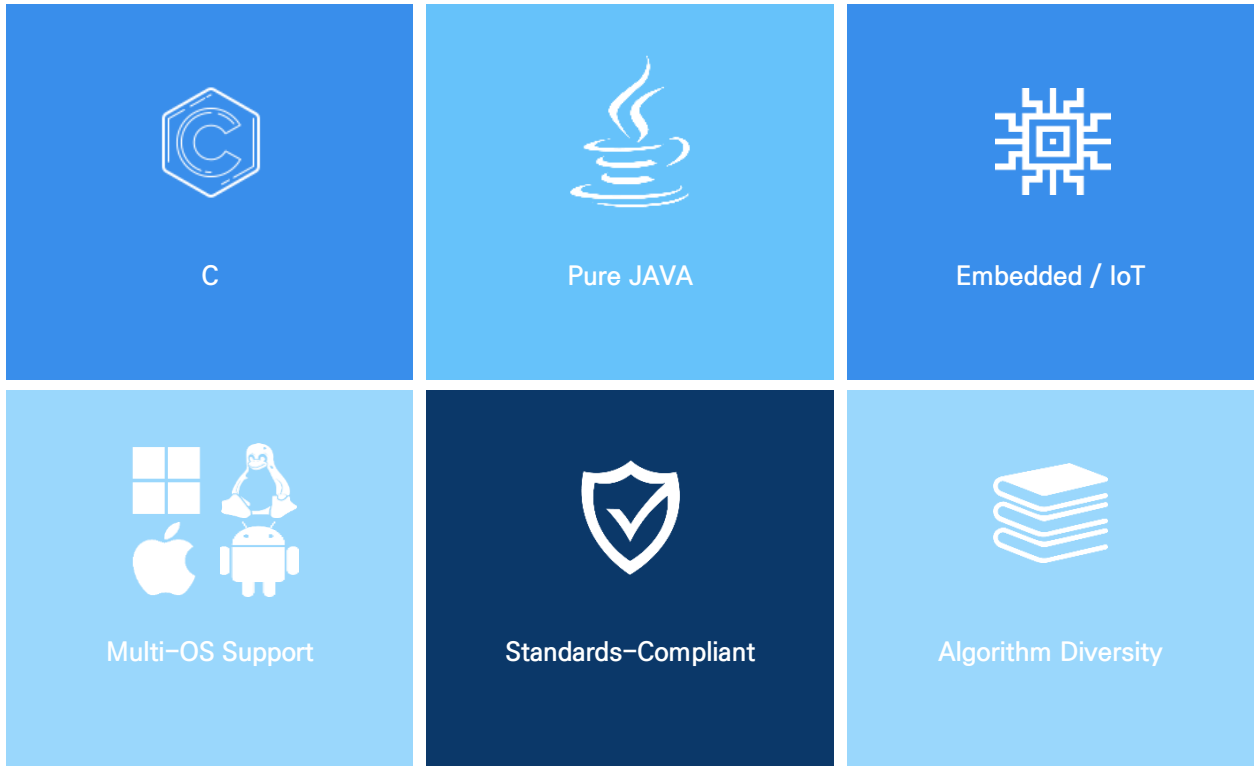
ypqc

Next-Gen PQC Security Module Against Quantum Threats



Next Authentication Platform
Whykeykey

양자컴퓨터란?

- 원리: 양자 역학의 '중첩'과 '얽힘' 현상을 활용한 초고속 연산
- 특징: 기존 슈퍼컴퓨터를 뛰어넘는 압도적인 연산 능력 확보
- 활용 분야: AI, 국방, 신약 개발, 우주항공 등 다양한 산업의 혁신을 주도할 전망

양자컴퓨터 시대의 도래

- CES 2025 : 인공지능(AI)과 반도체를 잇는 미래 기술로 주목
- 기술진보가 급진전되면서 향후 3년내 의미있는 성과로 이어질 것이란 관측이 제기됨
- 주요 업체 상용화 목표:
  - 구글: 2031년까지 양자컴퓨터 사용화를 목표로 총 6단계 상업화 로드맵을 제시.
  - IBM: 2029년까지 오류 수정 기능 갖춘 양자컴퓨터를 구현해 상용화하는 것을 목표.
  - 마이크로소프트: 아이온큐, 허니웰, 아톰컴퓨터 등 파트너사와 연계 및 연구 개발.
- 국내 : 2025년 3월 민관협력 양자전략위 출범
- 전망: 빅테크 기업의 각기 다른 전략으로 양자컴퓨팅 기술 개발을 가속

  → 양자 기술 상용화 가능성을 넓히는 만큼 양자컴퓨터의 상용화 시기는 더욱 단축될 전망.

양자컴퓨팅의 위협이 현실화 되면서 양자내성암호(PQC)로의 전환은 선택이 아닌 필수가 되었습니다.

1 암호체계의 붕괴 위험성

- 취약점: 양자컴퓨터의 '쇼어 알고리즘'* 은 대부분의 전자상거래에서 사용하는 RSA, ECC 등 기존 암호 체계를 쉽게 무력화
- 영향: 기존 전자상거래 및 국가 안보에 심각한 위협으로 작용
- 시급성: 모스카부등식** 에 따라, 양자 컴퓨터가 상용화되기 전에 선제적 대응이 반드시 필요
- 암호화폐: 비트코인, 이더리움 등 주요 암호화폐 시장에 대한 중대한 변화 예상

2 양자컴퓨팅 전환에 따른 위협 분석

구분	RSA2048 (Classical)	ECDSA(P256) (Classical)	Quantum Computing (Shor's Algorithm)
기반원리	소인수분해	이산로그	QFT 양자푸리에변환
시간복잡도	$O\left(e^{\sqrt[3]{\frac{64}{9}(\log n)(\log^2 n)^2}}\right)$ (지수시간)	$O(\sqrt{n})$ (지수시간)	$O\left((\log n)^3\right)$ (다항시간)
계산가능성	계산불가	계산불가	계산가능

* 쇼어 알고리즘(Shor's Algorithm): 양자 컴퓨터를 이용하여 큰 수를 빠르게 소인수분해할 수 있는 알고리즘. 소인수분해와 이산로그 문제를 비밀키 없이 다항시간 내 풀 수 있음.

** 모스카부등식 (Mosca's inequlity) : 양자컴퓨터는 선수집 후해독(SNDL, Store Now Decrypt Later) 방식의 공격 시도 블록체인상에 거래된 과거의 키를 풀어 해킹을 할 수 있음 양자내성암호는 해독 기술이 본격화 되기 수년 전에 미리 개발해야함

배경

- 양자컴퓨팅 기술의 발전으로 기존의 암호체계가 위협을 받음(Peter Shor)
- 양자컴퓨터의 상용화는 예상할 수 없지만 PQC는 미리 준비해야한다(모스카의 부등식)

What is PQC?

- 양자컴퓨팅 환경에서 해독 위협에 대응하는 새로운 암호.
- 국제표준 3종 (ML-KEM, ML-DSA, SLH-DSA)
- 국내표준 4종 (NTRU+, SMAUG-T, HAETAE, AIMER)

Ypqc

- ㈜와이키키소프트 기술연구소에서는 국내최초로 C/JAVA 언어기반 양자내성 암호 개발 및 테스트 완료
- 안정성 및 성능최적화 진행중

격자 기반 알고리즘 예시

Gen

$\zeta \leftarrow \{0,1\}^{256}$
$(\rho, \rho', K) \in \{0,1\}^{256} \times \{0,1\}^{512} \times \{0,1\}^{256} := \mathrm{H}(\zeta)$ ▷ H is instantiated as SHAKE-256
$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
$(\mathbf{s}_1, \mathbf{s}_2) \in S_\eta^\ell \times S_\eta^k := \mathsf{ExpandS}(\rho')$
$\mathbf{t} := \mathbf{A}\mathbf{s}_1 + \mathbf{s}_2$ ▷ Compute $\mathbf{A}\mathbf{s}_1$ as $\mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{s}_1))$
$(\mathbf{t}_1, \mathbf{t}_0) := \mathsf{Power2Round}_q(\mathbf{t}, d)$
$tr \in \{0,1\}^{256} := \mathrm{H}(\rho \parallel \mathbf{t}_1)$
return $(pk = (\rho, \mathbf{t}_1), sk = (\rho, K, tr, \mathbf{s}_1, \mathbf{s}_2, \mathbf{t}_0))$

Sign(sk, M)

$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
$\mu \in \{0,1\}^{512} := \mathrm{H}(tr \parallel M)$
$\kappa := 0, (\mathbf{z}, \mathbf{h}) := \perp$
$\rho' \in \{0,1\}^{512} := \mathrm{H}(K \parallel \mu)$ (or $\rho' \leftarrow \{0,1\}^{512}$ for randomized signing)
while $(\mathbf{z}, \mathbf{h}) = \perp$ do ▷ Pre-compute $\hat{\mathbf{s}}_1 := \mathtt{NTT}(\mathbf{s}_1)$, $\hat{\mathbf{s}}_2 := \mathtt{NTT}(\mathbf{s}_2)$, and $\hat{\mathbf{t}}_0 := \mathtt{NTT}(\mathbf{t}_0)$
  $\mathbf{y} \in \tilde{S}_{\gamma_1}^\ell := \mathsf{ExpandMask}(\rho', \kappa)$
  $\mathbf{w} := \mathbf{A}\mathbf{y}$ ▷ $\mathbf{w} := \mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{y}))$
  $\mathbf{w}_1 := \mathsf{HighBits}_q(\mathbf{w}, 2\gamma_2)$
  $\tilde{c} \in \{0,1\}^{256} := \mathrm{H}(\mu \parallel \mathbf{w}_1)$
  $c \in B_\tau := \mathsf{SampleInBall}(\tilde{c})$ ▷ Store c in NTT representation as $\hat{c} = \mathtt{NTT}(c)$
  $\mathbf{z} := \mathbf{y} + c\mathbf{s}_1$ ▷ Compute $c\mathbf{s}_1$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{s}}_1)$
  $\mathbf{r}_0 := \mathsf{LowBits}_q(\mathbf{w} - c\mathbf{s}_2, 2\gamma_2)$ ▷ Compute $c\mathbf{s}_2$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{s}}_2)$
  if $\|\mathbf{z}\|_\infty \geq \gamma_1 - \beta$ or $\|\mathbf{r}_0\|_\infty \geq \gamma_2 - \beta$, then $(\mathbf{z}, \mathbf{h}) := \perp$
  else
    $\mathbf{h} := \mathsf{MakeHint}_q(-c\mathbf{t}_0, \mathbf{w} - c\mathbf{s}_2 + c\mathbf{t}_0, 2\gamma_2)$ ▷ Compute $c\mathbf{t}_0$ as $\mathtt{NTT}^{-1}(\hat{c} \cdot \hat{\mathbf{t}}_0)$
    if $\|c\mathbf{t}_0\|_\infty \geq \gamma_2$ **or** the # of 1's in $\mathbf{h}$ is greater than ω, then $(\mathbf{z}, \mathbf{h}) := \perp$
  $\kappa := \kappa + \ell$
return $\sigma = (\tilde{c}, \mathbf{z}, \mathbf{h})$

Verify$(pk, M, \sigma = (\tilde{c}, \mathbf{z}, \mathbf{h}))$

$\mathbf{A} \in R_q^{k \times \ell} := \mathsf{ExpandA}(\rho)$ ▷ $\mathbf{A}$ is generated and stored in NTT Representation as $\hat{\mathbf{A}}$
$\mu \in \{0,1\}^{512} := \mathrm{H}(\mathrm{H}(\rho \parallel \mathbf{t}_1) \parallel M)$
$c := \mathsf{SampleInBall}(\tilde{c})$
$\mathbf{w}_1' := \mathsf{UseHint}_q(\mathbf{h}, \mathbf{A}\mathbf{z} - c\mathbf{t}_1 \cdot 2^d, 2\gamma_2)$ ▷ Compute as $\mathtt{NTT}^{-1}(\hat{\mathbf{A}} \cdot \mathtt{NTT}(\mathbf{z}) - \mathtt{NTT}(c) \cdot \mathtt{NTT}(\mathbf{t}_1 \cdot 2^d))$
return $[\![\|\mathbf{z}\|_\infty < \gamma_1 - \beta]\!]$ **and** $[\![\tilde{c} = \mathrm{H}(\mu \parallel \mathbf{w}_1')]\!]$ **and** $[\![\#$ of 1's in $\mathbf{h}$ is $\leq \omega]\!]$

Figure 4: The pseudo-code for deterministic and randomized versions of Dilithium. The only difference between the two versions is in Line 12, where ρ' is either a function of the key and message, or is chosen completely at random.

양자내성암호 표준 알고리즘 (2025.1. 기준)

표준등재기관	알고리즘	비고
NIST (미국)	**ML-KEM (CRYSTALS-KYBER)**	암호화 (격자기반)
NIST (미국)	**ML-DSA (CRYSTALS-DILITHIUM)**	디지털서명 (격자기반)
NIST (미국)	SLH-DSA (SPHINCS+)	디지털서명 (해시기반)
TTA (국내)	**Ring-Lizard**	암호화 (격자기반)
TTA (국내)	HiMQ	디지털서명 (다변수이차식 기반)
KpqC 공모전	AiMer	디지털서명 (해시기반)

알고리즘 표준화

- NIST(미국 국립표준기술연구소) : 3개의 표준 알고리즘 게시
- TTA(한국정보통신기술협회) : 2개의 알고리즘 발표 (암호화/디지털서명)

NIST National Institute of Standards and Technology

TTA

보안업계 움직임

- 삼성SDS : KAIST 와 산학협력으로 해시기반 디지털 서명 알고리즘 에이머(AiMer) 개발
- 라온시큐어 : 자사제품에 PQC 일부 반영
- 드림시큐리티 : 양자내성암호모듈 개발
- 크립토랩 : 알고리즘 표준화 및 킨설팅

SAMSUNG SDS

HEAAN CRYPTO LAB

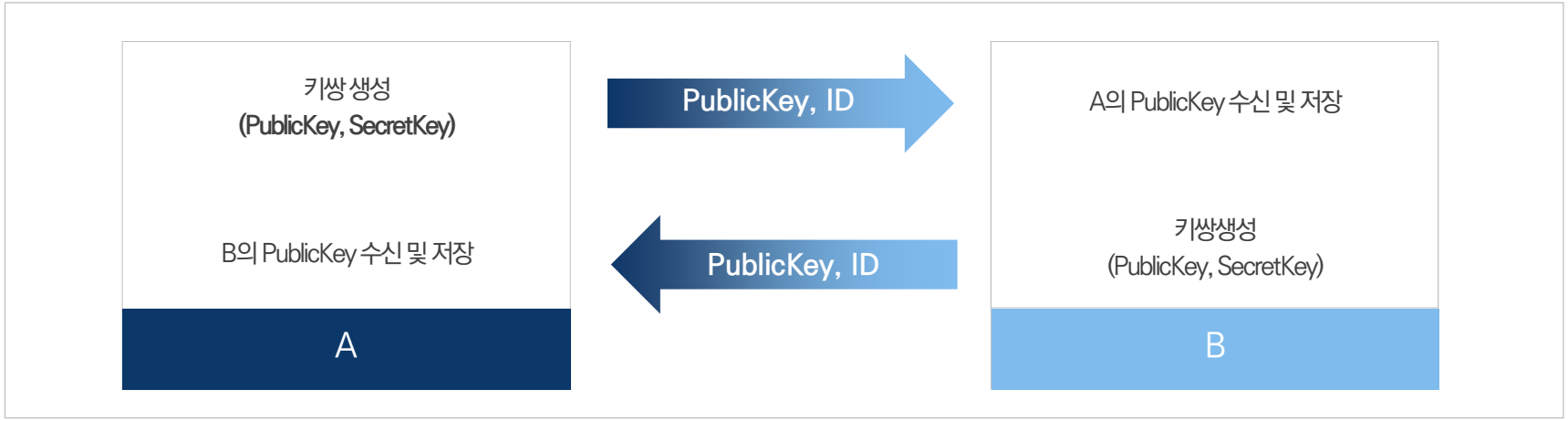
정부정책 움직임

- 검증필 암호모듈(KCMVP) PQC 알고리즘 대상 검토
- 국가기반의 PQC 인증서 발급체계 구축 프로젝트 시작
- 국방, 공공기관 PQC 도입 움직임

PQC 통신 방식 – 키 공유 과정

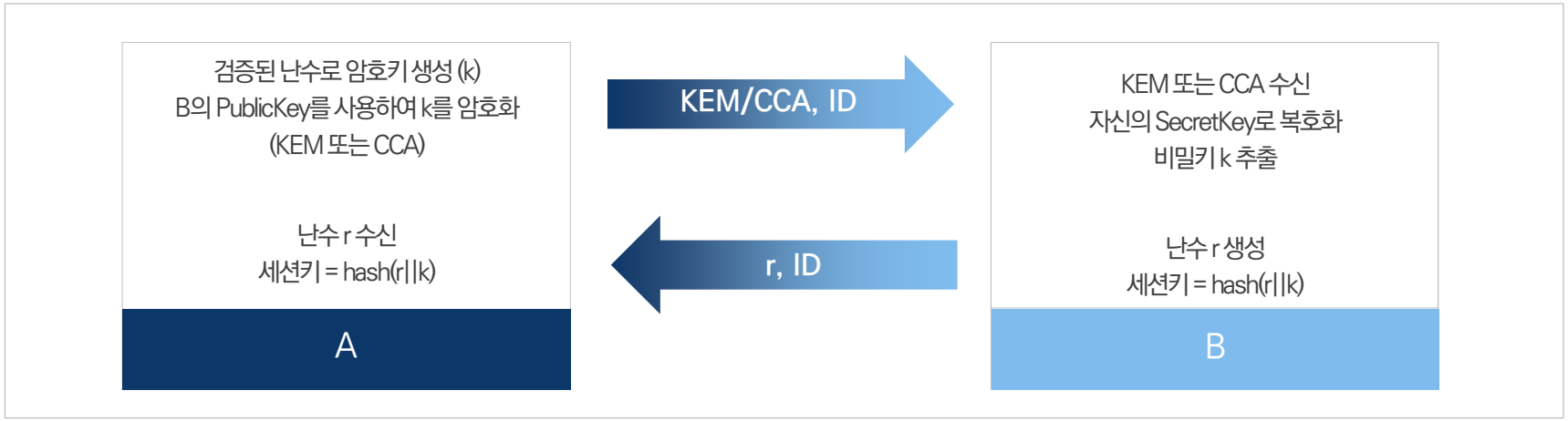
공개키 공유

- MLKEM / RLizard 방식
- MLDSA 도 동일
- 생성된 비밀키는 안전한 저 장소에 저장
- 상대방 공개키는 별도 DB 에 저장
- 인증서 형태로 전달(선택)
- 상호 키교환(선택)
- 사전에 보안파라미터 합의



암호키 공유

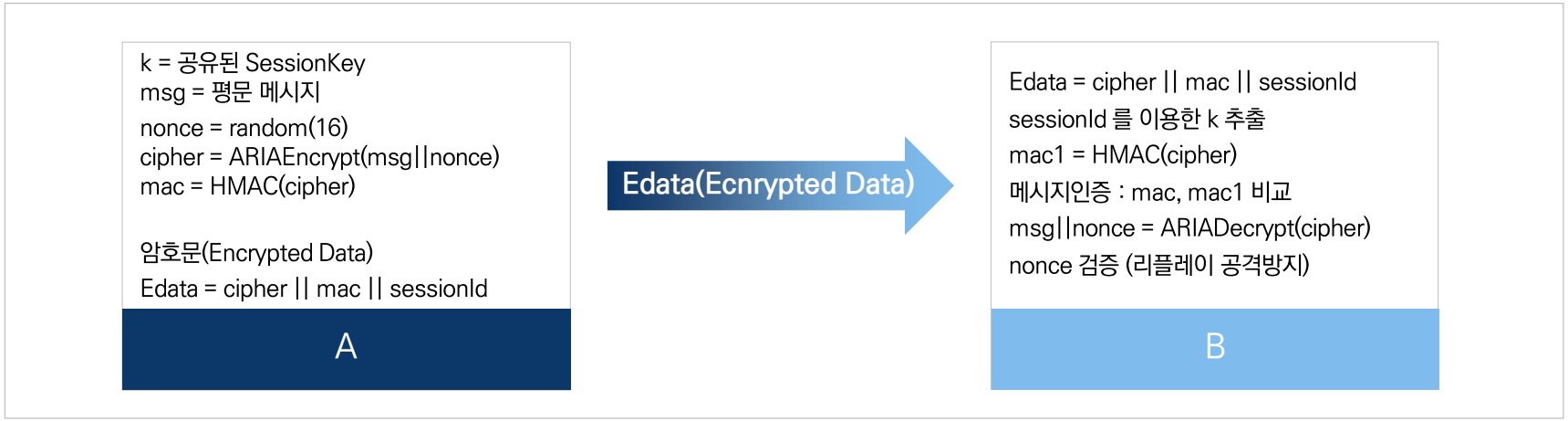
- MLKEM / RLizard 방식
- 상대방의 공개키로 암호키 를 암호화 하는 방식
- 추가난수고 세션키 생성
- 세션키 = 대칭키,IV,MAC 키로 구성
- 이후 암호통신은 세션키를 이용



PQC 통신방식 – 구간암호화 및 전자서명

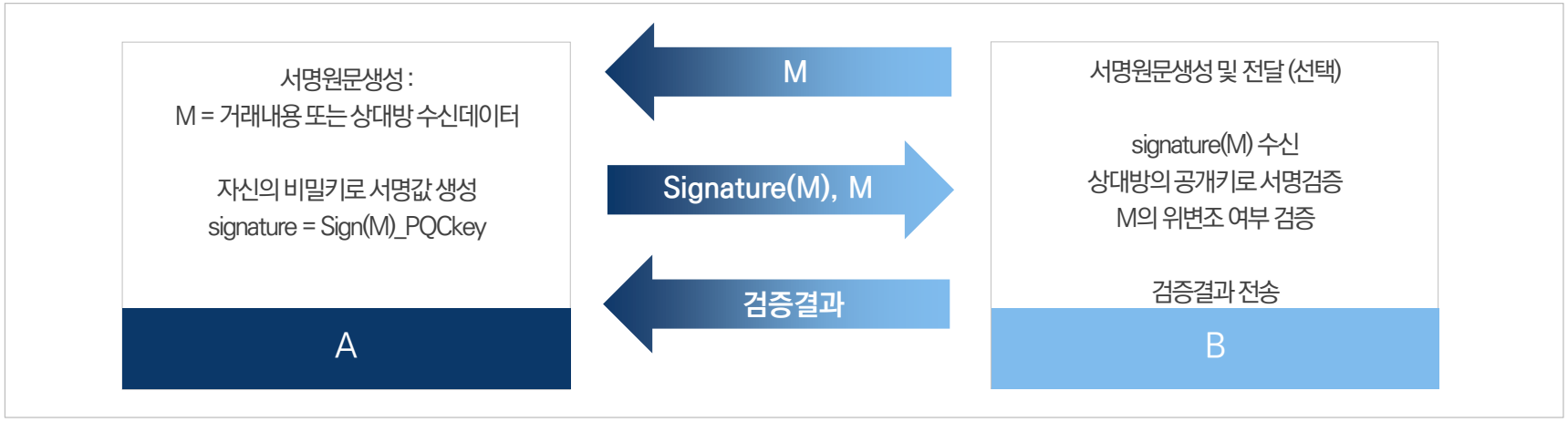
구간암호화

- MLKEM / RLizard
- 공유된 세션키를 이용하여 통신데이터를 암복호
- 메시지인증 코드 적용
- 리플레이 공격 방지
- A, B 는 같은 방식으로 암호문 생성/전달



전자서명

- MLDSA
- 자신의 비밀키로 전자서명 값 생성 및 전달
- 상대방의 공개키로 전자서명 검증
- 거래확인을 위한 Challenge-Response 방식 적용 가능
- 이후 거래증명을 위하여 서명값은 별도저장 권장
- 필요한 경우 인증서 이용



글로벌 표준화 및 국가별 로드맵에 따르면, 기업들은 2028년 이후의 안전한 기술 도입을 보장하기 위해 지금 즉시 양자내성암호(PQC)로의 전환을 시작해야합니다.

상용화 시기

상용화 시기

- 현재 양자컴퓨팅 기술의 발전 속도를 감안할 때 각국 주요기관 들은 양자내성 암호의 도입을 서두를 것을 제안함
- 미국 국립표준기술원(NIST) 은 주요기업들이 2028년까지 PQC 를 도입할 것을 권고
- 영국 사이버기관 NCSC는 최근 발표한 지침에서 기업에게 다음과 같이 권고
  - 2028년까지 취약한 시스템 식별
  - 2031년까지 중요 업그레이드 우선적 진행
  - 2035년까지 PQC로의 완전한 전환

알고리즘 표준화

표준화

- 현재 미국 중심으로 표준화가 진행
  - ML-KEM : 모듈격자기반의 표준 암호 알고리즘(FIPS203)
  - ML-DSA : 모듈격자기반의 표준 전자서명 알고리즘(FIPS204)
  - SLH-DSA : 해시기반의 표준 전자서명 알고리즘(FIPS205)
- 해시기반 알고리즘은 키사이즈, 서명사이즈가 크므로 특수 용도로 사용될 것으로 전망
- 국내 표준알고리즘(RLizard/HiMQ) 은 오래되어 4개의 신규 알고리즘으로 전환

와이키키소프트 개발 현황 및 전망

와이키키소프트

- 7개의 표준(국제 3개, 국내 4개) 알고리즘 개발:
  - **국제표준** : ML-KEM, ML-DSA, SLH-DSA
  - **국내표준**: NTRU+, Smaug-T, HAETAE, AIMer
- 안정성 및 성능최적화 작업중

관련 기사 (출처 : CSO)

NIST publishes timeline for quantum-resistant cryptography, but enterprises must move faster

News
Nov 13, 2024 • 6 mins

Encryption | Privacy | Security

NIST wants agencies to move off current encryption by 2035, but analysts say that enterprises cannot wait nearly that long; state actors are expected to achieve quantum at scale by 2028.

Credit: Shutterstock

The US National Institute of Standards and Technology (NIST) on Tuesday published its timetables for moving government agencies off current types of encryption onto what they hope will be quantum-resistant encryption by 2035. But analysts urge enterprises to move much more quickly, given that state actors are expected to achieve quantum at scale by 2028.

Mark Horvath, a Gartner VP analyst who tracks both quantum and cryptography, said the urgency for enterprises to move away from current encryption techniques is real. IBM has said it expects to have a 200-qubit quantum computer by 2030 and, Horvath said, "We assume that state actors are two years ahead of where the commercial vendors are."

In October, a research team in China was reported to have already broken RSA encryption via quantum, albeit not at scale.
In the newly published document, NIST distinguished between agencies getting rid of existing encryption entirely and just starting to scale it back. It used the term "deprecated" to mean that "the algorithm and key length/strength may be used, but there is some security risk. The data owner must examine this risk potential and decide whether to continue to use a deprecated algorithm or key length." It used the more stringent "disallowed" to describe the outright ban of the use of "the algorithm, key length/strength, parameter set, or scheme."

증가하는 시장의 요구와 산업 전반의 채택 흐름에 발맞추어, 전문적인 기술 이전 서비스를 통해 양자내성암호(PQC)의 상용화를 가속화하겠습니다.

〈 컨설팅 사업 추진 방향〉

PQC가 필요한 국내 유관업체 대상으로 기술 이전 및 컨설팅 진행
전자상거래 등 웹서비스에서 사용하는 TLS의 PQC 모듈화 판매

사업 배경

- 양자내성암호 기술이 이슈화 됨에 따라 국내 유관 보안업체 및 웹서비스 업체들의 관심 증폭
- 국내정보보안기업 814개 (2024년 기준) : PQC 기술적 내재화의 어려움, 고비용 부담

시장 동향

- 한컴위드, 드림시큐리티, 라온시큐어 등 국내 보안 상장사 중심으로 양자내성암호 솔루션화
- **삼성전자** – 갤럭시 S 시리즈에 PQC 기능을 탑재하여 사용자 데이터 보호
- **SK텔레콤**– 국내 최초 글로벌 VPN PQC 상용화

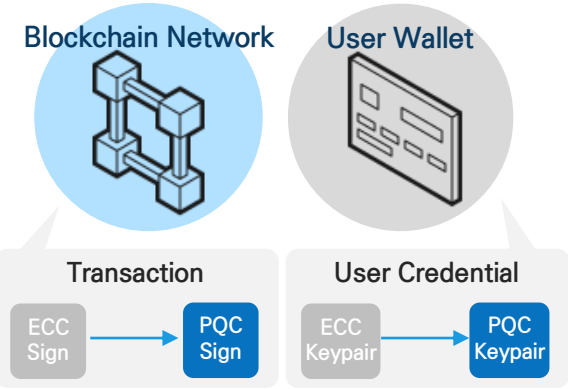
시장 규모

- 국내 정보보안 기업 800개 x 3천만원 = 240억원.
- 지속적인 모듈 업데이트를 통한 캐시플로우 발생

검증된 블록체인 전문성과 PQC 도입의 시급성을 바탕으로, 디지털 자산의 미래를 보호하기 위한 안전한 PQC 기반 환경 구축을 선도하고자 합니다.

〈 블록체인 사업 방향〉

블록체인 핵심 기술 대체 : 트랜잭션 서명 및 지갑 구조를 위한 양자내성기술 개발
PQC 기반 메인넷 구축 : 양자내성암호 기술이 적용된 자체 블록체인 메인넷 개발



배경

- 현재 대부분의 암호화폐는 공개키 암호화(ECC 기반) 방식을 사용
- 양자컴퓨터로 개인키 추출하여 트랜잭션의 위조와 이중 지불 문제 발생

기술 동향

- 유용한 양자컴퓨터가 나오려면 20년이 걸릴 것으로 예상한 젠슨황의 발표를 포함하여 지금 양자내성암호를 적용하는 것이 시기상조라는 분위기와 이에 반하여 양자컴퓨터의 등장은 2030년 보다 빠를 것이며 모스카 부등식에 근거하여 지금 적용하는 것이 적절하다는 의견으로 나뉘고 있음.

블록체인 개발역량

- 화이트박스 기반의 거래소 오픈
- 지갑 구조 연구
- 사설 블록체인 개발(하이퍼페브릭) 등의 경험 보유
- 메인넷 개발팀 구성 네트워크 보유 (투자유치후 결성)

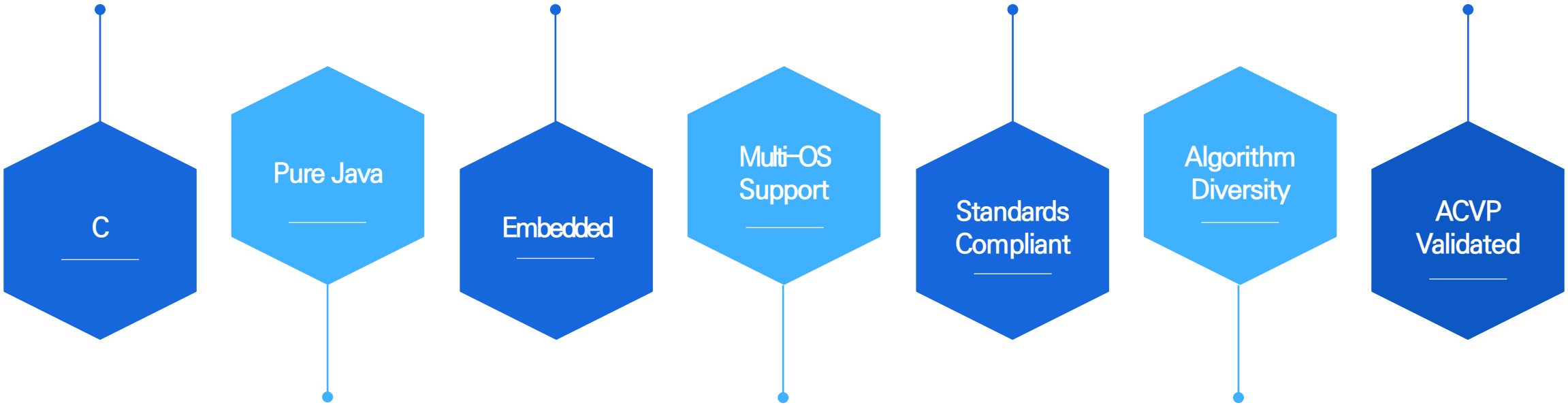
범용적이고 표준을 준수하며, 미래 지향적인 PQC 모듈 제공

순수 C언어로 작성되어 플랫폼간 이식성이 뛰어나며 최적화된 성능 발휘

제한된 환경에서도 동작할 수 있도록 메모리 사용량 최소화

NIST PQC 표준 및 최신 암호화 가이드라인 준수

NIST ACVP 자체 테스트를 통해 안전성 상호 운용성 인증



JNI없이 순수 JAVA로 구현되어 통합이 용이하고 높은 보안성

주요 운영체제와의 호환으로 기존 시스템에 즉시 도입 가능

국내/외 표준 7종 등 PQC 알고리즘 제공

철저한 개발 과정과 공신력 있는 검증, 수치로 증명된 결과를 바탕으로 신뢰를 제공합니다.

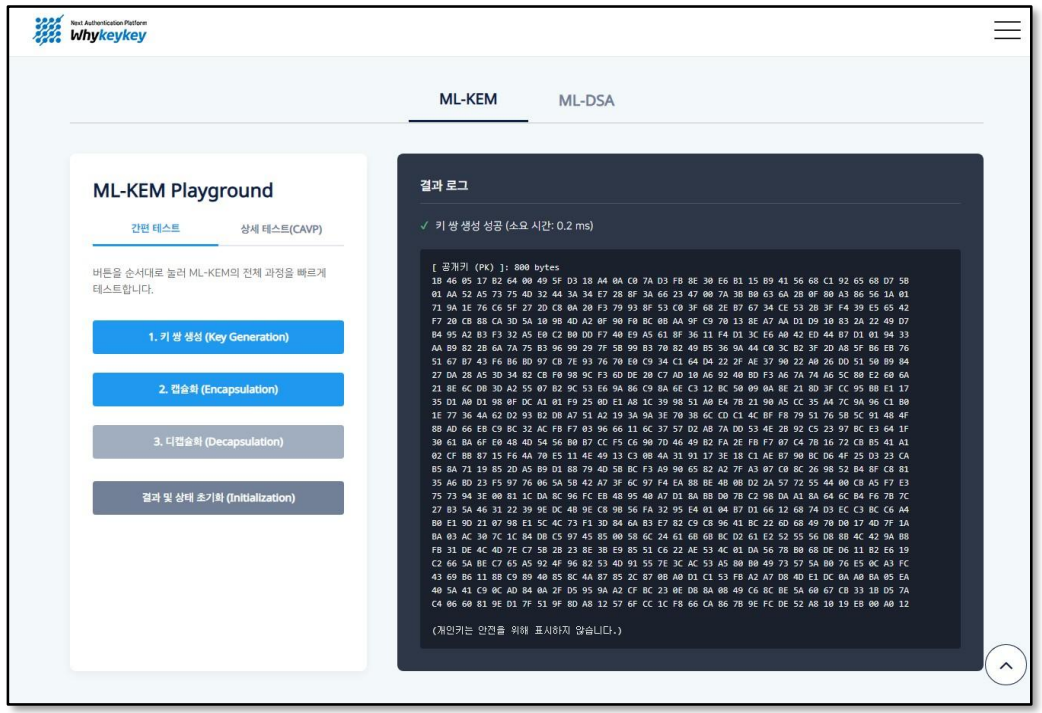
알고리즘 개발 역량

- 국제 표준 알고리즘: ML-KEM, ML-DSA, SLH-DSA 등 국제 표준 완벽 구현
- 국내 표준알고리즘: NTRU+, SMAUG-T, HAETAE, AIMER 알고리즘 구현 완료
- 국내 유일 C/JAVA 동시 개발된 PQC 모듈로, 최적의 솔루션 제공

Playground 테스트 환경 제공

- PQC 암호모듈 테스트 페이지 제공.
- 실시간 연산 시간 및 결과 제공

WhykeykeySoft PQC Playground (Click image to try)



PQC 원천 기술 개발사로서의 독보적인 전문성을 바탕으로, 우리는 새롭게 등장하는 글로벌 표준을 충족하고 가장 엄격한 보안 인증을 획득하도록 설계된, 미래에도 안전한 암호모듈을 만들어가고 있습니다

01 기술 로드맵

Continuous Innovation

- Expanding Algorithm Portfolio
  - ▸ 현재 KpqC 표준을 위한 4개 알고리즘 추가 개발 완료
  - ▸ 이를 통해 국내외 표준화 동향의 최전선 유지
- Enhanced Performance & Features
  - ▸ 성능 최적화 및 신기술(IoT, 블록체인 등) 융합을 위한 지속적인 R&D

02 시장 전략

Securing Leadership

- Targeting KCMVP Certification
  - ▸ 최종 알고리즘 발표 즉시 KCMVP 인증 준비 착수.
- Market Expansion & Dominance
  - ▸ 공공 : 공공기관 PQC 도입 의무화 예상, 시장 기회 선점. KpqC 준비를 통해 주요 공급자로 자리매김.
  - ▸ 민간 : 기존 모든 보안 제품에 대한 양자내성암호로의 원활한 업그레이드 제공.

03 핵심 경쟁력

Unmatched Expertise

- Fundamental Technology Ownership
  - ▸ 와이키키소프트는 자체 원천 기술을 기반으로 양자내성암호를 독자 개발한 국내 유일의 기업.
  - ▸ 이러한 깊이 있는 전문성은 고객에게 뛰어난 유연성, 지원, 그리고 장기적인 신뢰성을 보장.

Next Authentication Platform
Whykeykey

A. 55, Seongsuil-ro 8-gil, Seongdong-gu, Seoul, Korea

T. +82 2-576-4746

W. www.whykeykey.com

감사합니다