THALES

암호화 민첩성과 양자 컴퓨터의 위협

존 레이(John Ray)

Director, HSM Product Management

양자 경쟁의 시작







Microsoft

Google

rigetti

IBM

D:wave
The Quantum Computing Company™

IONQ

intel

Honeywell

THALES

양자 컴퓨팅에 주목해야 하는 이유

공개 키 인프라를 통한 신뢰 구축

- TLS, IPSEC, SSH, S/MIME...
- Microsoft RMS와 같은 정보 권한 관리 솔루션
- 소프트웨어 무결성을 유지하는 코드 서명 기술
- 진위 여부를 입증하는 문서 서명 솔루션

비대칭 키 프로토콜을 이용하는 PKI

- RSA, ECC 등

양자 컴퓨터 및 연구를 통한 PKI 및 코드 서명의 효율적인 해독

- 예측 불가능한 미래

기존의 "방식"을 유지할 수 있는 양자 내성 암호화(QRC)

- 현재 사용 중인 QSC 알고리즘과 키를 계속 사용할 수 있는 암호화 민첩성 제품

THALES

양자 컴퓨터가 암호화에 미치는 영향

그로버

1

암호화 알고리즘	유형	목적	대규모 QC의 영향
AES	대칭 키	암호화	길이가 긴 키 사용
SHA-2, SHA-3	----------	해시 함수	더 큰 출력값 반환

쇼어

2

암호화 알고리즘	유형	목적	대규모 QC의 영향
RSA	공개 키	서명, 키 설정	더 이상 안전하지 않음
디지털 서명 알고리즘	공개 키	서명, 키 교환	더 이상 안전하지 않음
ECDSA(타원 곡선 디지털 서명 알고리즘)	공개 키	서명, 키 교환	더 이상 안전하지 않음

한 줄 요약

양자 내성 암호화가 적용되지 않으면 네트워크를 통해 전송되었거나 전송될 모든 것이 도청과 공개에 취약해집니다.

— ETSI 백서 No. 8 양자 보안 암호화 및 보안

THALES

고위험: 인증된 소프트웨어

위험 대상

현장 수명이 길고 내구성이
뛰어난 연결 장치(IoT)

공격의 종류

양자 컴퓨팅을 이용하는
공격자에 의한 **위변조 된**
소프트웨어 업데이트

THALES

고위험: 비밀 통신

VPN 세션

핸드세이크

데이터 교환

쇼어 알고리즘을 이용한 양자 공격

키 설정

개인 키 획득

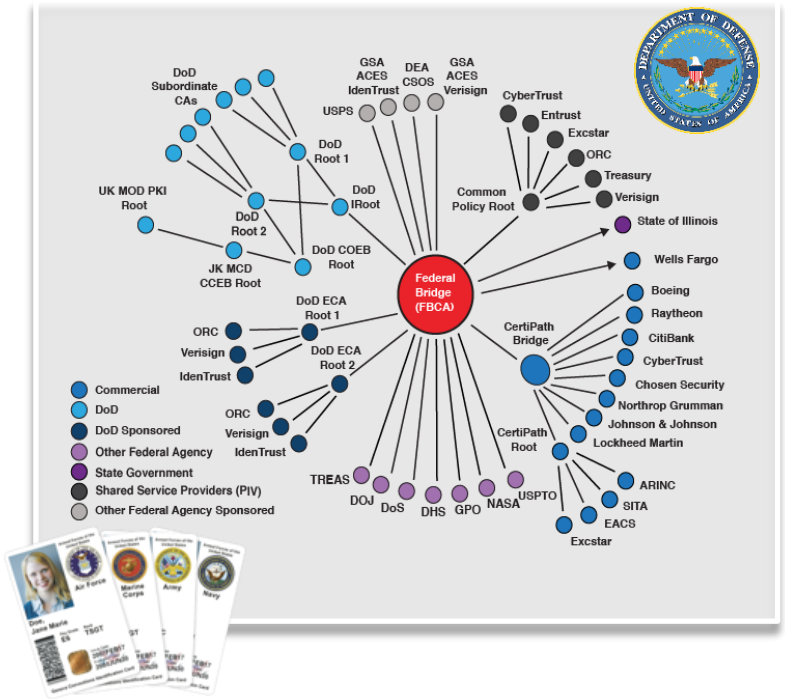
암호문

추출한 키를 이용한 해독

평문

THALES

고위험: 디지털 신원



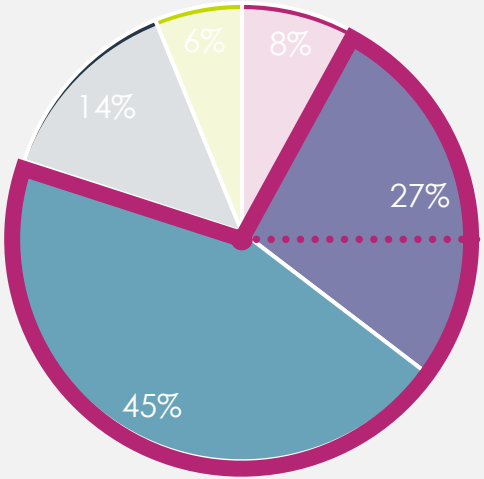
DoD 신원 관리 시스템은
450만 명 이상의 실사용자
를 보유하고 있습니다.

양자 보안 이중 인프라를 구축하는 것은 많은 시간과 비용이 소요되는 작업입니다.

THALES

양자 암호화가 조직에 영향을 미칠 것으로 예상되는 시기는?

2020 데이터 위협 보고서: 양자 암호화가 조직에 영향을 미칠 것으로 예상되는 시기



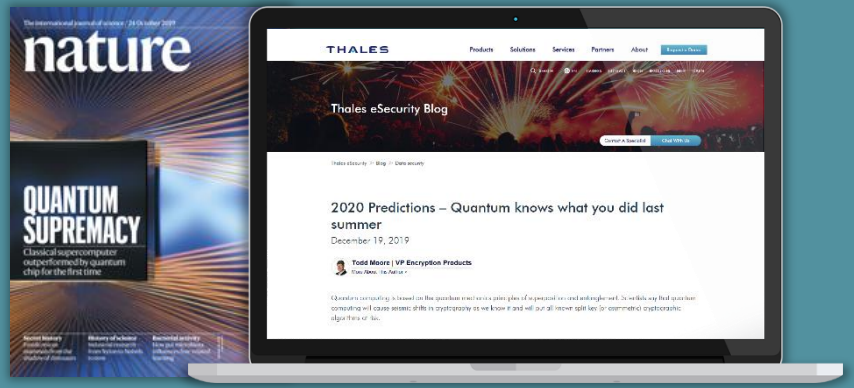
72%

향후 5년 이내에 조직에 영향이 있을 것이라고 답한 비율

N = 1,723 Q38. 양자 암호화가 귀사의 조직에 얼마나 빨리 영향을 미칠 것[illegible]고 생각하십니까?
Base=전체 응답자 출처: 2020 탈레스 데이터 위협 보고서, IDC, 2020년 12월

불과 **8%**

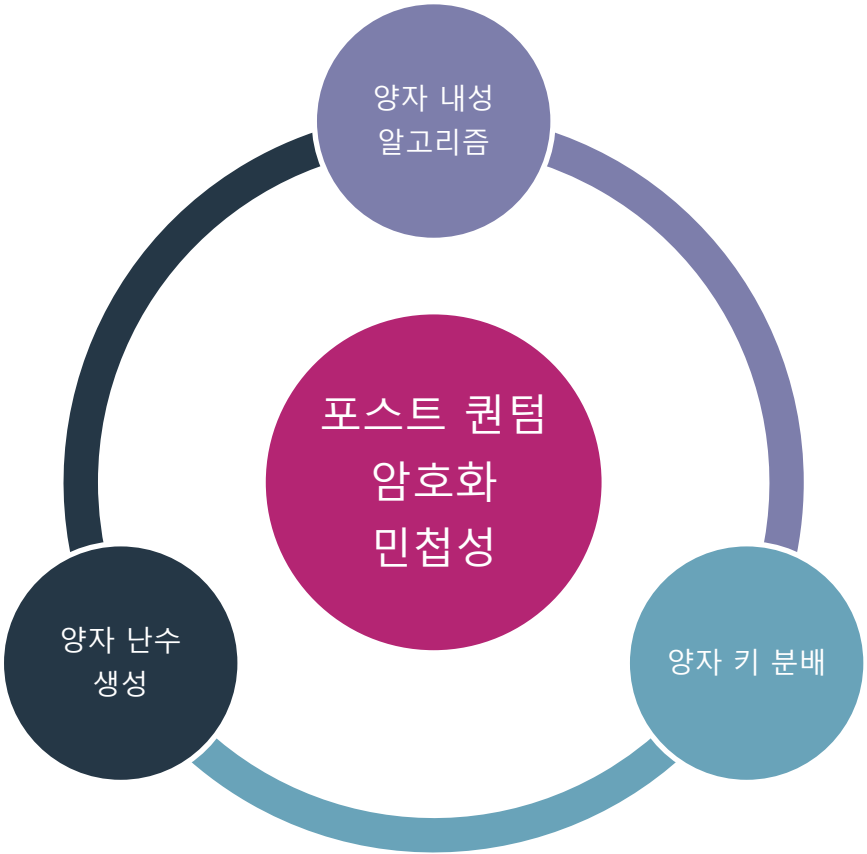
의 응답자만이 양자 암호화로 인해 조직이 영향을 받는 일은 "절대" 없을 것이라고 답했습니다.



THALES

대처방안

미래에 대비한 양자 전략 수립



THALES

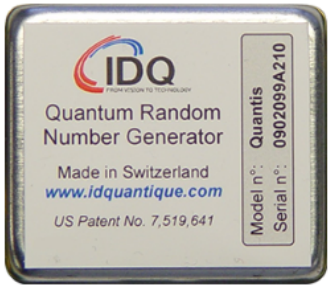
양자 방어: 양자 엔트로피

고비트율의 난수 소스

양자역학 고유의 무작위성 활용

이용 사례

- 암호화 키
- 온라인 게이밍



Quantis RNG OEM Component

HARDWARE RANDOM NUMBER GENERATOR EXPLOITING QUANTUM PHYSICS

Quantis provides instant entropy for high quality encryption keys and random draws right from boot up

- **True hardware random number generator (RNG)**
- **Uses quantum optics process to create true quantum randomness (passes all randomness tests)**

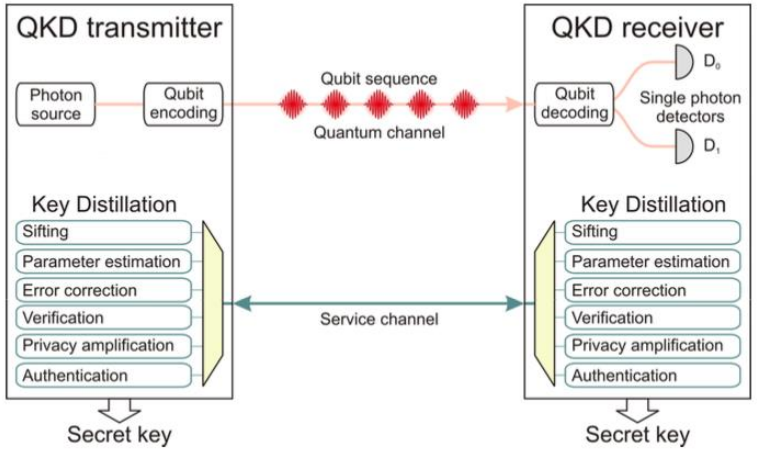
Swiss made and tested

- **Highly resilient to environmental perturbations**
- **High bit rate of 4Mbits/sec**
- **Affordable, compact and reliable**
- **Continuous status check and verification**

THALES

양자 방어: 양자 키 분배

- 양자역학의 특성 활용
- 키 공유에 대한 근본적으로 다른 접근 방식
- 수학이 아닌 물리학 원리에 따른 키 분배



- QKD 네트워크의 존재
  - ETSI QKD 사양

NEW QUANTUM PROJECT AIMS FOR ULTRA-SECURE COMMUNICATION IN EUROPE

Today marks the launch of a pilot project, OPENQKD, that will install a test quantum communication infrastructure in several European countries. It will boost the security of critical applications in the fields of telecommunications, health care, electricity supply and government services.

Press release from European Commission
September 3rd 2019 | 464 readers

THALES

양자 방어: 양자 내성 알고리즘(QRA)

새로운 알고리즘 유형

- 래티스 기반 암호화
- 다변수 암호화
- 해시 기반 암호화
- 코드 기반 암호화

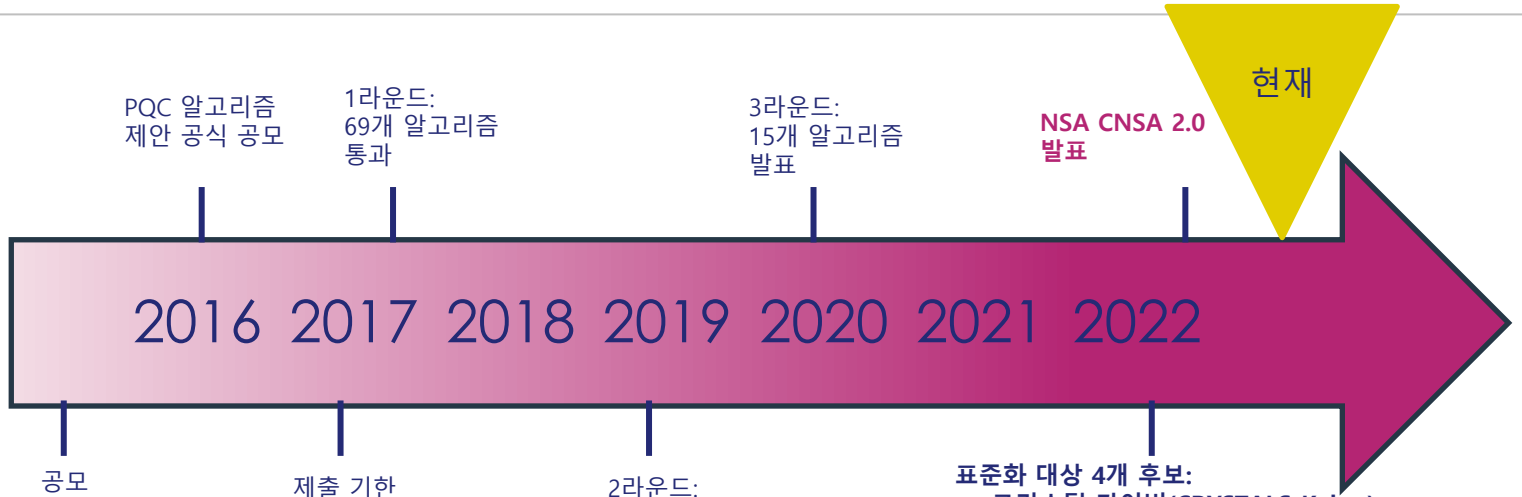
기존 알고리즘과 다른 작동 방식

- 키 크기, 패딩 체계, 대기 시간, 성능

필요한 것:

- 모든 알려진 공격과 향후 벌어질 **전형적인** 공격으로부터 보호
- 모든 알려진 공격과 향후 벌어질 **양자** 공격으로부터 보호

NIST 표준화 프로세스



표준은 2024년 발표 예상

* **팔콘**은 프랑스(렌1대학, PQ실드 SAS), 스위스(IBM), 캐나다(NCC 그룹) 및 미국(브라운 대학, 퀄컴)에 소재한 학계 및 산업 파트너와 함께 탈레스가 후원하여 공동으로 개발했습니다.

THALES

NSA CNSA 2.0 제안

2022년 9월 7일 발표

- 일반 암호화
  - 크리스털 카이버
- 디지털 서명
  - 크리스털 딜리슘(래티스)
- SW/FW 업데이트
  - LMS/XMSS(SP 800-208)

시기?

- SW/FW 서명 전환 곧 시작 예정
- 2025년까지 새로운 알고리즘을 사용하여 서명하는 새로운 SW/FW 진행
- 2035년 전환 완료 예정

* https://media.defense.gov/2022/Sep/07/2003071834/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS_.PDF

THALES

하이브리드 접근 방식 채택

NIST 제안:

- 암호화 민첩성 플랫폼을 활용해 원활한 전환을 구현하는 하이브리드 접근 방식

실제:

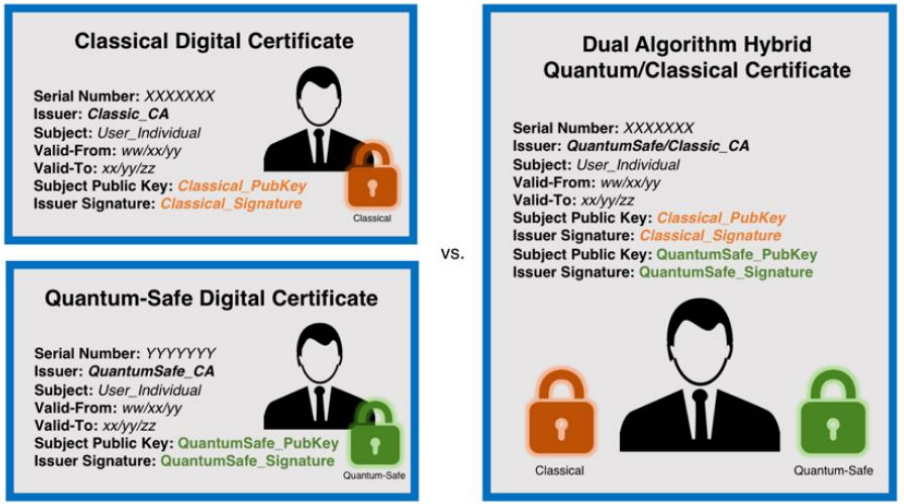
- RNG – QRNG를 NIST 인증 RNG와 결합
- 알고리즘 - 기존 알고리즘과 QRA를 이용한 대체 모드 지원

전환:

- 표준 승인 후 구현 및 재인증

양자 보안 하이브리드 다중 키 인증서 메커니즘

- 다수의 인증서
- 하이브리드 v3 익스텐션
- 복합 연결 키



크레딧: https://www.isara.com/cryptographic-certificates-quantum-safe/

THALES

Thales CPL – 양자 협업

THALES

상용화된 양자 보안 솔루션, Luna HSM

Luna PQC FM이 적용된 양자 내성 알고리즘

양자 보안 키를 **보호**하는 HSM

- 하드웨어 RoT를 이용한 **디지털 서명** 수행
- 해시 기반 서명 체계(SP 800-208)
- HSS – Hierarchical Signature Scheme(LMS의 다중 트리 버전)
- XMSS – Extended Merkle Signature Scheme
- XMSSMT – XMSS Multi-Tree
- 크리스털 딜리슘 서명
- 크리스털 카이버 키 캡슐화

ISARA

Luna HSM 맞춤형 양자 구현

- **Luna의 FM(기능 모듈)을 이용한 자체 포스트 퀀텀 암호화 메커니즘 구현**
- **파트너 FM 활용**

CRYPTONEXT SECURITY

OQS

IRONCAP

Luna HSM을 이용한 QRNG

- QRNG 및 Luna HSM의 보안 키 저장소를 통한 양자 엔트로피 주입
- 고품질의 난수가 절대적으로 중요한 응용 프로그램 처리

IDQ

QUANTINUUM

THALES

Luna HSM의 양자 접근 방식

탈레스 Accelerate Technology 파트너와의 협력

- 통합, API
- PKI 인증서 모델

표준 기관과의 협력

- 오아시스(PKCS#11)

코드 서명 권장 사항 충족을 위한 노력

- 표준 메커니즘(SP800-208)

시장 수요에 따른 4개 최종 후보 추가

- 크리스털 딜리슘
- 크리스털 카이버
- 팔콘, 스핑크스+
- **표준화가 되어있지 않아 사용 시 위험이 있습니다!**

표준화 후 FIPS 인증

아직 끝난 것이 아닙니다. 암호화 민첩성을 유지해야 합니다!

- BSI(독일)는 프로도켐(FrodoKEM)과 클래식 맥엘리스를 권장

THALES

상용화된 양자 보안 솔루션, HSE

양자 내성 알고리즘

QRA 지원을 위한 프레임워크

양자 키 분배

10년 이상 QKD를 지원해 온 HSE

QRNG

HSE 솔루션에 통합된 QRNG

THALES

퀀텀 위험성 평가

CYBER SECURITY AND FRAUDTECHNOLOGY INNOVATIONS

A Methodology for Quantum Risk Assessment

Authors: Dr. Michele Mosca, John Mulholland

Related Project: Quantum Threat and Mitigation

By Use Case | Data Protection | Cloud Security | PKI Security Solutions | PKI Credential Management | Data Security & Encryption | Access Security | Digital Transformation | Payment & Transactions | Quantum | IoT Security | Software Monetization | Zero Trust Security

Are You Post-Quantum Ready?

Although post-quantum is projected to be a few years away, an enterprise must start planning today to be post-quantum ready. Take this free risk assessment to learn if your organization is at risk of a post-quantum breach.

THALES

핵심 요약

양자 시대의 도래

- 양자 기능이 점차 가속화되고 있습니다.
- NIST는 양자 보안 표준의 마무리 단계에 있습니다.
- PKI 기반 암호화는 폐기될 것입니다.

위험 파악

- 기존 기술을 사용하면 장기 데이터에 위험을 초래합니다.
- 수집 및 초기 공격에 대한 취약성을 고려하십시오.

암호화 민첩성에 집중

- 암호화 민첩성 모범 사례를 지원할 인프라가 필요합니다.
- 기존 및 양자 보안 암호화 솔루션을 적용해 하이브리드 접근 방식을 취하십시오.

지금 바로 시작

- 암호화 민첩성 성숙도와 준비 상태를 평가하십시오.
- 양자 보안 아키텍처를 설계하십시오.
- 표준 확립 후에도 변화에 대비하십시오.

탈레스는 당사의 솔루션과 파트너십을 바탕으로 고객의 양자 보안 이니셔티브를 지원합니다.

THALES

THALES

감사합니다.

cpl.thalesgroup.com

탈레스 양자 리소스

웹 및 PQ 암호화 민첩성 위험 평가

- 포스트 퀀텀 암호화 민첩성 웹페이지
- 포스트 퀀텀 암호화 민첩성 위험 평가

백서

- 백서: 탈레스 Luna HSM 및 탈레스 HSE를 이용해 기존 보안 시스템을 민첩한 양자 보안 솔루션으로 업그레이드하기

인포그래픽

- HSE 암호화 민첩성 인포그래픽

PR

- 탈레스는 조직이 양자 컴퓨팅이 야기하는 미래의 보안 위협에 대처할 수 있도록 지원합니다. 2019년 8월 5일.
- 양자 컴퓨팅 시대가 도래함에 따라 디지서트, 젬알토, ISARA가 사물 인터넷(IoT)의 안전한 미래를 보장하기 위해 파트너십을 체결했습니다. 2018년 9월 20일.

웨비나

- 양자 보안 서명으로 수명이 긴 IoT 장치의 미래에 대비하기
- Quantum ISC² 준비하기
- 양자 위협의 난제: 양자 보안 전략 수립 방법

THALES