양자시대에도 인터넷은 안전할까?

공격과 수비의 개념

목차

1 공개키 암호와 그 기반문제들

2 양자컴퓨팅, 양자암호통신

3 양자내성 암호

주요 개념들

1) 공개키 암호의 기반문제 개념

2) 양자 컴퓨팅, 양자암호의 기초적 개념

3) 양자컴퓨터가 미래의 정보보안 분야에 미치는 영향

4) 양자 내성 암호가 양자 컴퓨터의 공격에 안전한 이유와 그 필요성

1. 공개키 암호와 그 기반문제들

Public- key Cryptography and its Underlying Problems

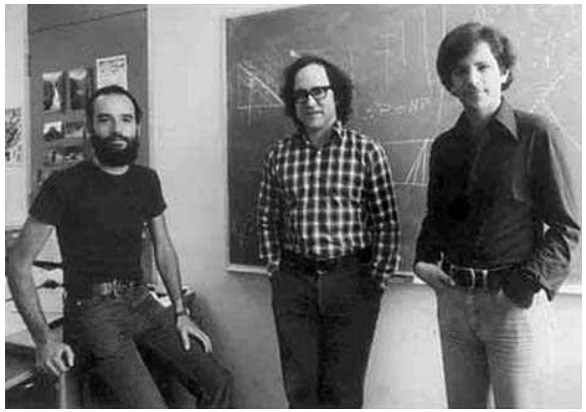
1) 암호화 : 정보보호의 가장 기본적인 설비

2) 대표적인 공개키 암호 – RSA & ECC

슈퍼 컴퓨터로도 계산하기 어려운 수학문제들을 기반으로 설계

RSA | **ECC**

$$N = pq$$
$$\phi(N) = (p-1)(q-1)$$
$$e \cdot d = 1 \ mod \ \phi(N)$$
$$C = M^e \ mod \ N$$
$$M = C^d \ mod \ N$$



➡ $N = pq$ 의 인수분해가 알려지면 비밀키 노출

2) 대표적인 공개키 암호 – RSA & ECC

슈퍼 컴퓨터로도 계산하기 어려운 수학문제들을 기반으로 설계

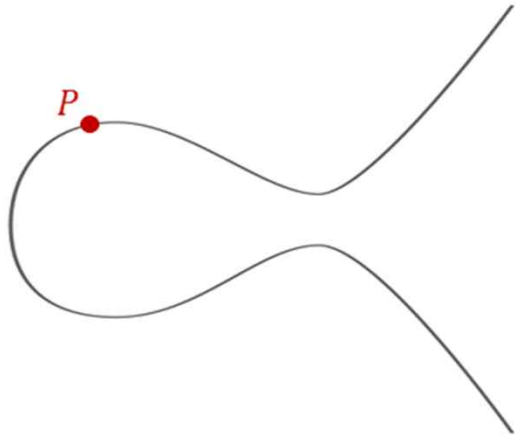
RSA

$$y^3 = x^3 + Ax + B$$

$$\lambda = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} \\ \dfrac{3x^2{}_1 + A}{2y_1} \end{cases}$$

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = -\lambda(x_3 - x_1) - y_1$$

ECC



➡ $Q = [x]P$인 x를
찾기 어렵기 때문에 안전함

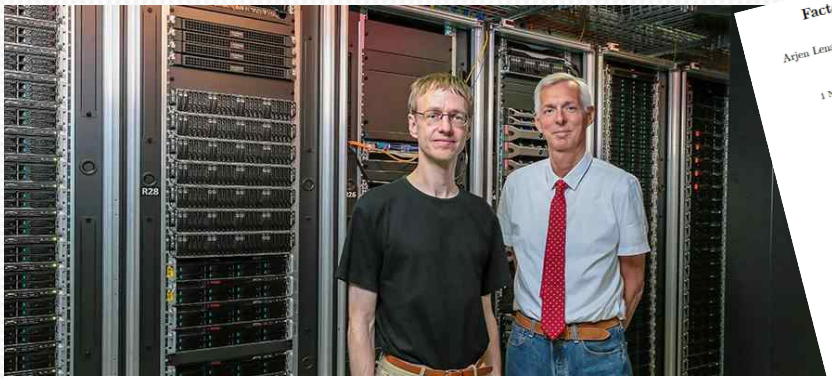
3) 암호의 보안 강도

Date	Minimum of Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm		Elliptic Curve	Hash(A)	Hach(B)
				Key	Group			
(Legacy)	80	2TDEA*	1024	160	1024	160	SHA-1**	
2016-2030	112	3TDEA	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2016-2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1
2016-2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224
2016-2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-512

2. 양자컴퓨팅, 양자암호통신

Quantum Computing,
Quantum Cryptography

4) 1024-bit RSA를 깨려면?



Factoring estimates for a 1024-bit RSA modulus

Arjen Lenstra[1], Eran Tromer[2], Adi Shamir[2], Wil Kortsmit[3], Bruce Dodson[4], James Hughes[5], Paul Leyland[6]

[1] Citibank, N.A. and Technische Universiteit Eindhoven, 1 North Gate Road, Mendham, NJ 07945-3104, USA, arjen.lenstra@citigroup.com
[2] Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot 76100, Israel, {tromer,shamir}@wisdom.weizmann.ac.il
[3] Technische Universiteit Eindhoven, P.O.Box 513, 5600 MB Eindhoven, The Netherlands, rcvvl@win.tue.nl
[4] Lehigh University, Bethlehem, PA 18015-3174, USA, bad0@lehigh.edu
[5] Storage Technology Corporation, 7600 Boone Ave No, Minneapolis, MN 55428, USA, James_Hughes@StorageTek.com
[6] Microsoft Research Ltd, 7 JJ Thomson Avenue, Cambridge, CB3 0FB, UK, pleyland@microsoft.com

Abstract. We estimate the yield of the number field sieve factoring algorithm when applied to the 1024-bit composite integer RSA-1024 and the parameters as proposed in the draft version [17] of the TWIRL hardware factoring device [18]. We present the details behind the resulting improved parameter choices from [18].

Keywords: 1024-bit RSA, factorization, number field sieve, TWIRL

1 Introduction

RSA with 1024-bit moduli is widely used. It is unlikely that breaking a single 1024-bit RSA modulus will change much, just as repeatedly breaking DES had, for obvious economic limited effect on legacy applications. Nevertheless, despite the possible lack of ...ical relevance, in cryptographic circles there is wide-spread interest in the ...d be to factor a 1024-bit RSA modulus (cf. [2], [12]). ...TWIRL', was pre- ...an innovative hardware device, ...moduli at a much lower cost than before. ...nd the draft of TWIRL [17]. ...ctorization of a 1024-bit ...for a 512-bit NFS factor- ...ge extrapolation from 512 ...Our goal was therefore to ...y uncertainties involved in ...hoped to get an indication ...turned out, our results sug- ...was subsequently adopted by ...arameters and to fine-tune the ...the factor... ...if the proposed para... ...gested that the choices were ... ...the authors of TWIRL. It allowed them to...

recent factoring experiment. Thus, we may conclude that using 90nm technology, a budget of 10M US$×year per factorization (in large quantities) leaves an ample safety margin — arguably, more than enough to account for estimation errors, relations that are lost due to

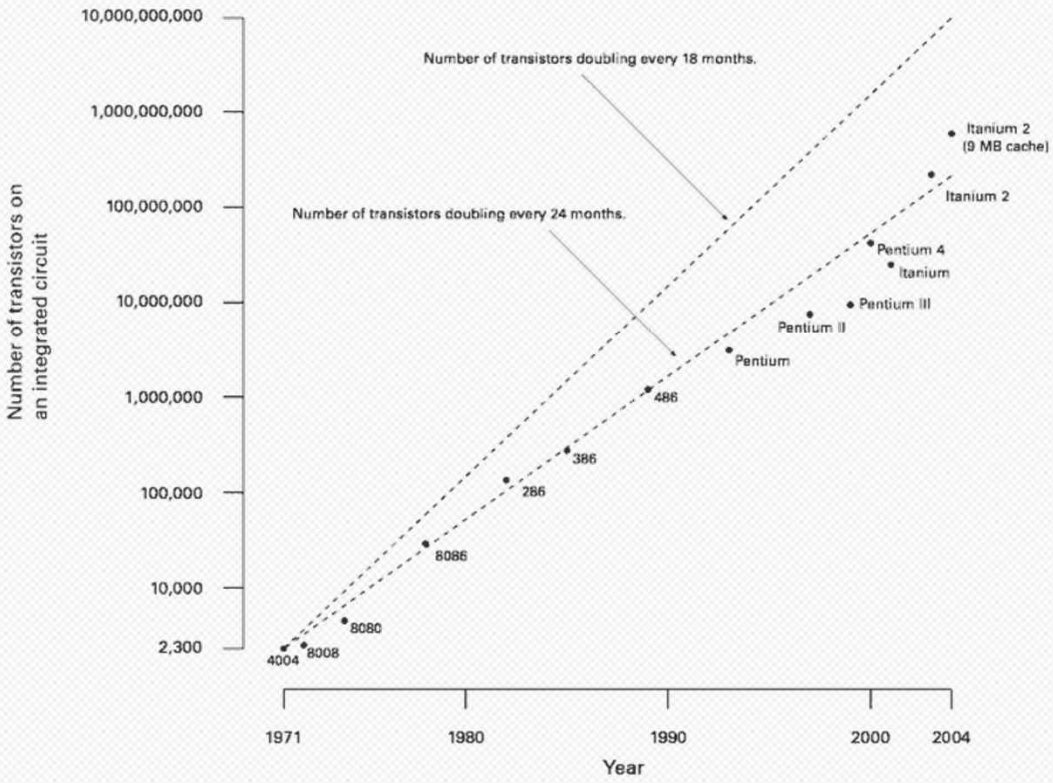
NIST의 자료를 이용한 추산

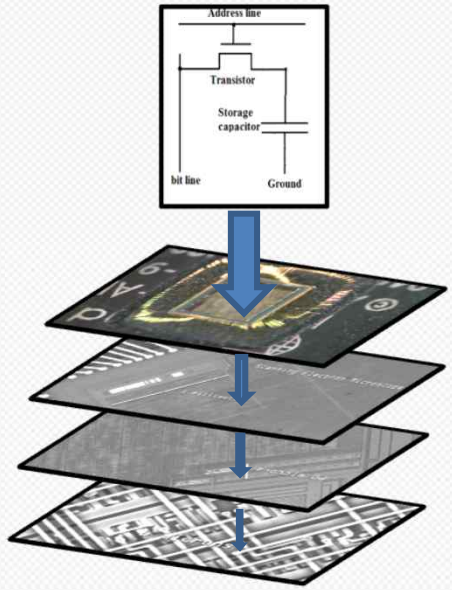
- 1024-bit security ~ 80-bit
- 2048-bit security ~ 112-bit → 2019~2030년 유효한 RSA의 강도
- 2003년경 트랜지스터 크기 90 nm
- 현재 트랜지스터 크기 약 5 nm 이하 (2~3 나노미터를 한계로 예측)
- 실제로는 아직까지 829비트(2020년)까지만 성공한 상태

1) 무어의 법칙

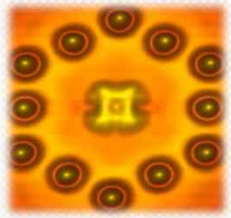
✔ 칩 안의 트랜지스터의 개수는
24개월마다 **2** 배가 된다.

(G. Moore 1965)





✔ **2015**년에는 독일- 일본- 미국
연구진이 분자 크기의 트랜지스터 구현



2030?

2) 양자현상

Heigenberg의 불확정성 원리

$$\Delta x \cdot \Delta p \geq \frac{\hbar}{2}$$

위치와 운동량의 불확정성 관계 존재

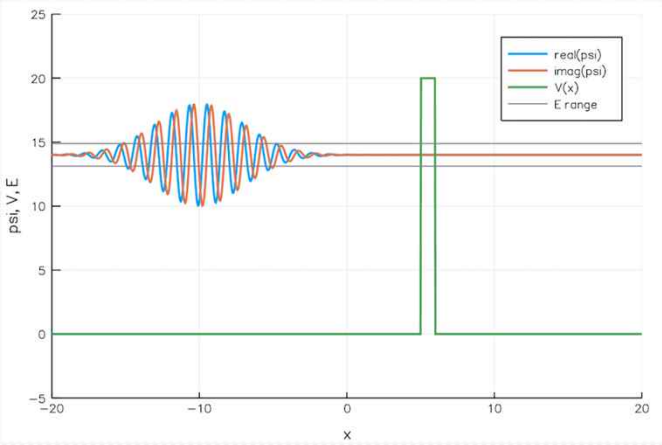
Schrödinger 방정식

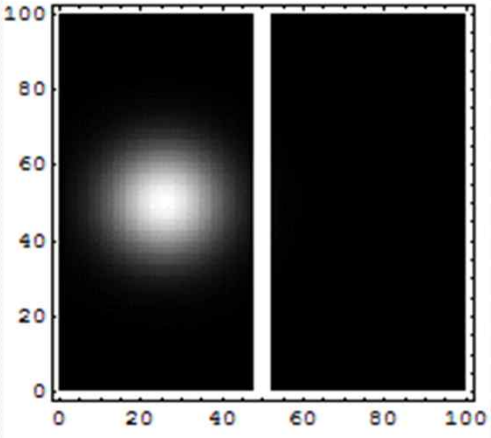
$$i\hbar \frac{\partial}{\partial t}\Psi = \hat{H}\Psi$$

입자의 불확정한 위치를 확률밀도를 나타내는 파동으로 표현하는 미분 방정식.

$$\hat{H} = -\frac{\hbar^2}{2m}\nabla^2 + V$$

입자의 위치를 나타내는 해 Ψ는 시간에 따라 변하는 파동함수, $|\Psi|^2$이 확률밀도함수.



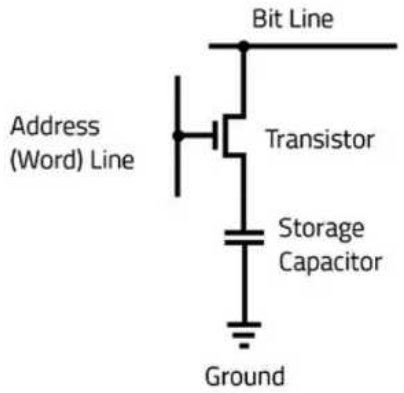


Planck 상수 $h = 6.626196 \times 10^{-27}\ J \cdot s$

Dirac 상수 $\hbar = \frac{h}{2\pi}$

3) Bit → Qubit

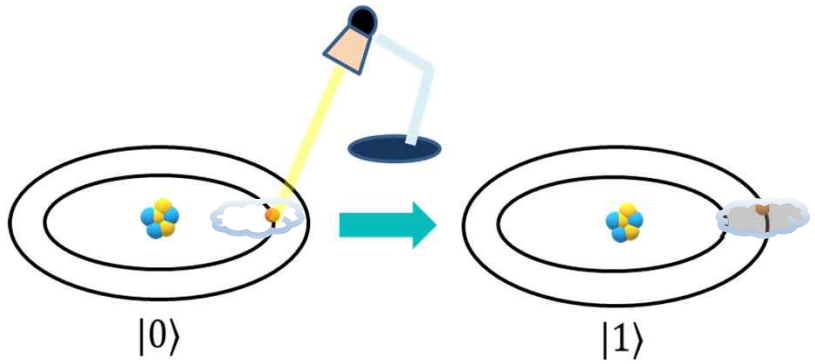
BIT



0 1

확정적 값을 가짐

QUBIT



불확정성에 의해

동 0 니고 1도

아닌 상태가 가능함

✔ Qubit의 구현예

✓ **초전도체 이용**

Google, IBM, Rigetti, QCI,…

✓ **이온 트랩 이용**

NIST, Oxford, Innsbruck, MIT, ETH,…

✓ **실리콘-기반 스핀 이용**

Intel, University of Cambridge, Harvard, …

✓ **토폴로지 이용**

Microsoft , …

6) 큐빗(Qubits)

- $1-$qubit → $\Psi = \alpha_0|0\rangle + \alpha_1|1\rangle, \quad \alpha_0, \alpha_1 \in \mathbb{C}$
- Ψ 가 $|0\rangle$일 확률 = $|\alpha_0|^2$, Ψ 가 $|1\rangle$일 확률 = $|\alpha_1|^2$

예) $\Psi = \frac{\sqrt{-1}}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$인 경우

Ψ가 $|0\rangle$일 확률=$\frac{1}{4}$, Ψ가 $|1\rangle$일 확률=$\frac{3}{4}$

이 개념을 여러 quibit으로 확장

- $n-$qubit → $\Psi = \alpha_0|0\cdots0\rangle + \alpha_1|01\rangle + \cdots + \alpha_{2^n-1}|1\cdots1\rangle$

⋮

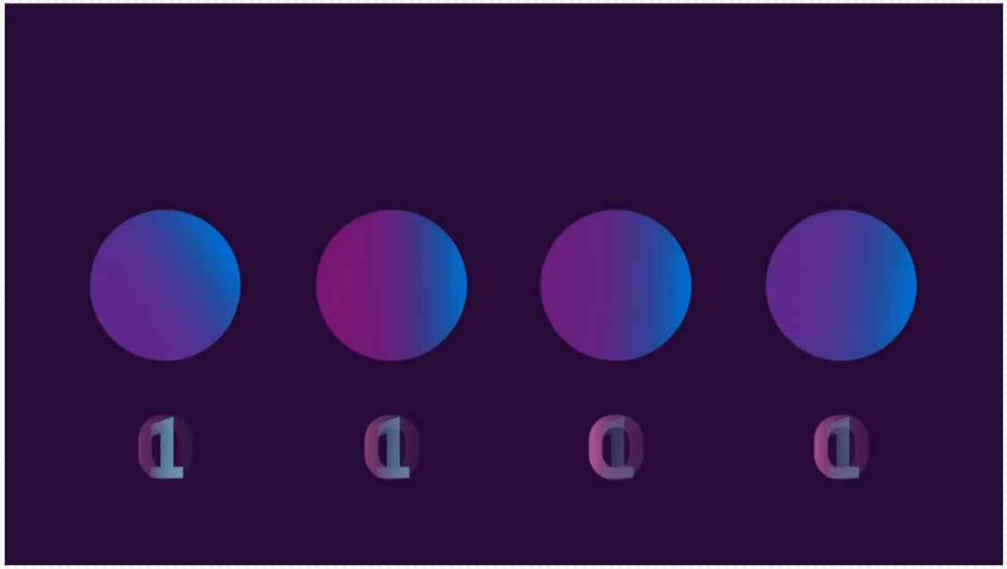
5) 양자 컴퓨팅에 사용되는 큐빗의 중요 성질 1

양자 중첩(Quantum Superposition)

✔ 레지스터에 값을 중첩시켜 저장

$$\Psi = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$$

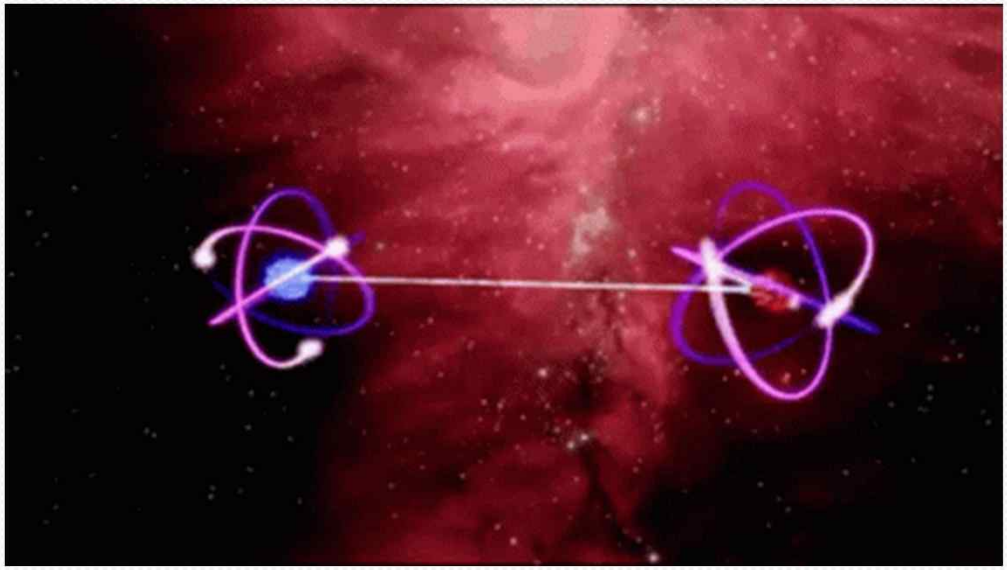


5) 양자 컴퓨팅에 사용되는 큐빗의 중요 성질 2

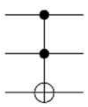
양자 얽힘(Quantum Entanglement)

✔ 두 **qubit**의 상태가 서로 독립적이지 않음

$$-\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$



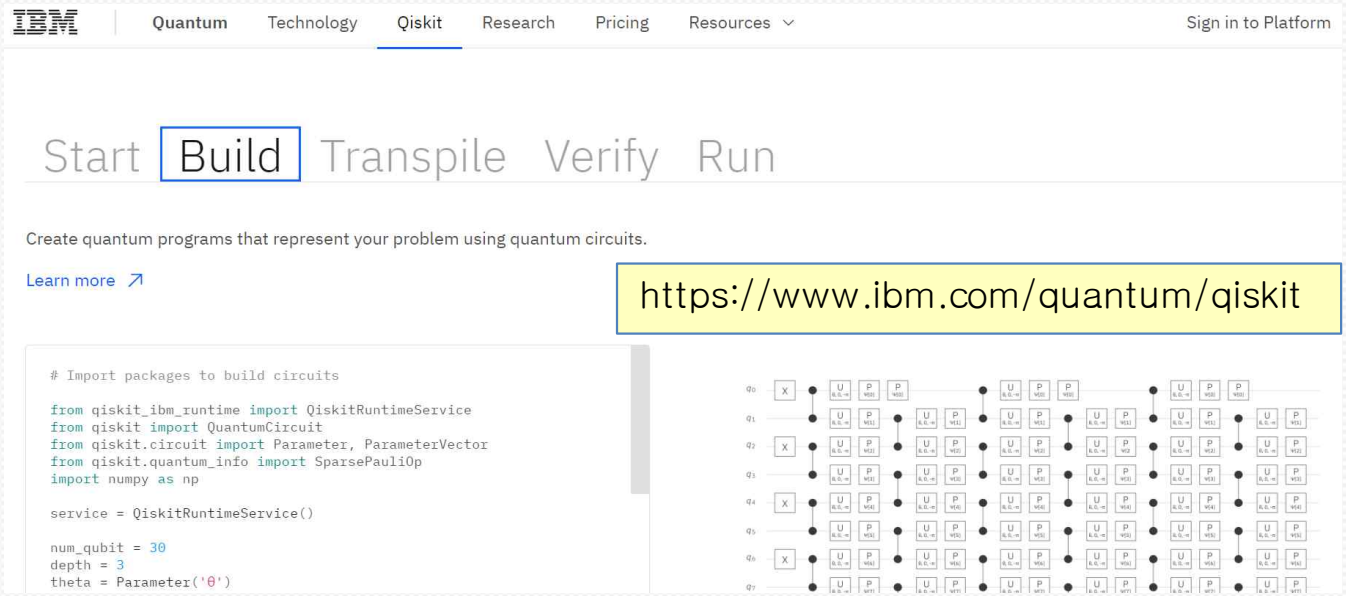
7) 양자 게이트(Quantum Gates)

Operator	Gate(s)	Matrix
Pauli-X (X)		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$

Quantum Computing Algorithms

8) 양자 알고리즘

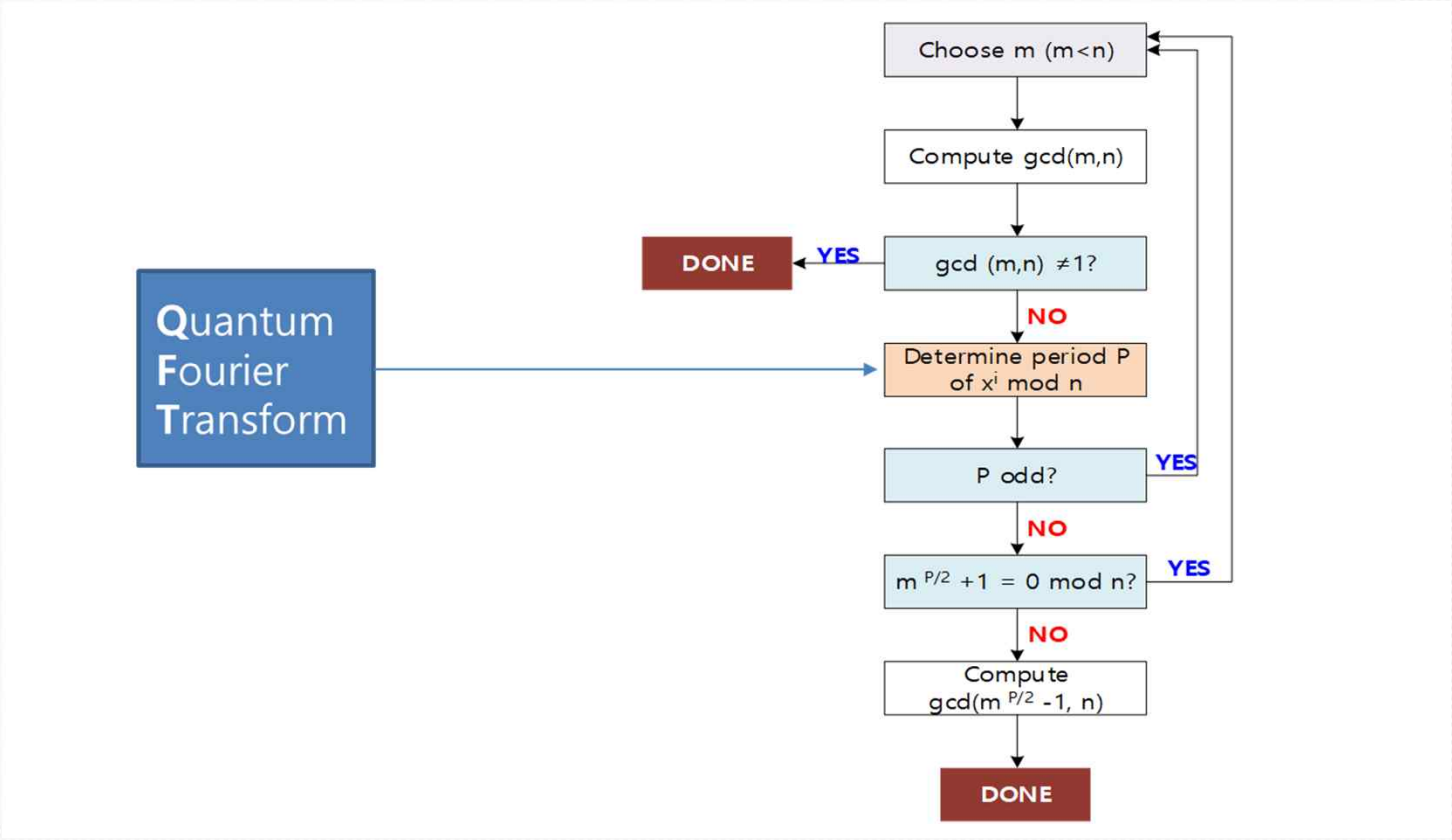
- ✔ 여러 개의 양자 게이트로 구성
- ✔ 고전적 컴퓨터로 수행할 수 없는 연산 수행 가능
- ✔ 양자 게이트를 이용하여 **qubit**들의 중첩과 얽힘 생성, 원하는 답이 나올 확률을 증폭시킨 후 측정



8) 양자 알고리즘

중요 양자 알고리즘 ①

쇼어 알고리즘 (Shor's Algorithm)



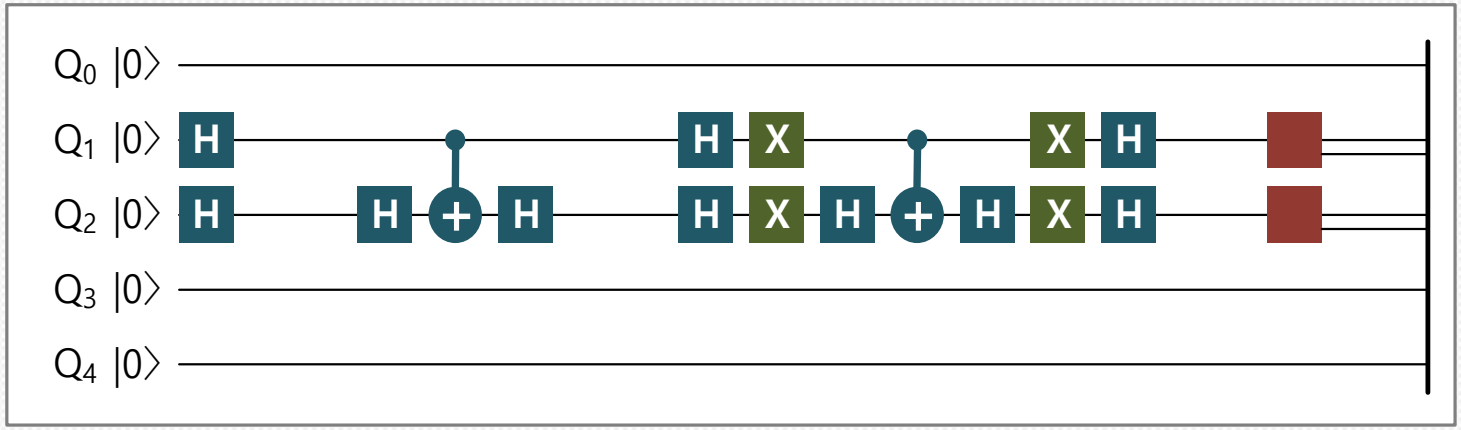
현재 사용되는 공개키 암호들을 효율적으로 해독(치명적)

8) 양자 알고리즘

중요 양자 알고리즘 ②

그로버 알고리즘 (Grover's Algorithm)

- 정렬되지 않은 **Database**를 검색하는 양자 알고리즘
- **Classical Computation** 으로는 $O(N)$ 의 검색 필요
- **Grover's Algorithm**을 이용하면 $O(N^{1/2})$ **Evaluation** 필요
- **Bennett, Bernstein, Brassard, Vazirani** 가 $O(N^{1/2})$ 보다 작은 **Quantum Solution** 은 없음을 증명



대칭키 암호의 키 전수조사에 사용(대응가능)

9) 양자 컴퓨터가 만들어지면...

› (미국 국립표준기술연구소) 보고서 NIST

Cryptographic Algorithm	Type	Purpose	Impact from large- scale quantum computer
AES-256	Symmetric Key	Encryption	Larger Key sizes needed
SHA-256, SHA-3		Hash functions	Larger output needed
RSA	Public Key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public Key	Signatures, key exchange	No longer secure
DSA (Finite Field Cryptography)	Public Key	Signatures, key exchange	No longer secure

HELP!

DEAD!

대칭키 알고리즘 → 키 길이 확대 필요

공개키 알고리즘 → 사용 불가능

3. 양자내성암호

Post- Quantum Cryptography

1) 양자내성 암호(PQC : Post-Quantum Cryptography)

양자 컴퓨터로도 풀기 어려운 계산 문제들을 이용하는 암호 알고리즘

- 양자 컴퓨터 개발이 가시화됨에 따라 **NSA**는 **2015**년 **8**월에 **Suite B**의 암호 알고리즘을 전부 **Post- Quantum Cryptography(PQC)** 로 개정하겠다고 공지함
- **NIST**는 **2016**년 **4**월 **'Reports on Post-Quantum Cryptography' NISTIR 8105** 를 통해 다음을 발표

공개키 암호는 양자 컴퓨터가 개발되면 더 이상 안전하지 않기 때문에, 이를 대비한 Post-Quantum Cryptography의 표준을 마련하기 위한 공모를 발표함

arstechnica.com/security

NSA preps quantum-resistant algorithms to head off crypto-apocalypse

Quantum computing threatens crypto as we know it. The NSA is taking notice.

by **Dan Goodin** - Aug 21, 2015 8:02pm JST

Share Tweet Email 90

IAD will initiate a transition to quantum resistant algorithms in the not too distant future. Based on experience in deploying Suite B, we have determined to start planning and communicating early about the upcoming transition to quantum resistant algorithms. Our ultimate goal is to provide cost effective security against a potential quantum computer. We are working with partners across the USG, vendors, and standards bodies to ensure there is a clear plan for getting a new suite of algorithms that are developed in an open and transparent manner that will form the foundation of our next Suite of cryptographic algorithms.

1) 양자내성 암호(PQC : Post-Quantum Cryptography)

NIST의 PQC 표준화 프로세스 진행 상황

Round 1

- 2017.11.30까지 82개의 알고리즘들 접수,
  2017.12.20.까지 69개의 Round 1 후보 선정
- 20 digital signature schemes, 49 Public Key Encryptions (PKE)
  & Key Encapsulation Mechanisms (KEM).

Round 2

- Round 1을 통과한 26개의 후보 알고리즘들 선정,
  2019년 1월 30일부터 Round 2 시작
- 9 Digital Signature Schemes, 17 PKEs & KEMs

1) 양자내성 암호(PQC : Post-Quantum Cryptography)

NIST의 PQC 표준화 프로세스 진행 상황

Round 3

- Round 2를 통과한 7개의 후보 알고리즘들 선정
  2020년 8월 1일부터 시작
- 3 Digital Signature Schemes, 4 PKEs & KEMs

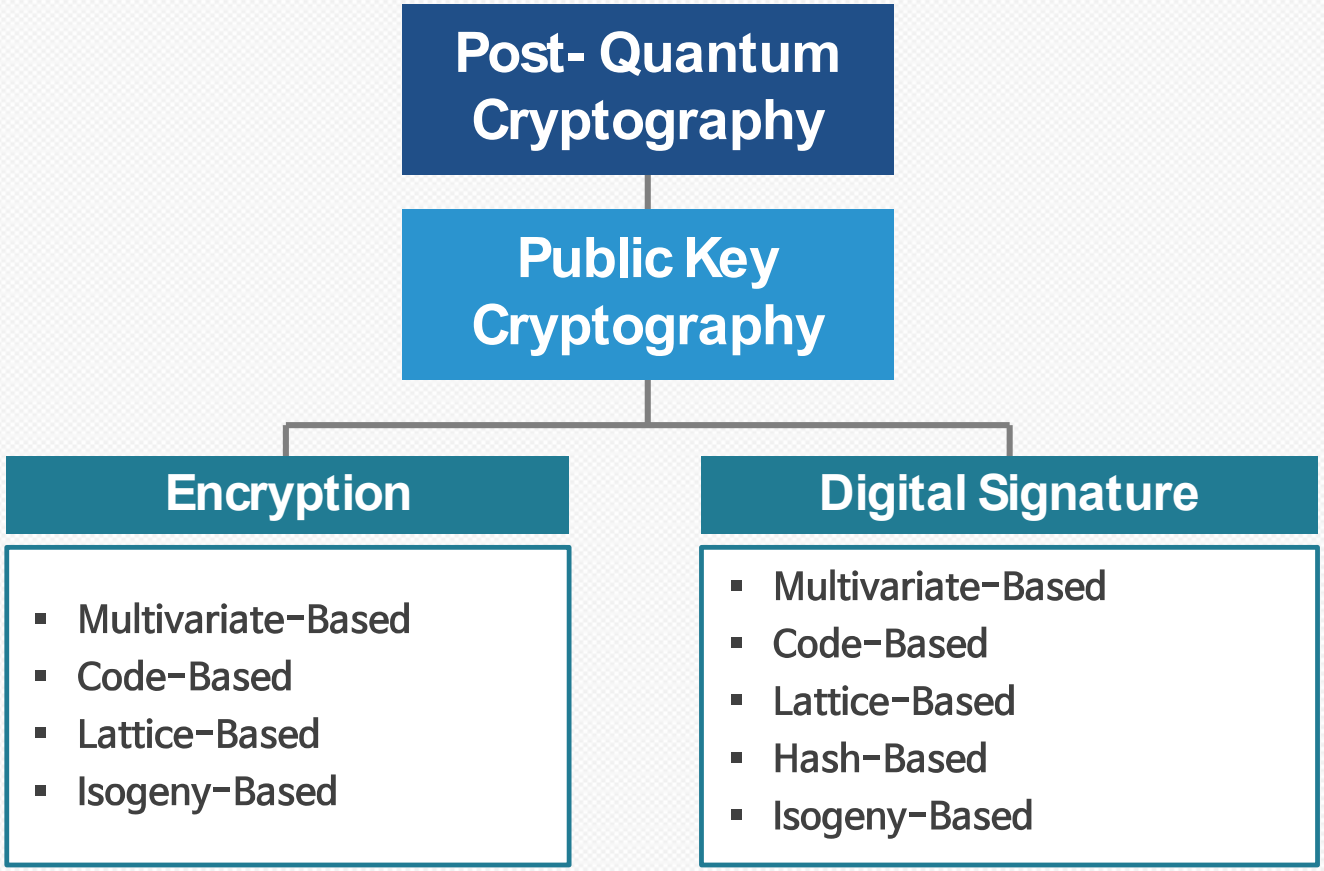
Round 4

- Round 3에 대해 추가적인 후보 알고리즘들 선정,
  2022년 7월 5일부터 시작.
- 4 PKEs & KEMs

Additional Signatures Round 1

- 추가적인 전자서명 후보 알고리즘들 선정, 2023년 7월경 시작.
- 40 Digital Signature Schemes

3) 대표적 양자내성암호들



3) 대표적 양자내성암호들

PQC 대표 알고리즘 ① : 다항식- 기반 암호 (Multivariate- Based Cryptography)

공개키가 다변수 함수의 집합으로 이루어진 암호 시스템

$$G(x_1, x_2, \dots, x_n) = (G_1(x_1, x_2, \dots, x_n), G_2(x_1, x_2, \dots, x_n), \dots, G_m(x_1, x_2, \dots, x_n)$$

Example

$$G_1(x_1, x_2) = 1 + x_1 + 2x_1x_2$$

$$G_2(x_1, x_2) = 1 + 3x_1 + x_2^2$$

$$G_3(x_1, x_2) = x_1x_2 + 3x_1 + x_1^2$$

Decryption

$$1 + x_1 + 2x_1x_2 = 6$$

$$1 + 3x_1 + x_2^2 = 8$$

$$x_1x_2 + 3x_1 + x_2^2 = 9$$

➡ $x_1,\ x_2$?

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ① : 다항식- 기반 암호
(Multivariate- Based Cryptography)

Security Base

Multivariate Quadratic Problem

유한체에서 다변수 이차 방정식을 푸는 것은 계산이 어렵다.

Isomorphism of Polynomial Problem

$P=T\circ Q\circ S$ 를 만족하는 **affine** 변환 S, T 를 찾는 것은 계산이 어렵다.

개인키 = 풀기 쉬운 다항식

$$1 + x_1 + 2x_1x_2 = 6$$
$$1 + 3x_1 + x_2^2 = 8$$
$$x_1x_2 + 3x_1 + x_2^2 = 9$$

$$x_1 = 2y_1 - y_2$$
$$x_2 = y_1 + y_2$$

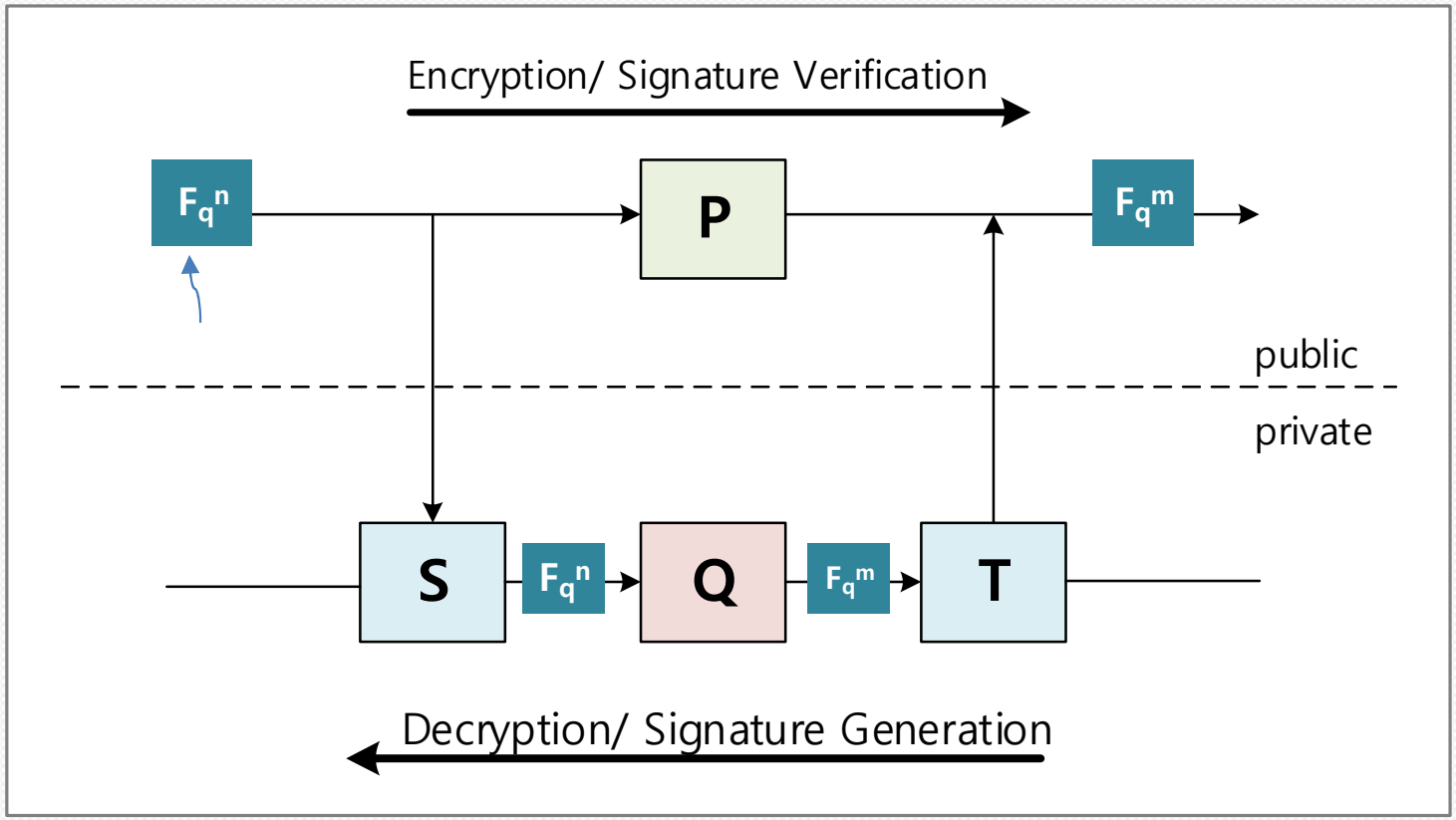
공개키 = 풀기 어려운 다항식

$$4y_1^2 - 2y_2^2 + 2y_1y_2 + 2y_1 - y_2 + 1 = 6$$
$$2y_1^2 + 2y_1y_2 + 6y_1 - 3y_2 + 1 = 8$$
$$3y_1^2 + 3y_1y_2 + 6y_1 - 3y_2 = 9$$

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ① : 다항식- 기반 암호 (Multivariate- Based Cryptography)

Basic Structure



데이터를 유한체($\mathbb{F}_{q^k}$) 원소로 인코딩하여 계산

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ① : 다항식- 기반 암호 (Multivariate- Based Cryptography)

장· 단점

장점	단점
▪ 다항 방정식을 푸는 방법의 불규칙성 때문에 부채널 공격에 대한 기본적 저항성 있음 ▪ 서명의 크기가 매우 작음	▪ 보안을 위해 크고 복잡한 중앙함수가 필요하므로 키 사이즈가 큼

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ② : 코드- 기반 암호 (Code- Based Cryptography)

Coding Theory

Goal	**Noisy Channel** 로 부터 코드 보호 
Encoder	메시지 **+ Redundancy**
Decoder	**Decoding Algorithm** 으로 오류가 발생했을 경우 고쳐서 올바른 **Code Word**로 바꿈

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ② : 코드- 기반 암호 (Code- Based Cryptography)

Security Base

- Random Linear Code 를 Decode 하는 것은 NP- hard

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ② : 코드- 기반 암호 (Code- Based Cryptography)

Idea

- 기존에는 **Noisy Channel**의 **Error** 를 감지하는데 **Coding** 을 이용
- **Code- Based Cryptography**는 임의로 **Error**를 메시지에 넣어 올바른 키를 아는 사용자만이 **Error**를 감지하고 **Decoding** 가능하게 함

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ②: 코드- 기반 암호
(Code- Based Cryptography)

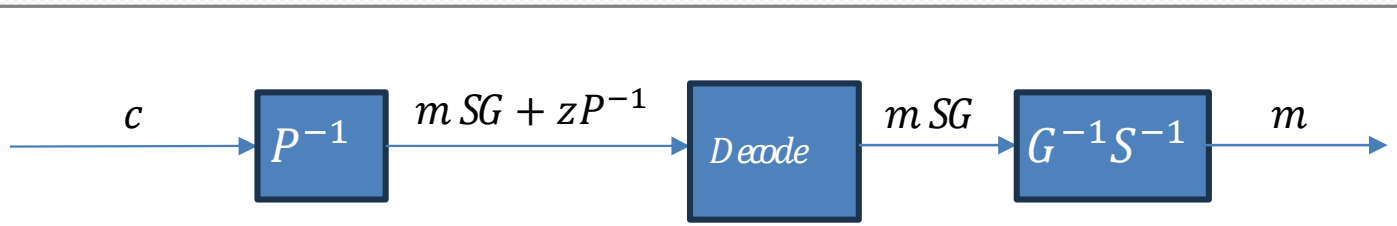
$G^{pub} = SGP$

G^{pub} : Public Key

S, G, P : Private Key

Encryption

Decryption



3) 대표적 양자내성암호들

PQC 대표 알고리즘 ② : 코드- 기반 암호 (Code- Based Cryptography)

장· 단점

장점	단점
▪ 암복호화 연산이 유한체 상에서 행렬 연산으로서 비교적 빠름 ▪ McEliece와 같은 알고리즘은 오랜 역사를 가지고 있어 보수적인 안전성을 가짐	▪ 기본적인 디코딩 행렬이 크기 때문에 키 사이즈가 매우 큼

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Lattice

✔ **Basis :** 공간의 점집합을 생성하는 독립된 방향을 가진 벡터들

예) $(\mathbf{1},\mathbf{0}),(\mathbf{0},\mathbf{1}) \in \mathbb{R}^2$의 선형 결합 $\boldsymbol{x}(\mathbf{1},\mathbf{0}) + \boldsymbol{y}(\mathbf{0},\mathbf{1})$,

$(\boldsymbol{x},\boldsymbol{y} \in \mathbb{R})$ 로 실 $\mathbb{R}^2$의 모든 점들을 생성할 수 있다.

✔ **Basis**의 정수 선형 결합으로 만들어지는 점집합을

격자**(lattice)** 라고 한다.

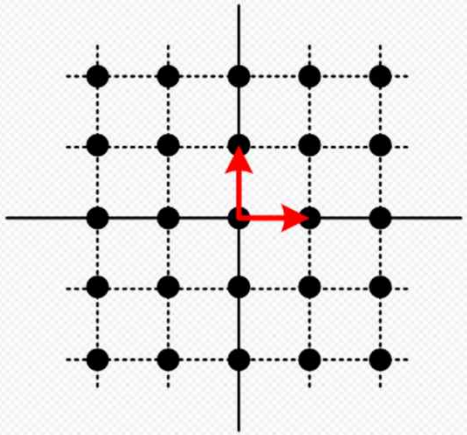
예) $\boldsymbol{x}(\mathbf{1},\mathbf{0}) + \boldsymbol{y}(\mathbf{0},\mathbf{1}),\ (\boldsymbol{x},\boldsymbol{y} \in \mathbb{Z})$

3) 대표적 양자내성암호들

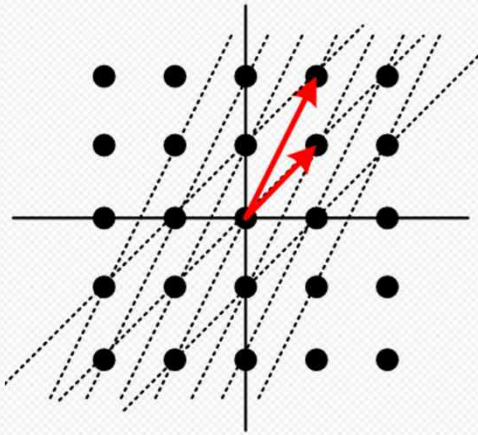
› PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Lattice

✔ 다른 **basis** 도 동일한 **lattice** 생성 가능



$e_1 = (1,0), e_2 = (0,1)$



$b_1 = (1,1), b_2 = (1,2)$

3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Security Base

Worst- case hardness of solving lattice-based problems

- Shortest Vector Problem (SVP)
- Closest Vector Problem (CVP)
- Learning with Errors (LWE)
- Short Integer Solution (SIS)

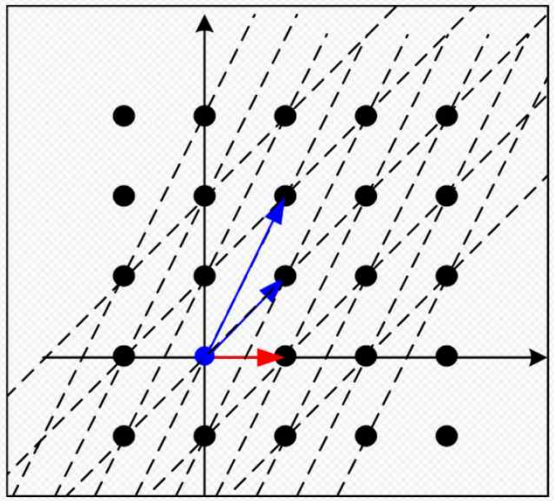
3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Lattice- based problems

Shortest Vector Problem (SVP)

Lattice base B 가 주어졌을 때,
Lattice L(B) 에서 가장 작은 **0** 이 아닌 벡터를 찾는 문제



$b_1 = (1,1), b_2 = (1,2)$

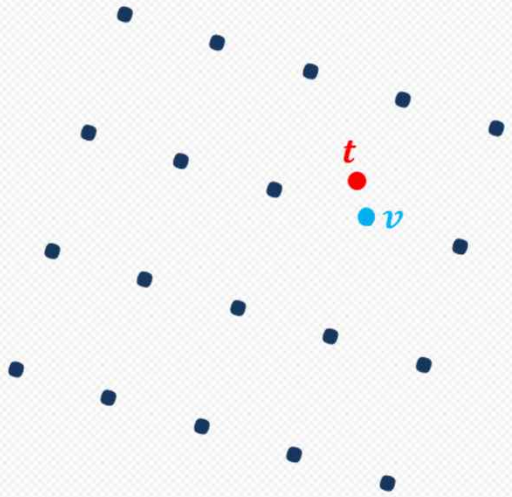
3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Lattice- based problems

Closest Vector Problem (CVP)

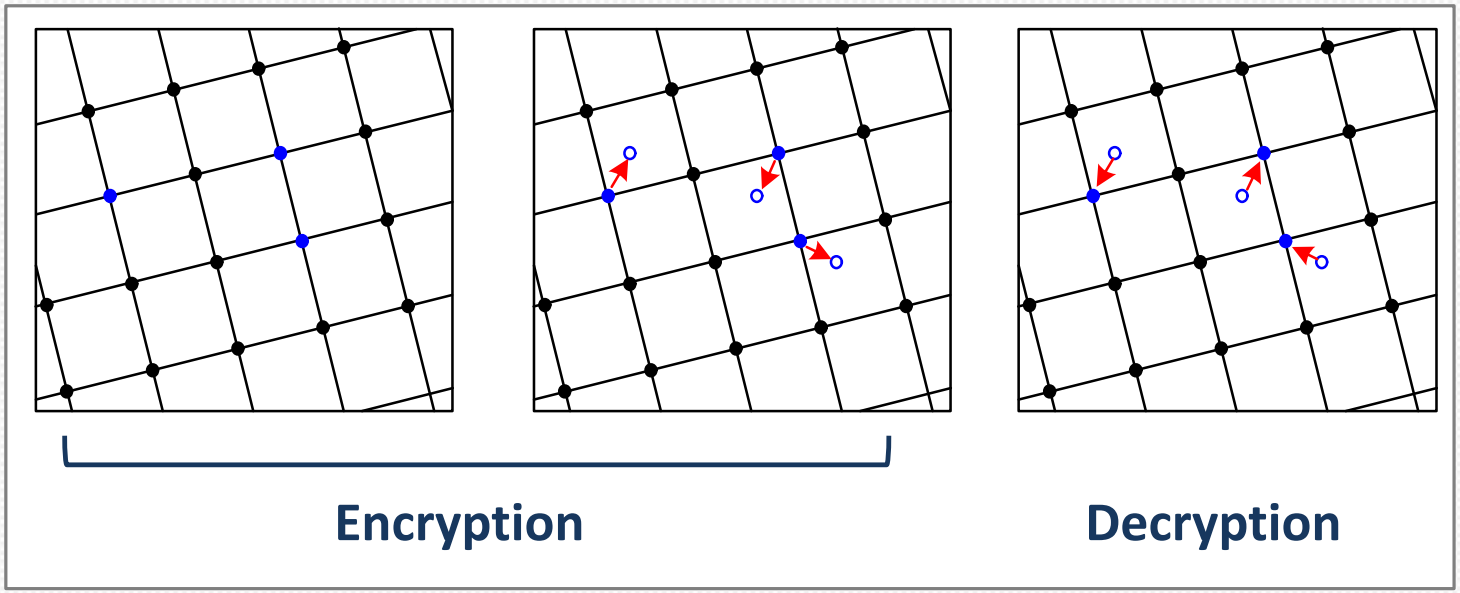
Lattice base B 와 target vector t가 주어졌을 때, Lattice Point v $\in \mathcal{L}(B)$ 중 t와 제일 가까운 점 찾기



3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

Basic Concept



3) 대표적 양자내성암호들

PQC 대표 알고리즘 ③ : 격자- 기반 암호 (Lattice- Based Cryptography)

장· 단점

장점	단점
▪ Worst-case 기반 Strong Security Proof ▪ 비교적 쉬운 Implementation	▪ 널리 적용되는 MLWE, MLWR 문제 등이 원래의 LWE, LWR 문제에 비해 얼마나 안전한지 알려지지 않음

4) NIST PQC 공모 요구사항

1 보안성

- 전부터 널리 사용되어 온 Transport Layer Security(TLS), Secure Shell(SSH)와 같은 다양한 응용에서 사용될 수 있는 보안성을 가져야 함

2 구현 비용과 효율성

- 공개키, 암호문, 서명의 크기 그리고 주요 연산인 키 생성, 공개키 연산, 개인키 연산의 성능, 복호화 실패율을 고려

4) NIST PQC 공모 요구사항

3 알고리즘과 구현 특성

- 암호 알고리즘이 다양한 플랫폼에서 사용 가능하여야 하며, 병렬 연산이 가능하고, 분석이 용이한 단순한 구조를 가질 것
- 부채널 공격 저항성 원활한 보급을 위한 특허 방지 관련 사항들 포함

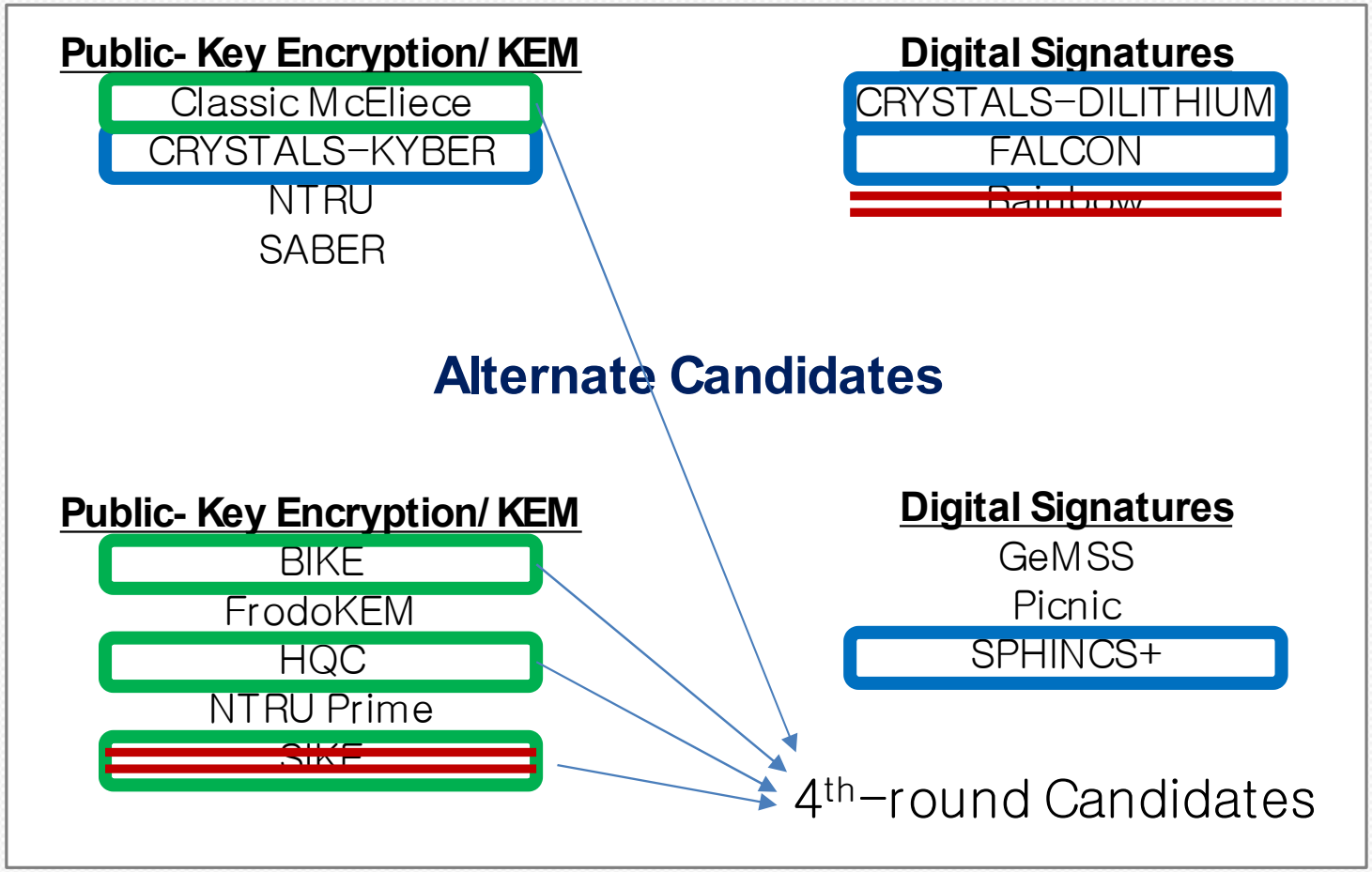
5) NIST PQC 공모 보안 강도 범주

› 보안 강도 범주를 정의 **5**가지

1	키 전수조사에 있어 128-bit 비도를 가지는 범주(eg. AES128)
2	충돌공격에 대해 256-bit 비도를 가지는 범주 (eg. SHA256/SHA3-256)
3	키 전수조사에 있어 192-bit 비도를 가지는 범주(eg. AES192)
4	충돌공격에 대해 384-bit 비도를 가지는 범주 (eg. SHA384/SHA3-384)
5	키 전수조사에 있어 256-bit 비도를 가지는 범주(eg. AES256)

6) NIST PQC 3rd-round Candidates

Third- Round Finalists



7) NIST PQC 선정 주요 알고리즘 키 사이즈 비교

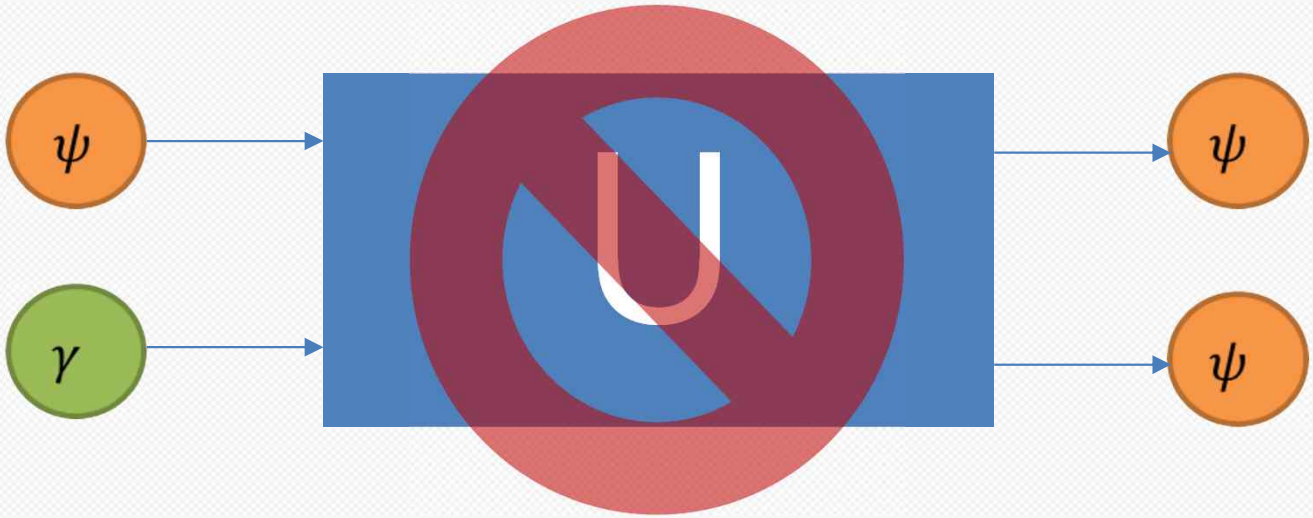
Security Level	Algorithm	Public key size (in bytes)	Private key size (in bytes)	Ciphertext/ Signature size (in bytes)
1	Kyber512	800	1632	768
2	Dilithium2	1312	2528	2420
3	Kyber768	1184	2400	1088
5	Falcon1024	1793	2305	1330
5	Kyber1024	1568	3168	1588

4. 기타 양자보안설비

Other Quantum Communication Equipments

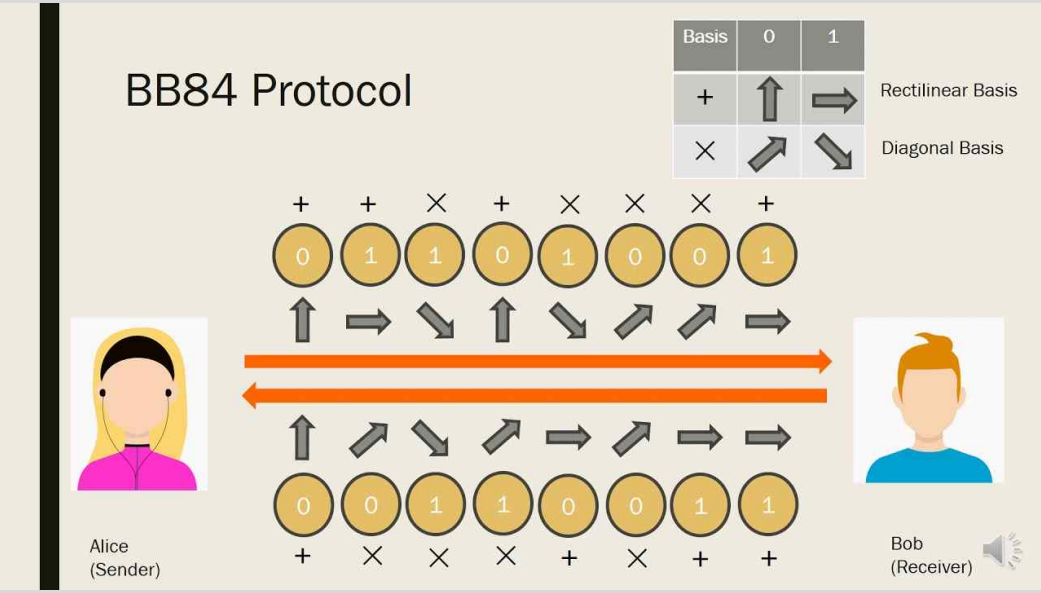
11) 복제 불가능 정리(No Cloning Theorem)

양자 비트의 정보를 복제할 수 있는
유니터리 변환 (양자 게이트) 은 존재하지 않음



< 양자 암호통신의 기초가 되는 원리 >

12) 양자 암호 (통신 프로토콜)



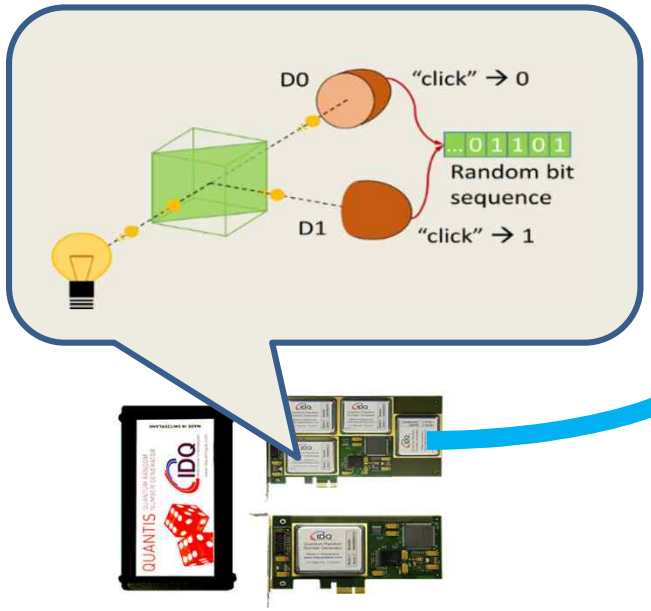
- **BB84**
  - **Charles Bennett** 와 **Gilles Brassard**가 **1984**년에 제안
- 광자(빛) 를 두 방향으로 편광시켜 **0**과 **1**을 표현
- 별도의 양자 통신 장비 상에서 구현
- 복제불가능 정리(**No- cloning theorem)** 에 의해 도청 즉시 정보가 훼손되어 감지됨

물리적 현상을 이용하며 Shor 알고리즘이나 Grover 알고리즘의 공격 대상이 되지 않음. 따라서 양자공격에 안전한 통신 방법으로 여겨진다.

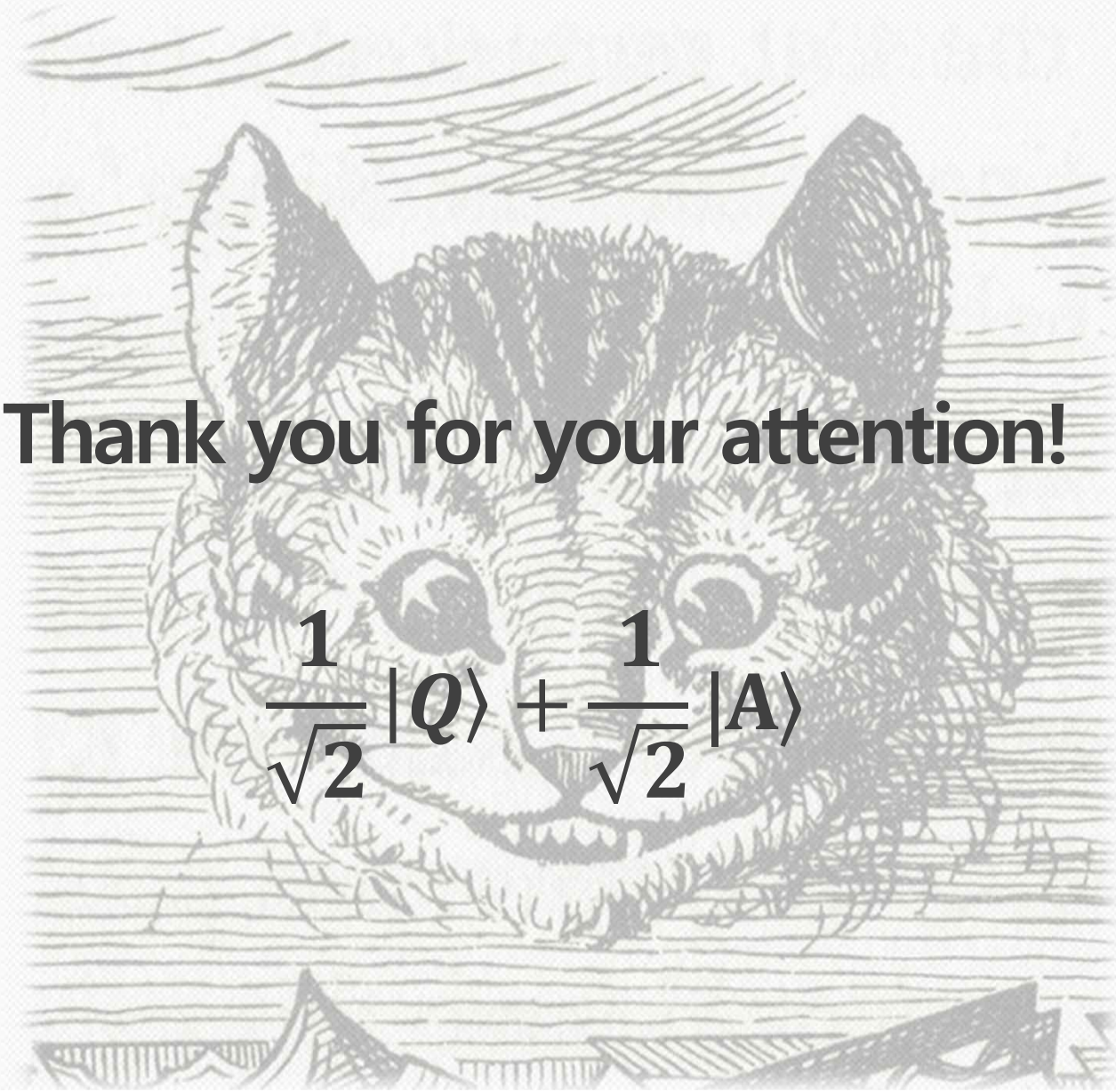
양자 난수 생성기

(Quantum Random Number Generator)

기기에서 안전한 암호 키 생성을 위해
수백 비트 이상의 변화하는 상태가 필요



양자 상태의 불안정성을 이용하여 난수열 생성
시스템 상태가 단순한 IoT 장비 등에서 유용함



Thank you for your attention!

$$\frac{1}{\sqrt{2}}|Q\rangle + \frac{1}{\sqrt{2}}|A\rangle$$