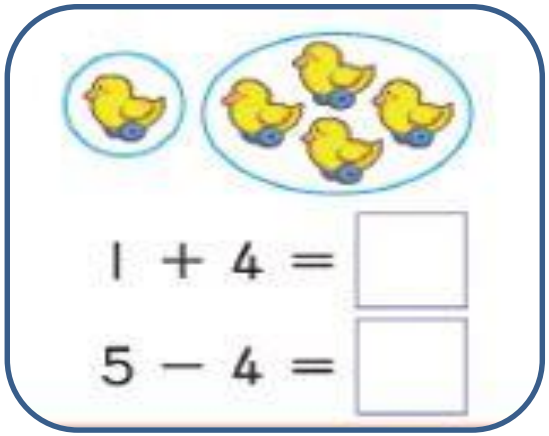
5. 맺음말

1. 양자 컴퓨팅

Computation & Computer?

- Wikipedia의 정의

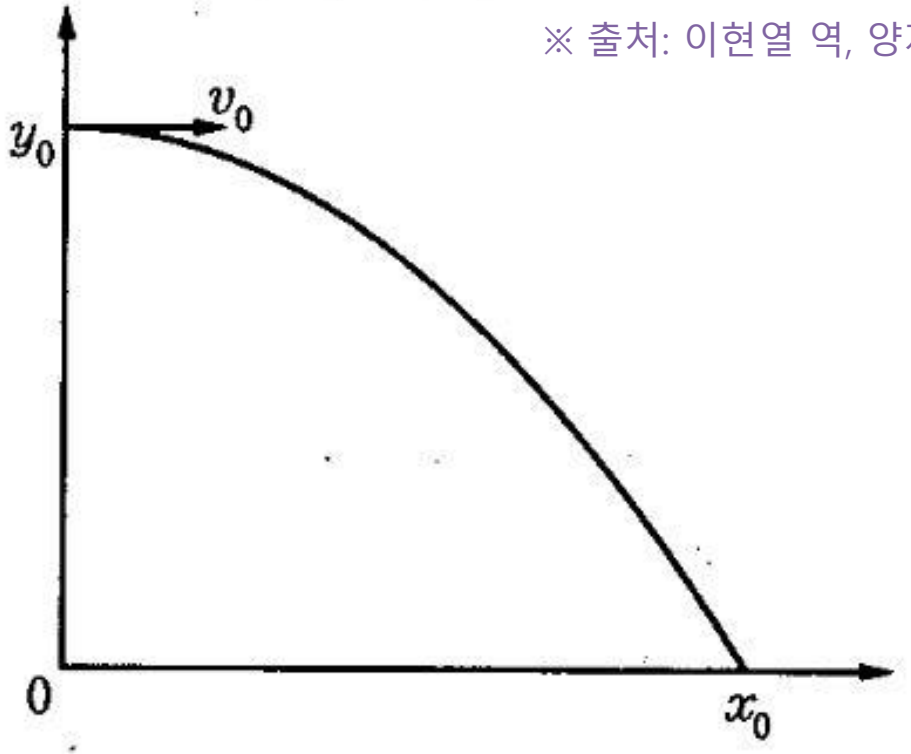
A **computation** is any type of calculation that includes both arithmetical and non-arithmetical steps and which follows a well-defined model (e.g. an **algorithm**). Mechanical or electronic devices (or, historically, people) that perform computations are known as **computers**.



Computation & Computer?

- $y = \sqrt{x}$ computer?

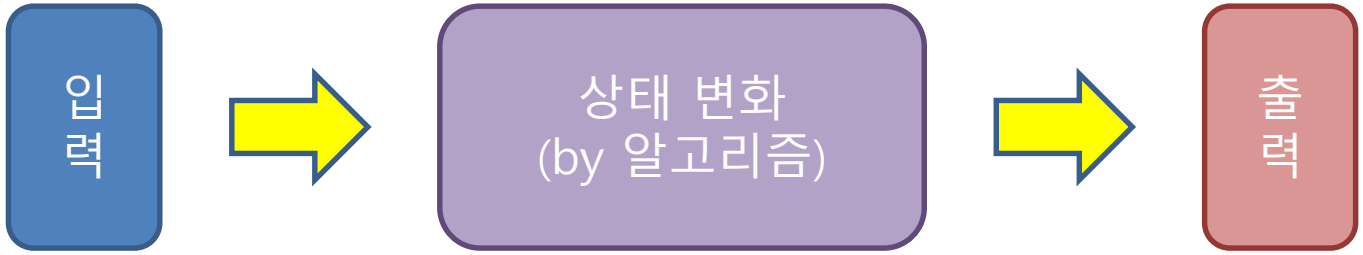
※ 출처: 이현열 역, 양자컴퓨터 기초수리, 대영사.



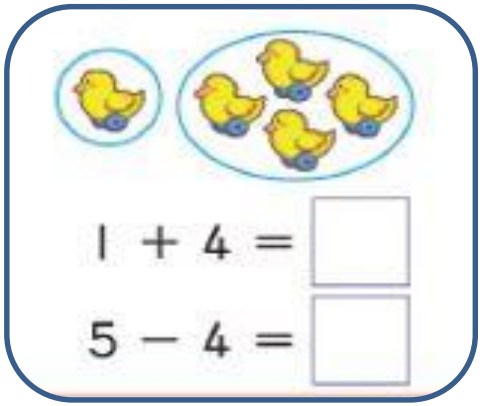
$$y = -\frac{g}{2v_0}x^2 + y_0$$

Computation & Computer?

- Computer: 물리적 시스템
- Computation: 물리적 시스템의 상태 변화 과정

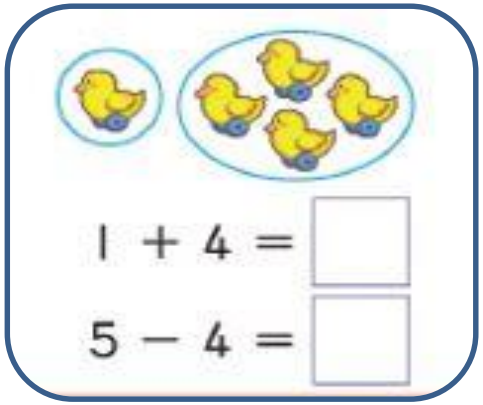


- 좋은 컴퓨터의 기준: 계산 속도



Computation & Computer?

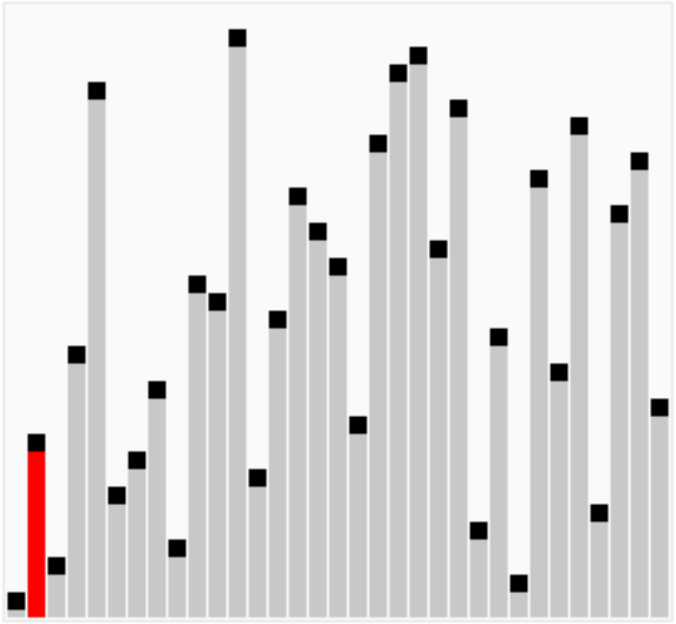
- 계산 속도 결정 요인
  - 문제 (종류, 입력 크기)
  - 물리적 자원(HW) 특성
  - 알고리즘(SW) 특성



- 알고리즘 성능 측정 기준: 계산 복잡도(Complexity)
  - 입력 크기에 대한 기본 연산 단위(step) 수행 횟수

Computation & Computer?

- 정렬(Sorting) 알고리즘
  - 문제: 무작위로 입력된 n개의 자연수를 크기 순으로 나열
  - 고전 컴퓨터상의 알고리즘
    - $O(n^2)$: 버블 정렬, 선택 정렬, 삽입 정렬....
    - $O(nlogn)$: 병합 정렬, 힙 정렬, 퀵 정렬, ...



```
void Bubble_Sort(int a[], int len)
{
    for(int i = len - 1; i > 0; i--)
        for (int j = 0; j < i; j++)
            if (a[j] > a[j+1])
            {
                int t = a[j];
                a[j] = a[j + 1];
                a[j + 1] = t;
            }
}
```

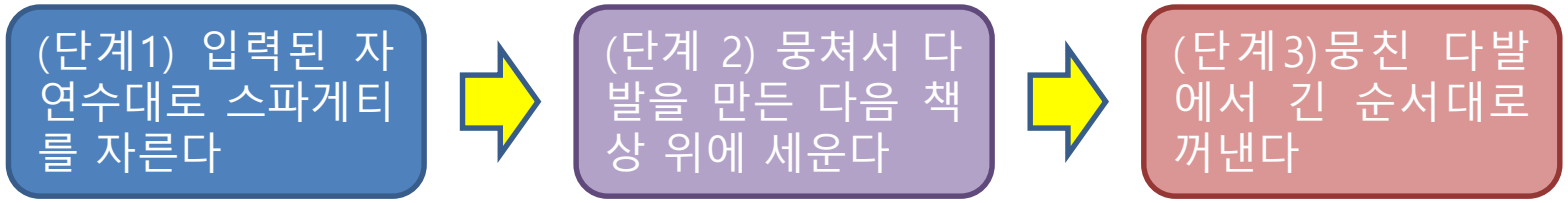
※ 출처: https://ko.wikipedia.org/wiki/정렬알고리즘

Computation & Computer?

- 스파게티 컴퓨터(?)

※ 출처: 이현열 역, 양자컴퓨터 기초수리, 대영사.

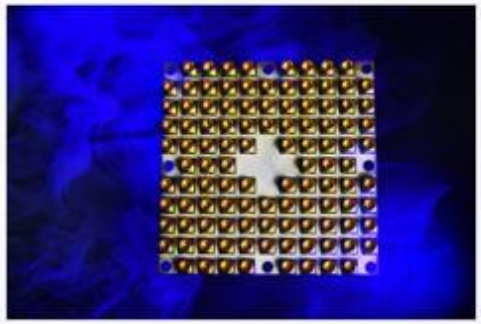
  - 리소스: 충분히 긴 n개의 딱딱한 스파게티 가닥
  - 정렬 알고리즘



  - Complexity: $O(n) = 2n + 1$
  - 성능 향상 요인
    - 계산에 사용한 물리적 리소스 변경
    - 계산(상태 변화) 방식의 변경
  - 단점: 정렬 외에 할 수 있는 일이 없다!

Computation & Computer?

- 고전 컴퓨터 ⇒ 양자 컴퓨터
  - 물리 시스템: 전자기학 ⇒ 양자역학
  - 리소스: 비트 ⇒ 큐비트
  - 계산 방식(모델): 다양
  - 성능 향상 요인?



Intel's 49-qubit chip
"Tangle-Lake"

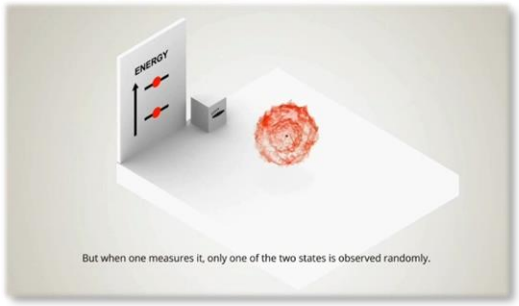
Google's 72-qubit chip
"Bristlecone"

IBM's 50-qubit
quantum computer

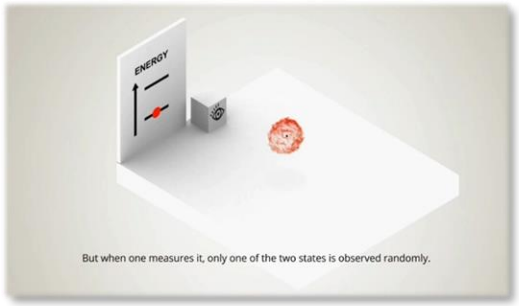
※ 출처: D. Moody, Let's Get Ready to Rumble: The NIST PQC "Competition, PQCrypto 2018, Apr. 2018.

양자역학

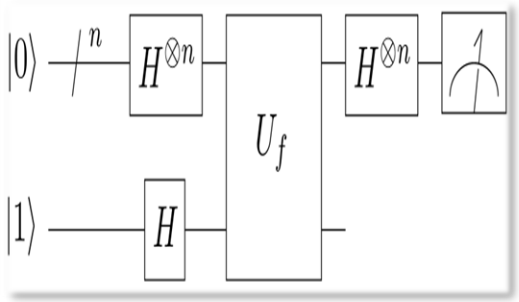
- 핵심 개념
  - 양자화(quantization)
  - 중첩(superposition)
  - 불확정성의 원리(uncertainty principle)
  - 측정(measurement)에 의한 붕괴(collapse)
  - 간섭(interference), 얽힘(entanglement) 등등



- 유용한 가설임
  - 원자 레벨에서의 비상식적인 현상 설명 가능
  - 양자컴퓨터 등 실용적 활용

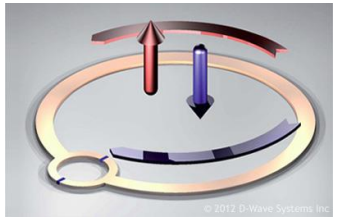


- Cryptographer의 접근법
  - 암호분석용 양자알고리즘의 핵심 요소
  - 단시일내 제대로 된 이해는 난해
  - 인지⇒수용⇒활용 : 양자 역학 ≒ 선형 대수



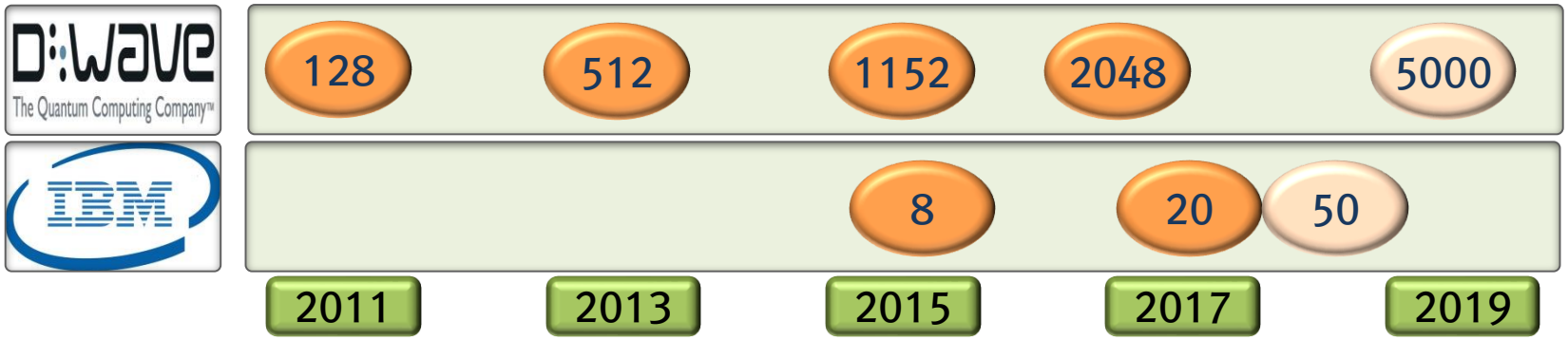
비트 vs 큐비트

- 큐비트(Qubit)
  - 양자수가 2인 물리적 실체
  - 원자 수준의 물질을 기반으로 구현



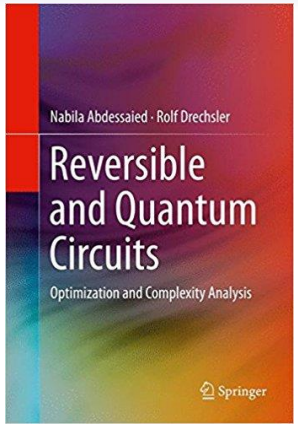
구현 물질	초전도	이온 덫	양자 점	위상 물질	광학계
개발사	D-Wave/Google/IBM	IonQ	Intel	MicroSoft	Optalysis

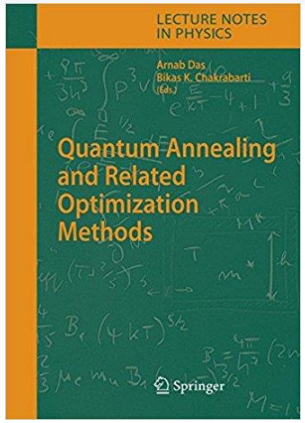
- 발전 추세



양자컴퓨터

- 계산 모델
  - 게이트(Gate) : Quantum Circuit
  - 단열 연산(Annealing)
  - .....





- D-Wave v.s. IBM

개발사	구현 방식	계산 모델	비고
D-Wave	초전도	Annealing	QUBO 문제 해결에 특화
IBM	초전도	Gate	큐빗 상태 유지 시간: ⟨⟨ ms

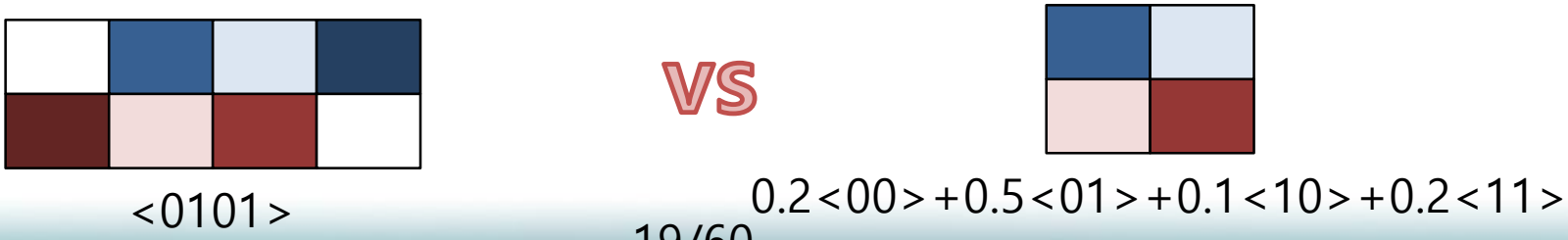
※ QUBO: Quadratic Unconstrained Binary Optimization $H_1 = \sum_i h_i s_i + \sum_{i<j} J_{i,j} s_i s_j$

- D-Wave에서는 Shor 알고리즘 동작 불가
  - QUBO 문제로 변환 후, 200,099(18비트) 인수분해 성공('17.2.)

양자컴퓨터

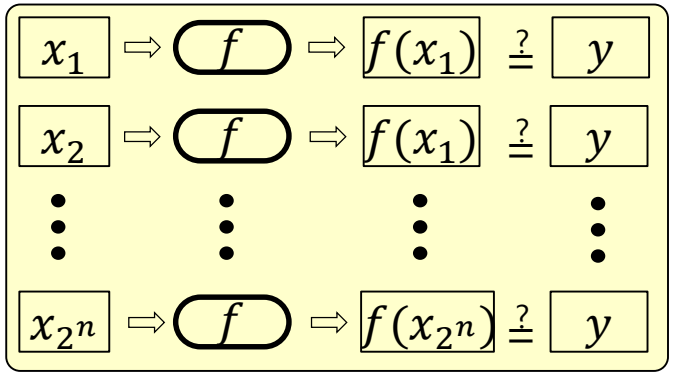
- 비트 vs 큐비트
  - 1비트 저장 가능 정보: 0 또는 1
  - 1큐비트 저장 가능 정보: 0과 1이 확률적으로 존재(중첩)

  - n-비트 저장 가능 정보: $0 \sim 2^{n-1}$ 중 1개
    - 인접 비트들은 독립적으로 정보 저장/변화
  - n-큐비트 저장 가능 정보: $0 \sim 2^{n-1}$ 이 확률적으로 존재
    - 인접 비트들의 정보가 상호간에 영향을 줌(얽힘, 간섭)

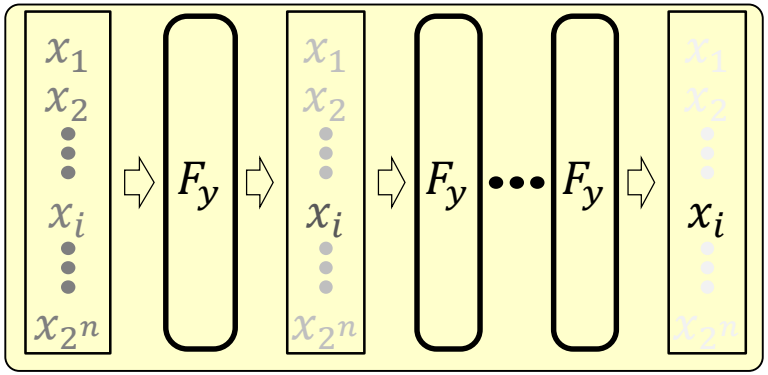


양자컴퓨터

- 가능한 장점
  - 2^n 개의 정보(상태)를 n개의 큐비트에 저장 가능
  - 2^n 개의 정보(상태)를 동일한 방식으로 동시에 계산(변화) 가능
- (주의) 고전적 의미의 병렬 계산을 의미하지는 않음!
  - 결과 획득을 위해서는 반드시 '관측'이라는 과정 필요
  - 관측 전까지는 모든 상태에 대한 정보 내재
  - 관측 후에는 1개 상태에 대한 값만 확인 가능
- 유용한 양자 알고리즘?
  - 원하는 상태 값이 관측될 확률을 높이는 과정



(a) 고전 컴퓨팅 환경에서 병렬 탐색 방법

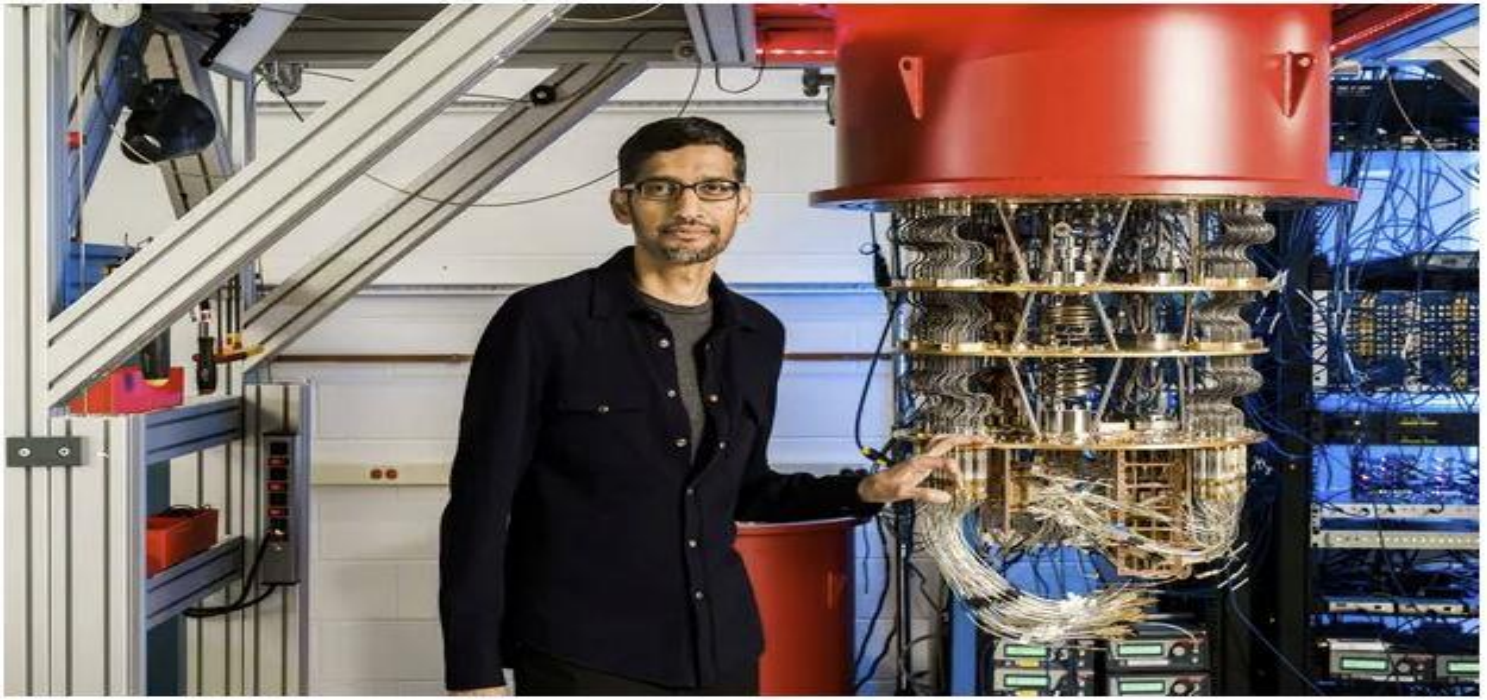


(b) 양자 컴퓨팅 환경에서 탐색 방법

양자컴퓨터 실용화 가능성

Google claims it has achieved 'quantum supremacy' – but IBM disagrees

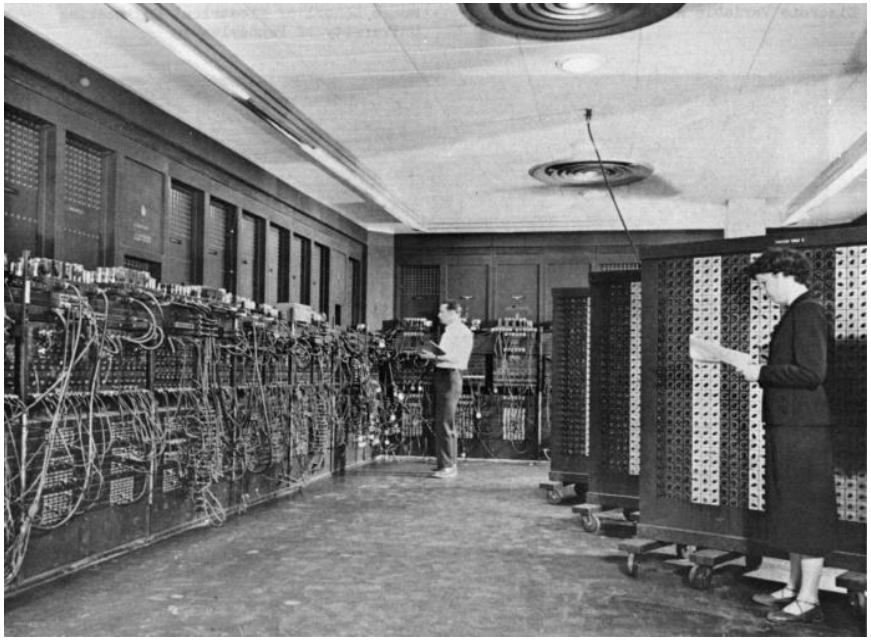
Task that would take most powerful supercomputer 10,000 years 'completed by quantum machine in minutes'



▲ Sundar Pichai, pictured with the Sycamore Quantum processor, compared the feat to building the first rocket to reach space. Photograph: Reuters

※ 출처: Guardian, 2019. 10.23. https://www.theguardian.com/technology/2019/oct/23.

양자컴퓨터 실용화 가능성



VS

Quantum Computing in the NISQ era and beyond

John Preskill

Institute for Quantum Information and Matter and Walter Burke Institute for Theoretical Physics,
California Institute of Technology, Pasadena CA 91125, USA
30 July 2018

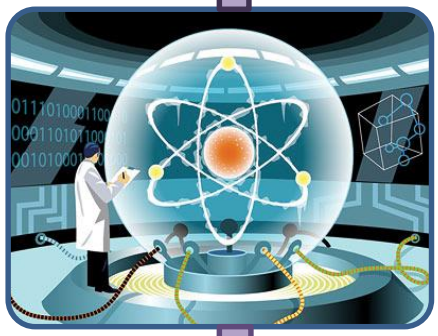
Noisy Intermediate-Scale Quantum (NISQ) technology will be available in the near future. Quantum computers with 50-100 qubits may be able to perform tasks which surpass the capabilities of today's classical digital computers, but noise in quantum gates will limit the size of quantum circuits that can be executed reliably. NISQ devices will be useful tools for exploring many-body quantum physics, and may have other useful applications, but the 100-qubit quantum computer will not change the world right away — we should regard it as a significant step toward the more powerful quantum technologies of the future. Quantum technologists should continue to strive for more accurate quantum gates and, eventually, fully fault-tolerant quantum computing.

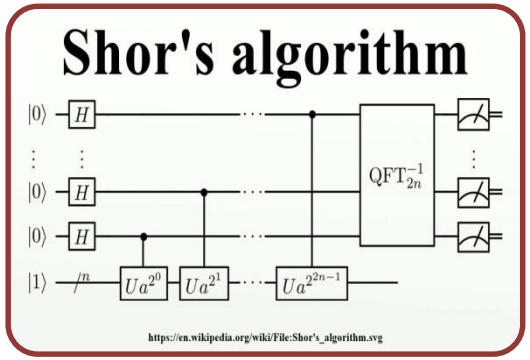
※ NISQ: Noisy Intermediate Scale Quantum Computer

2. 양자 암호분석

양자컴퓨터의 영향

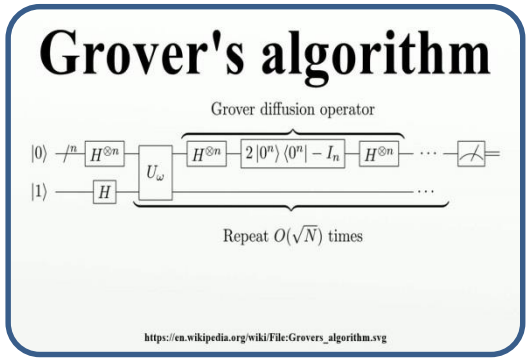
- 이론적 결과





n비트 공개키 암호

- 인수분해, DLP 계산 가능
- 복잡도: $O(n^3)$
- 새로운 기반문제 발굴 필요



n비트 비밀키 암호

- 전수조사 공격 안전도 저하
- 복잡도: $O(2^{n/2})$
- 키 크기 검토 필요

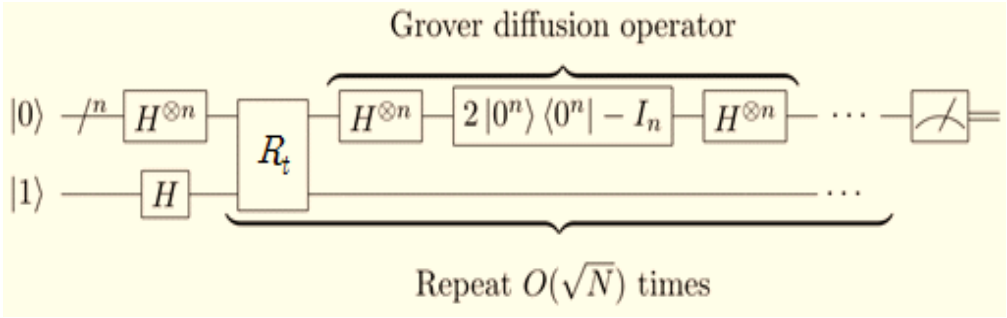
양자컴퓨터의 영향

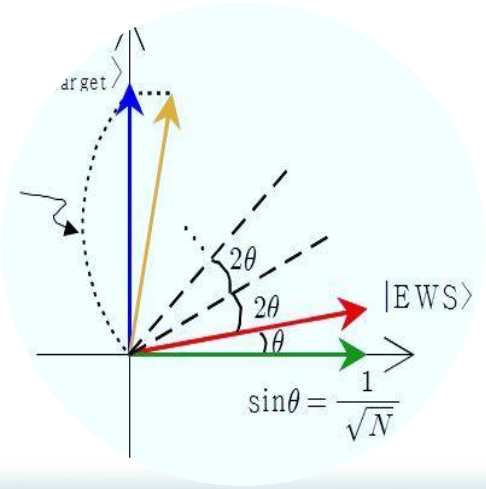
- 비밀키 암호: Grover 알고리즘
  - 기능: 집합 X와 함수 f가 주어졌을 때 x_{target}을 찾는 양자 알고리즘

$$X = \{x_1, \cdots, x_N\},$$

$$f: X \to \{0,1\}, \qquad f(x) = \begin{cases} 1, & if\ x = x_{target} \\ 0, & if\ x \neq x_{target} \end{cases}$$

  - 계산 복잡도 : $\mathcal{O}(\sqrt{N})$
    - Grover iteration = 반전 연산자(R) + 확산 연산자(D)
    - Grover iteration 수가 증가할수록 target을 찾을 확률 증가
      - Optimal 횟수 $\cong \frac{\pi}{4}\sqrt{N}$





양자컴퓨터의 영향

- 비밀키 암호

  - 256비트 암호는 적어도 2050년까지는 안전!

양자컴퓨터의 영향

- 공개키 암호

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

Craig Gidney[1,*] and Martin Ekerå[2]

[1]*Google Inc., Santa Barbara, California 93117, USA*
[2]*KTH Royal Institute of Technology, SE-100 44 Stockholm, Sweden*
Swedish NCSA, Swedish Armed Forces, SE-107 85 Stockholm, Sweden

(Dated: May 24, 2019)

We significantly reduce the cost of factoring integers and computing discrete logarithms over finite fields on a quantum computer by combining techniques from 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 (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.

※ 출처: C. Gidney et al., How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits, arXiv preprint:1905.09749, May 2019.

Shor 알고리즘

- 인수분해와 주기 탐색
  - 인수분해: 두 소수 p, q의 곱 N이 주어졌을 때 p, q를 찾는 문제
  - 주기 탐색 문제로 환원 가능

알고리즘

① N과 서로 소인 a 선택

② $a^k \bmod N$ 의 주기 r 탐색 (a의 $order$)

$$a^r = 1 \bmod N$$

$$a^r - 1 = \left(a^{\frac{r}{2}} + 1\right)\left(a^{\frac{r}{2}} - 1\right) = Apq$$

③ 다음 경우는 ①로 회귀

(r 이 홀수) 또는 ($a^{r/2} = -1 \bmod N$)

④ 다음 계산을 통해 p, q 계산

GCD($a^{r/2} + 1, N$), GCD($a^{r/2} - 1, N$)

예제 ($35 = 5 \times 7$)

① N=35, $a = 3$

② $r = 12$

3 9 27 11 33 21

17 16 13 4 12 1

③ OK

($r = 12$) & ($3^6 = 21 \bmod N$)

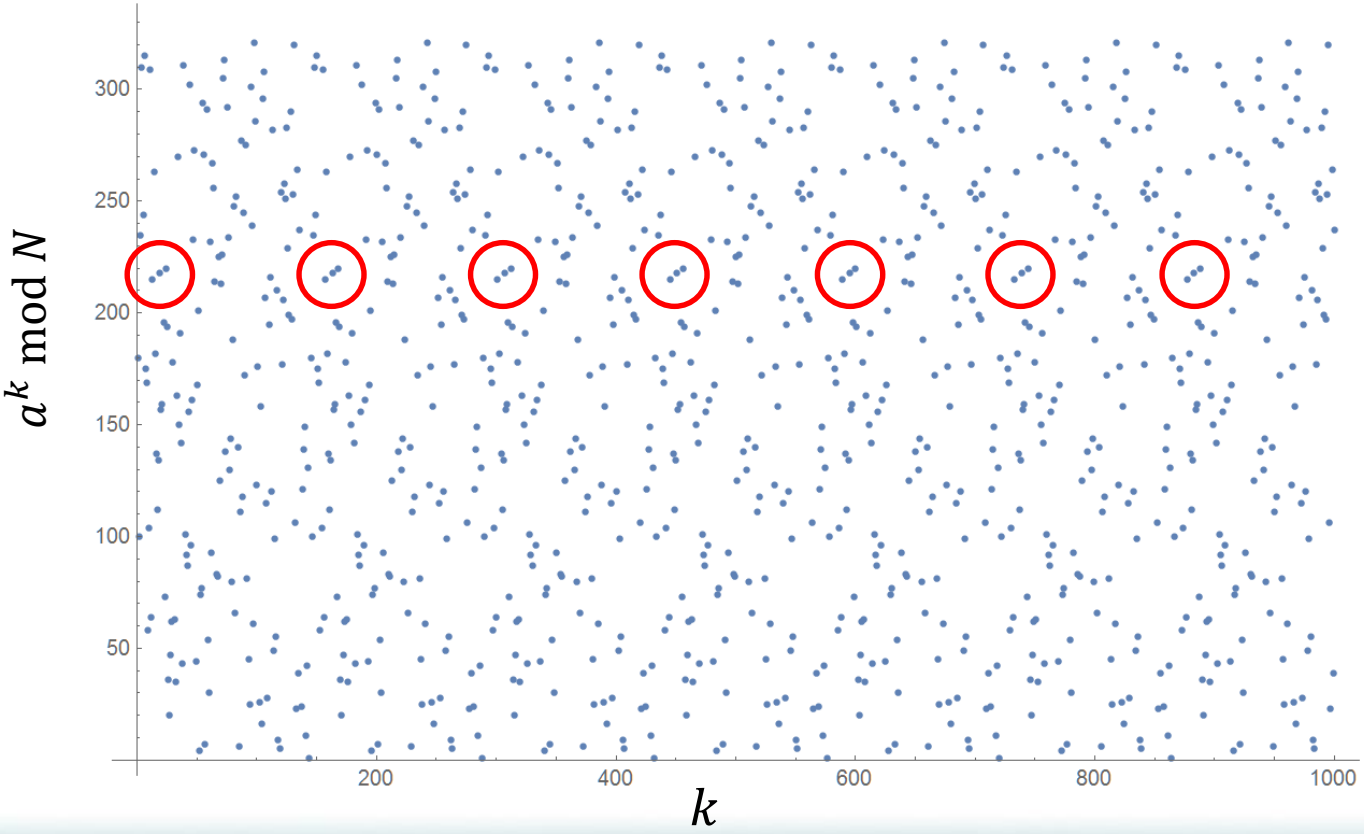
④ $3^6 = 729$

$730 = 2 \cdot 5 \cdot 73,\ 728 = 2^3 \cdot 7 \cdot 13$

  - ②번 과정이 가장 핵심 ⇒ 양자 주기 탐색 (Shor 알고리즘)

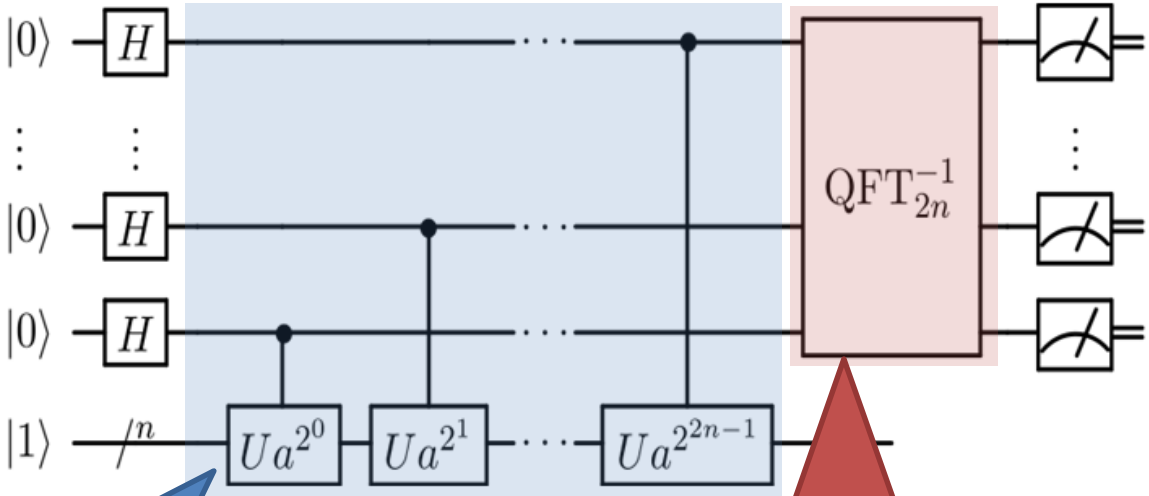
Shor 알고리즘

- 알고리즘 필요 사항(기능)
  - $a^k \ mod \ N$ 중첩 계산
  - 높은 확률로 관측되는 값으로부터 r 계산



Shor 알고리즘

- $a^k \ mod \ N$ 의 주기 탐색 알고리즘



ModExP

$$|a\rangle|1\rangle \rightarrow |a\rangle|a^k \ mod \ N\rangle$$

Quantum Fourier Transform

$$|a\rangle \rightarrow \frac{1}{\sqrt{m}} \sum_{b=0}^{m-1} e^{2\pi i \frac{a}{m} b} |b\rangle$$

3. 포스트 퀀텀 암호

본격적인 관심 배경

- NSA의 CNSA Suite 발표(2015.8.)

Rapid and secure information sharing is important to protect our Nation, its citizens and its interests. Strong cryptographic algorithms are vital tools that contribute to our national security and help address the need for secure, interoperable communications. The National Security Agency (NSA) is responsible for approving solutions for protecting National Security Systems (NSS). Many systems in the NSS community are planned over decade timescales, have very long lifetimes after deployment, and are used to protect data that requires confidentiality for years beyond that.

Since 2005, a specific set of elliptic curve based algorithms, the Suite B cryptographic algorithms as specified by the National Institute of Standards and Technology (NIST), have been used by NSA in solutions approved for protecting classified and unclassified NSS. After observing the past decade of progress in quantum computing research, NSA endorses the increasing consensus that quantum computers will pose a threat in the future and that protocols using public key algorithms in the market place today will eventually need to be addressed. Given the longevity and unique nature of NSS and the costs of converting

Commercial cryptogra… NSS systems up to …

Algorithm	Function		
Advanced Encryption Standard (AES)	Block ciphe… used fo… info…		
Elliptic Curv… Diffie-He… (ECDH… Ex… ge	…metric …gorithm used for key establishment		
Elliptic Curve Digital Signature Algorithm (ECDSA)	Asymmetric algorithm used for digital signatures	FIPS Pub 186-4	Use Curve P-384
Secure Hash Algorithm (SHA)	Used for computing a condensed …	FIPS Pub 180-4	Use SHA-384

NSA endorsed the increasing consensus that quantum computers will pose a threat in the future and that protocols using public key algorithms in the market place today will eventually need to be addressed.

NIST PQC 표준화

THE SHIP HAS SAILED

The NIST Post-Quantum Crypto "Competition"

Dustin Moody, NIST

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

※ 출처: D. Moody, The Ship has Sailed: The NIST PQC "Competition", Asiacrypt 2017, Dec. 2017.

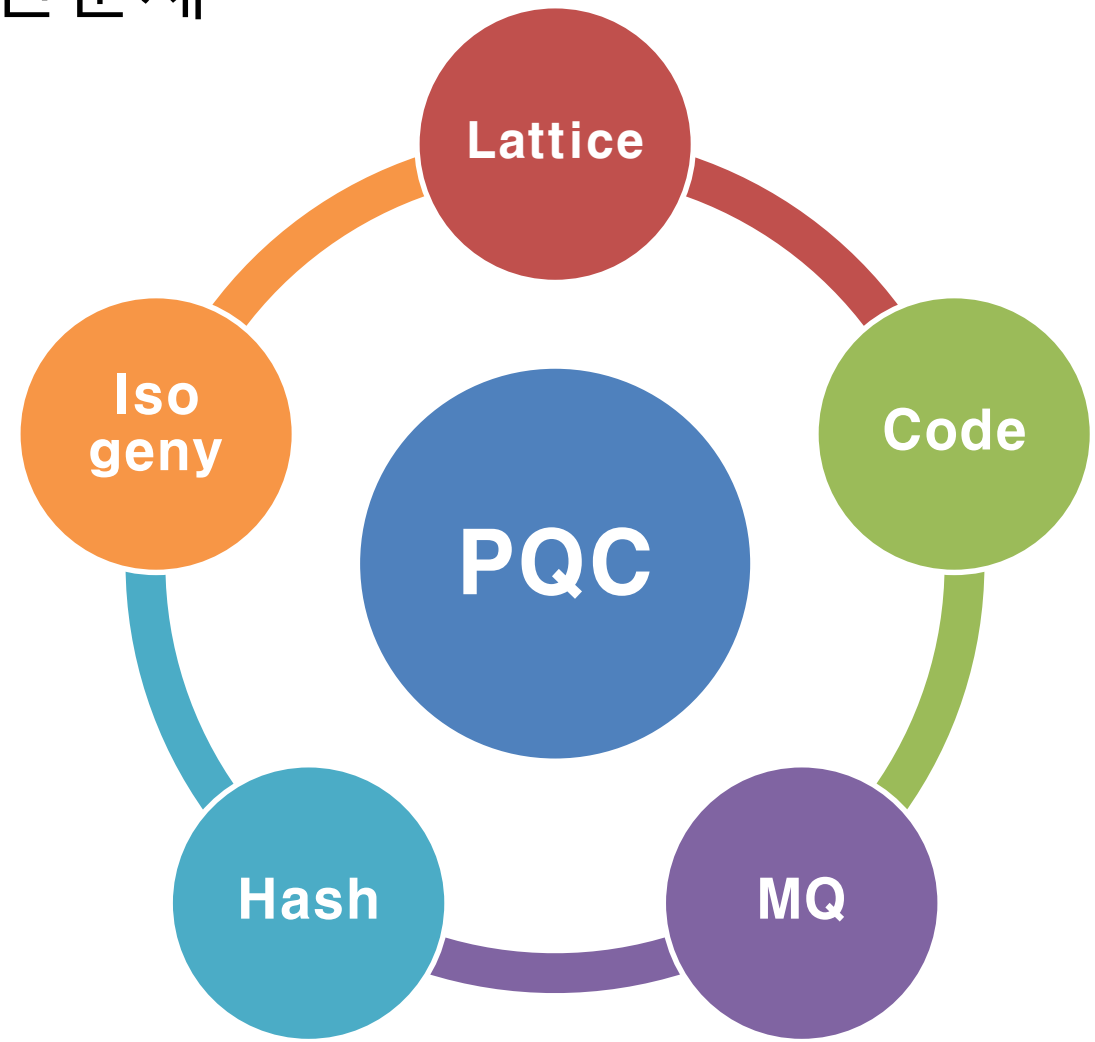
NIST PQC 표준화

- 대상
  - Signatures (FIPS 186-4)
  - Encryption (SP 800-56B)
  - Key-establishment (KEMs) (SP 800-56A)

- 경과 및 계획
  - 2016. 08. : Submission requirements & evaluation criteria
  - 2017. 11. : Deadline for submissions
  - 2018. 04. : 1st NIST PQC Workshop
  - 2019. 01. : 2nd Round
  - 2019. 08. : 2nd NIST PQC Workshop
  - 2020. 06. : 3rd Round
  - 2022-2024 : Draft standards available

NIST PQC 표준화

- PQC 기반문제



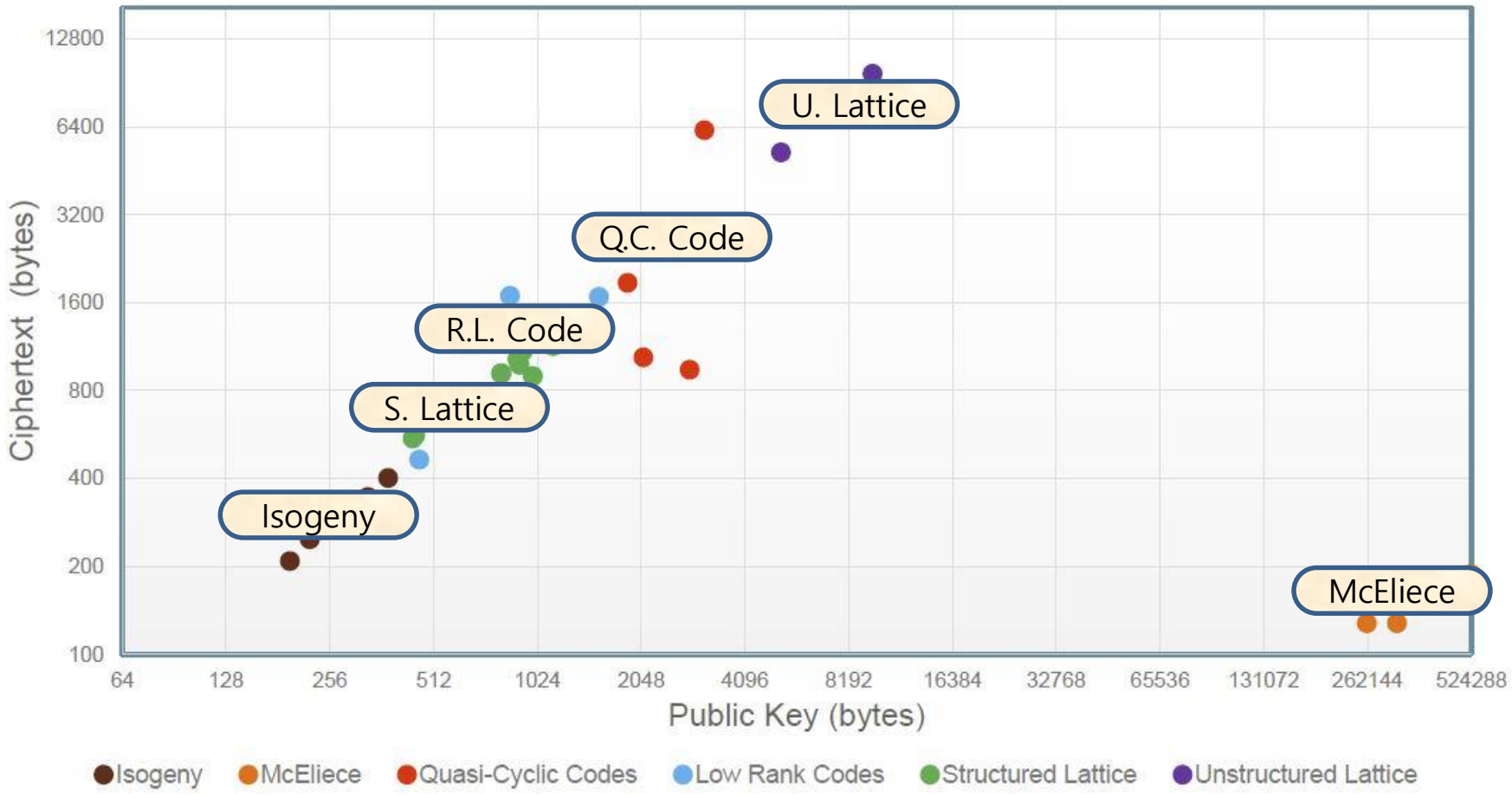
NIST PQC 표준화

- PQC 기반문제

기반문제	특징	대표 알고리즘
Lattice	✓ 가장 유력한 프리미티브 ✓ 고효율, 고활용성	NTRU/NTRUSign (1997) Kyber/Dilithium (2017)
Code	✓ 오랜 역사, 간결, 튼튼한 기반이론 ✓ 큰 키크기, 서명 구성 난해	McEliece (1978) CAKE (2017)
Multivariate Polynomial	✓ 짧은 서명길이 ✓ 큰 키크기, 암호 구성 난해	HFE (1996) PFLASH (2015)
Hash	✓ 서명 위주 ✓ 높은 안전성, 비효율	Merkle hash tree (1979) SPHINCS (2014)
Isogeny	✓ 작은 키크기, ECC 활용 가능 ✓ 난해한 이론/연산, 많은 분석 필요	SIDH (2011)

NIST PQC 표준화

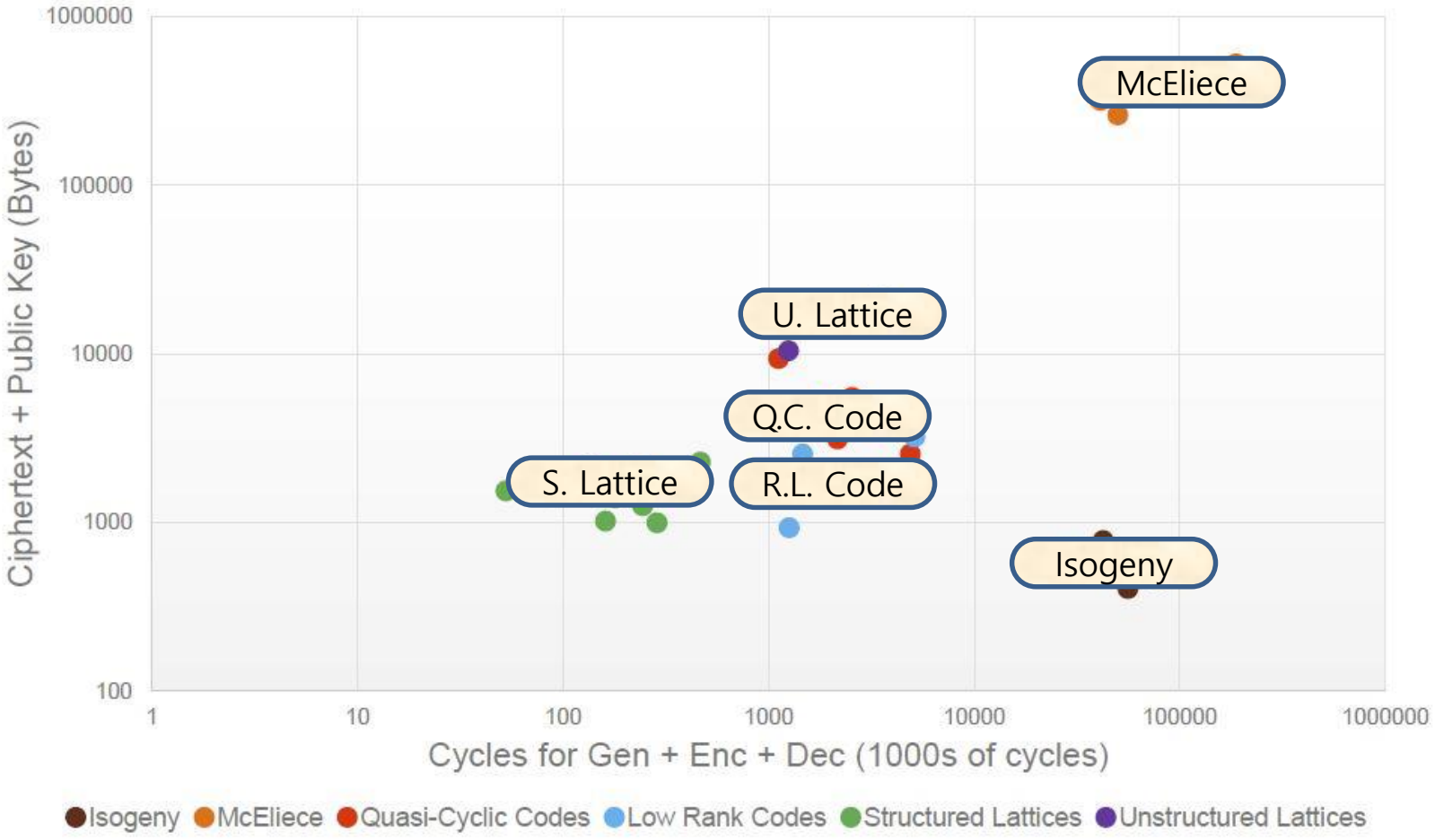
- KEM 효율성: 공개키/암호문 크기(Log scale)



※ 출처: D. Moody The 2nd Round of the NIST PQC Standardization Process, Opening Remarks at PQC 2019, Aug. 2019.

NIST PQC 표준화

- KEM 효율성: 연산 속도(Log scale)



※ 출처: D. Moody The 2nd Round of the NIST PQC Standardization Process, Opening Remarks at PQC 2019, Aug. 2019.

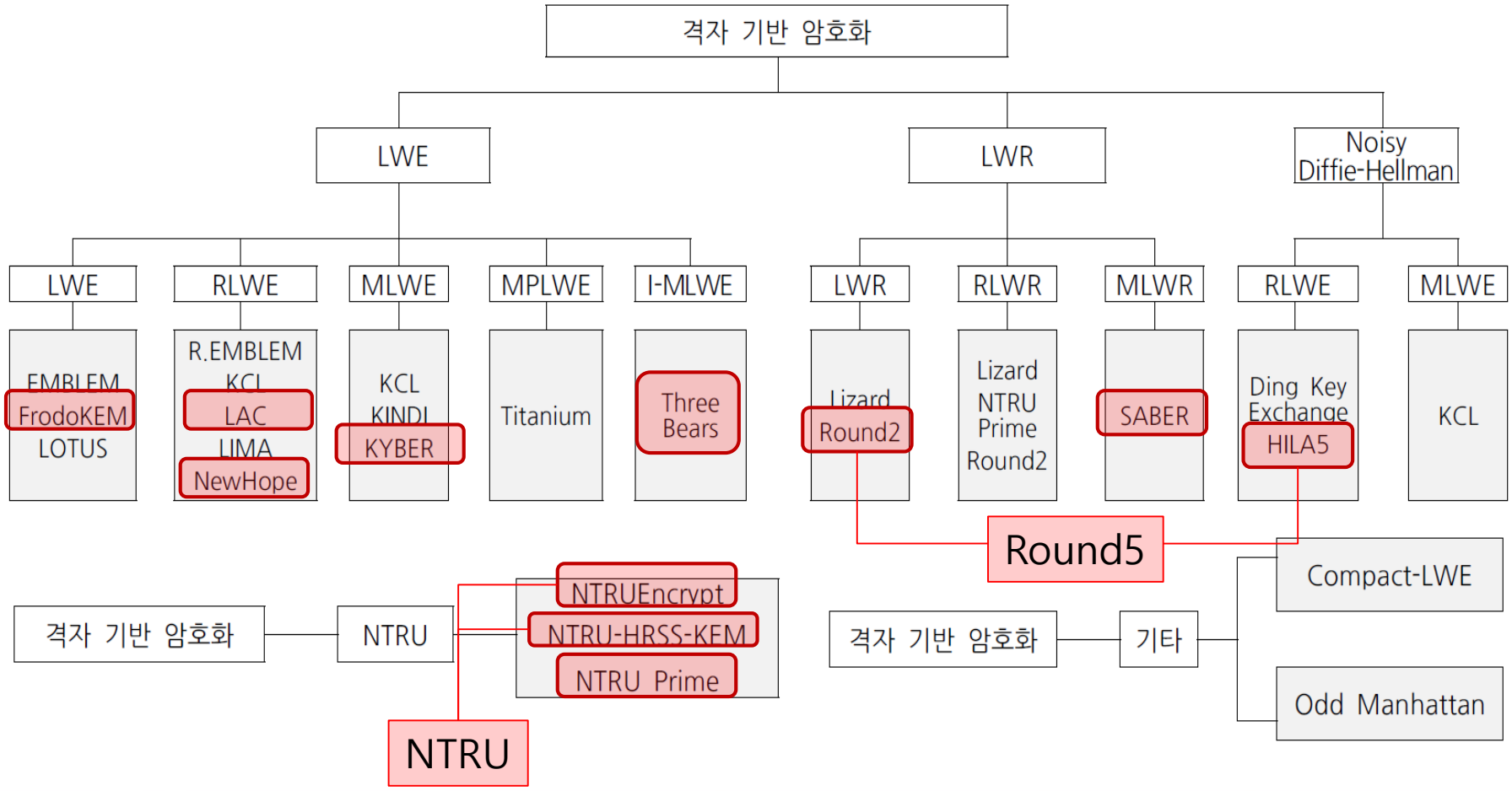
NIST PQC 표준화

- 라운드별 선정 알고리즘 수

기반문제	기능	1라운드	2라운드	선정 비율
Lattice	KEM/PKE	21	9	43 %
	Sign	5	3	60 %
Code	KEM/PKE	16	7	44 %
	Sign	2	0	0 %
MQ	KEM/PKE	3	0	0 %
	Sign	7	4	57 %
Hash	Sign	2	1	33 %
기타	KEM/PKE	5	1	29 %
	Sign	3	1	33 %
합 계	KEM/PKE	45	17	38 %
	Sign	19	9	47 %

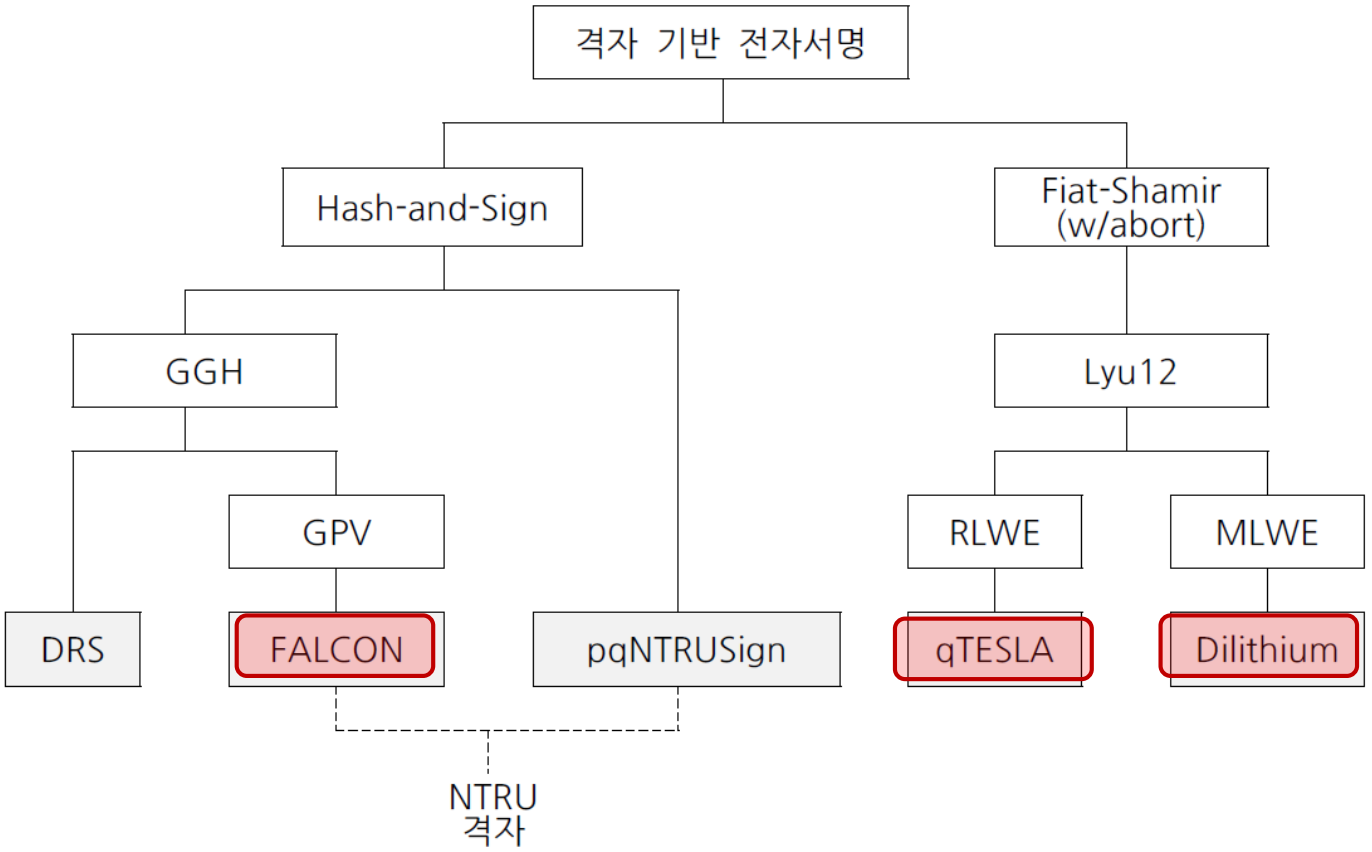
격자 기반 암호

- NIST PQC 선정 알고리즘(KEM/PKE)



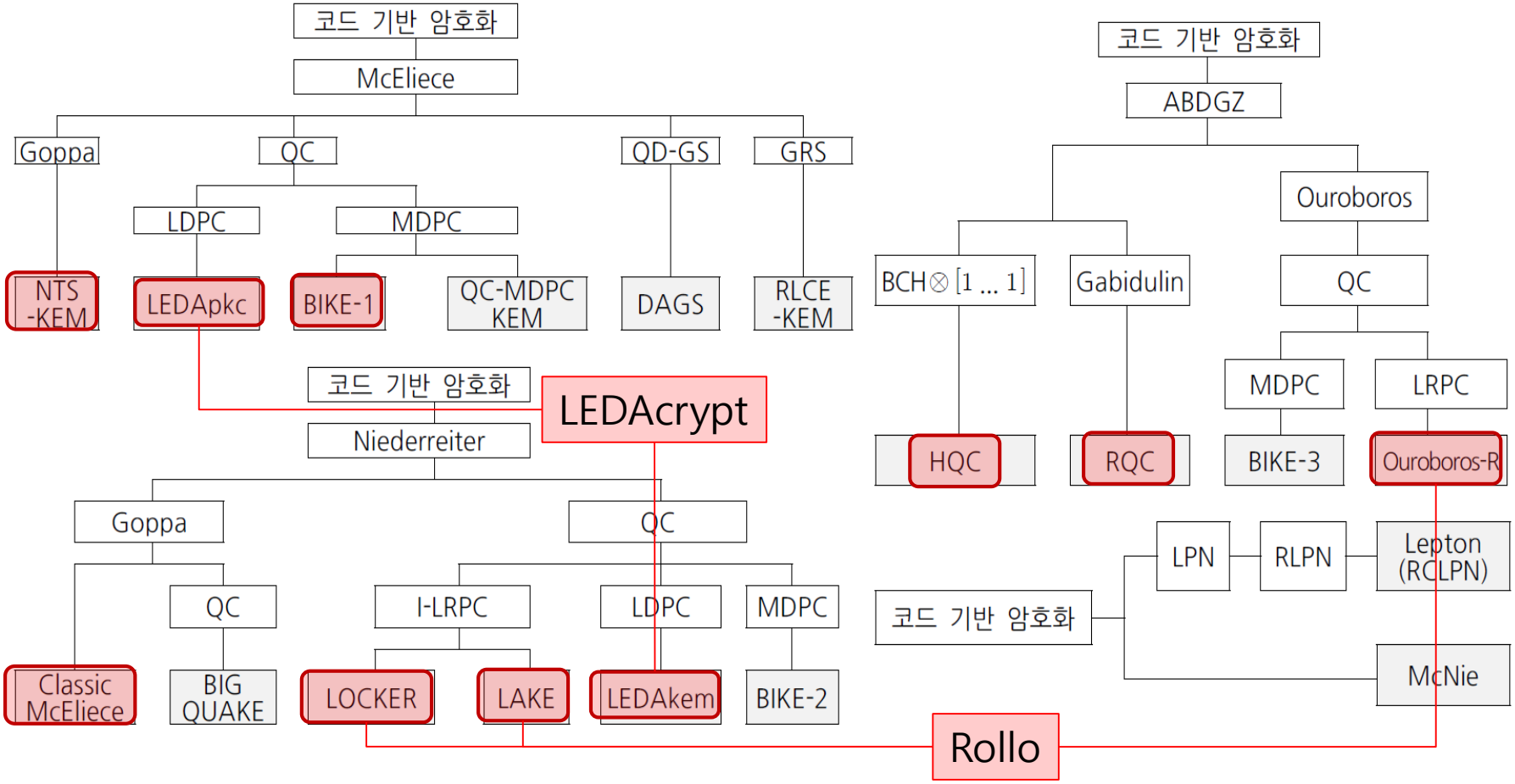
NIST PQC 표준화 선정 알고리즘

- 격자 기반 서명



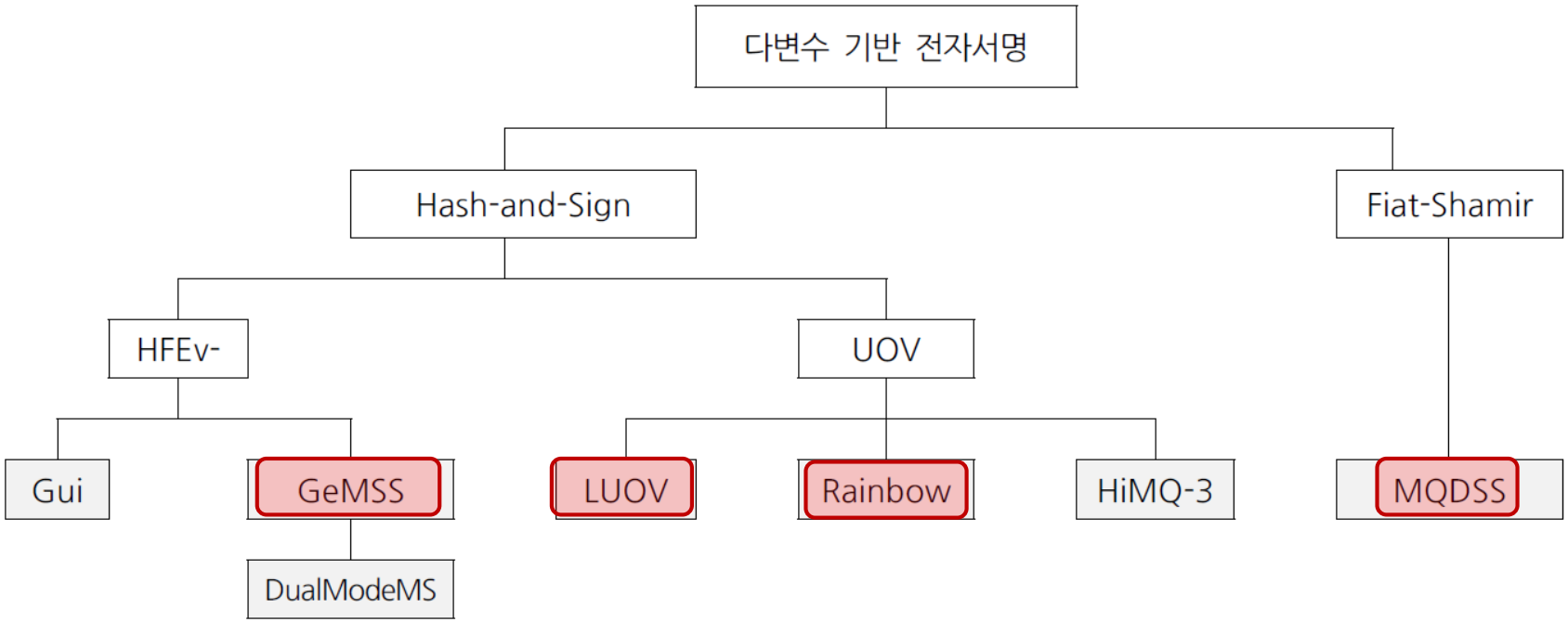
NIST PQC 표준화 선정 알고리즘

- 코드 기반 PKE/KEM



NIST PQC 표준화 선정 알고리즘

- MQ 기반 전자서명



NIST PQC 표준화 선정 알고리즘

- 2라운드 알고리즘 선정 기준
  - 다양한 기반문제/유형 선택
  - Merge 알고리즘은 가급적 선정
  - 신규 문제 기반 알고리즘은 대부분 제외
  - 동일 기반문제/유형별 1~2종 선택
    - 취약성 발견 알고리즘 제외
    - 남은 후보 중 "대표" 알고리즘 선정

- 3라운드 알고리즘 선정 기준
  - NIST 공지: focus on efficiency!
  - 학계 주장
    - Don't rush this!
    - Keep the focus on cryptanalysis!

4. PQC 적용 관련 주요 이슈

기반문제 안전성

Out of the 69 "complete and proper" submissions received by NIST, 23 are based on either the LWE or the NTRU family of lattice problems. Whilst techniques for solving these problems are well known, there exist different schools of thought regarding the asymptotic cost of these techniques, and more specifically, of the BKZ lattice reduction algorithm. This algorithm, which combines SVP calls in projected sub-lattices or "blocks", is a vital building block in attacks on these schemes. These differences can result in the same scheme being attributed several different security levels, and hence security categories, depending on the *cost model* being

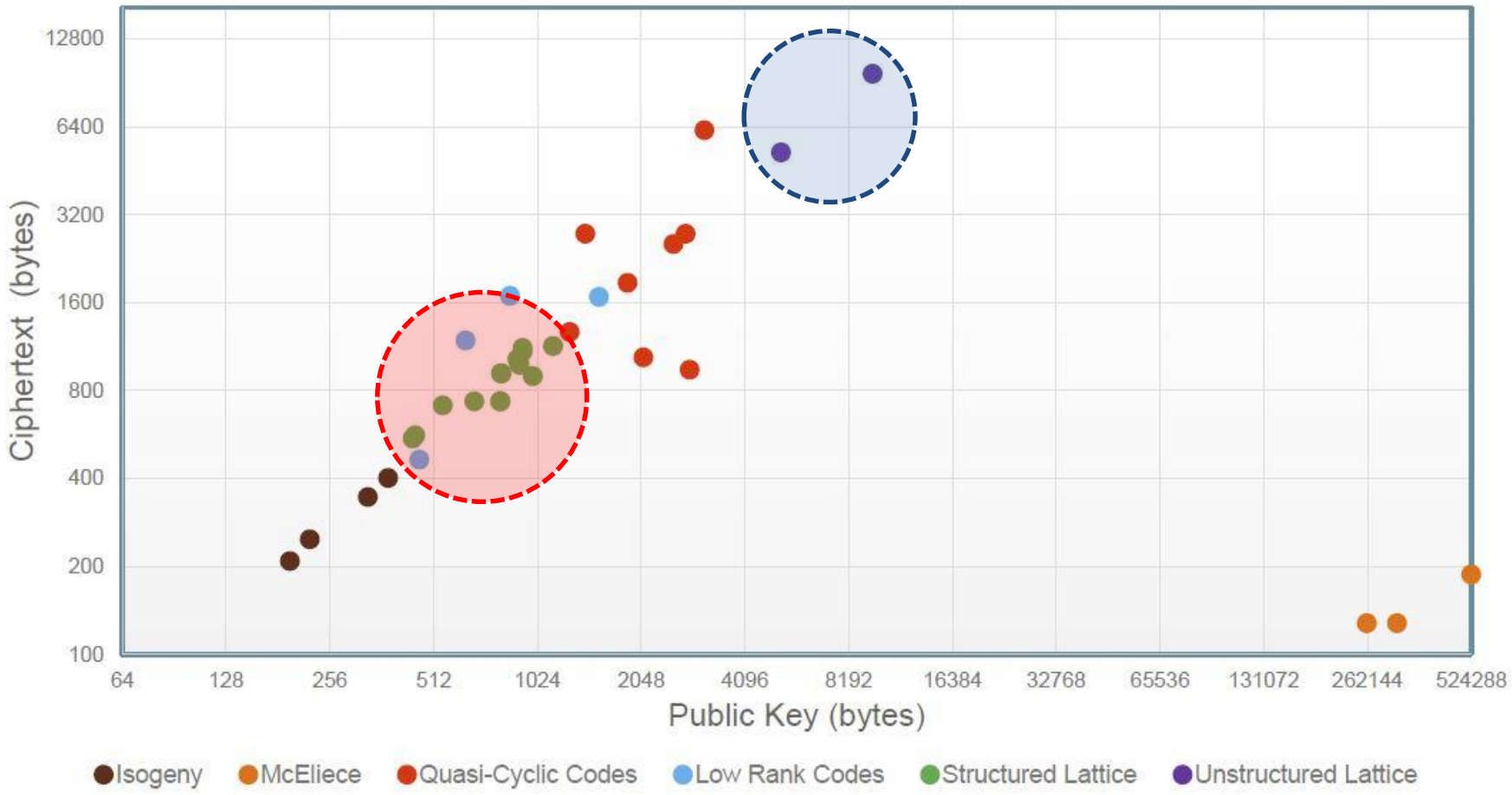
※ M. R. Albrecht et al., Estimate all the {LWE, NTRU} schemes!, SCN 2018, Aug. 2018.

2.1. Does "security" accurately report security against known attacks?
In general, the answer to this type of question is "no". Computing the cost of known attacks against lattice systems (never mind the difficulty of predicting the impact of unknown attacks) is a bleeding-edge research problem. Existing estimates of this cost combine various calculations that are loosely inspired by known attacks but that include quite a few oversimplifications and potential oversimplifications. The resulting errors can lead to a variety of problems:

※ D. Bernstein, Visualizing size-security tradeoffs for lattice-based encryption, IACR ePrint 2019/655.

기반문제 안전성

- Structured Lattice(RLWE,MLWE,...)의 안전성



기반문제 안전성

- Structured Lattice(RLWE,MLWE,...)의 안전성

Those broken schemes were using a special class of principal ideals, but these works also showed how to solve SVP for principal ideals in the *worst-case* in quantum polynomial time for an approximation factor of $\exp(\tilde{O}(\sqrt{n}))$. This exposed an unexpected hardness gap between general lattices and some structured ones, and called into question the hardness of various problems over structured lattices, such as Ideal-SVP and Ring-LWE.
In this work, we generalize the previous result to general ideals. Precisely,

polynomial time for an approximation factor of $\exp(\tilde{O}(\sqrt{n}))$.
Although it does not seem that the security of Ring-LWE based cryptosystems is directly affected, we contribute novel ideas to the cryptanalysis of schemes based on structured lattices. Moreover, our result shows a deepening of the gap between general lattices and structured ones.

※ R. Cramer et al., Short Stickeberger Class Relations and Application to Ideal-SVP, Eurocrypt 17.

양자컴퓨팅 공격에 대한 안전성

- NIST의 입장

Quantum Security

- No clear consensus on best way to measure quantum attacks

- Uncertainties
  - The possibility that new quantum algorithms will be discovered, leading to new attacks
  - The performance characteristics of future quantum computers, such as their cost, speed and memory size

- For PQC standardization, need to specify concrete parameters with security estimates

※ D. Moody, Let's Get Ready to Rumble: The NIST PQC "Competition, PQCrypto 2018, Apr. 2018.

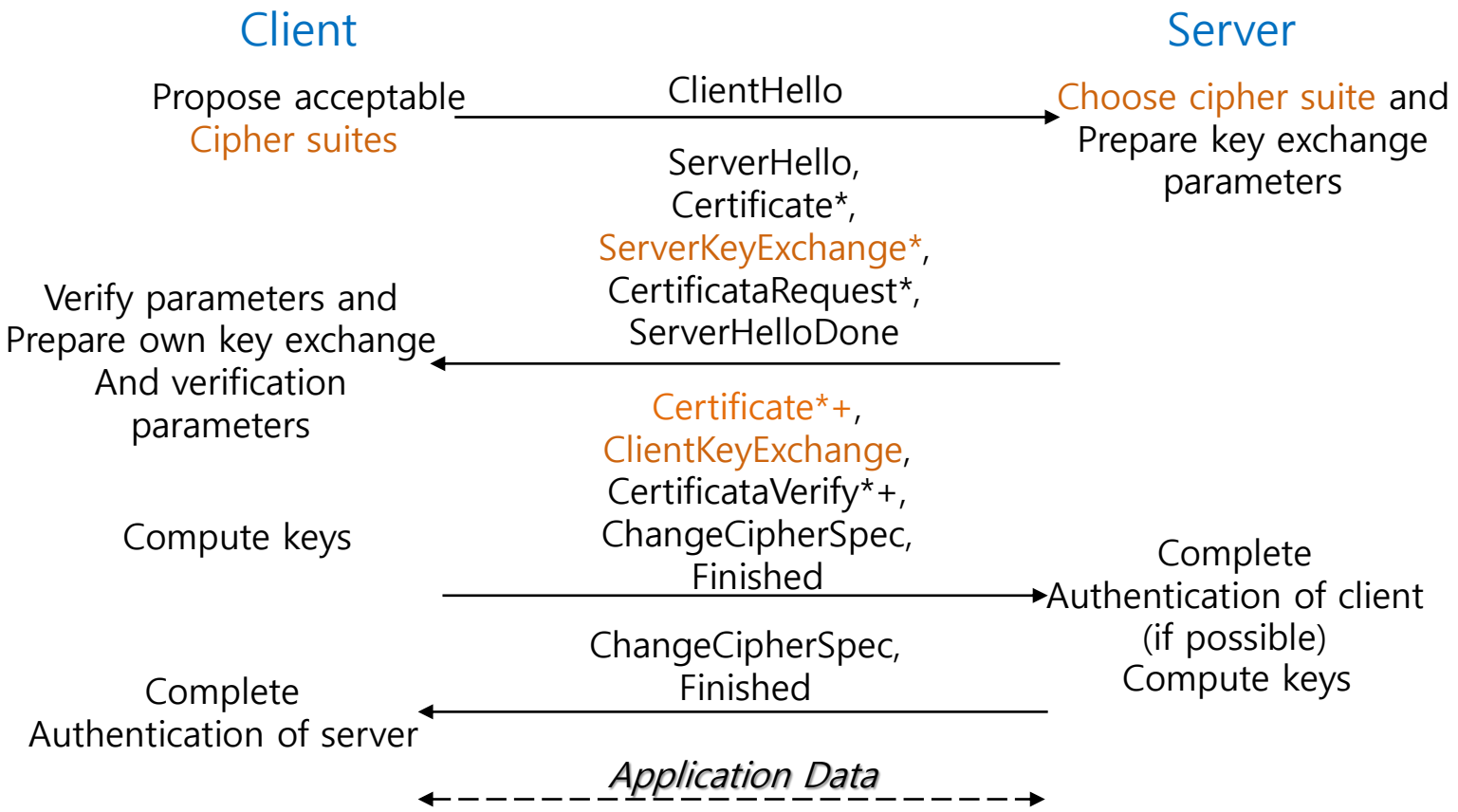
양자컴퓨팅 공격에 대한 안전성

- NIST PQC 표준화의 정량적 안전성 기준

카테고리		안전성 기준	게이트 수
1	AES128	어떠한 공격 방법도 128비트 블록암호의 키 전수 조사에 필요한 양보다 많은 계산 자원이 요구됨	2^{170}/MAXDEPTH 양자 게이트
2	SHA3-256	어떠한 공격 방법도 256비트 해쉬함수의 충돌쌍 탐색에 필요한 양보다 많은 계산 자원이 요구됨	2^{146} 고전 게이트
3	AES192	어떠한 공격 방법도 192비트 블록암호의 키 전수 조사에 필요한 양보다 많은 계산 자원이 요구됨	2^{233}/MAXDEPTH 양자 게이트
4	SHA3-384	어떠한 공격 방법도 384비트 해쉬함수의 충돌쌍 탐색에 필요한 양보다 많은 계산 자원이 요구됨	2^{210} 고전 게이트
5	AES256	어떠한 공격 방법도 256비트 블록암호의 키 전수 조사에 필요한 양보다 많은 계산 자원이 요구됨	2^{298}/MAXDEPTH 양자 게이트

Bandwidth

- 보안 프로토콜 적용 가능성
  - PQC 주요 적용처: TLS, IPsec, …



Bandwidth

- 보안 프로토콜 적용 관련 연구들
  - M. Braithwaite. Experimenting with post-quantum cryptography, July 2016.
  - M. Campagna et al., Hybrid Post-Quantum Key Encapsulation Methods (PQ KEM) for Transport Layer Security 1.2 (TLS)., IETF, May 2019.
  - F. Kiefer et al,. Hybrid ECDHE-SIDH key exchange for TLS. Internet-Draft draft-kiefer-tls-ecdhe-sidh-00, IETF, Nov. 2018. Work in Progress.
  - A. Langley. Post-quantum confidentiality for TLS, Apr. 2018.
  - J. M. Schanck et al., A Transport Layer Security (TLS) extension for establishing an additional shared secret. Internet-Draft draft-schanck-tls-additional-keyshare-Engineering Task Force, Apr. 2017. Work in Progress.
  - D. Stebila et al., Design issues for hybrid key exchange in TLS 1.3. Internet-Draftdraft-stebila-tls-hybrid-design-01, IETF, July 2019. Work in Progress.
  - W. Whyte et al., Quantum-safe hybrid (QSH) key exchange for Transport Layer Security (TLS) version 1.3., IETF, Oct. 2017. Work in Progress.
  - E. Crockett et al., Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH, IACR ePrint 2019/858, Jul. 2019.
  - ……

Bandwidth

- 보안 프로토콜 적용 실험 사례(KEM)

1st circle: PQ only
2nd circle: hybrid ECDH

● = success

◓ = fixable by changing implementation parameter

○ = would violate spec or otherwise unresolved error

† = algorithm on testing branch

	s2n (TLS 1.2)	OpenSSL 1.0.2 (TLS 1.2)	OpenSSL 1.1.1 (TLS 1.3)	OpenSSH
BIKE1-L1 (round 1)	–●	●●	●●	●●
BIKE1-L3 (round 1)	––	●●	●●	●●
BIKE1-L5 (round 1)	––	●●	●●	●●
BIKE2-L1 (round 1)	––	●●	●●	●●
BIKE2-L3 (round 1)	––	●●	●●	●●
BIKE2-L5 (round 1)	––	●●	●●	●●
BIKE3-L1 (round 1)	––	●●	●●	●●
BIKE3-L3 (round 1)	––	●●	●●	●●
BIKE3-L5 (round 1)	––	●●	●●	●●
FrodoKEM-640-AES	––	●●	●●	●●
FrodoKEM-640-SHAKE	––	●●	●●	●●
FrodoKEM-976-AES	––	●●	●●	●●
FrodoKEM-976-SHAKE	––	●●	●●	●●
FrodoKEM-1344-AES	––	◓◓	◓◓	●●
FrodoKEM-1344-SHAKE	––	◓◓	◓◓	●●
Kyber512	––	●●	●●	●●
Kyber768	––	●●	●●	●●
Kyber1024	––	●●	●●	●●
LEDAcrypt-KEM-LT-12†	––	●●	●●	●●
LEDAcrypt-KEM-LT-32†	––	●●	●●	●●
LEDAcrypt-KEM-LT-52†	––	●●	●●	●●
NewHope-512-CCA	––	●●	●●	●●
NewHope-1024-CCA	––	●●	●●	●●
NTRU-HPS-2048-509	––	●●	●●	●●
NTRU-HPS-2048-677	––	●●	●●	●●
NTRU-HPS-4096-821	––	●●	●●	●●
NTRU-HRSS-701	––	●●	●●	●●
NTS-KEM(12,64)†	––	○○	○○	○○
LightSaber-KEM	––	●●	●●	●●
Saber-KEM	––	●●	●●	●●
FireSaber-KEM	––	●●	●●	●●
SIKEp503 (round 1)	–●	––	––	––
SIKEp434	––	●●	●●	●●
SIKEp503	––	●●	●●	●●
SIKEp610	––	●●	●●	●●
SIKEp751	––	●●	●●	●●

FrodoKEM 976, 1344

- OpenSSL 1.0.2 / TLS 1.2: too large for a pre-programmed buffer size, but easily fixed by increasing one buffer size
- OpenSSL 1.1.1 / TLS 1.3: same

NTS-KEM

- OpenSSL 1.0.2 / TLS 1.2: theoretically within spec's limitation of 2^{24} bytes, but buffer sizes that large caused failures we couldn't track down
- OpenSSL 1.1.1 / TLS 1.3: too large for spec (2^{16}-1 bytes)
- OpenSSH: theoretically within spec but not within RFC's "SHOULD", but couldn't resolve bugs

※ 출처: E. Crockett et al., Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.

Bandwidth

- 적용 실험 주요 결과
  - Unstructured lattice 암호는 적용 어려움
    - 예: FrodoKEM
  - Structured lattice 암호는 적용 가능
    - 예: NewHope, NTRU
  - Hybrid mode 적용도 가능

	ECDHE		RLWE		HYBRID	
	ECDSA	RSA	ECDSA	RSA	ECDSA	RSA
Connections / second						
- 1B payload	645.9	177.4	507.5 (1.27x)	164.2 (1.08x)	362.9 (1.78x)	145.1 (1.22x)
- 1KiB payload	641.6	177.0	505.9 (1.27x)	163.8 (1.08x)	361.0 (1.78x)	145.0 (1.22x)
- 10KiB payload	630.2	176.2	494.9 (1.27x)	161.9 (1.09x)	356.2 (1.77x)	144.1 (1.22x)
-100KiB payload	487.6	161.2	397.6 (1.23x)	150.2 (1.07x)	300.5 (1.62x)	134.3 (1.20x)
Connection time(ms)	6.0	14.0	45.6 (7.6x)	54.0 (3.9x)	47.2 (7.9x)	54.6 (3.9x)
Handshake (bytes)	1,278	2,360	9,469 (7.4x)	10,479 (4.4x)	9,607 (7.5x)	10,690 4.5x

※ 출처: W. Bos et al., Post-quantum key exchange for the TLS protocol from the ring learning with errors problem, IEEE S&P 2015.

Bandwidth

- 적용 실험의 문제점
  - 서명은 기존 알고리즘 사용

> Although there have been several Internet-Drafts and experimental implementations of PQ and/or hybrid key exchange in TLS as noted in Section 3.1, none of those works considered PQ or hybrid authentication. This is likely to due to the general consensus that confidentiality against quantum adversaries is a more urgent need than authenticity, since quantum adversaries could retroactively attack confidentiality of any passively recorded communication sessions, but could not retroactively impersonate parties establishing a (completed) communication session. Nonetheless, the advent of a quantum computer would mean that we would eventually need to migrate to post-quantum authentication, meriting some preliminary investigation.

※ 출처: E. Crockett et al., Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH.

  - TLS의 서명 관련 제약 조건
    - X.509 Certificate의 서명 관련 확보 가능 공간: 2^{24} – 1(16M) bytes
    - 서명 크기: 2^{16} – 1(64K) bytes

기타 사항

- 고속/안전 구현 기술
  - 기존 공개키암호 대비 구현 난해
  - 많은 메모리 또는 연산량 필요
  - 부채널분석 등 물리적 공격에 대한 대응 필요
  - 전반적으로 구현기술은 미성숙
- 표준화
  - 국제: NIST, ETSI, ISO 등 진행 중
  - 국내: 미미
- 정책
  - CMVP 등 평가체계
  - 적용 활성화 방안

5. 맺음말

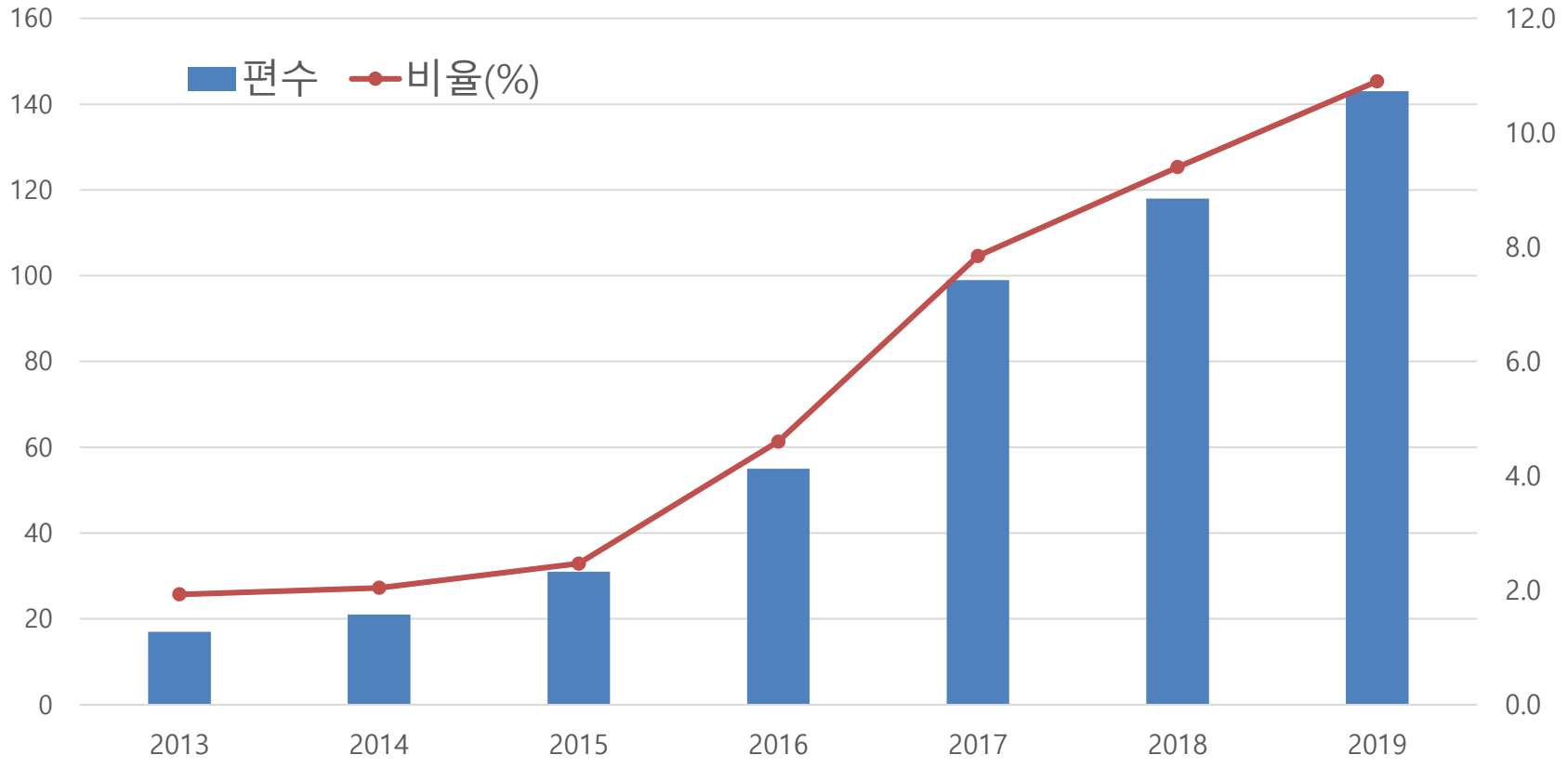
PQC 필요성?

- 안전한 PQC 체계 구축의 효과
  - 소규모 양자컴퓨터는 개발 가능할 수 있음
  - 암호해독용 양자컴퓨터 개발에는 대규모 투자 필요
  - 개발 의지 봉쇄 가능

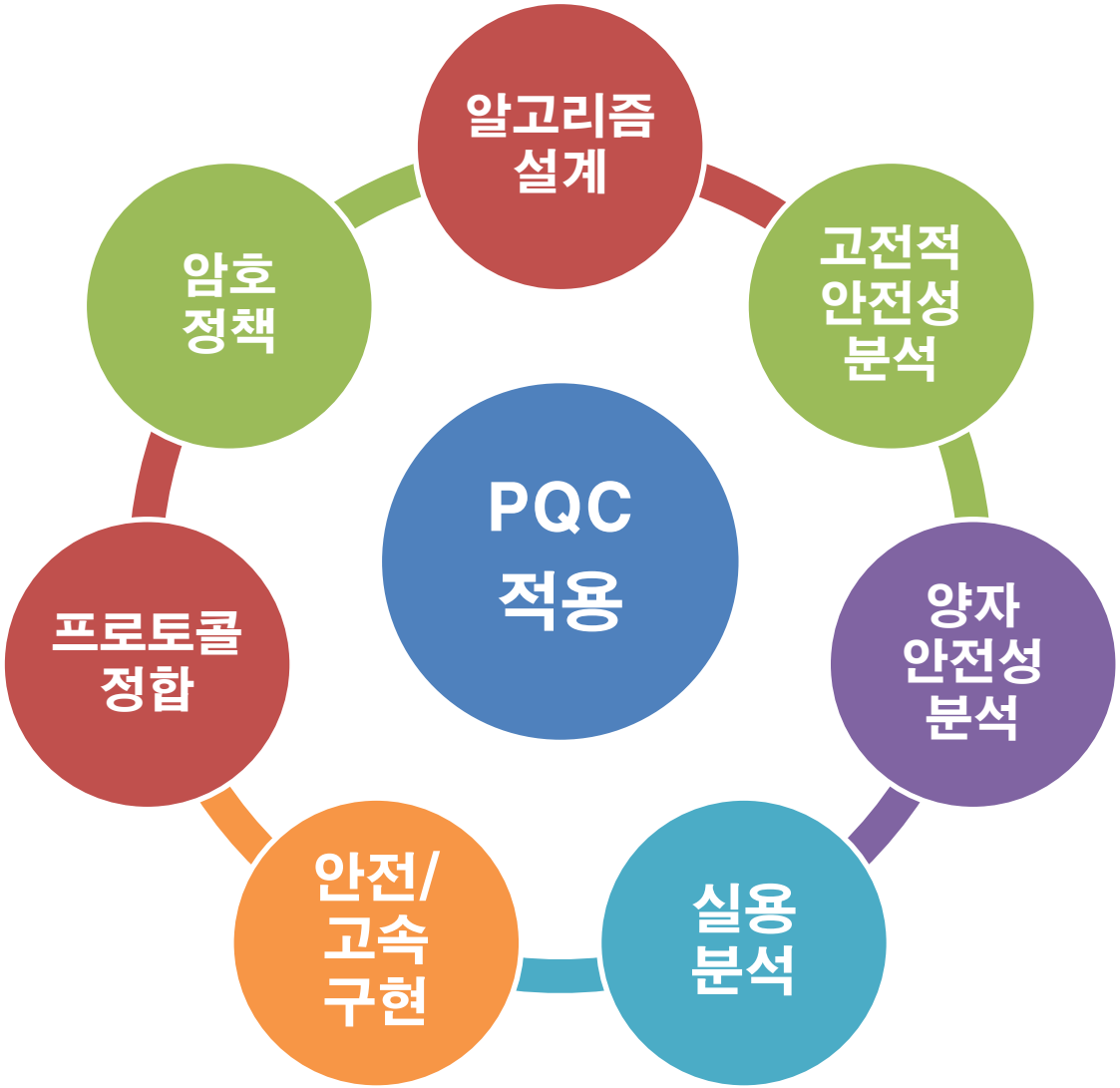
- RSA, ECC는 대체할 때가 되지 않은지…
  - RSA: 1978년, ECC: 1985년
  - 격자, 코드, MQ 문제의 장점 존재
    - 계산 이론적 안전성 보장
    - 신규 암호 서비스에 적용 가능성

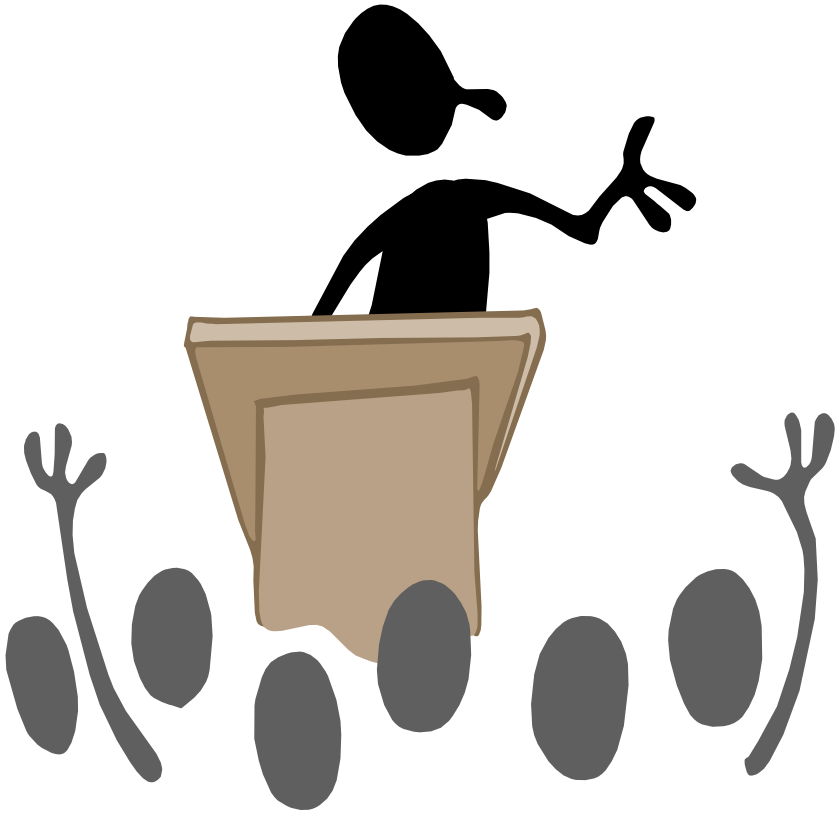
PQC 필요성?

- 암호학의 중요 분야로 정착
  - IACR ePrint 논문 검색 결과 (쿼리: Quantum)



PQC 적용을 위해서는?





Questions?