NORMA

양자 시대 보안 요구 사항과 PQC 도입사례

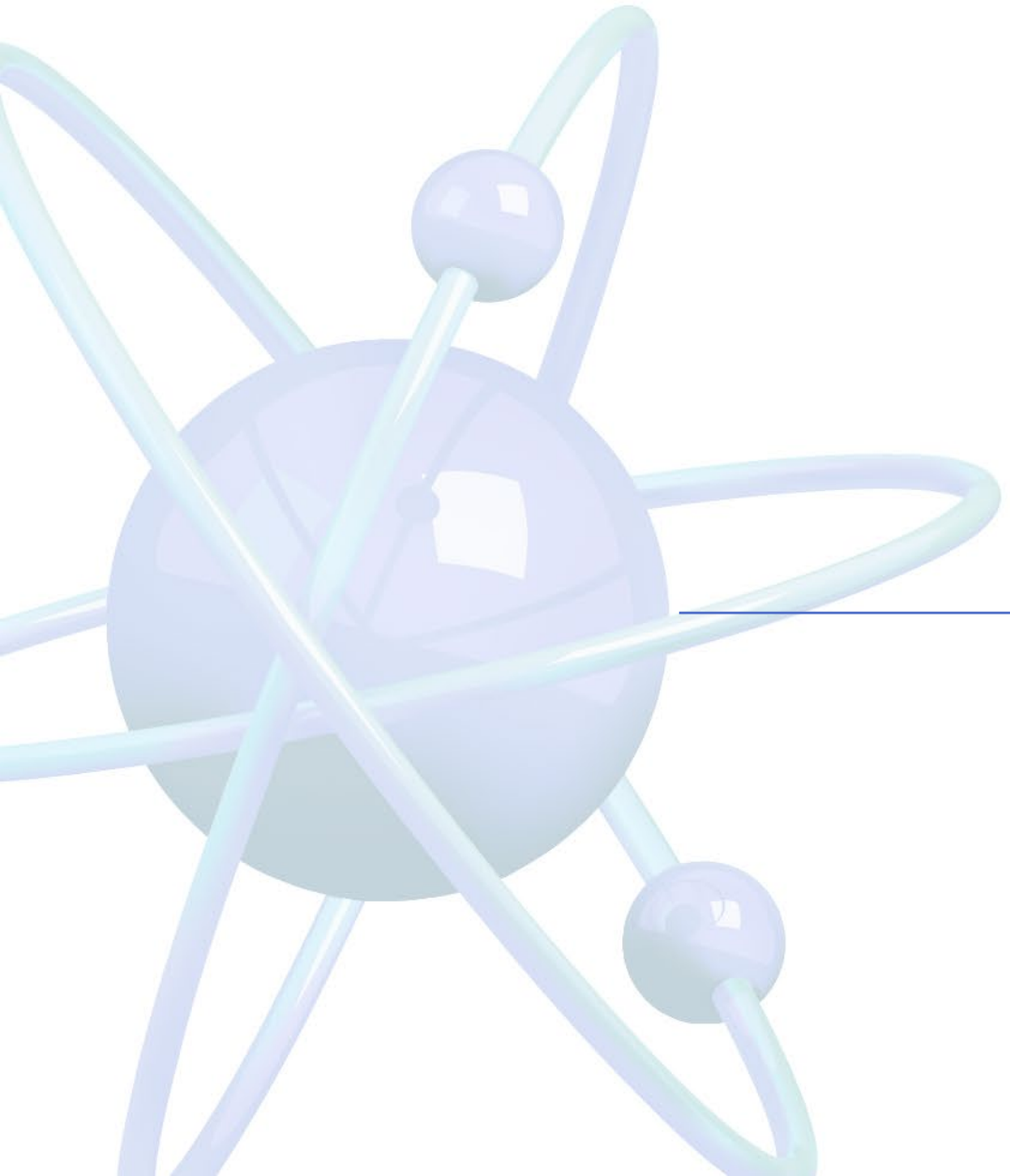
노르마 정현철 대표

안전한 양자컴퓨터 시대를 위한 보안 준비 사항

2023. 03. 02

NORMA

Contents



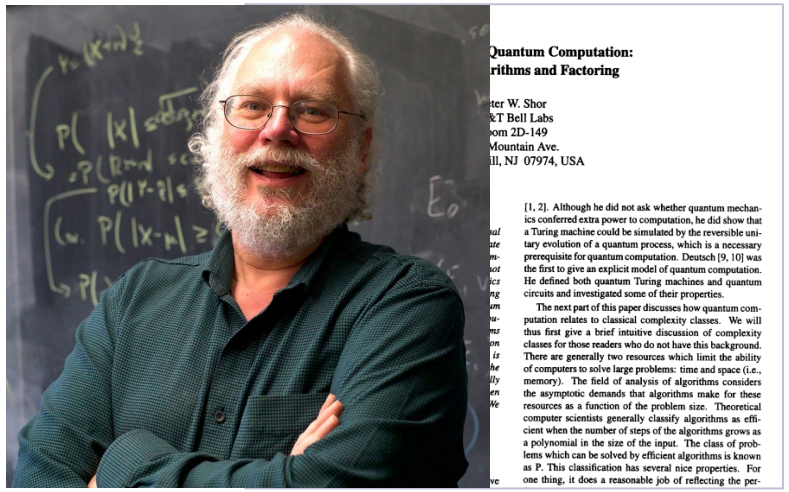
양자 컴퓨터의 위협

양자 알고리즘

인수 분해

공개키 암호에 미치는 영향

쇼어 알고리즘



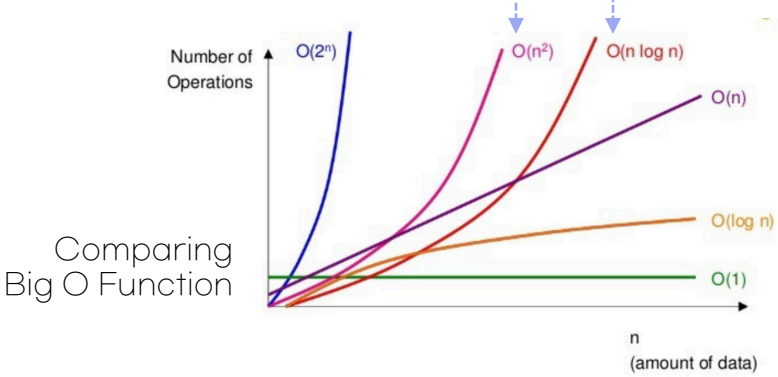
Quantum Computation:
rithms and Factoring

ter W. Shor
&T Bell Labs
oom 2D-149
Mountain Ave.
ill, NJ 07974, USA

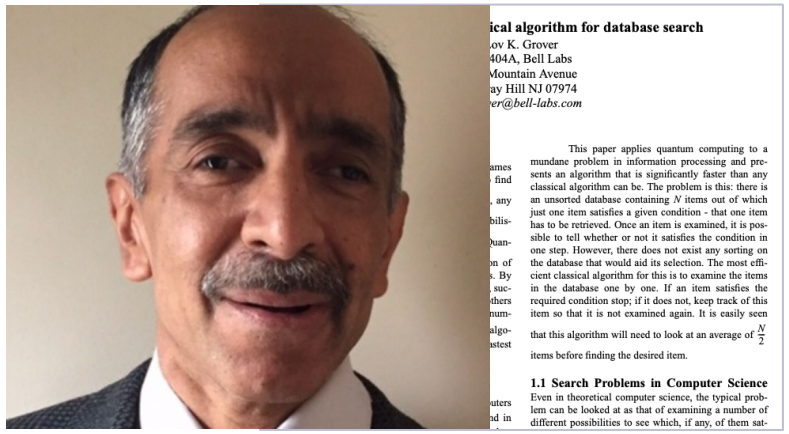
[1, 2]. Although he did not ask whether quantum mechanics conferred extra power to computation, he did show that a Turing machine could be simulated by the reversible unitary evolution of a quantum process, which is a necessary prerequisite for quantum computation. Deutsch [9, 10] was the first to give 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 per-

- 1994년, 미국 수학자 **피터 쇼어**(Peter Shor) 개발
- 다항식 시간 안에 정수의 소인수를 찾는 양자 알고리즘
  - 고전 인수 분해 알고리즘은 숫자가 커질수록 연산량이 지수 함수를 따라서 증가 (= 어려움)
  - 쇼어 알고리즘을 이용하면 다항 함수를 따라서 증가 (= 쉬움)
- 2048-bit 소인수 분해에 약 8시간 소요
  (2019년, 구글 양자 컴퓨터 연구팀)



그로버 알고리즘



ical algorithm for database search
ov K. Grover
404A, Bell Labs
Mountain Avenue
ay Hill NJ 07974
er@bell-labs.com

This paper applies quantum computing to a mundane problem in information processing and presents an algorithm that is significantly faster than any classical algorithm can be. The problem is this: there is an unsorted database containing N items out of which just one item satisfies a given condition - that one item has to be retrieved. Once an item is examined, it is possible to tell whether or not it satisfies the condition in one step. However, there does not exist any sorting on the database that would aid its selection. The most efficient classical algorithm for this is to examine the items in the database one by one. If an item satisfies the required condition stop; if it does not, keep track of this item so that it is not examined again. It is easily seen that this algorithm will need to look at an average of $\frac{N}{2}$ items before finding the desired item.

1.1 Search Problems in Computer Science

Even in theoretical computer science, the typical problem can be looked at as that of examining a number of different possibilities to see which, if any, of them sat-

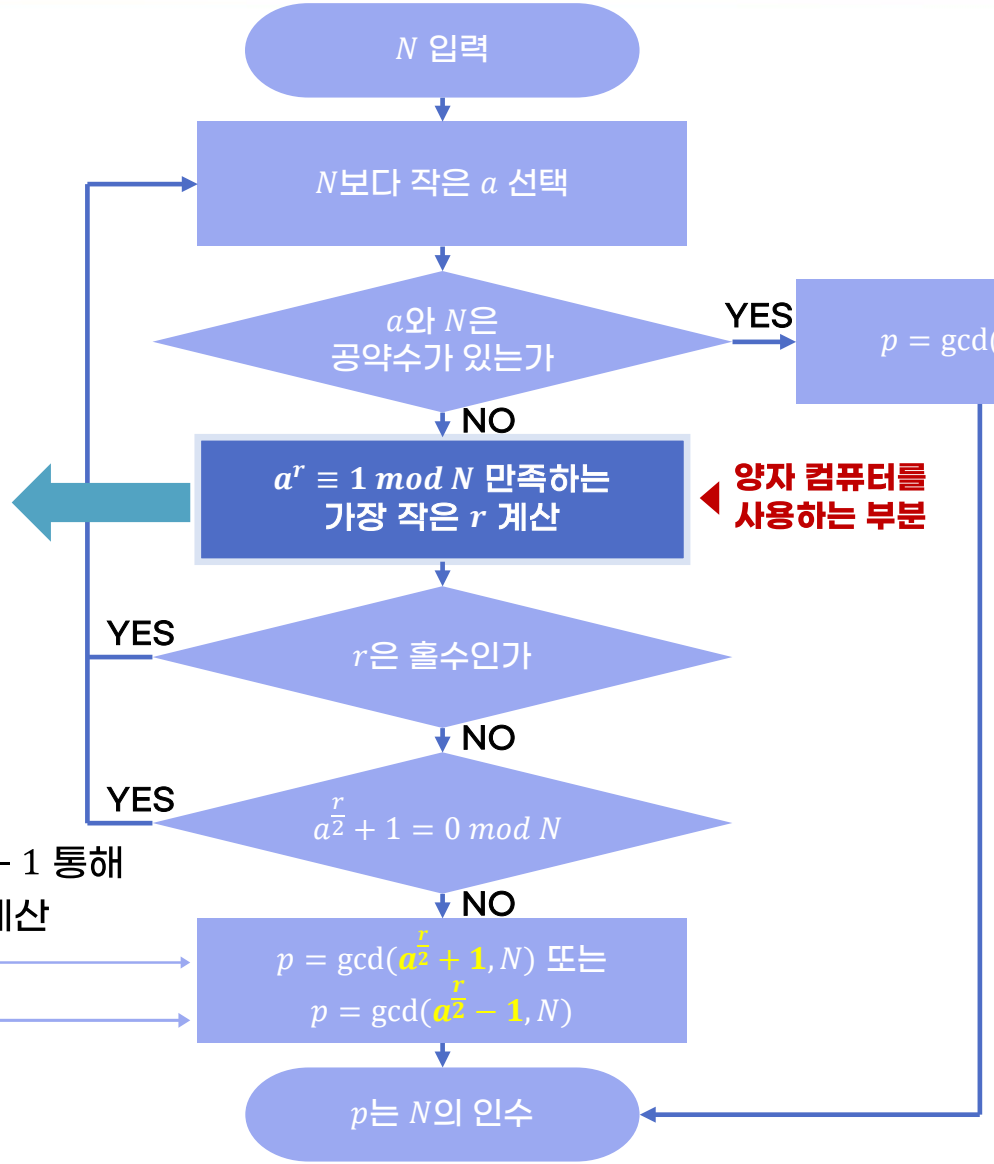
- 1996년, 인도 수학자 **로브 그로버**(Lov Grover) 개발
- 정리되지 않은 데이터를 빠르게 검색하는 양자 알고리즘
- N 개의 데이터 탐색
  - 고전적인 방법으로는 보통 $N/2$ 번, 최악의 경우 N 번 확인해야 함
  - 그로버 알고리즘을 이용하면 $\sqrt{N}$ 번만 확인하면 됨

주기 r 찾기 문제

$a^r \equiv 1 \; mod \; N$

$\Leftrightarrow a^r - 1 = k \cdot N$

$\Leftrightarrow \left(a^{\frac{r}{2}} + 1\right) \cdot \left(a^{\frac{r}{2}} - 1\right) = k \cdot N$



RSA

- PKI 및 인증서 등에서 사용
- 큰 숫자의 소인수 분해가 어려움에 기반
- 빠른 인수 분해가 가능하다면,
  RSA 암호는 깨질 수 있음

ECC

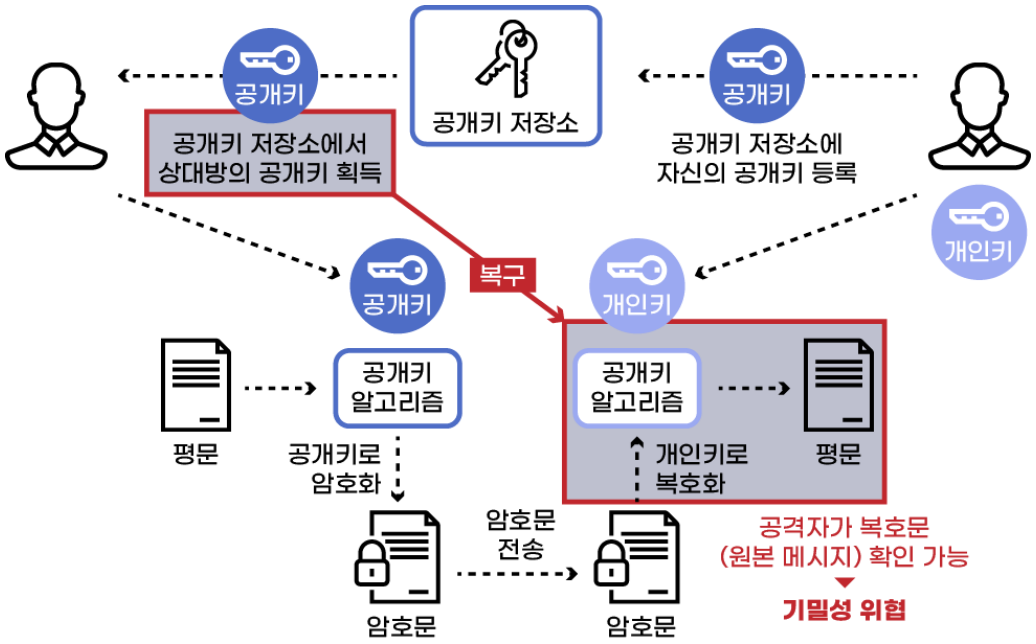
- 블록체인 등에서 사용 (ECDSA)
- 타원곡선 이론에 기반
- 지수 연산 $a^r \equiv x$ 대신
  로그 연산 $r \equiv \log_a x$ 으로 변형하여
  쇼어 알고리즘 적용 가능

공개키 암호란? 암호화와 복호화에 다른 키를 사용하는 암호 방식 (예: RSA, ECC)

- 공개키 암호화 : 공개키로 암호화, 개인키로 복호화
- 디지털 서명 : 개인키로 암호화(= 서명), 공개키로 복호화(= 검증)

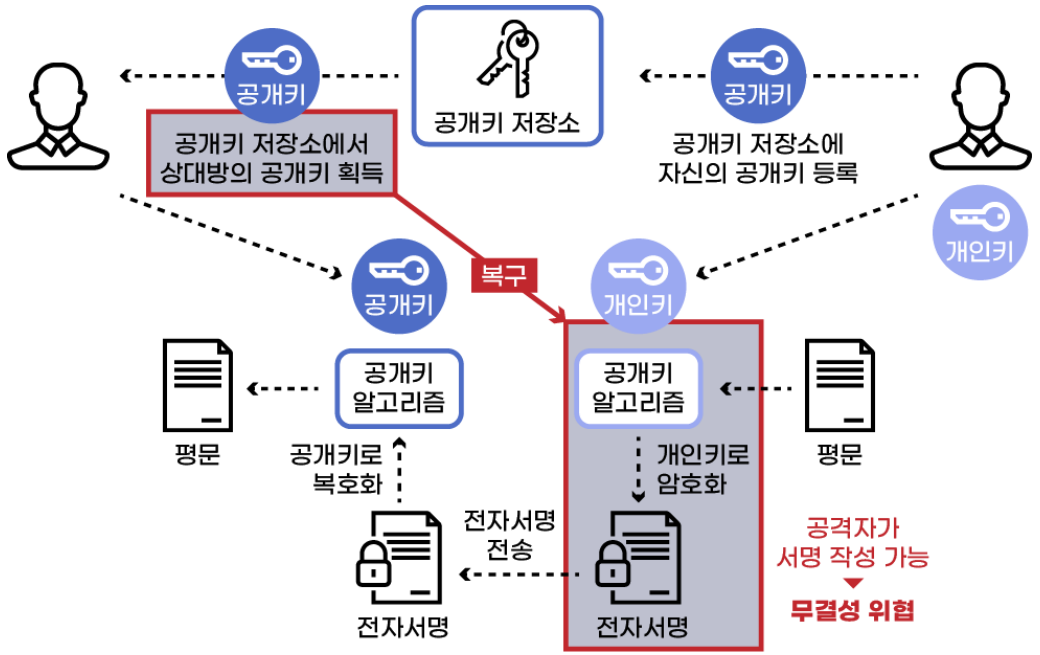
공개키 암호화

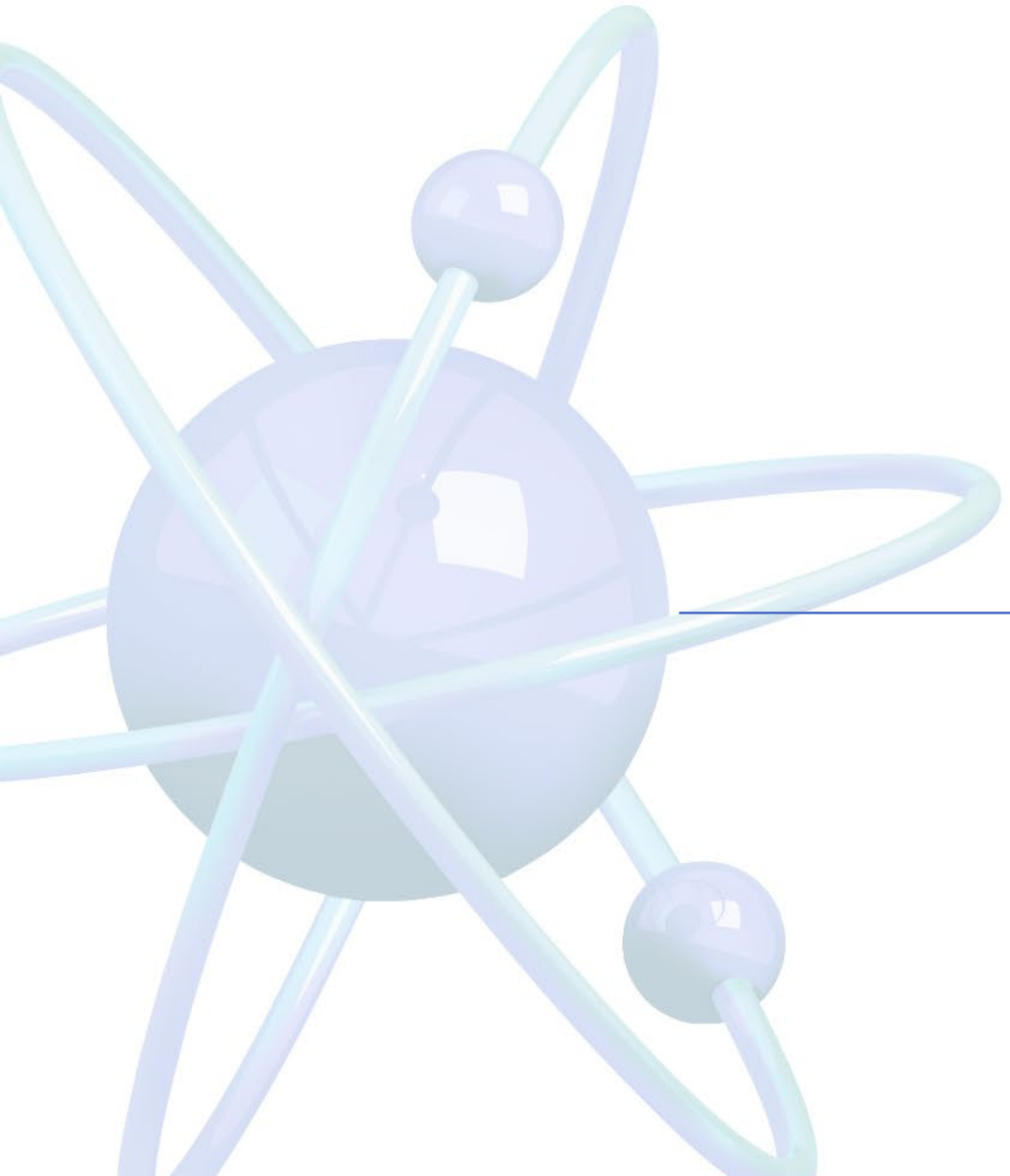
개인키를 가지고 있는 사용자만 내용을 확인할 수 있음



디지털 서명

개인키로 만들어진 서명을 누구나 확인할 수 있음



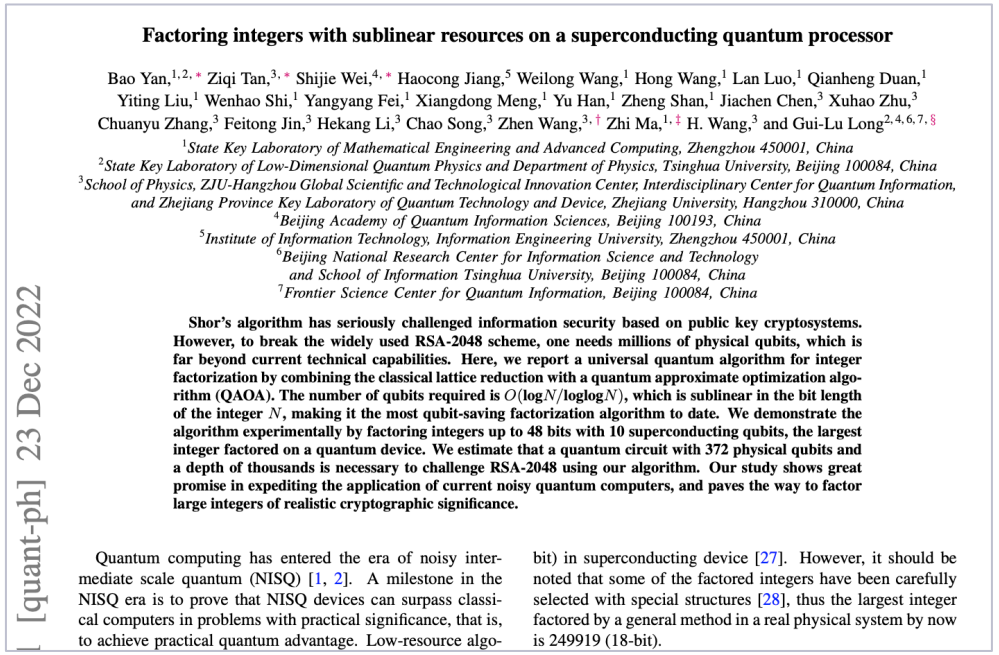


공개키 암호의 유효기한

공개키 암호 공격 사례 - 중국

공개키 암호 공격 사례 - 노르마

NIST의 경고



[quant-ph] 23 Dec 2022

Factoring integers with sublinear resources on a superconducting quantum processor

Bao Yan,[1,2,*] Ziqi Tan,[3,*] Shijie Wei,[4,*] Haocong Jiang,[5] Weilong Wang,[1] Hong Wang,[1] Lan Luo,[1] Qianheng Duan,[1] Yiting Liu,[1] Wenhao Shi,[1] Yangyang Fei,[1] Xiangdong Meng,[1] Yu Han,[1] Zheng Shan,[1] Jiachen Chen,[3] Xuhao Zhu,[3] Chuanyu Zhang,[3] Feitong Jin,[3] Hekang Li,[3] Chao Song,[3] Zhen Wang,[3,†] Zhi Ma,[1,‡] H. Wang,[3] and Gui-Lu Long[2,4,6,7,§]

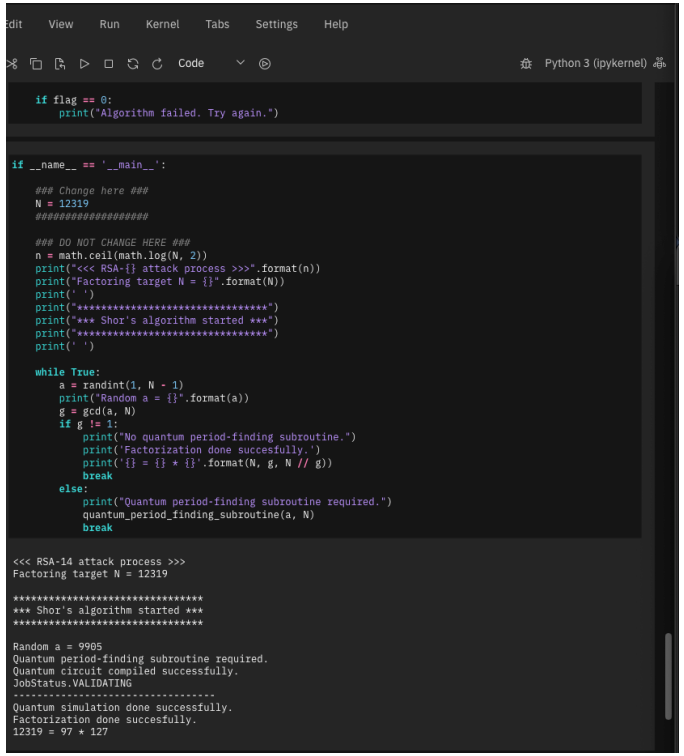
[1]*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China*
[2]*State Key Laboratory of Low-Dimensional Quantum Physics and Department of Physics, Tsinghua University, Beijing 100084, China*
[3]*School of Physics, ZJU-Hangzhou Global Scientific and Technological Innovation Center, Interdisciplinary Center for Quantum Information, and Zhejiang Province Key Laboratory of Quantum Technology and Device, Zhejiang University, Hangzhou 310000, China*
[4]*Beijing Academy of Quantum Information Sciences, Beijing 100193, China*
[5]*Institute of Information Technology, Information Engineering University, Zhengzhou 450001, China*
[6]*Beijing National Research Center for Information Science and Technology and School of Information Tsinghua University, Beijing 100084, China*
[7]*Frontier Science Center for Quantum Information, Beijing 100084, China*

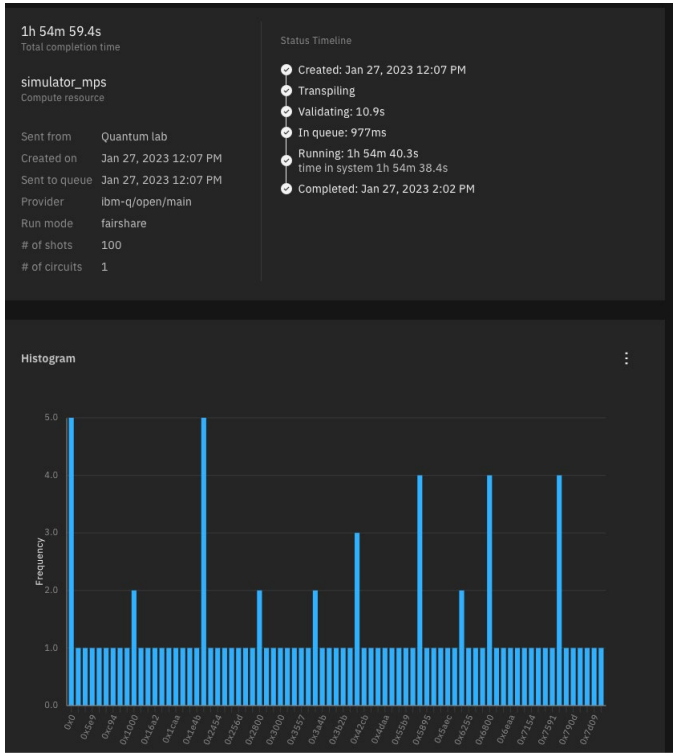
Shor's algorithm has seriously challenged information security based on public key cryptosystems. However, to break the widely used RSA-2048 scheme, one needs millions of physical qubits, which is far beyond current technical capabilities. Here, we report a universal quantum algorithm for integer factorization by combining the classical lattice reduction with a quantum approximate optimization algorithm (QAOA). The number of qubits required is $O(\log N/\log\log N)$, which is sublinear in the bit length of the integer N, making it the most qubit-saving factorization algorithm to date. We demonstrate the algorithm experimentally by factoring integers up to 48 bits with 10 superconducting qubits, the largest integer factored on a quantum device. We estimate that a quantum circuit with 372 physical qubits and a depth of thousands is necessary to challenge RSA-2048 using our algorithm. Our study shows great promise in expediting the application of current noisy quantum computers, and paves the way to factor large integers of realistic cryptographic significance.

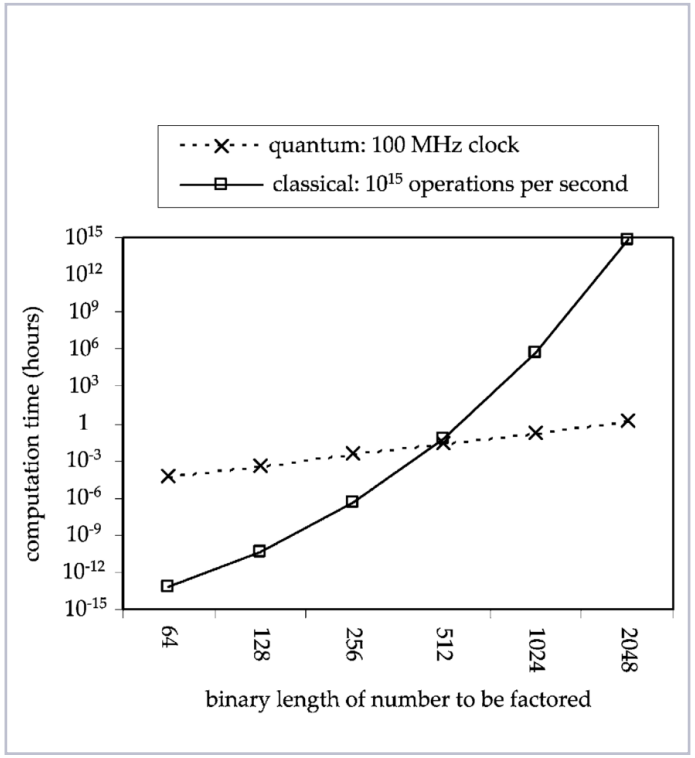
Quantum computing has entered the era of noisy intermediate scale quantum (NISQ) [1, 2]. A milestone in the NISQ era is to prove that NISQ devices can surpass classical computers in problems with practical significance, that is, to achieve practical quantum advantage. Low-resource algorithm (qubit) in superconducting device [27]. However, it should be noted that some of the factored integers have been carefully selected with special structures [28], thus the largest integer factored by a general method in a real physical system by now is 249919 (18-bit).

Factoring integers with sublinear resources on a superconducting quantum processor

- 22년 12월에 발표된 논문
- 10큐비트 사용하여 48-bit 크기의 수를 인수 분해 성공
- 2048-bit 인수 분해를 위해서는 372큐비트 필요함
  즉, 가까운 미래에 RSA-2048 공격 가능할 것으로 예상
- 수행한 테스트의 소요시간에 관한 결과가 빠져 있고,
  RSA-2048까지 시간 증가 속도가 불분명함
- 테스트 환경에 대한 검증이 빠져 있고,
  논문 후반부에 작성된 테스트를 실제로 수행하였는지 알기 어려움







14-bit 인수분해

- 58큐비트 사용, 약 두 시간 소요
- 특정 수가 아닌, 임의의 수에 대하여 약 두 시간 소요 (58큐비트 사용)
- IBM Quantum simulator 즉, 모두가 사용할 수 있는 환경에서 테스트
- 양자 컴퓨터의 성능이 충분히 발전하면
  512-bit부터는 고전 컴퓨터보다 훨씬 빠르게 인수 분해
- IEEE QSW 컨퍼런스 제출 준비 중

NISTIR 8105 Report on Post-Quantum Cryptography

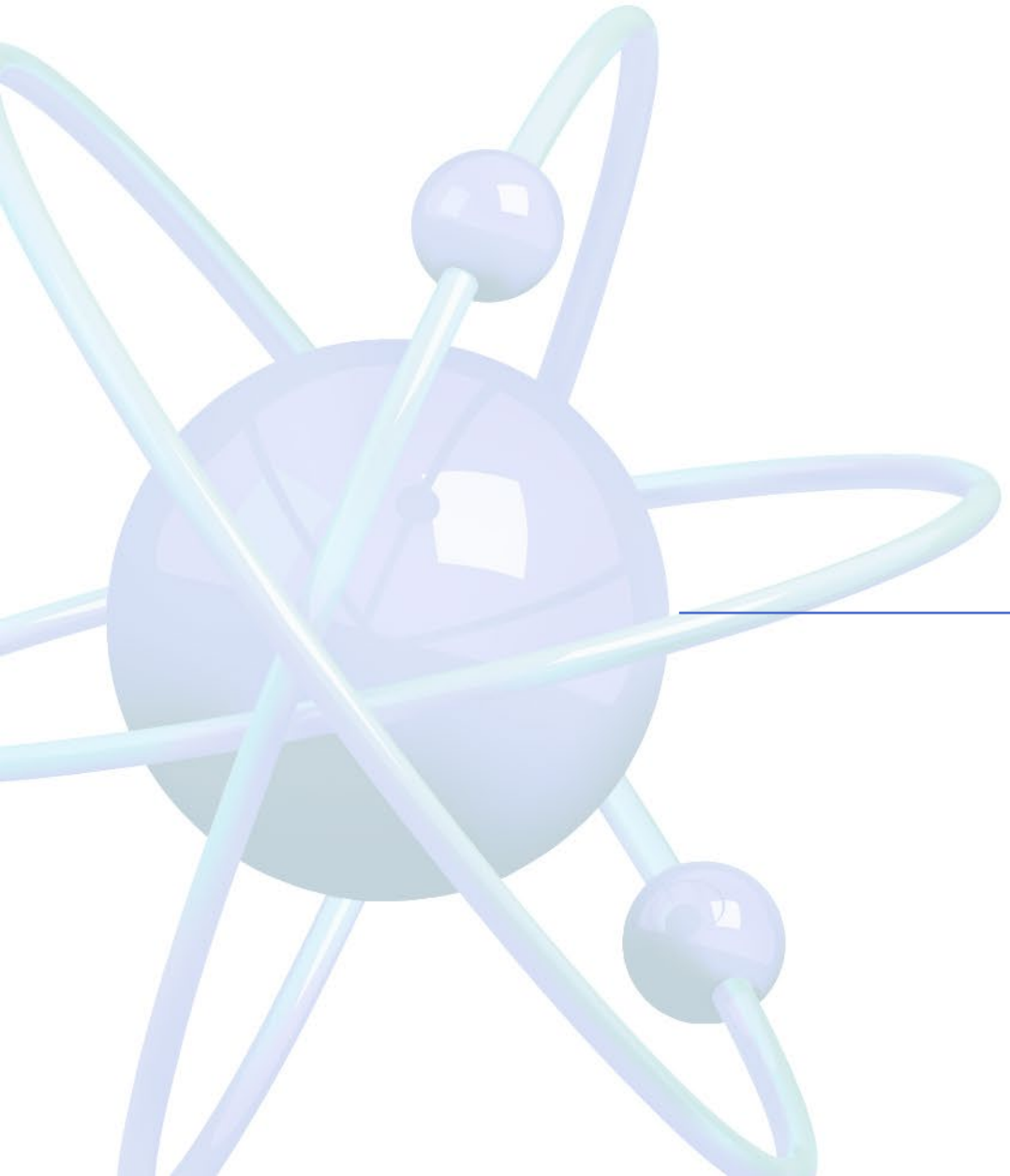
Cryptographic Algorithm	Type	Purpose	Impact from large-scale quantum computer
AES	Symmetric key	Encryption	Larger key sizes needed
SHA-2, SHA-3		Hash functions	Larger output needed
RSA	Public key	Signatures, key establishment	No longer secure
ECDSA, ECDH (Elliptic Curve Cryptography)	Public key	Signatures, key establishment	No longer secure
DSA (Finite Field Cryptography)	Public key	Signatures, key establishment	No longer secure

It is unclear when scalable quantum computers will be available. However, in the past year or so, researchers working on building a quantum computer have estimated that it is likely that a **quantum computer capable of breaking 2000-bit RSA in a matter of hours could be built by 2030** for a budget of about a billion dollars [11]. This is a serious long-term threat to the cryptosystems currently standardized by NIST.

◀ Impact of Quantum Computing on Common Cryptographic Algorithms

NIST는 양자 컴퓨터로 인해 **공개키 암호가 안전하지 않다**고 밝히며 특히 **RSA는 2030년에 2000-bit가 몇 시간 내로 깨질 것**이고 이는 현재의 표준 암호 시스템에 심각함 위협이라고 언급함

NORMA



양자시대 어떻게 대비해야 하는가

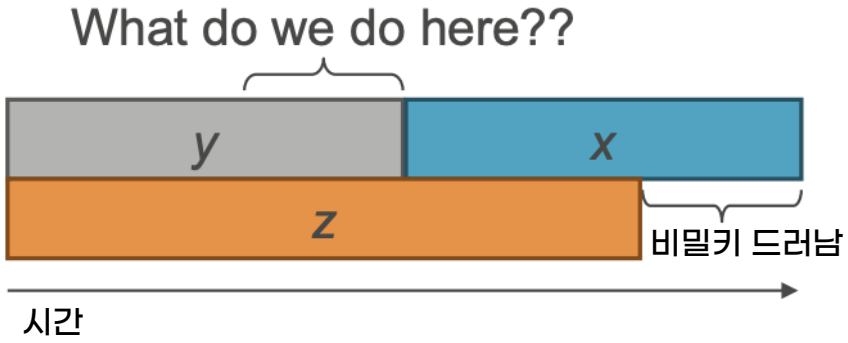
양자 이후 시대를 준비하는 경로

Harvest Now, Decrypt Later

Mosca Theorem

2015년 4월 Michele Mosca (Waterloo 대학 교수)

Theorem 1: If $x + y > z$, then worry.

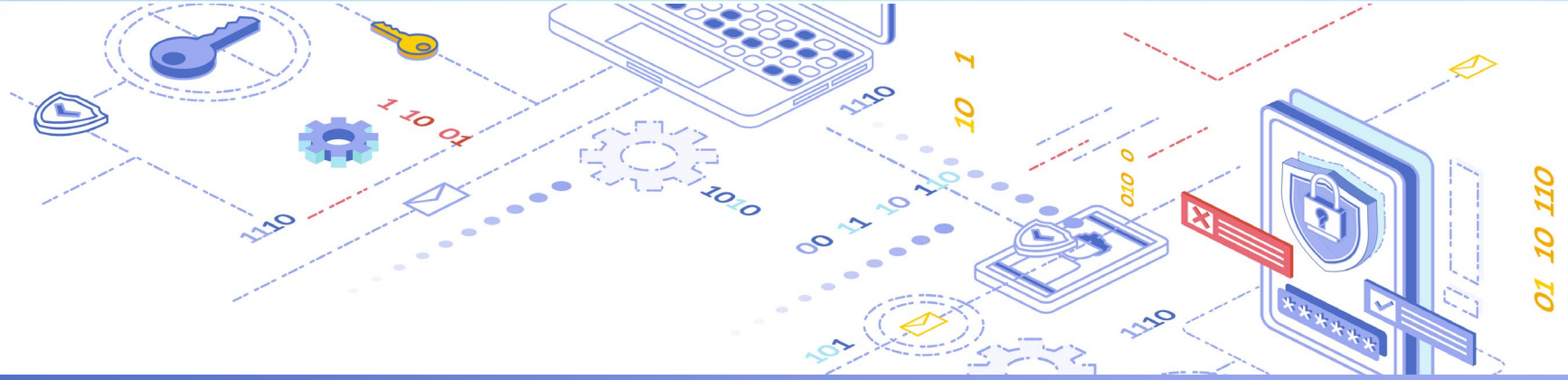


마이그레이션 시간 + 보안 시간이 붕괴 시간보다 클 경우 문제 발생

x : 보안 시간
(데이터를 안전하게 보호해야 하는 시간)

y : 마이그레이션 시간
(안전한 솔루션으로 바꾸는 데 걸리는 시간)

z : 붕괴 시간
(양자 컴퓨터가 현재 사용되는 암호를 깨기까지의 시간)



Harvest Now, Decrypt Later

Harvest Now

다가올 미래에는 양자 컴퓨터로 인해 현재 사용되는 암호가 깨질 것이므로 공격자는 데이터를 수집하여 암호화된 채로 모아둠

Decrypt Later

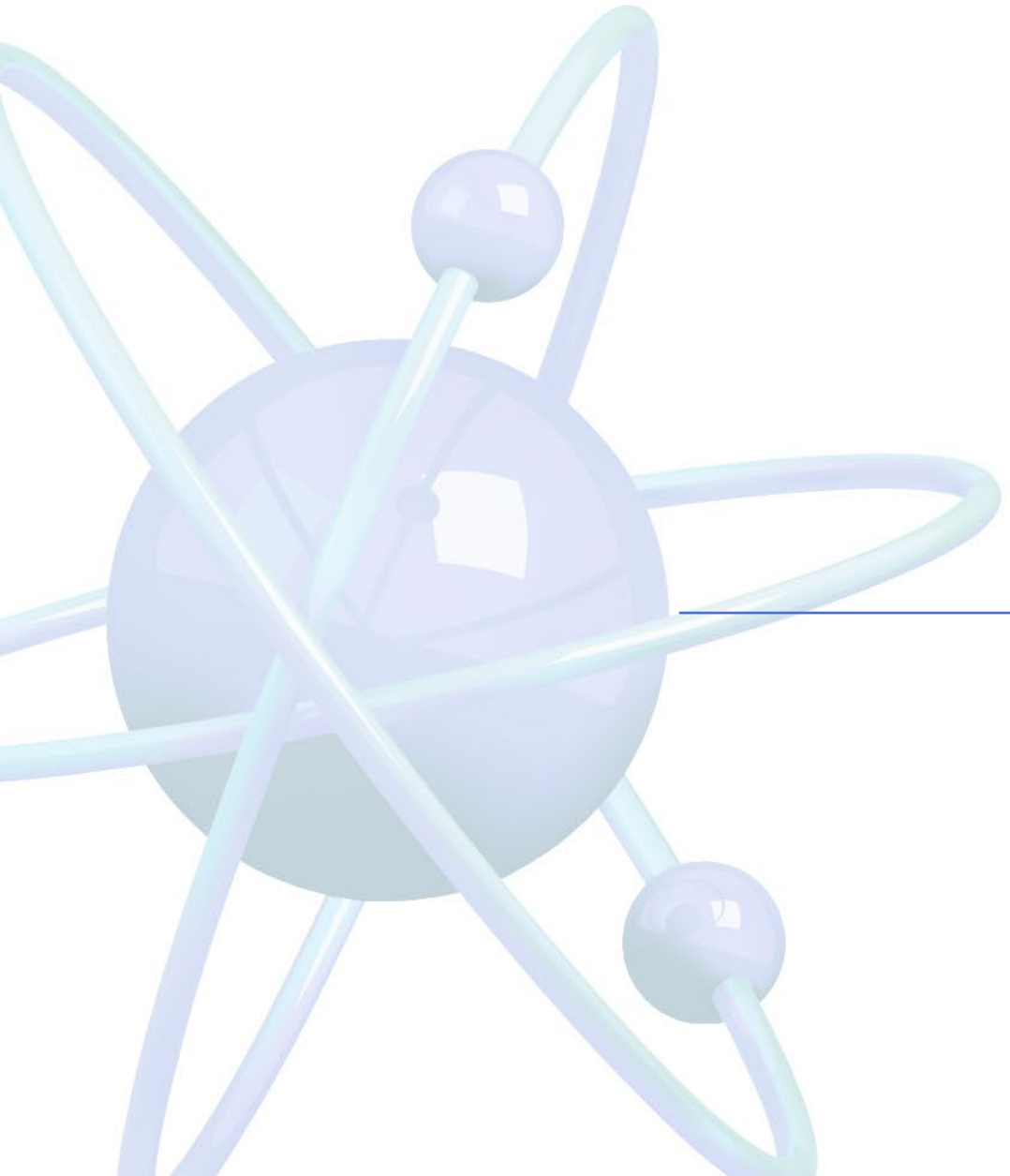
양자 컴퓨터가 충분히 발전하여 현재 사용되는 암호를 깨는 시점에 그동안 모아둔 데이터를 복호화하여 내용을 확인하고 이를 악용함

- 양자 컴퓨팅에 의한 보안 약화를 고려하는 조직 중 절반 이상 (50.2%)이 HNDL 공격의 위험에 노출되어 있다고 생각함
- 양자 컴퓨팅 기술 활용과는 별개로 양자 이후 세계에서의 사이버 보안 위험 대비가 필요함
- 민감 데이터를 장기간 보관해야 하는 산업은 HNDL 공격에 특히 취약함

- 양자 위협에 대한 취약성 평가를
  - 1년 내에 완료 : 45%
  - 5년 내에 완료 : 16.2%
  - 계획 없거나 지켜볼 것 : 13%
  - 모르겠음 또는 해당사항 없음 : 25.8%

많은 조직이 아직 양자 위협에 내성이 있는 안전한 조치를 구현하지 않음

NORMA



Post-Quantum Cryptography

PQC vs QKD

PQC 분류

PQC 표준화

PQC
(Post-Quantum Cryptography)

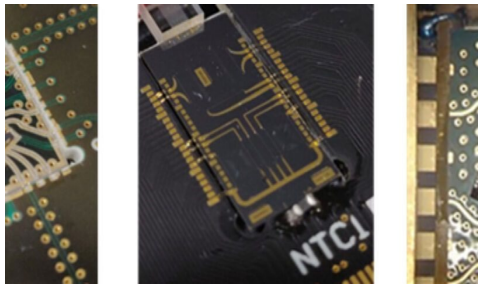
양자 내성 암호
양자 컴퓨팅 환경에서도 안전하게 암호 기술을
이용할 수 있도록 하는 새로운 공개키 암호

SW

- 양자 알고리즘으로도 쉽게 해결할 수 없는 수학적 난제 기반
- 소프트웨어만으로 구현 가능
- 별도의 장비 없이도 기존 인프라에 적용 가능
- 기존의 공개키 암호 알고리즘 대체
  (키 교환을 위한 캡슐화 및 서명 기능 포함)
- NIST(미국), KpqC(한국) 등에서 표준화 절차 진행 중

QKD
(Quantum Key Distribution)

양자 키 분배
양자역학적 특성을 이용하여 암호 통신을 위한
키를 안전하게 분배하는 기술



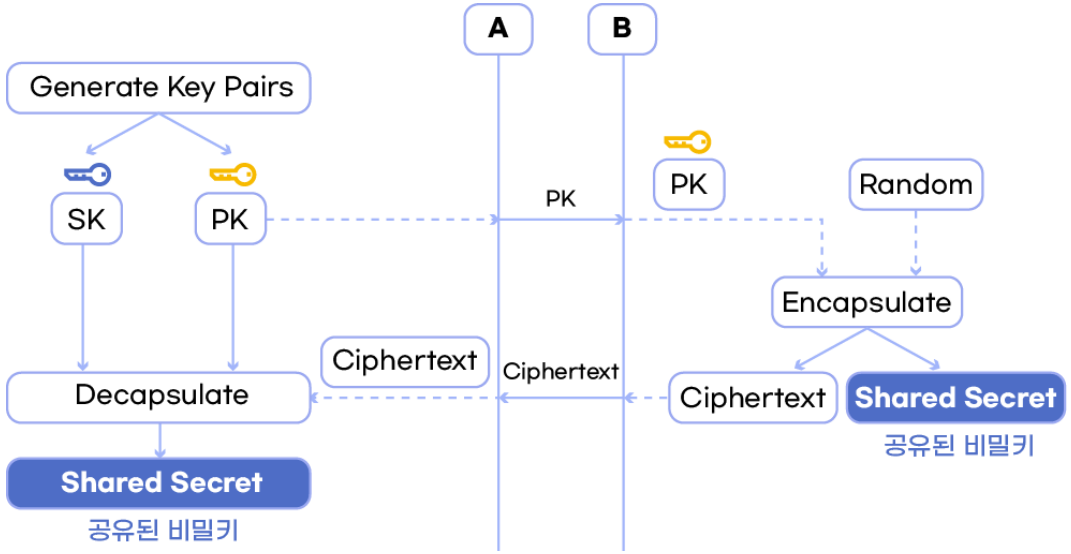
HW

- 양자의 복제 불가능 및 측정 후 상태가 붕괴하는 원리 기반
- 양자를 제어할 수 있는 하드웨어 필요
- 전용 장비가 필요하고 비교적 고비용
- 공개키 암호가 아닌, 키 교환 기능만 가능
  (서명을 위한 기능은 없음)
- NSA는 QKD 사용을 지원하지 않겠다고 발표

PQC

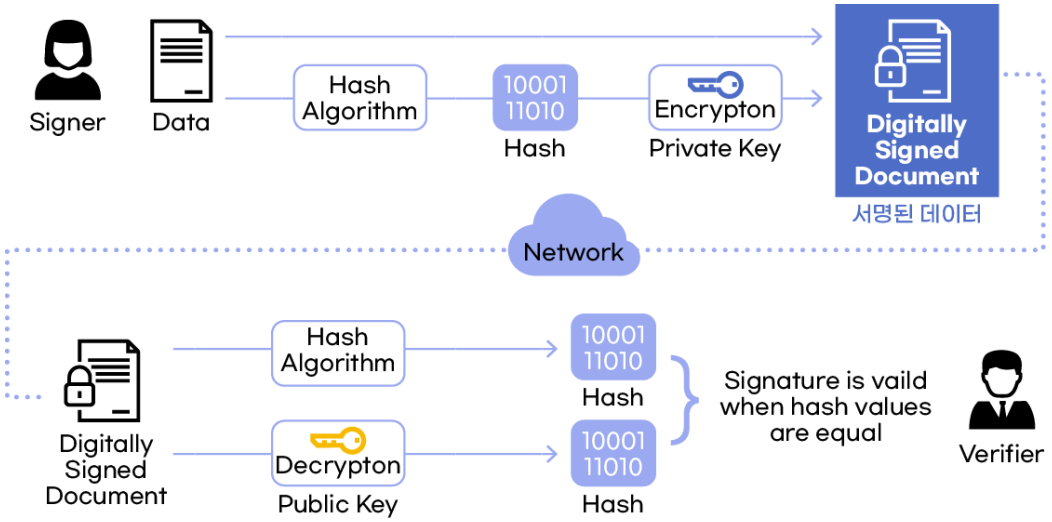
격자 기반 암호	해시 기반 암호	코드 기반 암호	다변수 암호	아이소제니 기반 암호

키 설정



공개키로 암호화(캡슐화)한 데이터를
개인키로 복호화(캡슐해제)하여 키를 교환하는 과정

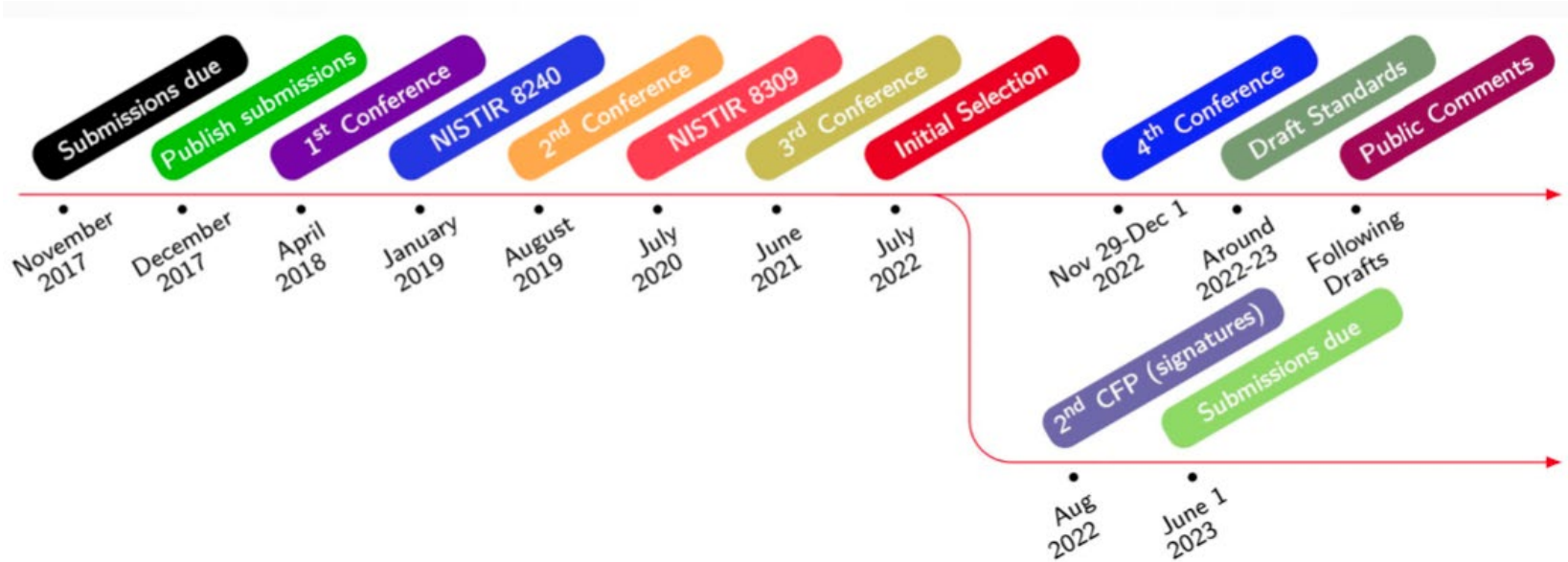
디지털 서명



개인키로 암호화(서명)한 데이터를
공개키로 복호화(검증)하여 사용자를 확인하는 과정

NIST

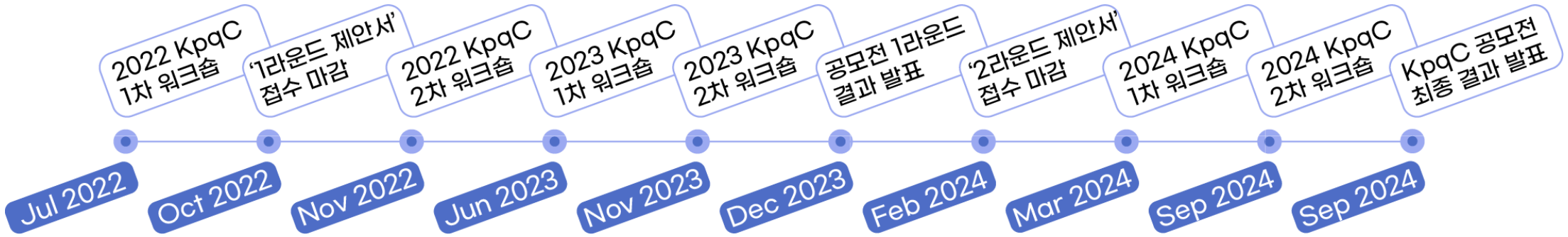
- 현재 표준화 대상 및 4라운드 후보 알고리즘 발표 완료
  - 2016년 12월, 알고리즘 제안 요청
  - 2017년 12월, 1라운드 제출 알고리즘 발표
  - 2019년 1월, 2라운드 후보 알고리즘 발표
  - 2020년 7월, 3라운드 후보 알고리즘 발표
- 표준화 대상 공개키 암호화 및 키 설정 알고리즘
  - CRYSTALS-KYBER (격자 기반)
- 표준화 대상 디지털 서명 알고리즘
  - CRYSTALS-DILITHIUM (격자 기반)
  - FALCON (격자 기반)
  - SPHINCS+ (해시 기반)



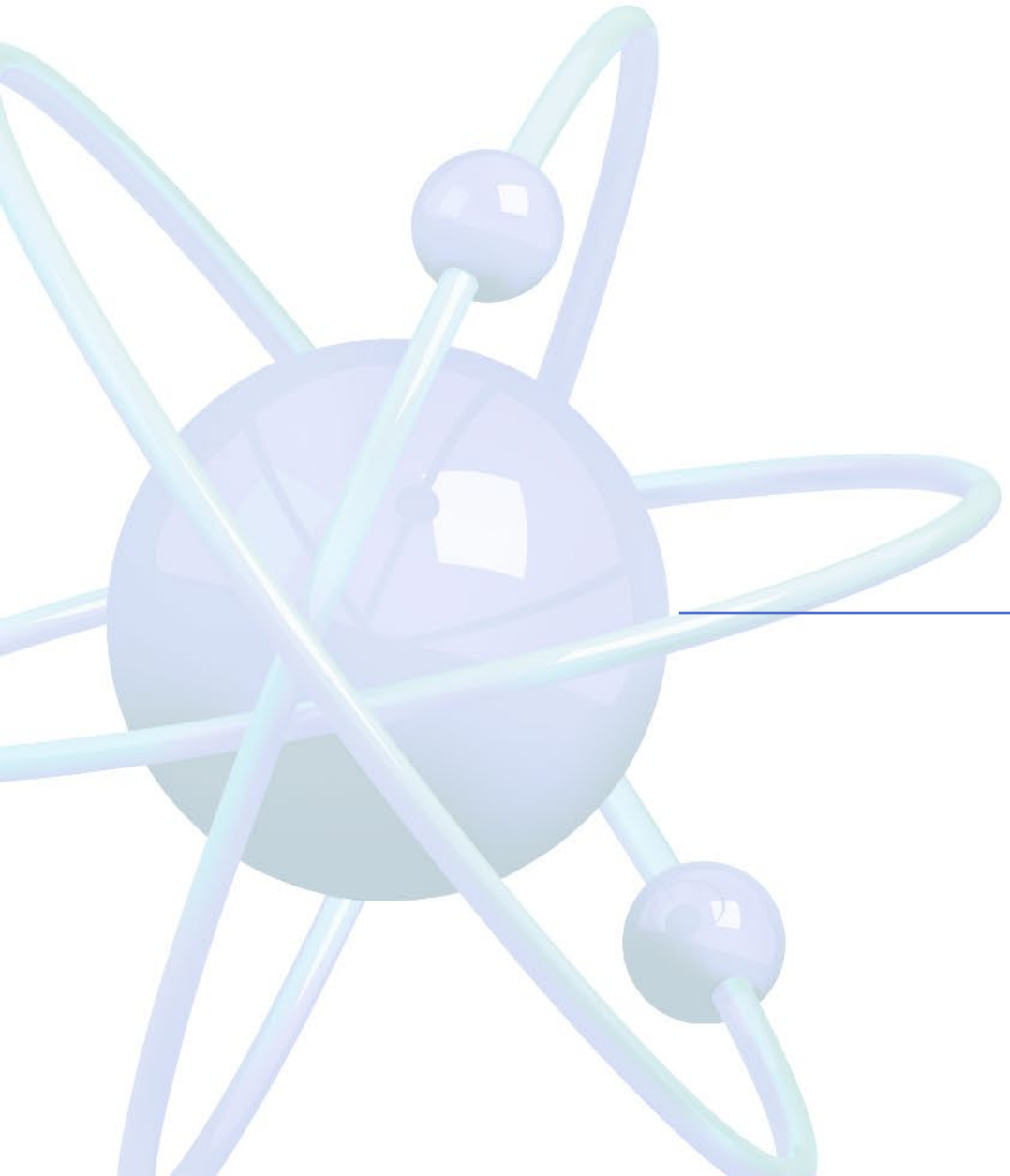
KpqC

- 현재 1라운드 제출 알고리즘 발표 완료
  - 2021년 11월, 알고리즘 제안 요청
  - 2024년 표준 알고리즘 선정 목표
- 1라운드 제출 알고리즘
  - 공개키 암호화 및 키 설정 알고리즘 7종
  - 디지털 서명 알고리즘 9종

- **노르마**
  - 1라운드 제출 알고리즘 중 NTRU+ 개발에 참여
  - 다른 PQC 알고리즘에 대한 협업도 추진 중



NORMA



Q Care 도입 사례

SSL VPN

SASE 플랫폼 SSL 통신

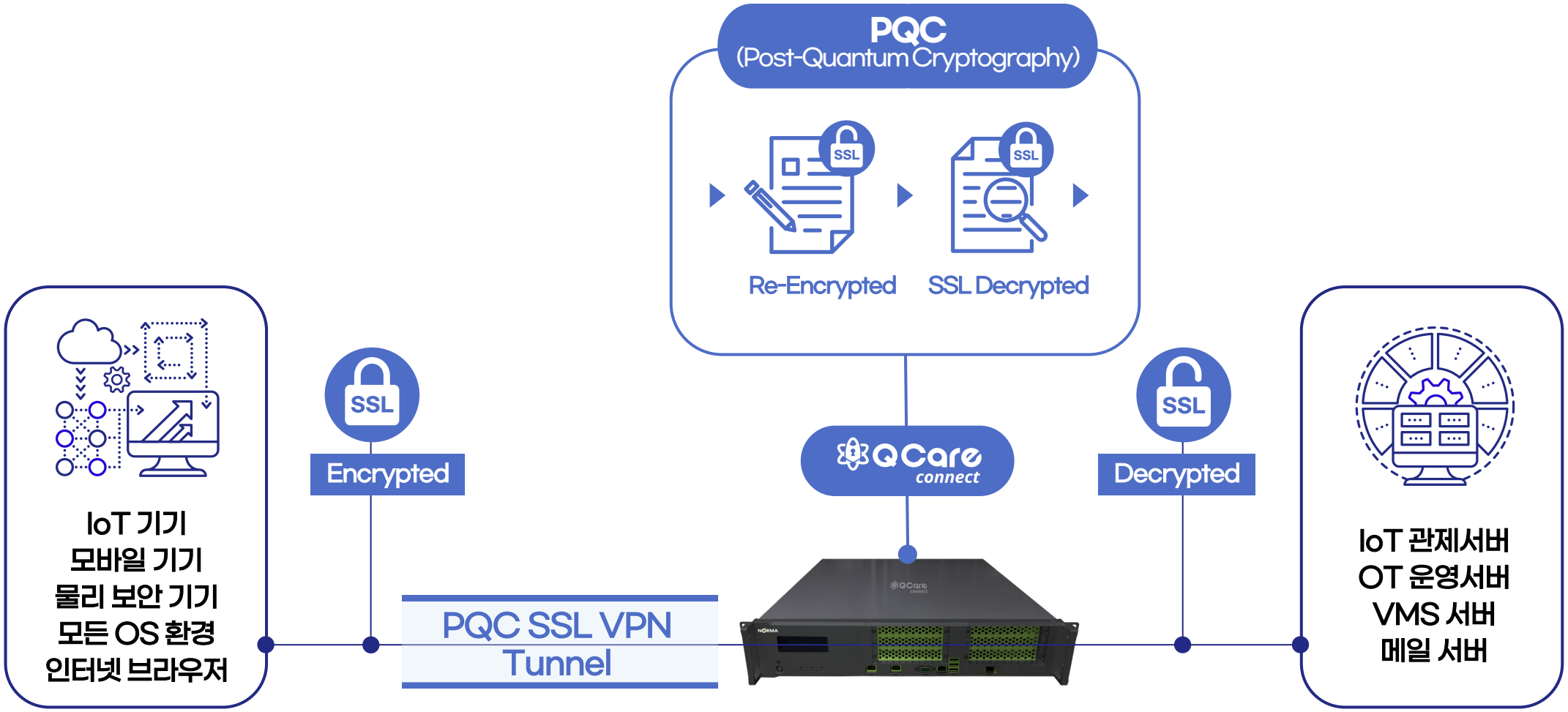
CCTV 구간 암호화

PKI

블록체인

Bluetooth

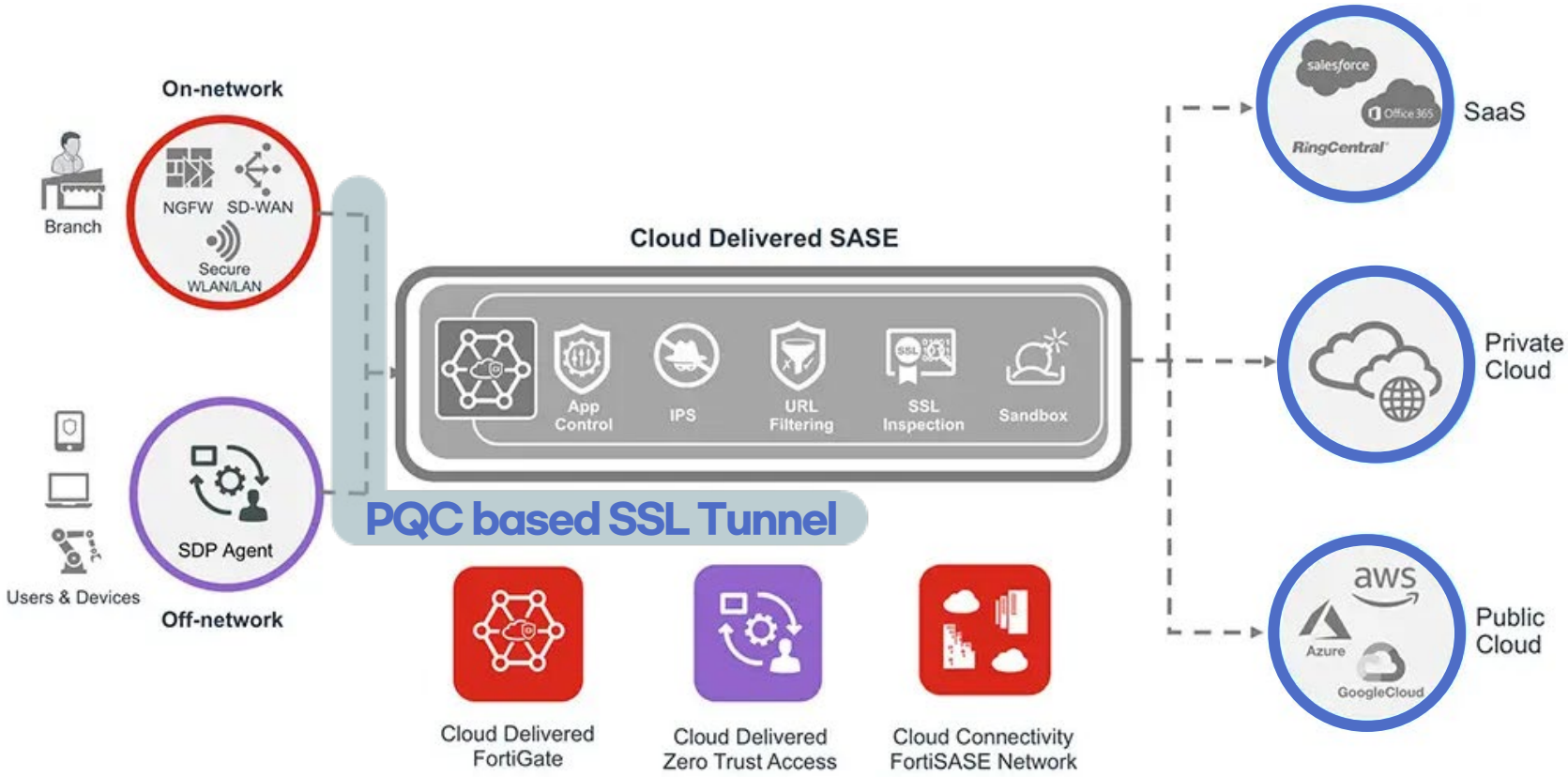
SSL VPN 공개키 암호화 PQC 구현



NIA, 2022년 지능형 초연결망 선도확산 지원사업

- SSL 키 생성 알고리즘 구성 (CA 인증서 & 키 활용)
- 서버와 클라이언트 간 암호화 키 교환 알고리즘 구성/설계
- 알고리즘 변경 (기존 RSA → PQC)

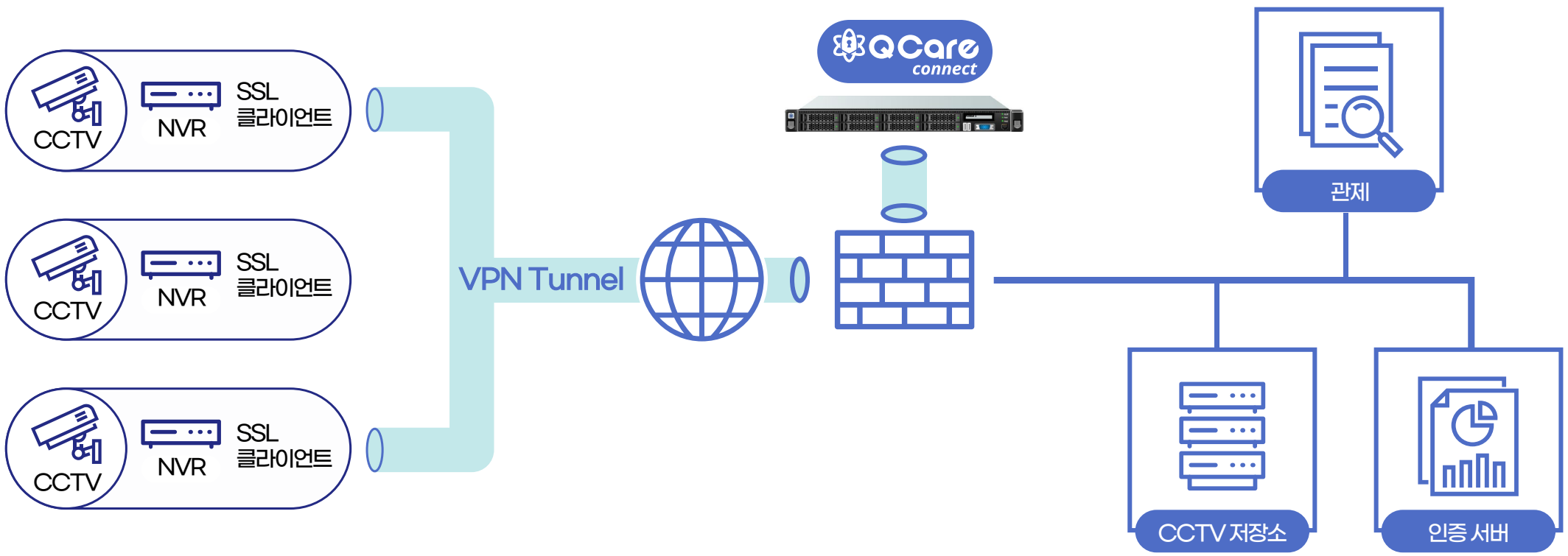
특허 등록 완료



H건설사, 현장 CCTV 구간 암호화에 PQC 적용

- 건설현장 CCTV를 실시간 관제센터 전송 사업
- SSL VPN 클라이언트를 NVR에 탑재 후 VPN 구성
- 홈네트워크 월패드 PQC 기반 SSL VPN 사업
- NIST PQC 표준 알고리즘 및 노르마 PQC 알고리즘 구현
- PQC 디지털 서명 및 PKE/KEM 알고리즘 함께 적용

특허 등록 완료



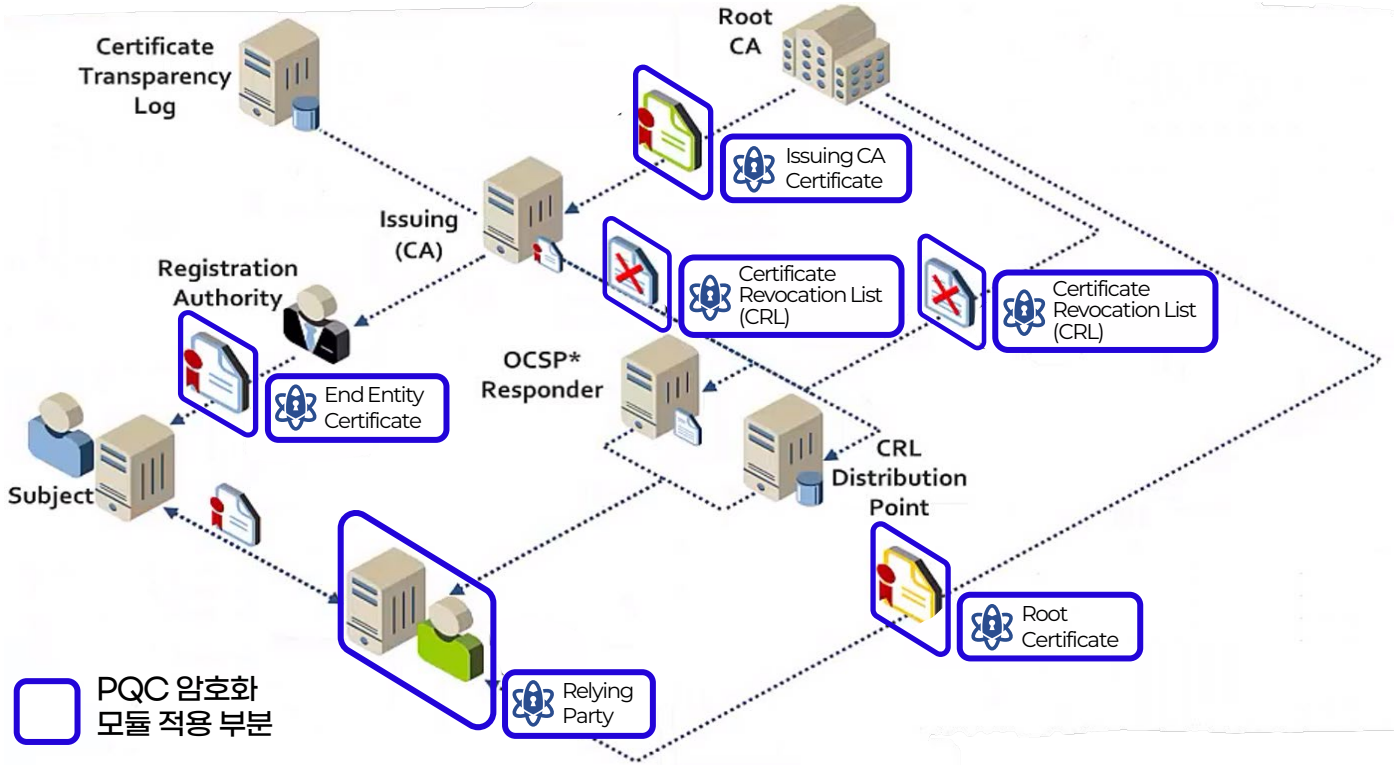
공개키 인프라에서 사용되는 RSA를 PQC로 대체

- PKI는 디지털 인증의 생성, 관리, 배포, 사용, 저장, 파기와 공개키 암호 관리에 사용되는 역할, 정책, H/W, S/W, 절차의 총칭
- 전자상거래 등 민감한 정보를 담은 이메일을 포함한 다양한 네트워크 활동에 있어 정보의 안전한 전송이 목적
- 기존 PKI에 사용되는 RSA 알고리즘에 PQC 모듈 추가

특허 출원 중

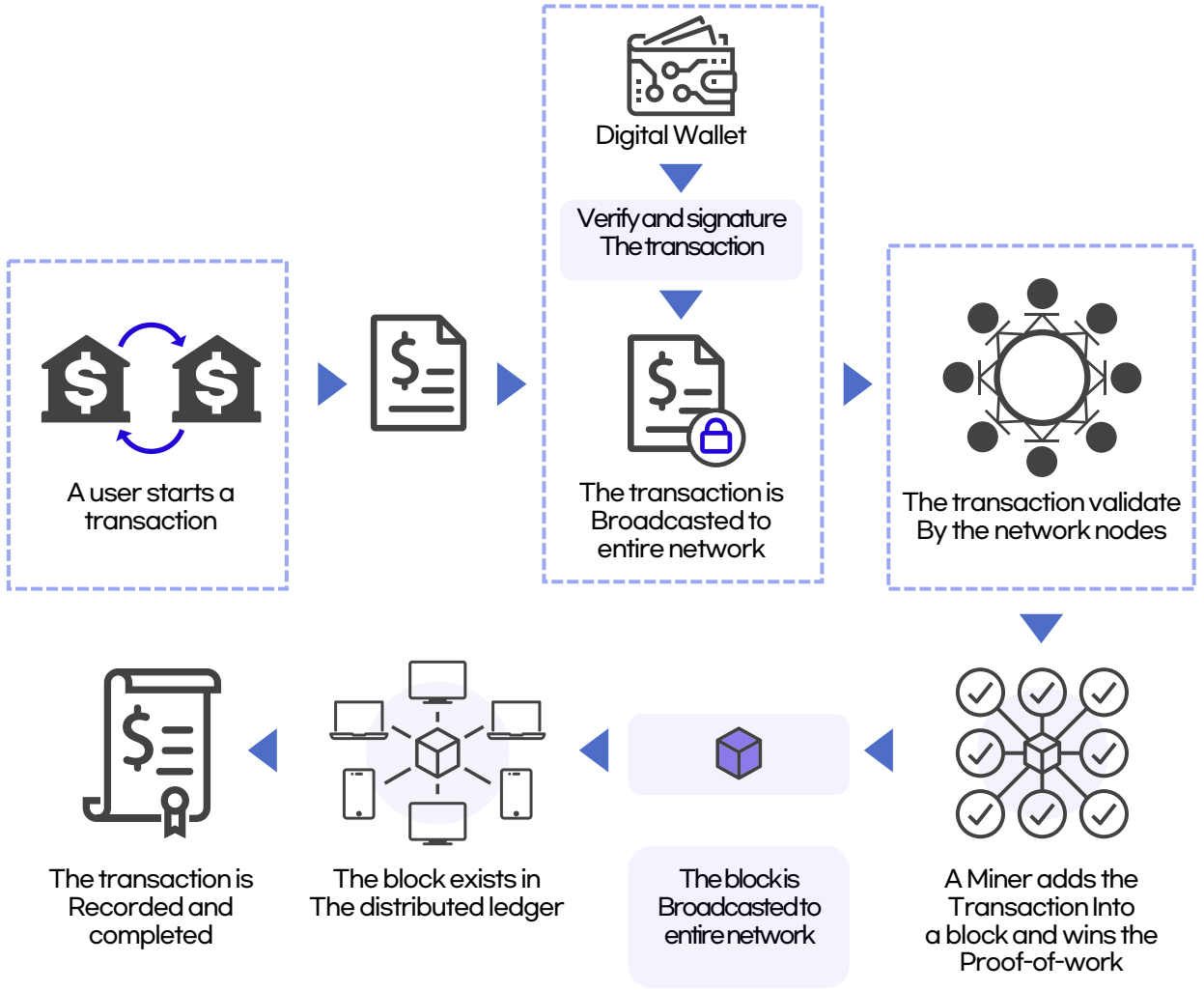
일반적인 기능

- 인증서 발급
- 인증서 관리
- 인증서 배포
- 인증서 사용
- 인증서 저장
- 인증서 취소



PKI Overview

블록체인에 사용되는 ECC를 PQC로 대체



1. 사용자(user)가 트랜잭션 생성
2. 트랜잭션에 **서명** 후 공개키와 함께 전송
3. 네트워크 노드에서 트랜잭션 **검증**
4. 채굴자가 블록에 트랜잭션 추가
   ▶ PoW 보상으로 암호화폐 획득함
5. 블록체인에 추가, 업데이트 전파
6. 트랜잭션이 기록됨으로써 완료

트랜잭션 서명 및 검증에 사용되는
기존의 ECC 알고리즘을
PQC 알고리즘으로 대체

특허 출원 중

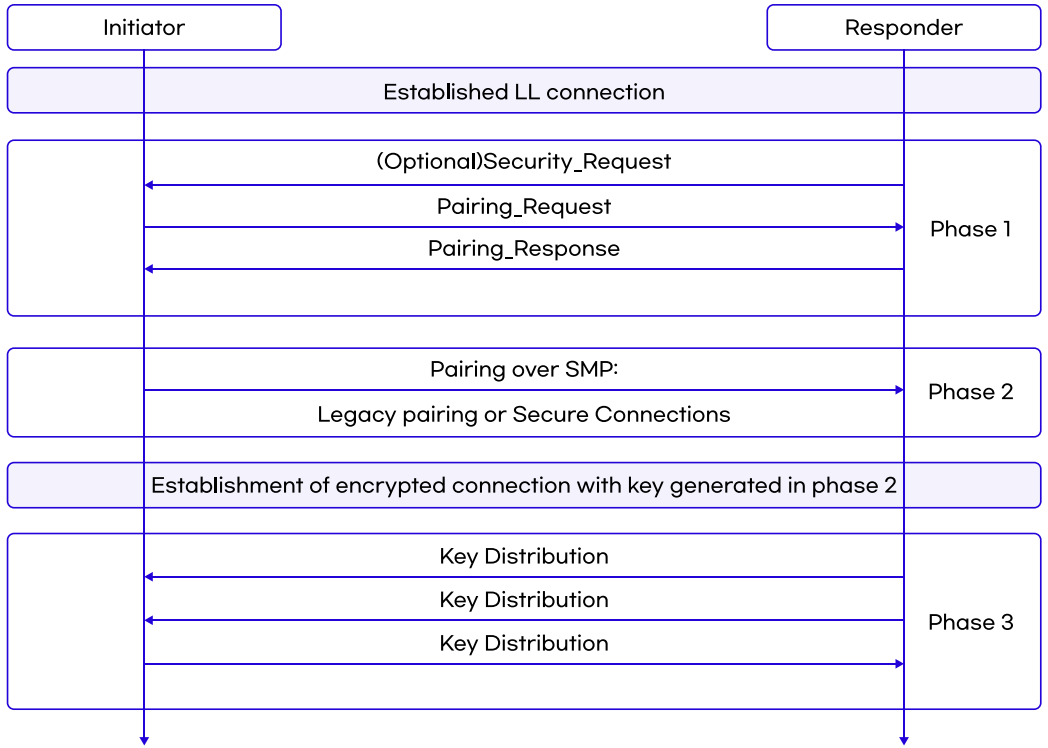
Bluetooth에서 사용되는 ECC를 PQC로 대체

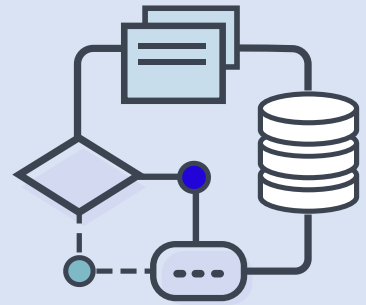
- 페어링은 링크 암호화에 사용할 수 있는 키를 설정 하기 위해 수행되며 아래와 같이 3단계로 진행

Phase1 페어링 정보 교환

Phase2 페어링 키 생성

Phase3 암호화 키 교환





Bluetooth 페어링 시 사용되는
기존의 ECC 알고리즘을
PQC 알고리즘으로 대체

특허 등록 완료

NORMA

감사합니다