비양자내성암호 알고리즘 탐지 동향

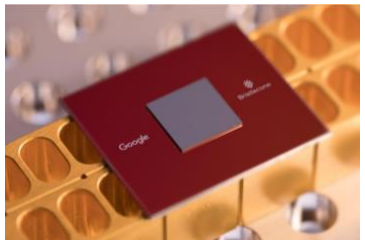
2025. 07.16

성신여자대학교 김수리

Contents

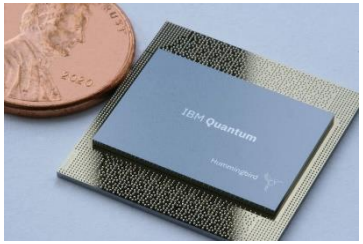
Introduction [1/13]

- 양자 컴퓨팅 기술 현황



Google 72-qubit chip
"Bristlecone"
March 2018

IBM 20-qubit quantum computer
"Q System One"
January 2019
(53-qubit, September 2019)



IBM 65-qubit chip
"Hummingbird"
August 2020

IBM 1121-qubit chip
"Condor"
December 2023

Introduction [2/13]

- 암호에 영향을 미치는 양자 알고리즘

Grover's Algorithm

- Quantum algorithm that finds specific member in unstructured dataset
- Classical computation : $O(N)$ operation
- Grover's algorithm : $O(N^{1/2})$ evaluation
- 키 공간의 복잡도를 안전성의 기반으로 두는 대칭키 암호에 영향

Shor's Algorithm

- Quantum algorithm for integer factorization
- Complexity
  - GNFS : $\exp\left(\left(\sqrt[3]{64/9}+o(1)\right)(\ln n)^{\frac{1}{3}}(\ln\ln n)^{\frac{2}{3}}\right)$
  - Shor : $O((logN)^2(\log\log N)(\log\log\log N))$
- 주기를 찾는 알고리즘으로 RSA, DSA, ECC 에 적용 가능

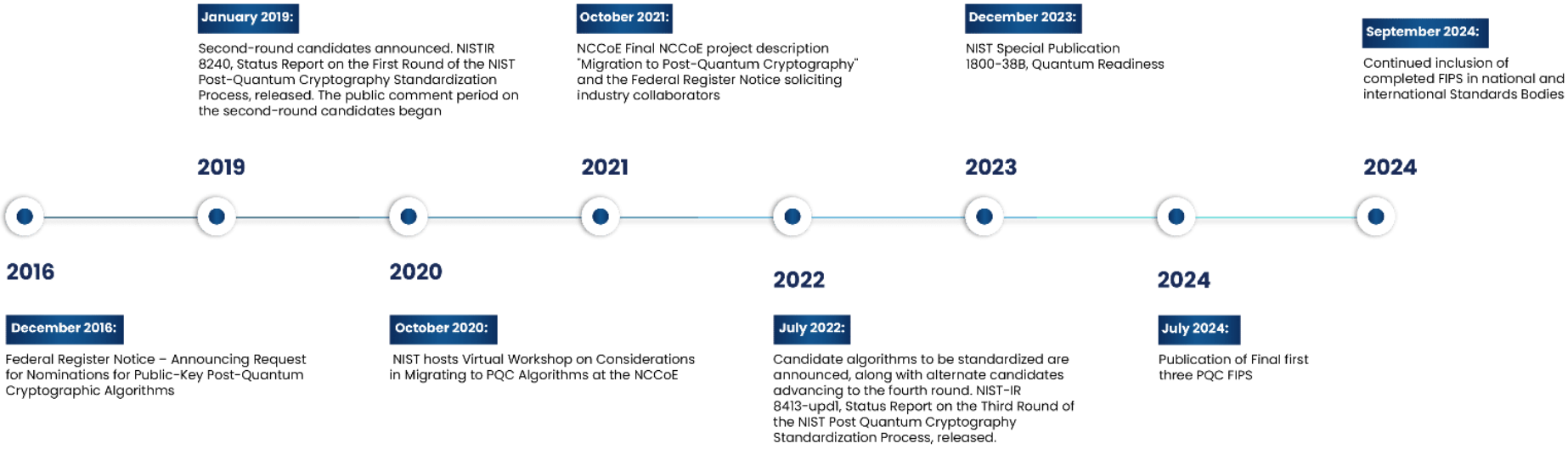
Introduction [3/13]

- Impact on cryptography
  - NIST plans for the future
    - Reports on Post-Quantum Cryptography" –NISTIR 8105, April 2016
    - 대칭키/해시 ➔ 키 사이즈 및 출력값 증가
    - 공개키 ➔ PQC로의 전환 필요

Type	Cryptographic Algorithm	Purpose	Impact
Symmetric Key	AES	Encryption	Larger key size needed
	SHA2 SHA3	Hash function	Larger output needed
Public Key	RSA	Signature/ Key establishment	**NO LONGER SECURE**
	ECDSA, ECDH	Signature/ Key exchange	
	DSA	Signature/ Key exchange	

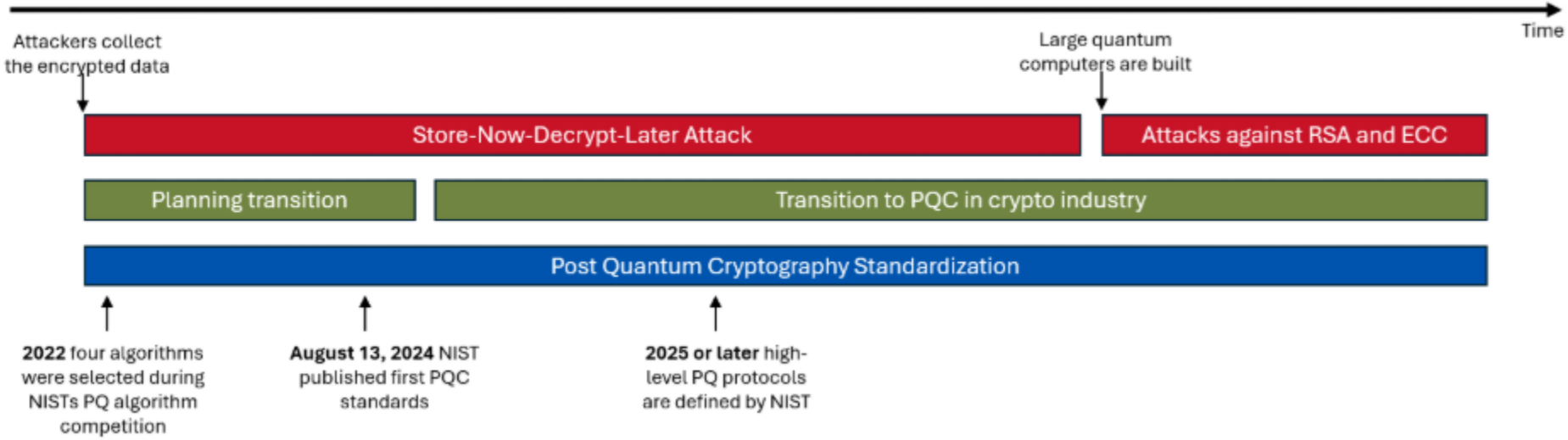
Introduction [4/13]

- NIST PQC Standardization project



Introduction [5/13]

- PQC로의 전환
  - Post-quantum cryptography timeline



https://www.intel.com/content/www/us/en/developer/articles/technical/post-quantum-cryptography.html

Introduction [6/13]

- PQC로의 전환
  - 양자 컴퓨팅 환경으로 인해 기존의 암호 알고리즘 사용에 변화가 필요
    - 대칭키/해시 ➔ 키 길이 증가, 출력값 증가
    - 공개키 ➔ PQC 암호로 전환
  - 현재 정보 시스템은 다양한 플랫폼 위에서 운영되고 있으며, 이 시스템 내에는 양자 컴퓨터에 취약한 고전 암호 사용
    - 웹 브라우저, 운영체제, 펌웨어, IoT 기기, 네트워크 장비 등 …
  - **이를 수동적으로 탐지하는데 한계가 존재**

실제 운영환경에서 비양자내성암호를 효율적으로 탐지할 수 있는 기술 및 도구 개발 필요

Introduction [7/13]

- Quantum Computing Cybersecurity Preparedness ACT H.R. 7535
  - 2022년 미국 백악관에서 양자 보안에 대한 체계적 대응을 위해 법제화
  - 현재 사용중인 정보기술 자산 중 양자컴퓨팅에 취약한 요소 파악하고 이를 인벤토리화하여 지속적으로 관리해야함을 명시

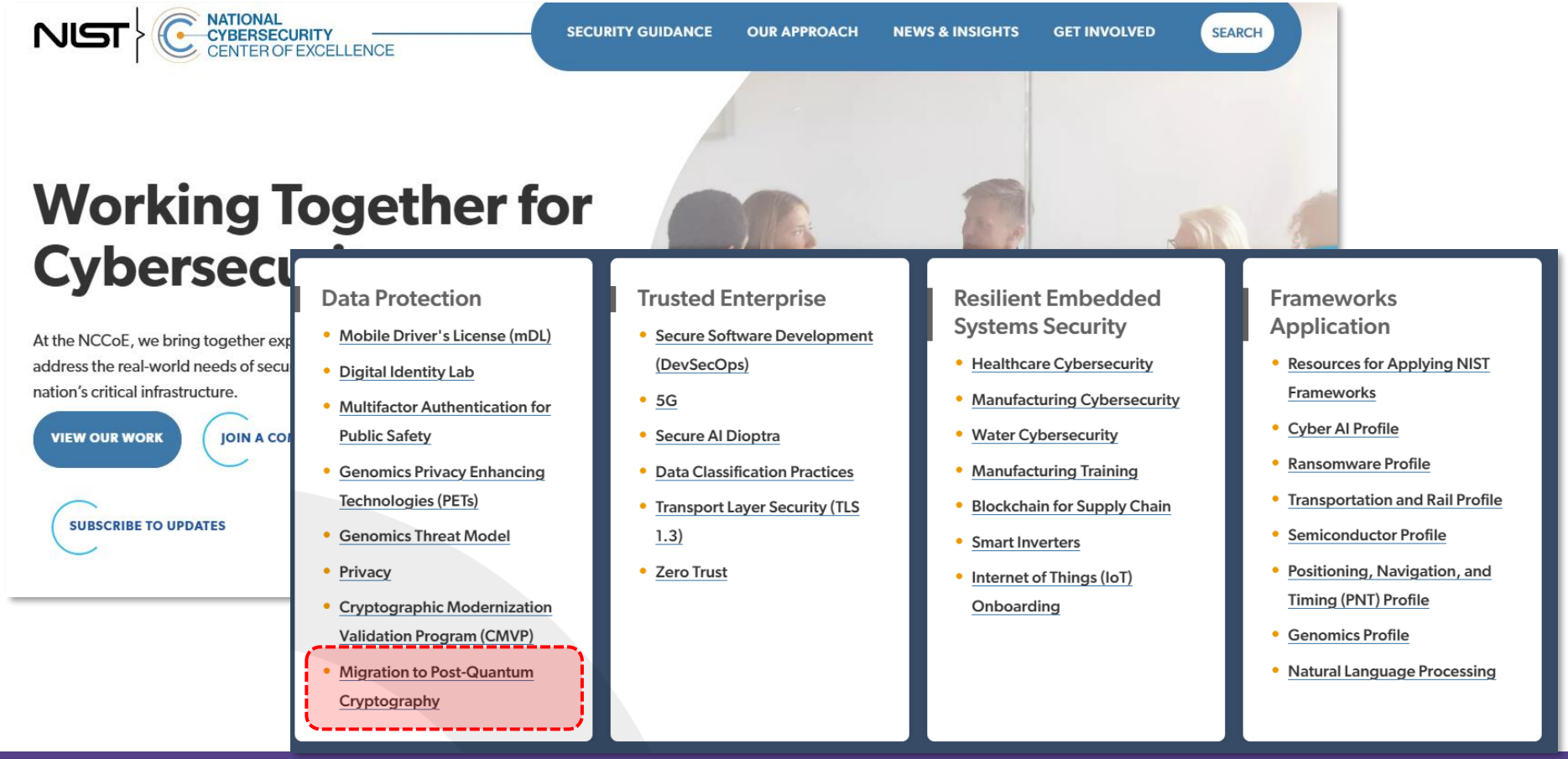
(a) Findings.--Congress finds the following:
(1) Cryptography is essential for the national security of the United States and the functioning of the economy of the United States.
(2) The most widespread encryption protocols today rely on computational limits of classical computers to provide
(4) The rapid progress of quantum computing suggests the potential for adversaries of the United States to steal sensitive encrypted data today using classical computers, and wait until sufficiently powerful quantum systems are available to decrypt it.

양자컴퓨터 기반 암호해독에 취약한 정보기술을 파악하고 migration 하는 지침 필요
- **요구사항 : 취약한 정보기술 목록 수립**
- **지침 추가 사항 : 우선순위 마련, 최대한 자동화 강조**

(a) Inventory.--
(1) Establishment. <<NOTE: Deadline. Guidelines.>> --Not later than 180 days after the date of enactment of this Act, the Director of OMB, in coordination with the National Cyber
CISA, shall
chnology to
a minimum--
ement for each
nt inventory of
information technology in use by the agency that is vulnerable to decryption by quantum computers, prioritized using the criteria described in subparagraph (B);
(B) <<NOTE: Criteria.>> criteria to allow agencies to prioritize their inventory efforts; and
(C) a description of the information required to be reported pursuant to subsection (b).
(2) Additional content in guidance.--In the guidance established by paragraph (1), the Director of OMB shall include, in addition to the requirements described in that paragraph--
(A) a description of information technology to be prioritized for migration to post-quantum cryptography; and

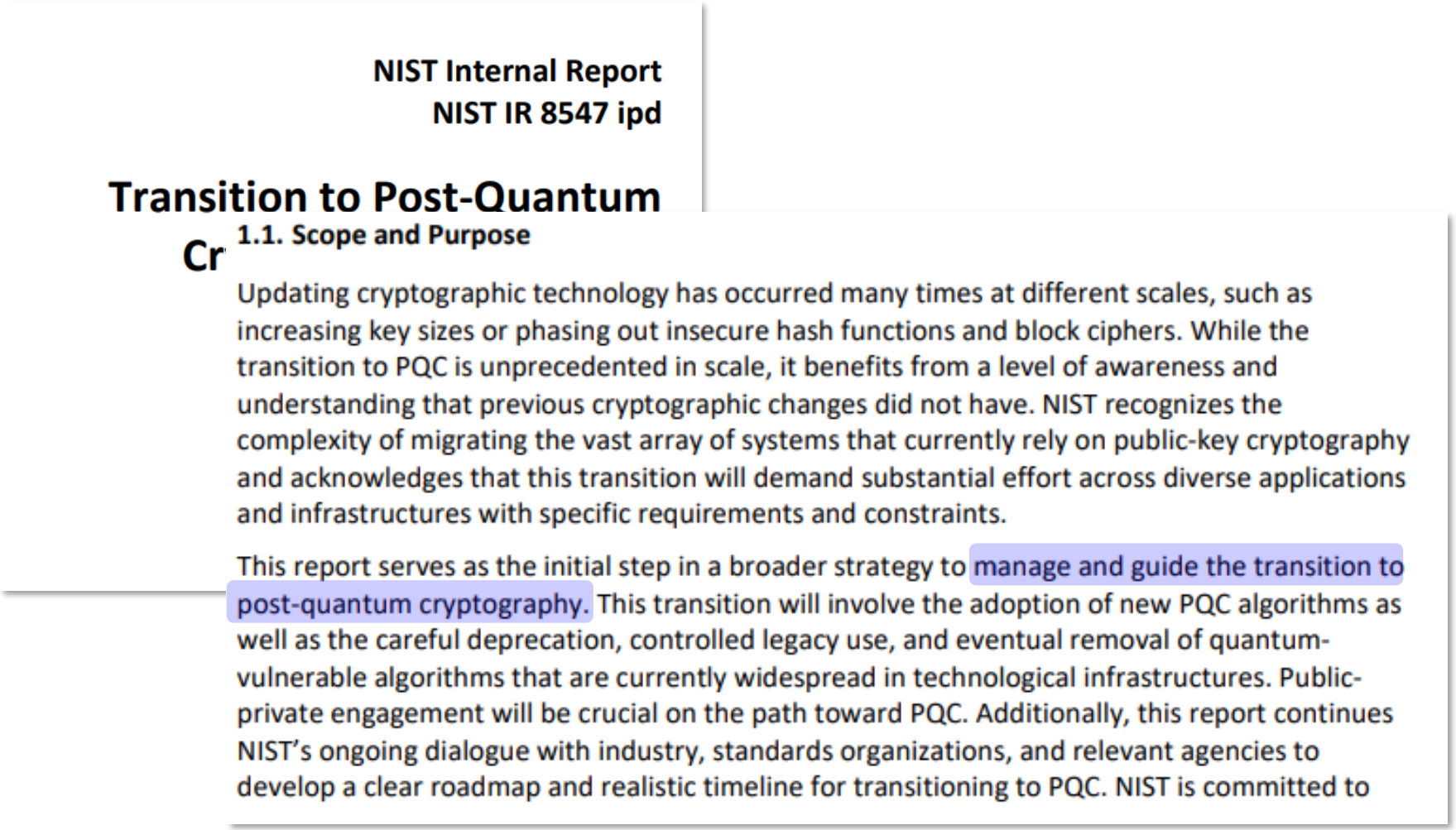
Introduction [8/13]

- NIST NCCoE (National Cybersecurity Center of Excellence)
  - NIST 산하에 설치된 사이버보안 전문연구소
  - 실제 산업계의 문제를 해결하기 위해 실용적이고 상용화 가능한 사이버보안 솔루션 개발을 목적으로 설립



Introduction [9/13]

- NIST IR 8547 “Transition to Post-Quantum Cryptography Standards” (2024)



NIST Internal Report
NIST IR 8547 ipd

Transition to Post-Quantum
Cr

1.1. Scope and Purpose

Updating cryptographic technology has occurred many times at different scales, such as increasing key sizes or phasing out insecure hash functions and block ciphers. While the transition to PQC is unprecedented in scale, it benefits from a level of awareness and understanding that previous cryptographic changes did not have. NIST recognizes the complexity of migrating the vast array of systems that currently rely on public-key cryptography and acknowledges that this transition will demand substantial effort across diverse applications and infrastructures with specific requirements and constraints.

This report serves as the initial step in a broader strategy to manage and guide the transition to post-quantum cryptography. This transition will involve the adoption of new PQC algorithms as well as the careful deprecation, controlled legacy use, and eventual removal of quantum-vulnerable algorithms that are currently widespread in technological infrastructures. Public-private engagement will be crucial on the path toward PQC. Additionally, this report continues NIST’s ongoing dialogue with industry, standards organizations, and relevant agencies to develop a clear roadmap and realistic timeline for transitioning to PQC. NIST is committed to

Introduction [10/13]

- NIST IR 8547 “Transition to Post-Quantum Cryptography Standards”
  - 양자 내성 암호로의 전환이 필요한 부분을 언급 후 보안강도 제시
  - 보안강도별 권장 파라미터 제시

Table 1: Post-Quantum Security Categories

Security Category	Attack Type	Example
1	Key search on a block cipher with a 128-bit key	AES-128
2	Collision search on a 256-bit hash function	SHA-256
3	Key search on a block cipher with a 192-bit key	AES-192
4	Collision search on a 384-bit hash function	SHA3-384
5	Key search on a block cipher with a 256-bit key	AES-256

Introduction [11/13]

- NIST IR 8547 “Transition to Post-Quantum Cryptography Standards”

분류	기존 알고리즘	보안강도	전환기한	대체 알고리즘
전자서명	ECDSA [FIPS 186]	112	Deprecated after 2030 Disallowed after 2035	MLDSA [FIPS 204] SLH-DSA [FIPS 205] LMS,HSS [SP800208] XMSS,XMSS ^{MT} [SP800208]
		≥128	Disallowed after 2035	
	EdDSA [FIPS 186]	≥128	Disallowed after 2035	
	RSA [FIPS 186]	112	Deprecated after 2030 Disallowed after 2035	
		≥128	Disallowed after 2035	

Introduction [12/13]

- NIST SP 1800-30B : Approach, Architecture, and Security Characteristics of Public Key Application Discovery Tools
  - 조직들이 자신의 IT 시스템 내에서 **양자 취약암호가 어디에, 어떻게 사용되는지 자동으로 탐지하여 전환계획을 수립할 수 있도록 하는 도구와 방법론을** 제안
  - 도구 설계 방식
    - 입력 소스
      - 개발 파이프라인
      - 운영시스템 (실행파일, 암호 라이브러리, 인증서 등등)
      - 네트워크 트래픽

- NIST SP 1800-38C : Testing Draft Standards for Interoperability and Performance
  - 양자 내성 알고리즘 간의 호환성 문제 식별
  - 각 조직이 자체 PQC 전환을 위해 유사한 상호 운용성 테스트 방안 제안
  - PQC 교체 후 성능이나 호환성 검증 방안 제시

Introduction [13/13]

- CISA (Cybersecurity & Infrastructure Security Agency)
  - 양자내성암호로의 전환을 위해 비양자내성암호를 자동 식별하는 Automated Cryptography Discovery and Inventory (ACDI) tool 개발 강조
  - CISA/NSA/NIST 와 작업 timeline 제시 (~2035년 완료)

국외 비양자내성암호 탐지 동향

- 국외 기업 및 연구 단체에서는 비양자내성암호 탐지도구 개발을 진행하고 있음
  - C-DOT (Center for Development of Telematics/인도)
    - 자동 탐지 기술 개발 프로젝트 추진 (2025/02/27 접수마감)

Automated tool to discover Quantum-vulnerable Crypto Algorithms

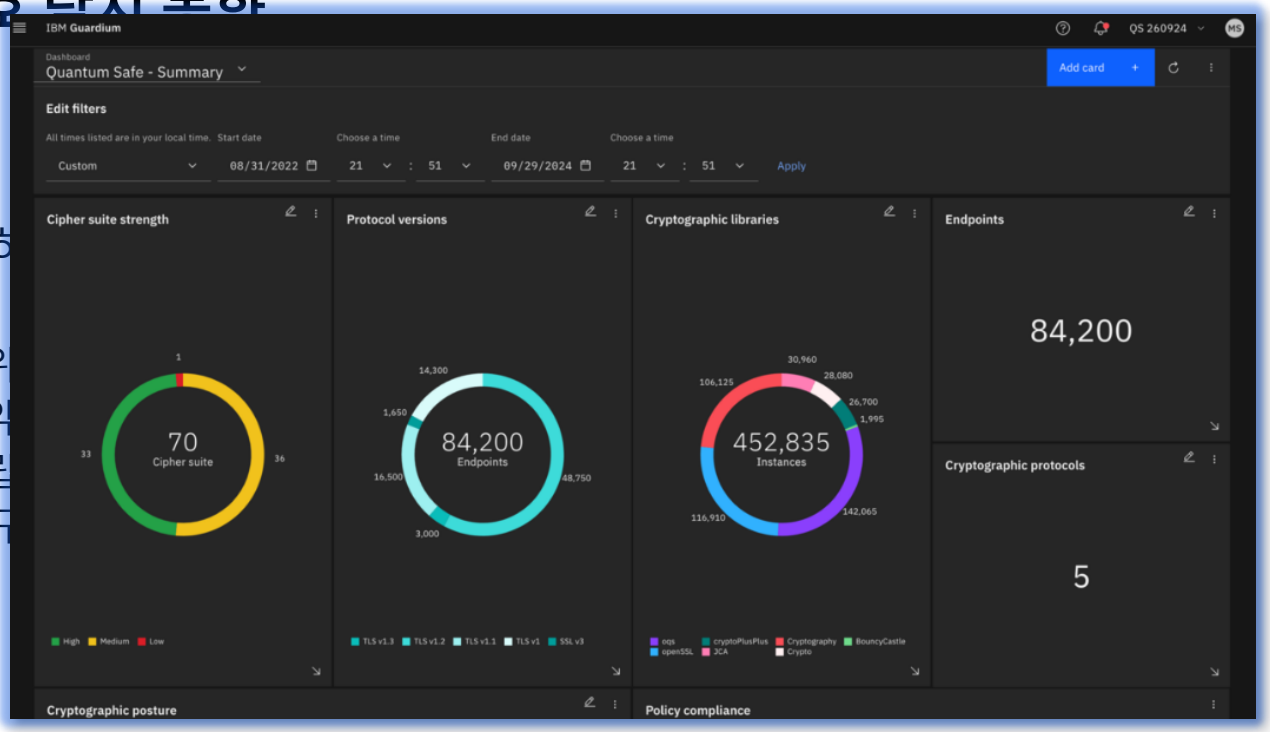
1	**Problem Statement**	Development of Automated Tool (combination of black box tester and security scanner agent on the target device itself) to scan target device for discovery of generic security vulnerabilities and Quantum-vulnerable cryptographic algorithms.
2	**Technology Area**	Post Quantum Cryptography (PQC), Vulnerability Assessment
3	**Project Introduction**	With the advents of quantum computers, classical public-key cryptosystems such as RSA, ECDH, and ECDSA shall no longer be secure as the underlying mathematical hard problems shall be efficiently solved using Shor's quantum

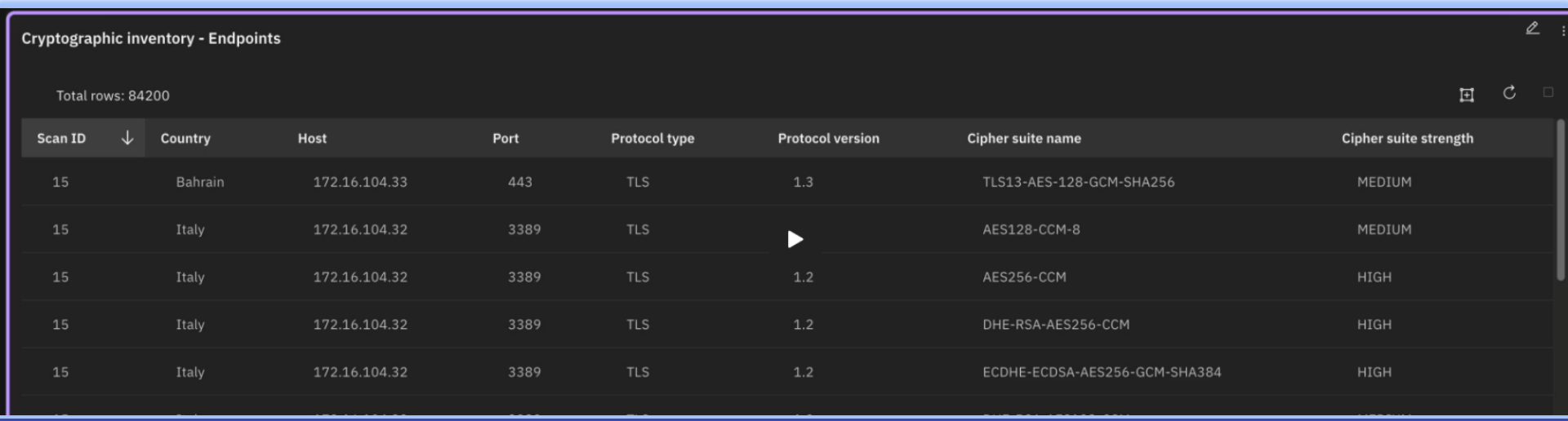
국외 비양자내성암호 탐지 동향

- IBM Quantum Safe
  - PQC 암호로 전환하기 위한 기술,서비스, 인프라 포괄하는 솔루션
  - 주요 기능
    - 암호화 사용 위치 탐색 및 관찰
    - 취약 지점 파악 및 위험 분석
    - 전환 전략 수립
    - Crypto Agility 구현

국외 비양자내성암호 탐지 동향

- IBM Quantum Safe
  - PQC 암호로 전환
  - 주요 기능
    - 암호화 사용 위
    - 취약 지점 파악
    - 전환 전략 수립
    - Crypto Agility 구

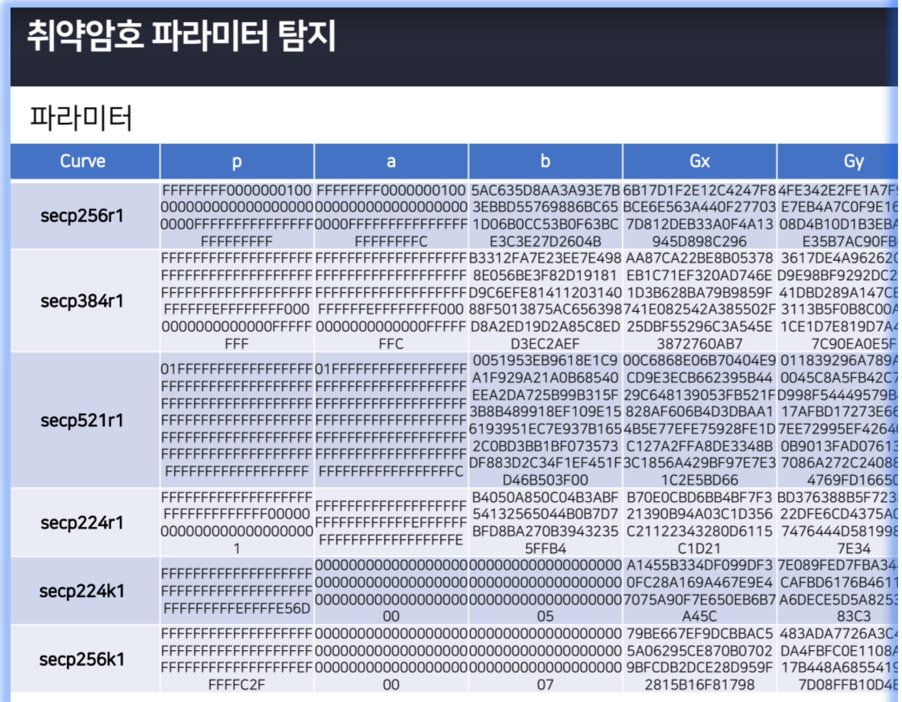




Scan ID	Country	Host	Port	Protocol type	Protocol version	Cipher suite name	Cipher suite strength
15	Bahrain	172.16.104.33	443	TLS	1.3	TLS13-AES-128-GCM-SHA256	MEDIUM
15	Italy	172.16.104.32	3389	TLS		AES128-CCM-8	MEDIUM
15	Italy	172.16.104.32	3389	TLS	1.2	AES256-CCM	HIGH
15	Italy	172.16.104.32	3389	TLS	1.2	DHE-RSA-AES256-CCM	HIGH
15	Italy	172.16.104.32	3389	TLS	1.2	ECDHE-ECDSA-AES256-GCM-SHA384	HIGH

국내 비양자내성암호 탐지 동향

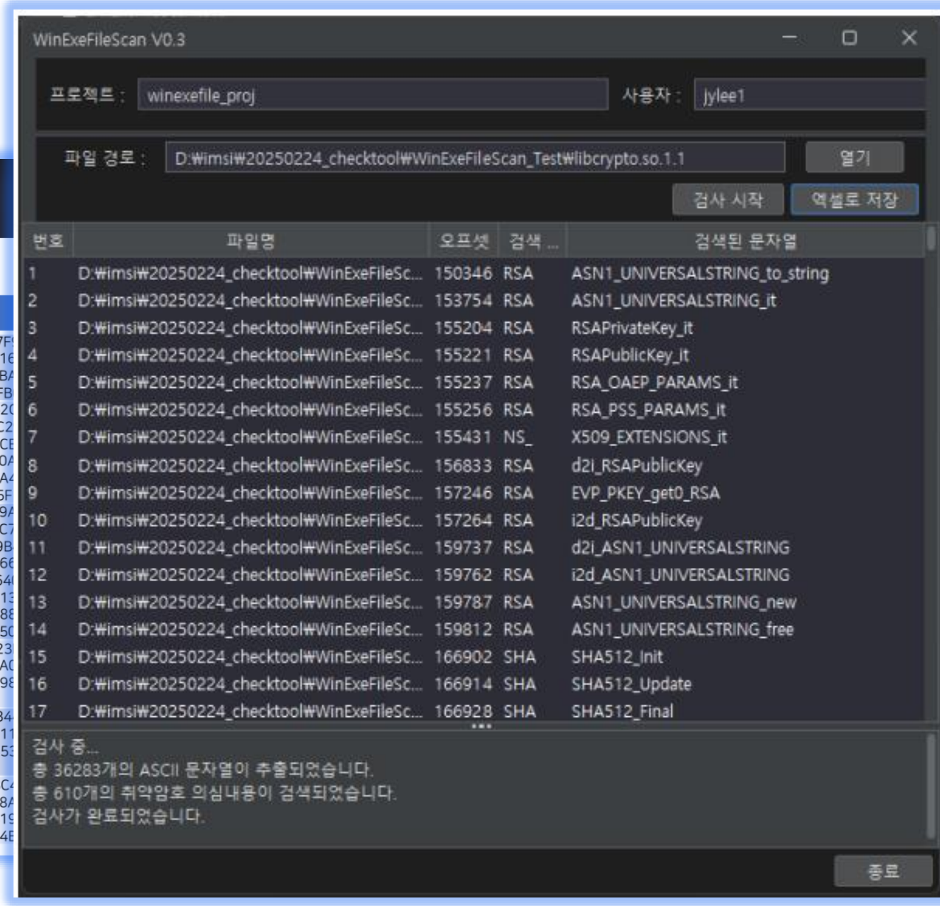
- NSHC
  - 실행파일 대상으로 비양자내성암호 분석
  - 취약암호 관련 문자열 포함 여부 분석
  - 결과와 위치 분류하여 엑셀에 저장



취약암호 파라미터 탐지

파라미터

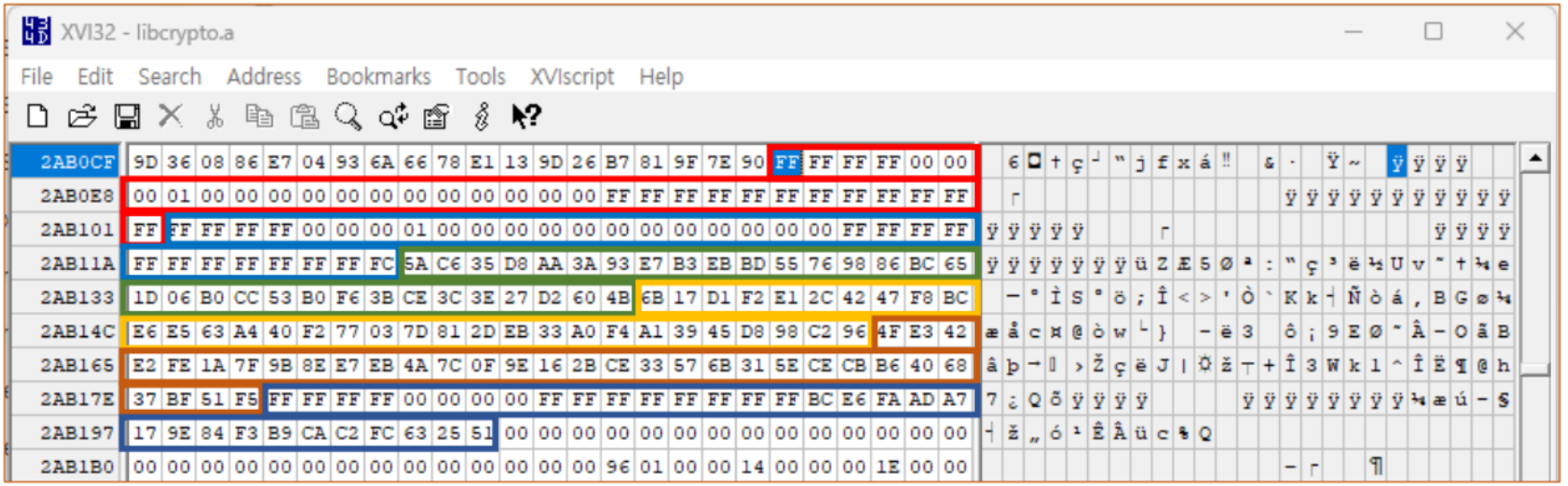
Curve	p	a	b	Gx	Gy
secp256r1	FFFFFFFF0000000100 000000000000000000 0000FFFFFFFFFFFFFF FFFFFFFFF	FFFFFFFF0000000100 000000000000000000 0000FFFFFFFFFFFFFF FFFFFFFFC	5AC635D8AA3A93E7B 3EBBD55769886BC65 1D06B0CC53B0F63BC E3C3E27D2604B	6B17D1F2E12C4247F8 BCE6E563A440F27703 7D812DEB33A0F4A13 945D898C296	4FE342E2FE1A7F E7EB4A7C0F9E16 08D4B10D1B3EBA E35B7AC90FB
secp384r1	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFEFFFFFFFF000 0000000000000FFFFF FFF	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFEFFFFFFFF000 0000000000000FFFFF FFC	B3312FA7E23EE7E498 8E056BE3F82D19181 D9C6EFE81411203140 88F5013875AC656398 D8A2ED19D2A85C8ED D3EC2AEF	AA87CA22BE8B05378 EB1C71EF320AD746E 1D3B628BA79B9859F 741E082542A385502F 25DBF55296C3A545E 3872760AB7	3617DE4A96262 D9E98BF9292DC2 41DBD289A147CE 3113B5F0B8C00A 1CE1D7E819D7A4 7C90EA0E5F
secp521r1	01FFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFF	01FFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFC	0051953EB9618E1C9 A1F929A21A0B68540 EEA2DA725B99B315F 3B8B489918EF109E15 6193951EC7E937B165 2C0BD3BB1BF073573 DF883D2C34F1EF451F D46B503F00	00C6868E06B70404E9 CD9E3ECB662395B44 29C648139053FB521F 828AF606B4D3DBAA1 4B5E77EFE75928FE1D C127A2FFA8DE3348B 3C1856A429BF97E7E3 1C2E5BD66	011839296A789A 0045C8A5FB42C7 D998F54449579B 17AFBD17273E66 7EE72995EF4264 0B9013FAD07613 7086A272C24088 4769FD16650
secp224r1	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFF00000 000000000000000000 1	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFEFFFFFF FFFFFFFFFFFFFFFFE	B4050A850C04B3ABF 54132565044B0B7D7 BFD8BA270B3943235 5FFB4	B70E0CBD6BB4BF7F3 21390B94A03C1D356 C21122343280D6115 C1D21	BD376388B5F723 22DFE6CD4375A0 7476444D581998 7E34
secp224k1	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFEFFFFE56D	000000000000000000 000000000000000000 000000000000000000 00	000000000000000000 000000000000000000 000000000000000000 05	A1455B334DF099DF3 0FC28A169A467E9E4 7075A90F7E650EB6B7 A45C	7E089FED7FBA34 CAFBD6176B4611 A6DECE5D5A8253 83C3
secp256k1	FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFFF FFFFFFFFFFFFFFFFEF FFFFC2F	000000000000000000 000000000000000000 000000000000000000 00	000000000000000000 000000000000000000 000000000000000000 07	79BE667EF9DCBBAC5 5A06295CE870B0702 9BFCDB2DCE28D959F 2815B16F81798	483ADA7726A3C4 DA4FBFC0E1108A 17B448A685541 7D08FFB10D4B



국내 비양자내성암호 탐지 동향

- NSHC
  - Example : 바이너리 파일 상에서의 파라미터 검색

Curve	p	a	b	Gx	Gy	n
secp256r1	FFFFFFFF000000010000000000000000000000000000000FFFFFFFFFFFFFFFF	FFFFFFFF000000010000000000000000000000000000000FFFFFFFFFFFFFFFC	5AC635D8AA3A93E7B3EBBD55769886BC651D06B0CC53B0F63BCE3C3E27D2604B	6B17D1F2E12C4247F8BCE6E563A440F277037D812DEB33A0F4A13945D898C296	4FE342E2FE1A7F9B8EE7EB4A7C0F9E162BCE33576B315ECECBB6406837BF51F5	FFFFFFFF00000000FFFFFFFFFFFFFFFFBCE6FAADA7179E84F3B9CAC2FC632551



libcrypto.a in openssl_3.4.1

비양자내성암호 탐지 연구 동향

비양자내성암호 탐지 연구 동향

- 바이너리 탐색 기술
  - 소프트웨어의 바이너리 파일을 분석하고 내부 동작과 구조 파악하는 기술

	내용	주요도구
정적 분석	• 프로그램을 실행하지 않고 바이너리 파일을 역어셈블하거나 디컴파일하여 코드 흐름 파악	• IDA Pro, Ghidra, Radare2
동적 분석	• 프로그램을 실제로 실행하여 실행중의 메모리 상태, 레지스터 값, 시스템 호출 등을 분석	• 디버거 (GDB), 동적분석도구 (OllyDbg, x64dbg)
코드 분석	• 동적분석+정적분석 • 어셈블리 코드를 해석하고 프로그램의 기능을 이해하여 기능을 파악하고 구조를 분석	• IDA Pro, Hex-rays Decompiler

비양자내성암호 탐지 연구 동향

- 기존 암호 탐지
  - 정적분석
    - Initialization vector, look-up table (S-Boxes) 을 통해 암호 사용 분석
    - 암호학적 API 탐지
  - 동적 분석
    - 런타임 시점에 lop 구조, input-output relation 분석
    - 실행시에 유의미한 trace를 생성하는 것이 어려움

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - IEEE Access, 2024
  - 양자 컴퓨팅 환경에 대응하기 위한 비양자내성암호 탐지 기술 관련한 논문
  - QED (Quantum-vulnerable Executable Detection) toolchain 제안
  - API level 에서 비양자내성암호 탐지
  - Real-world dataset 사용
    - 200 개의 software executables
    - 실제환경에서는 90% 이상의 탐지율

비양자내성암호 탐지 연구 동향

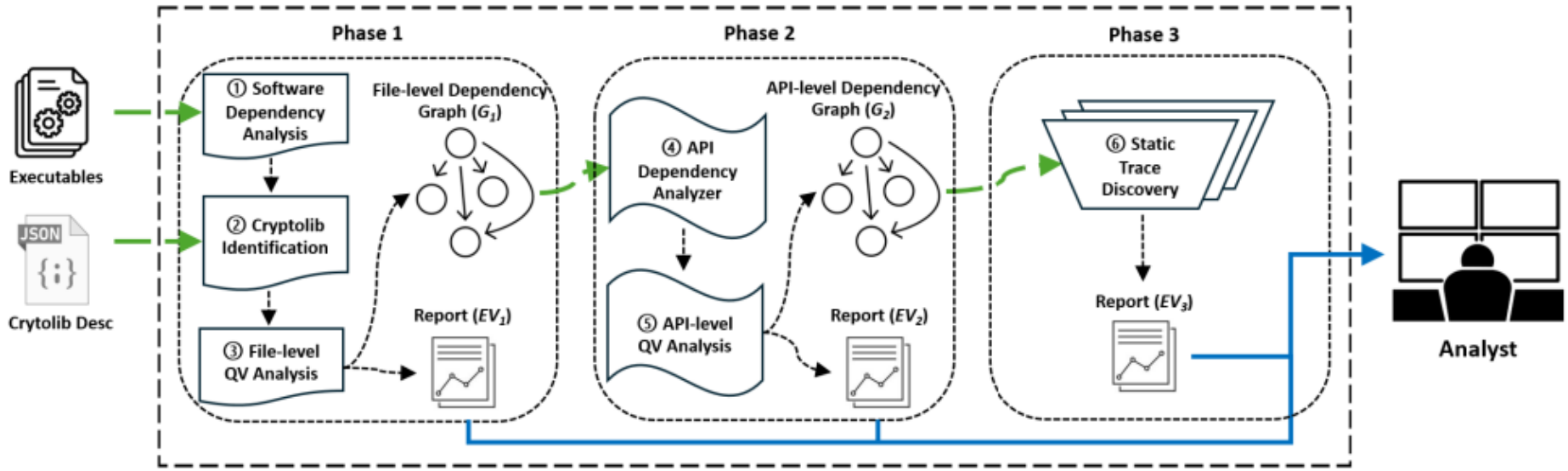
- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - Target
    - 리눅스 운영체제
    - C, C++ 로 쓰여진 software
    - Linux executable, Linkable Format (ELF)
    - 암호학적 라이브리를 Dynamic linking 으로 사용하는 환경만 고려 (.so)
      - 자체 라이브러리 구현이나 정적으로 링크한 실행파일은 고려하지 않음 (.a)
  - Implementation
    - Python
    - Pyelftools library 로 ELF 파일 확인
    - QED의 그래프는 NetworkX 라이브러리 사용
    - 코드 공개
    - 전체적인 내부와 외부 함수 및 라이브러리를 그래프 형태로 모델링하고 실제로 연결되는지를 그래프 탐색을 통해 분석

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - 설계 방법
    - Phase 1 : 파일 수준 종속성 분석
      - 실행파일이 사용하는 모든 shared library 탐색
      - 이 중 비양자내성암호 (**Quantum Vulnerable, QV**)를 포함하는 라이브러리 (OpenSSL, wolfSSL, MbedTLS) 확인
        - libcrypto.so
    - Phase 2 : API 수준 분석
      - 실제 호출되는 외부 API 조사하여 비양자내성암호를 사용하는 API 사용 여부 확인
      - 비양자내성암호를 직접 호출하지 않는 경우 제거 ➔ false positive 감소
    - Phase 3 : 정적 추적 분석
      - Main 함수부터 비양자내성암호 API 까지 호출경로가 실제 존재하는지 검증
      - 실제 호출 가능성을 정적으로 입증

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - 설계 방법



비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - Example of report

```
"EV_1": [
  {
    "path": [
      "/usr/bin/sftp",
      "/usr/lib/libcrypto.so.1.1"
    ]
  }
  ,
  {
    "path": [
      "/usr/bin/dig",
      "/usr/lib/libdns.so",
      "/usr/lib/libcrypto.so.1.1"
    ]
  }
  ,
  {
    "path": [
      "/usr/bin/nmap",
      "/usr/lib/libssl.so.1.1",
      "/usr/lib/libcrypto.so.1.1"
    ]
  }
  ...
  {
    "path": [
      "/usr/bin/curl",
      "/usr/lib/libcurl.so.4",
      "/usr/lib/libcrypto.so.1.1"
    ]
  }
]
```

```
"EV_2": [
  {
    "path": [
      "/usr/bin/nmap",
      "/usr/lib/libssl.so.1.1",
      "/usr/lib/libcrypto.so.1.1"
    ],
    "QV_apis": [
      "DSA_do_sign",
      "DSA_do_verify",
      "EVP_PKEY_get1_DSA",
      ...
      "RSA_verify"
    ]
  }
  ...
  {
    "path": [
      "/usr/bin/curl",
      "/usr/lib/libcurl.so.4",
      "/usr/lib/libcrypto.so.1.1"
    ],
    "QV_apis": [
      "DH_get0_key",
      "DSA_get0_key",
      "DSA_get0_pqg",
      "EVP_PKEY_get0_DH",
      ...
      "RSA_get0_key"
    ]
  }
]
```

```
"EV_3": [
  {
    "static-trace": [
      [
        "/usr/bin/nmap",
        "main"
      ],
      [
        "/usr/bin/nmap",
        "sub_3f340"
      ]
      ...
      [
        "/usr/bin/nmap",
        "SSL_CTX_new"
      ],
      [
        "/usr/lib/libssl.so.1.1",
        "SSL_CTX_new"
      ]
      ...
      [
        "/usr/lib/libssl.so.1.1",
        "EVP_PKEY_get0_RSA"
      ],
      [
        "/usr/lib/libcrypto.so.1.1",
        "EVP_PKEY_get0_RSA"
      ]
    ]
  }
]
```

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - 실험 결과
    - Synthetic Dataset (40개 파일)
      - OpenSSLv1.1.1 OpenSSLv3.3.1, MbedTLS v2.28.9, wolfSSlv5.7.2
      - SHA-512, AES-256 (Non QV) , DH, RSA, ECDSA (QV)
    - Direct Dependency Set
      - 각 라이브러리마다 5개의 예제 프로그램 작성
      - 각 프로그램은 해당 라이브러리의 API를 직접 호출
    - Indirect Dependency Set
      - 중간 shared library 경유하여 사용하도록 설계
      - 각 실행파일은 이 wrapper 라이브러리를 동적으로 링크

QED's Phases (→)	P1		P1 +P2		P1 +P2 +P3	
Synthetic Dataset (↓)	TP/FN (TPR)	TN/FP (TNR)	TP/FN (TPR)	TN/FP (TNR)	TP/FN (TPR)	TN/FP (TNR)
Direct Dependency	12/0 (100%)	0/8 (0%)	12/0 (100%)	8/0 (100%)	12/0 (100%)	8/0 (100%)
Indirect Dependency	12/0 (100%)	0/8 (0%)	12/0 (100%)	0/8 (0%)	12/0 (100%)	8/0 (100%)
Total	24/0 (100%)	0/16 (0%)	24/0 (100%)	8/8 (50%)	24/0 (100%)	16/0 (100%)

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - 실험 결과
    - Real-World Dataset (226개 실행파일)
      - Coreutils, UnixBench, curl/ssh 등 네트워크 도구, TPM 도구 포함
      - 평균분석시간 : 4초/ 실행파일
    - Dataset
      - Coreutils, UnixBench
        - 암호학적 프로그램이 아님
        - 정확히 탐지할 경우 non-QV로 분류되어야 함
      - Network
        - Curl, ssh, sftp, sshd, telnet, tracepath, wget, ping, scp
        - 7 프로그램이 OpenS니 v1l1. 사용

Phases (→)	P1		P1 +P2		P1 +P2 +P3	
Set (↓)	TP/FN (TPR)	TN/FP (TNR)	TP/FN (TPR)	TN/FP (TNR)	TP/FN (TPR)	TN/FP (TNR)
Coreutils	0/0 (100%)	109/0 (100%)	n/a	n/a	n/a	n/a
UnixBench	0/0 (100%)	18/0 (100%)	n/a	n/a	n/a	n/a
Network	7/0 (100%)	4/2 (67%)	7/0 (100%)	6/0 (100%)	6/1 (86%)	6/0 (100%)

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography

```
suhrikim@ex-desk:~/qed$ ls
APIAnalysis.py      dataset-make.sh          mbedtls-install.sh  __pycache__  test.txt
BaseAnalysis.py     datasets                 openssl-install.sh  qed.py       tpm-install.sh
crypto_desc.py      FileDepend
dataset-install.sh  install.sh
suhrikim@ex-desk:~/qed$
```

```
#openssl_APIs = list_dynsym("/usr/lib/x86_64-linux-gnu/libcrypto.so.1.1", openss
openssl11_APIs = ['DH_security_bits', 'i2d_RSAPublicKey', 'PEM_read_RSAPublicKey
                  'EC_KEY_OpenSSL', 'RSA_print', 'RSA_padding_check_PKCS1_OAEP_mgf
                  'DH_get0_g', 'DHparams_print_fp', 'd2i_RSAPublicKey', 'DH_get0_p
                  'EC_POINT_copy', 'EC_POINT_free', 'i2d_RSAPrivateKey', 'EC_KEY_M
                  'RSA_padding_add_PKCS1_PSS', 'DSAparams_print_fp', 'DH_check_par
                  'DH_compute_key_padded', 'DH_get_default_method', 'd2i_EC_PUBKEY
                  'DHparams_print', 'PKCS7_RECIP_INFO_get0_alg', 'EC_KEY_get0_priv
                  'RSA_size', 'RSA_X931_generate_key_ex', 'PEM_read_DSA_PUBKEY', '
                  'PEM_read_bio_DHparams', 'RSA_meth_set_sign', 'EC_POINT_oct2poin
                  'RSA_get0_multi_prime_crt_params', 'RSA_meth_get_verify', 'RSA_g
                  'DH_get_2048_224', 'DH_meth_new', 'EVP_PKEY_get1_RSA', 'DSA_new'
                  'EC_KEY_up_ref', 'd2i_ECParameters', 'DH_get_2048_256', 'RSA_met
                  'PEM_read_bio_DSAparams', 'RSA_padding_check_X931', 'ECDSA_sign_
                  'DH_set_flags', 'DH_generate_key', 'BN_RECP_CTX_set', 'd2i_DSA_S
                  'PEM_read_ECPKParameters', 'd2i_RSA_PUBKEY', 'DSA_meth_get_mod_e
                  'EC_KEY_priv2buf', 'DSA_meth_get_finish', 'EC_GFp_simple_method'
```

탐지할 API 목록 라이브러리별 정의

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography

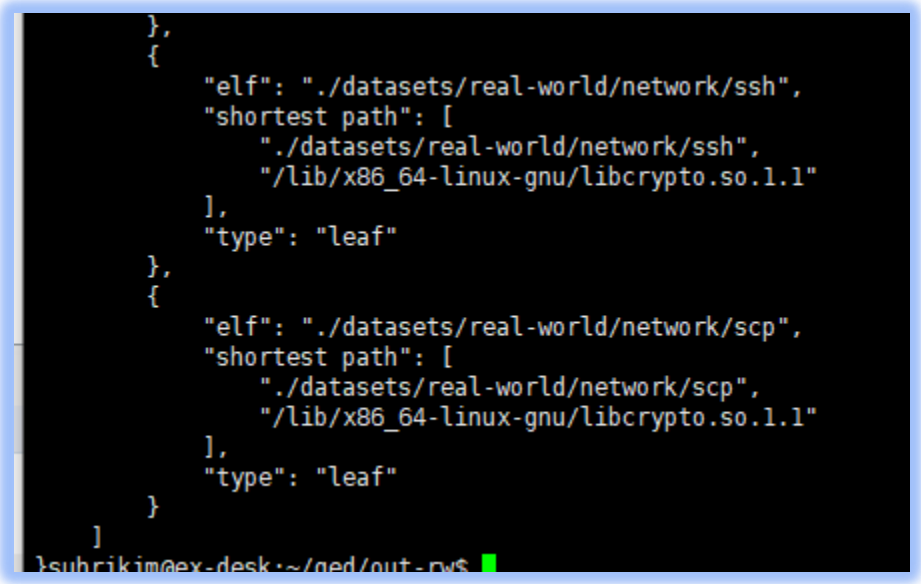
```
suhrikim@ex-desk:~/qed$ ls
APIAnalysis.py      dataset-make.sh          mbedtls-install.sh  __pycache__  test.txt
BaseAnalysis.py     datasets                 openssl-install.sh  qed.py       tpm-install.sh
crypto_desc.py      FileDependencyAnalysis.py  out-rw
dataset-install.sh  install.sh               out-syn
suhrikim@ex-desk:~/qed$
```

```c
#include <openssl/ec.h>
#include <openssl/obj_mac.h>
#include <openssl/err.h>
#include <stdio.h>
#include <stdlib.h>

// Function to create a new EC key pair and print the public key
void generate_ec_key(FILE *out) {
    EC_KEY *ec_key = NULL;
    const EC_POINT *pub_key = NULL;
    char *pub_key_hex = NULL;
    size_t key_size;

    // Create a new EC key pair
    ec_key = EC_KEY_new_by_curve_name(NID_X9_62_prime256v1);
    if (ec_key == NULL) {
        fprintf(out, "Error creating EC key\n");
        ERR_print_errors_fp(out);
        return;
    }

    // Generate the EC key pair
    if (EC_KEY_generate_key(ec_key) != 1) {
        fprintf(out, "Error generating EC key\n");
        ERR_print_errors_fp(out);
        EC_KEY_free(ec_key);
        return;
    }
```

테스트용 데이터셋 생성 가능

비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography



비양자내성암호 탐지 연구 동향

- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - Example : 해시 함수 사용 경우

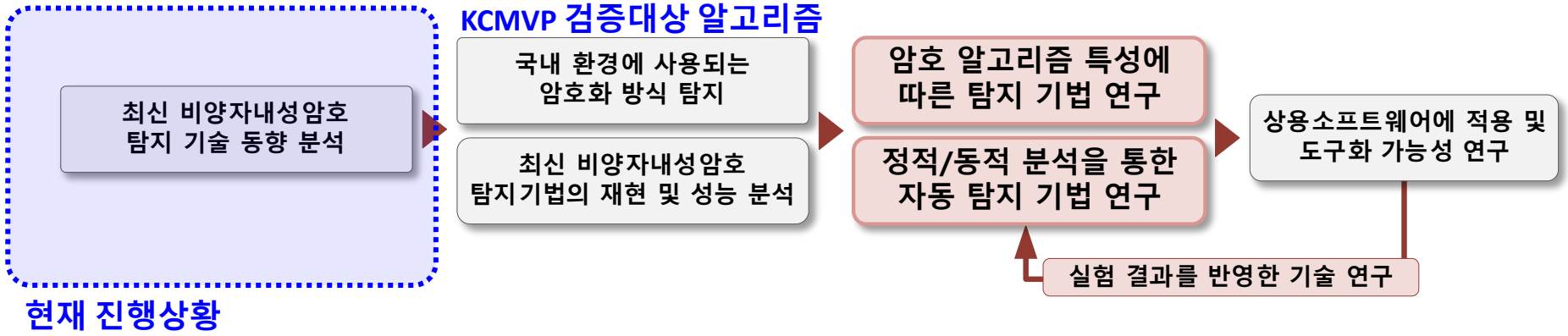
```
suhrikim@ex-desk:~/qed/fibsout$ cat api.txt
{
    "metadata": {
        "num_apps_before": 5,
        "num_total_before": 6,
        "num_apps_after": 0,
        "num_total_after": 1
    },
    "QV_apps": [],
    "report": [
        {
            "elf": "/lib/x86_64-linux-gnu/libcrypto.so.1.1",
            "api": [],
            "path": [
                "/lib/x86_64-linux-gnu/libcrypto.so.1.1"
            ],
            "type": "root"
        }
    ]
```

비양자내성암호 탐지 연구 동향

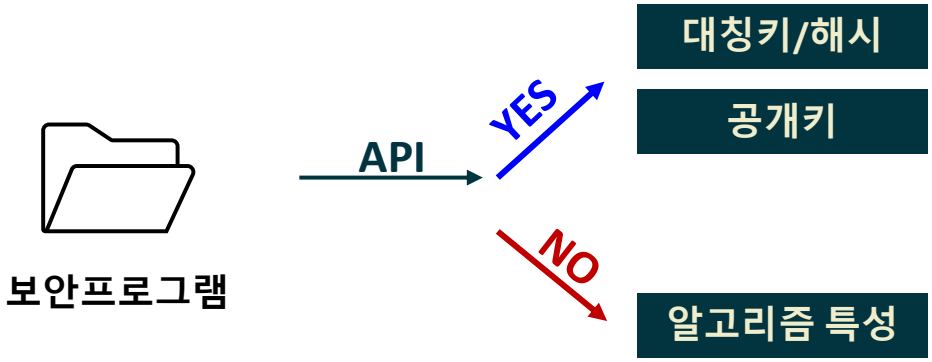
- A Toolchain for Assisting Migration of Software Executables Towards Post-quantum Cryptography
  - 실험 결과
    - OpenSSL 사용하는 경우 높은 정확도로 탐지
    - 자체 구현하거나 지정된 API 이외의 API 사용하는 경우 탐지 어려움

향후 계획

- 다양한 상용프로그램 분석을 통한 탐지 기술 목록화

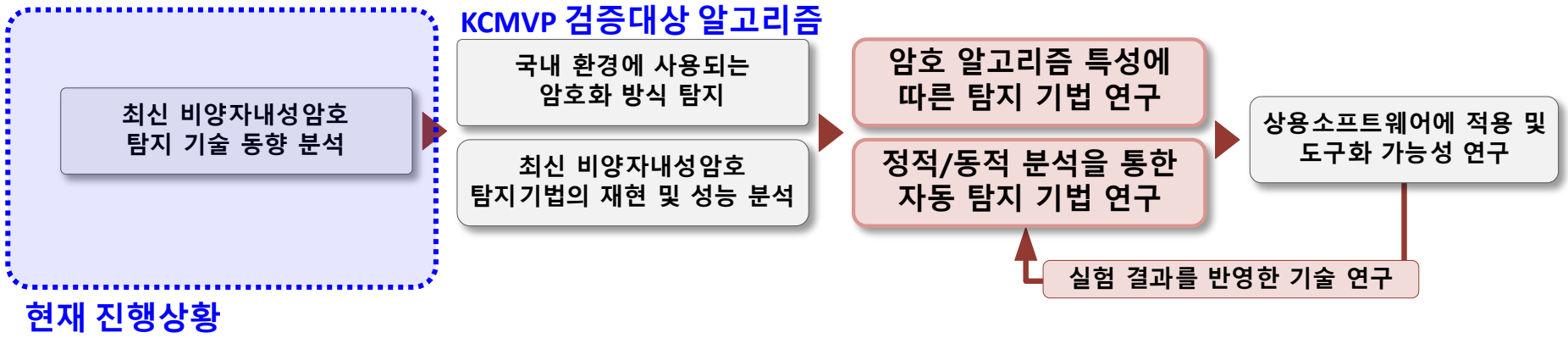


- 목표



향후 계획

- 다양한 상용프로그램 분석을 통한 탐지 기술 목록화



- 목표
  - 바이너리분석을 통해 1차 탐지
    - 사용된 API, 파라미터 , OID 등 활용
  - 알고리즘 특성을 활용한 2차 탐지

Thank you