아 제목 뭐로 하지

최유빈

목차

당신은 무엇을 아는가

내용 이해에서 막히면 아래 중에 모르는게 있는지 체크해보십쇼

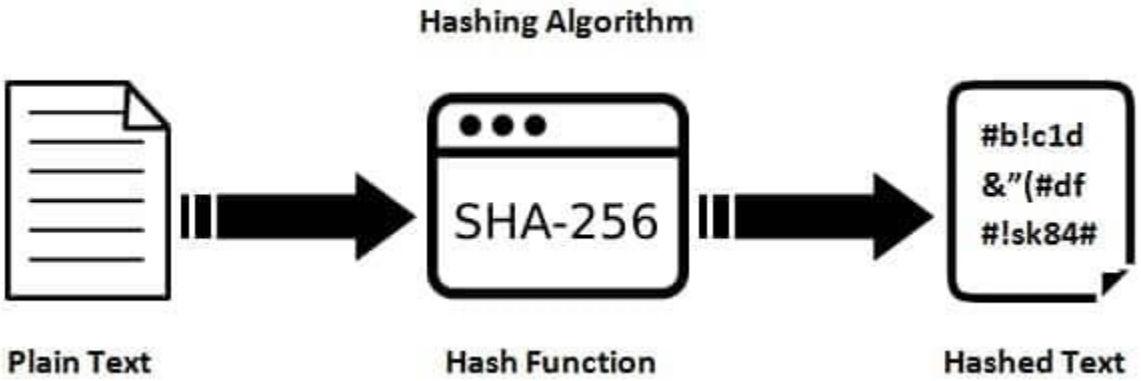
- 기초 시간복잡도 계산
-

왜 PQC인가

= 왜 PQC가 아닌건 안되는가

왜 PQC인가

왜 PQC인가

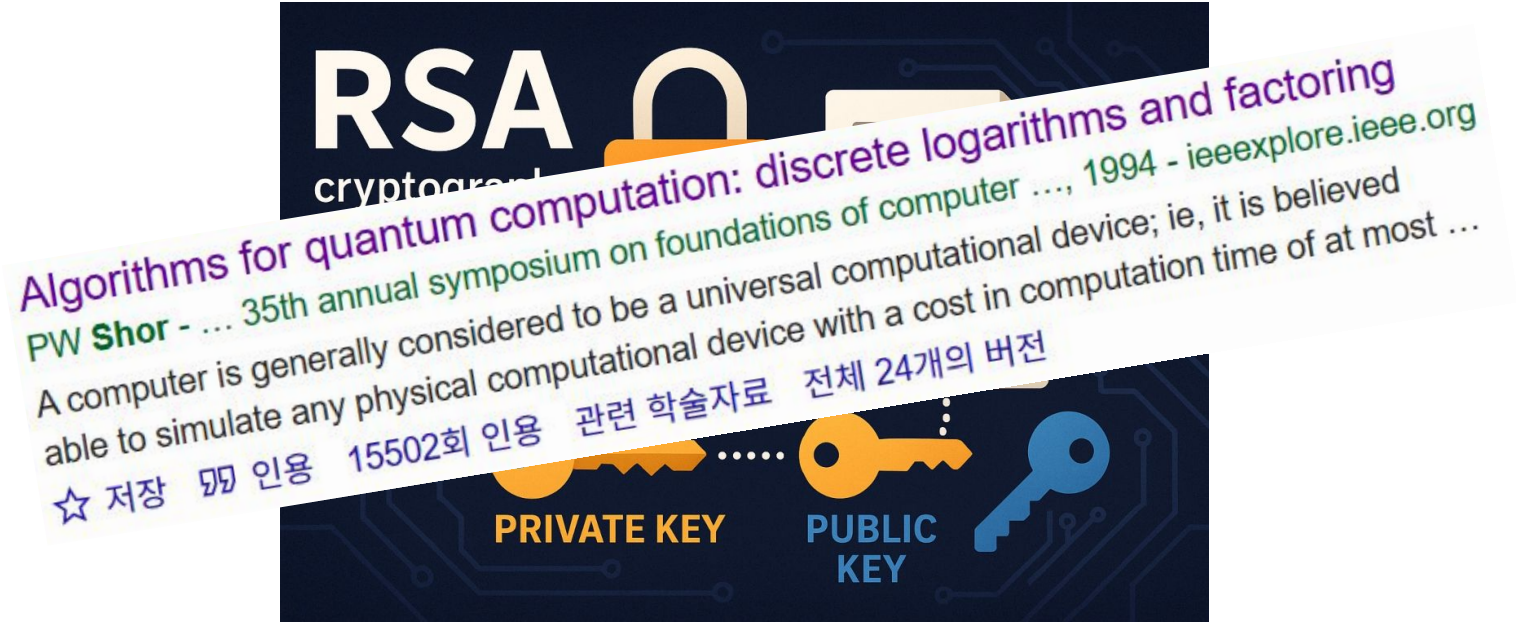

Hashing Algorithm
SHA-256
#b!c1d
&"(#df
#!sk84#
Plain Text
Hash Function
Hashed Text

왜 PQC인가


Quantum mechanics helps in searching for a needle in a haystack
LK Grover - Physical review letters, 1997 - APS
Quantum mechanics can speed up a range of search applications over unsorted data. For example, imagine a phone directory containing N names arranged in completely random order…
☆ 저장 99 인용 6700회 인용 관련 학술자료 전체 20개의 버전
Plain Text
Hash Function

왜 PQC인가

왜 PQC인가


RSA
Algorithms for quantum computation: discrete logarithms and factoring
PW Shor - … 35th annual symposium on foundations of computer …, 1994 - ieeexplore.ieee.org
A computer is generally considered to be a universal computational device; ie, it is believed able to simulate any physical computational device with a cost in computation time of at most …
☆ 저장 99 인용 15502회 인용 관련 학술자료 전체 24개의 버전
PRIVATE KEY
PUBLIC KEY

왜 PQC인가

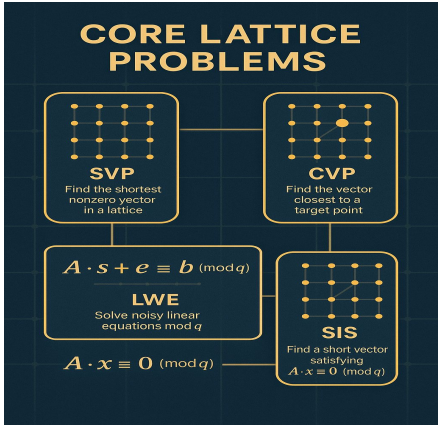

Harvest now, decrypt later (HNDL)
Years can pass
Step 1.
Data exfiltration
Steals encrypted traffic or files
Cold storage
Keeps ciphertext for years
Step 2.
Years can pass
Step 3.
Advances in quantum computing
Waits for quantum systems
Years can pass
Decrypt later
Shor's breaks RSA/ECC
Step 4.
Step 5.
Use the plaintext
Read, sell, or forge identities

왜 PQC인가

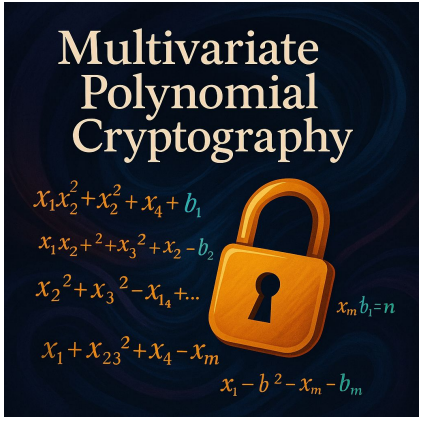

[01101>
QU
[01101>
[01101>
[01101>
CISA
NIST
NATIONAL SECURITY AGENCY
Quantum-Readiness:
Migration to Post-Quantum
Cryptography
CYBERSECURITY INFORMATION SHEET

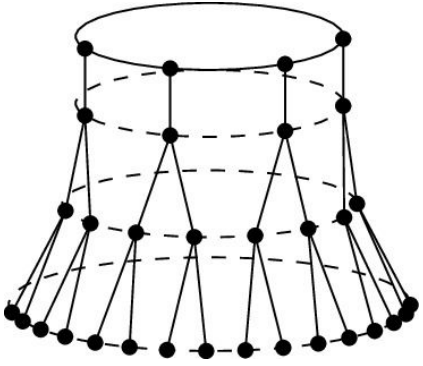
무엇이 PQC인가

무엇이 PQC인가


CORE LATTICE PROBLEMS
SVP
Find the shortest nonzero vector in a lattice
CVP
Find the vector closest to a target point
$A \cdot s + e \equiv b \pmod{q}$
LWE
Solve noisy linear equations mod q
SIS
Find a short vector satisfying $A \cdot x \equiv 0 \pmod{q}$
$A \cdot x \equiv 0 \pmod{q}$

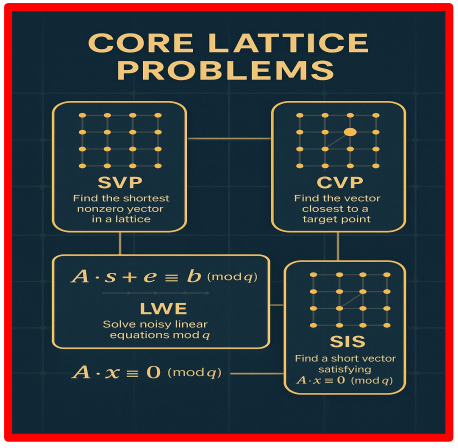

HASH
5A7C9F8D
BLOCK
BLOCK
BLOCK
HASH-BASED CRYPTOGRAPHY


Multivariate Polynomial Cryptography

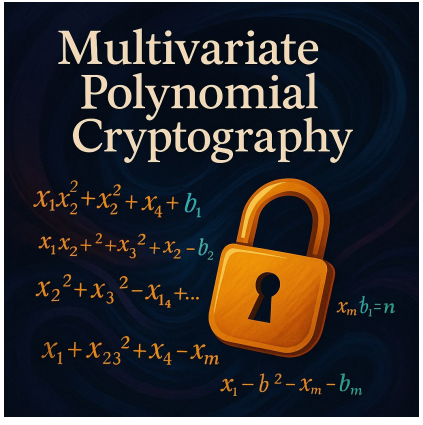


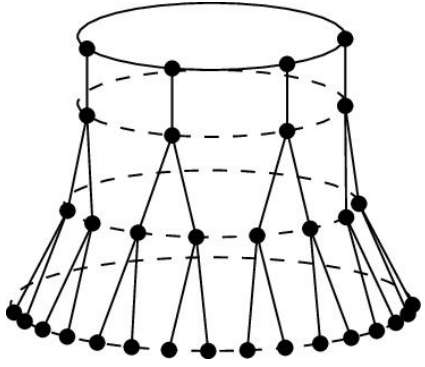

CODE-BASED CRYPTOGRAPHY

무엇이 PQC인가


CORE LATTICE PROBLEMS
SVP
Find the shortest nonzero vector in a lattice
CVP
Find the vector closest to a target point
$A \cdot s + e \equiv b \pmod{q}$
LWE
Solve noisy linear equations mod q
SIS
Find a short vector satisfying $A \cdot x \equiv 0 \pmod{q}$
$A \cdot x \equiv 0 \pmod{q}$


10101
HASH
HASH
HASH
HASH
HASH
5A7C9F8D
1A3B56EF
BLOCK
BLOCK
BLOCK
HASH-BASED CRYPTOGRAPHY


Multivariate Polynomial Cryptography




CODE-BASED CRYPTOGRAPHY

무엇이 PQC인가

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*

무엇이 PQC인가

- FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard*
- FIPS 204, *Module-Lattice-Based Digital Signature Standard*
- FIPS 205, *Stateless Hash-Based Digital Signature Standard*

	n	q	k	η_1	η_2	d_u	d_v	required RBG strength (bits)
ML-KEM-512	256	3329	2	3	2	10	4	128
ML-KEM-768	256	3329	3	2	2	10	4	192
ML-KEM-1024	256	3329	4	2	2	11	5	256

Table 2. Approved parameter sets for ML-KEM

보안 수준 - Pre-Quantum

Table 1: ECDSA Security Parameters

Bit length of n (i.e. len(n))	Comparable Security Strength
224 - 255	approximately len(n)/2; at least 112 bits
256 - 383	approximately len(n)/2; at least 128 bits
384 - 511	approximately len(n)/2; at least 192 bits
≥ 512	approximately len(n)/2; at least 256 bits

보안 수준 - Pre-Quantum

Table 1: ECDSA Security Parameters

Bit length of n (i.e. len(n))	Comparable Security Strength
224 - 255	approximately len(n)/2; at least 112 bits
256 - 383	approximately len(n)/2; at least 128 bits
384 - 511	approximately len(n)/2; at least 192 bits
≥ 512	approximately len(n)/2; at least 256 bits

보안 수준 - Pre-Quantum

Table 1. Summary of our attacks on various ciphers.

Cipher	(Rounds)	Key bits	Best Previous Attack			Our Attack		
			Data	Type	Time	Data	Type	Time
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{32}	KP	2^{33}
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{17}	CP/CC	2^{17}
4K-Feistel	(∞)	192	—		—	2^{32}	KP	2^{33}
4K-Feistel	(∞)	192	—		—	2^{17}	CP/CC	2^{17}
4K-DES*	(∞)	192	—		—	2^{17}	CP/CC	2^{17}
Brown-Seberry-DES*	(∞)	56	—		—	128	CP/CC	2^{7}
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	KP	$2^{87.5}$
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	CO	2^{95}
Even-Mansour	(—)	$2n$	$2^{n/2}$	CP	$2^{n/2}$	$2^{n/2}$	KP	$2^{n/2}$
GOST$\oplus$	(20)	256	—		—	2^{33}	KP	2^{70}

보안 수준 - Pre-Quantum

Table 1. Summary of our attacks on various ciphers.

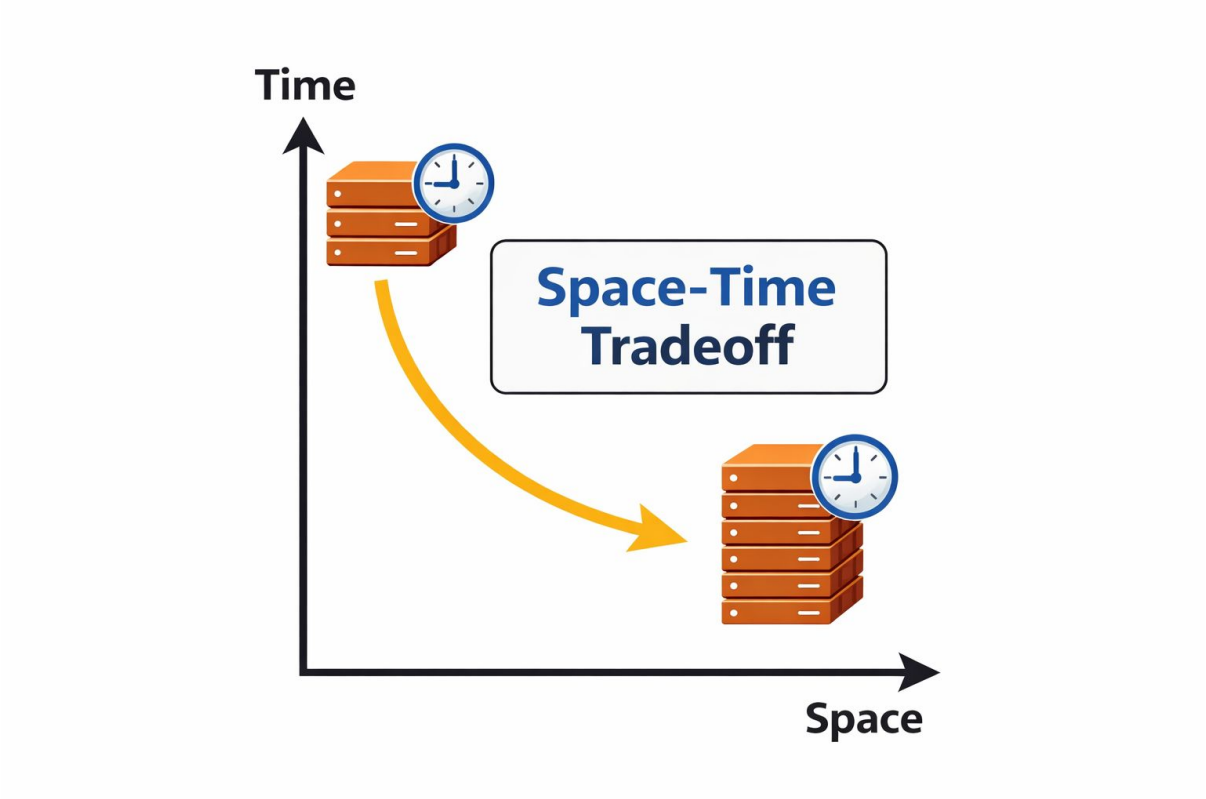
Cipher	(Rounds)	Key bits	Best Previous Attack			Our Attack		
			Data	Type	Time	Data	Type	Time
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{32}	KP	2^{33}
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{17}	CP/CC	2^{17}
4K-Feistel	(∞)	192	—		—	2^{32}	KP	2^{33}
4K-Feistel	(∞)	192	—		—	2^{17}	CP/CC	2^{17}
4K-DES*	(∞)	192	—		—	2^{17}	CP/CC	2^{17}
Brown-Seberry-DES*	(∞)	56	—		—	128	CP/CC	2^{7}
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	KP	$2^{87.5}$
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	CO	2^{95}
Even-Mansour	(—)	$2n$	$2^{n/2}$	CP	$2^{n/2}$	$2^{n/2}$	KP	$2^{n/2}$
GOST⊕	(20)	256	—		—	2^{33}	KP	2^{70}

보안 수준 - Pre-Quantum

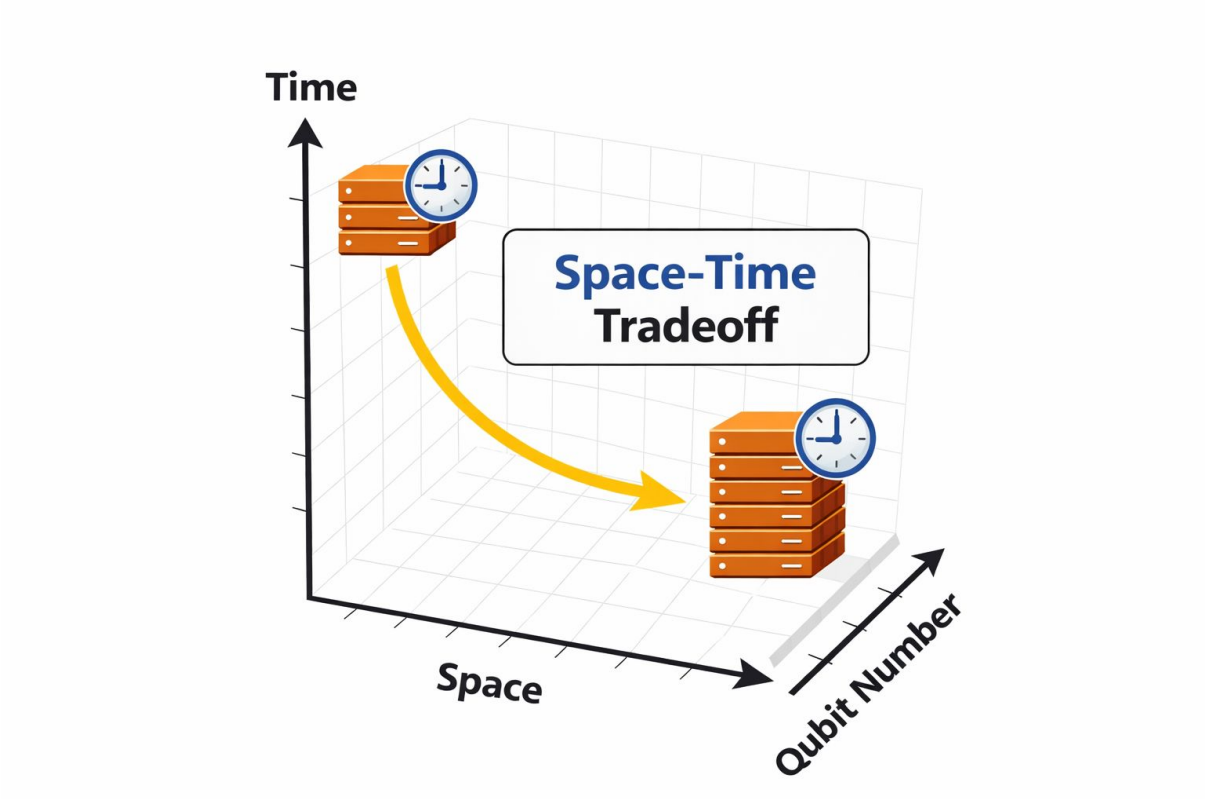
Table 1. Summary of our attacks on various ciphers.

Cipher	(Rounds)	Key bits	Best Previous Attack			Our Attack		
			Data	Type	Time	Data	Type	Time
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{32}	KP	2^{33}
2K-DES	(∞)	96	2^{32}	KP	2^{50}	2^{17}	CP/CC	2^{17}
4K-Feistel	(∞)	192	—	–	—	2^{32}	KP	2^{33}
4K-Feistel	(∞)	192	—	–	—	2^{17}	CP/CC	2^{17}
4K-DES*	(∞)	192	—	–	—	2^{17}	CP/CC	2^{17}
Brown-Seberry-DES*	(∞)	56	—	–	—	128	CP/CC	2^{7}
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	KP	$2^{87.5}$
DESX	(16)	184	2^{m}	CP	2^{121-m}	$2^{32.5}$	CO	2^{95}
Even-Mansour	(—)	$2n$	$2^{n/2}$	CP	$2^{n/2}$	$2^{n/2}$	KP	$2^{n/2}$
GOST⊕	(20)	256	—	–	—	2^{33}	KP	2^{70}

보안 수준 - Pre-Quantum



보안 수준 - Post-Quantum



보안 수준 - Post-Quantum

The three parameter sets included in Table 2 were designed to meet certain security strength categories defined by NIST in its original Call for Proposals [4, 18]. These security strength categories are explained further in Appendix A.

Using this approach, security strength is not described by a single number, such as "128 bits of security." Instead, each ML-KEM parameter set is claimed to be at least as secure as a generic

= 숫자 하나로 표현 못한다

보안 수준 - Post-Quantum

1. Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 128-bit key (e.g. AES128)
2. Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 256-bit hash function (e.g. SHA256/ SHA3-256)
3. Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 192-bit key (e.g. AES192)
4. Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for collision search on a 384-bit hash function (e.g. SHA384/ SHA3-384)
5. Any attack that breaks the relevant security definition must require computational resources comparable to or greater than those required for key search on a block cipher with a 256-bit key (e.g. AES 256)

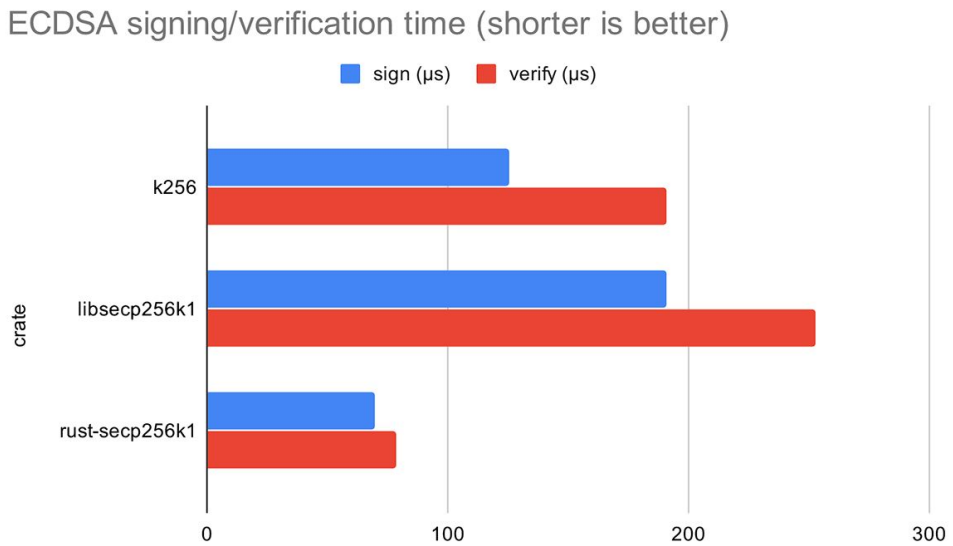
보안 수준 - Post-Quantum

1. AES-128 깨는거랑 비슷한 자원이 필요함
2. SHA-256 충돌 찾기랑 비슷한 자원이 필요함
3. AES-192 깨는거랑 비슷한 자원이 필요함
4. SHA-384 충돌 찾기랑 비슷한 자원이 필요함
5. AES-256 깨는거랑 비슷한 자원이 필요함

보안 수준 - Post-Quantum

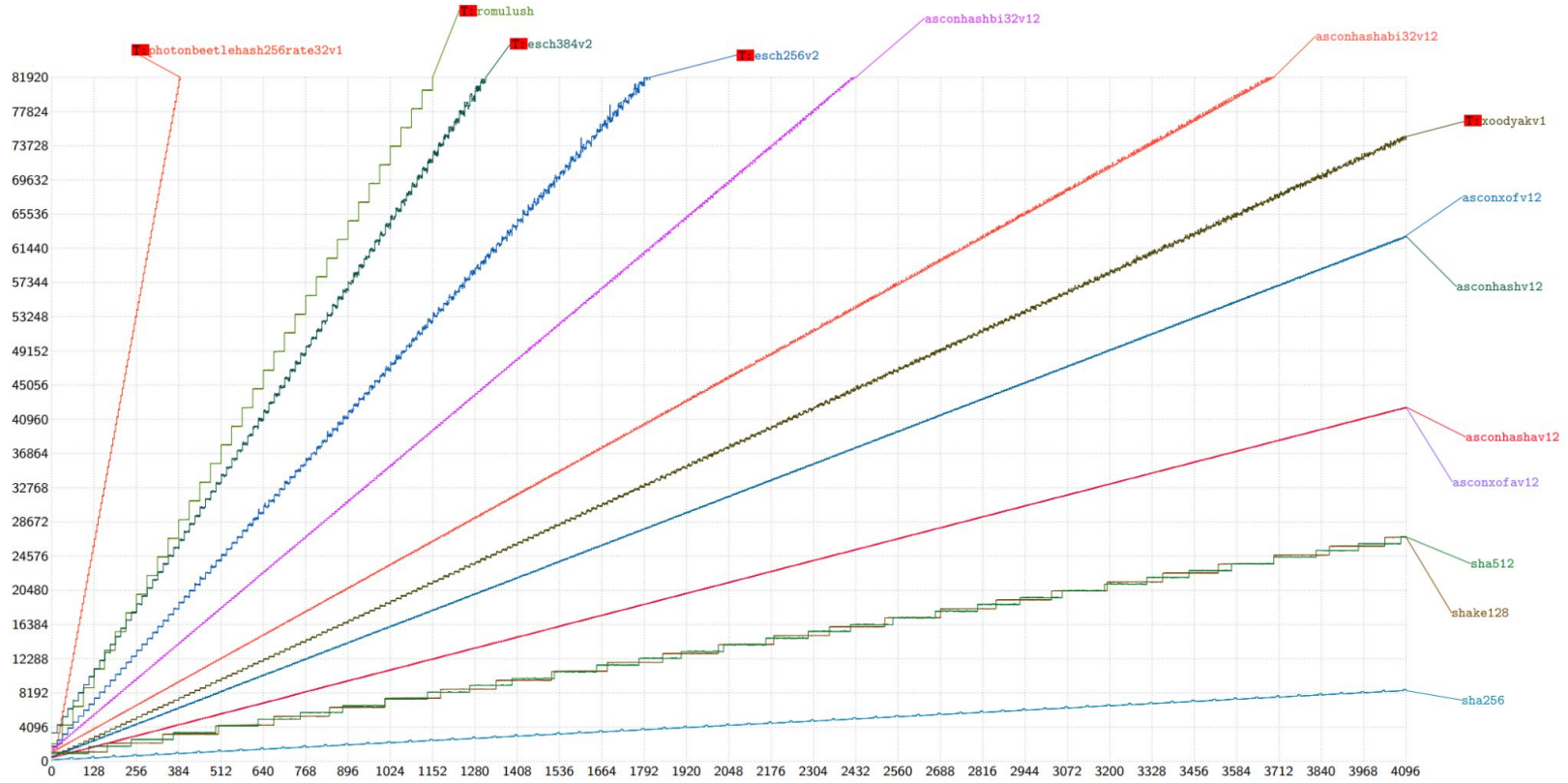
1. AES-128 깨는거랑 비슷한 자원이 필요함
2. SHA-256 충돌 찾기랑 비슷한 자원이 필요함
3. AES-192 깨는거랑 비슷한 자원이 필요함
4. SHA-384 충돌 찾기랑 비슷한 자원이 필요함
5. AES-256 깨는거랑 비슷한 자원이 필요함

PQC 벤치마크



https://github.com/tarcieri/rust-secp256k1-ecdsa-bench

PQC 벤치마크 - Winternitz Signature



PQC 벤치마크 - Winternitz Signature

- SHA256: ~2 cycle/byte

- 128byte Winternitz Signature with SHA256
  - KeyGen: ~2×256×256 = 131072 cycle
  - Signing: ~2×256×128 = 65536 cycle on avg
  - Verification: ~2×256×128 = 65536 cycle on avg

https://bench.cr.yp.to/graph/aarch64-pi5-hash-nistlwc.pdf

PQC 벤치마크 - SQISign

Cycle counts for an optimized implementation using platform-specific assembly running on an Intel *Raptor Lake* CPU:

parameter set	keygen	signing	verifying
NIST - I	43.3 megacycles	101.6 megacycles	5.1 megacycles
NIST - III	134.0 megacycles	309.2 megacycles	18.6 megacycles
NIST - V	212.0 megacycles	507.5 megacycles	35.7 megacycles

https://sqisign.org/

PQC 벤치마크 - SQISign

Cycle counts for an optimized implementation using platform-specific assembly running on an Intel *Raptor Lake* CPU:

parameter set	keygen	signing	verifying
NIST - I	43.3 megacycles	101.6 megacycles	5.1 megacycles
NIST - III	134.0 megacycles	309.2 megacycles	18.6 megacycles
NIST - V	212.0 megacycles	507.5 megacycles	35.7 megacycles

Short-Quarternion-Isogeny Signature

https://sqisign.org/

PQC 벤치마크

	Avg Cycle	Ratio
ECDH	192K	1
Winternitz (SHA256)	~190K	~1
SQISign(NIST Group I Set)	43M	~224

PQC 벤치마크

Algorithm	Public key (bytes)	Ciphertext (bytes)	Key gen. (ms)	Encaps. (ms)	Decaps. (ms)
ECDH NIST P-256	64	64	0.072	0.072	0.072
SIKE p434	330	346	13.763	22.120	23.734
Kyber512-90s	800	736	0.007	0.009	0.006
FrodoKEM-640-AES	9,616	9,720	1.929	1.048	1.064

Table 1: Key exchange algorithm communication size and runtime

Algorithm	Public key (bytes)	Signature (bytes)	Sign (ms)	Verify (ms)
ECDSA NIST P-256	64	64	0.031	0.096
Dilithium2	1,184	2,044	0.050	0.036
qTESLA-P-I	14,880	2,592	1.055	0.312
Picnic-L1-FS	33	34,036	3.429	2.584

Table 2: Signature scheme communication size and runtime

https://eprint.iacr.org/2019/1447.pdf

PQC 벤치마크

Algorithm	Public key (bytes)	Ciphertext (bytes)	Key gen. (ms)	Encaps. (ms)	Decaps. (ms)
ECDH NIST P-256	64	64	0.072	0.072	0.072
SIKE p434	330	346	13.763	22.120	23.734
Kyber512-90s	800	736	0.007	0.009	0.006
FrodoKEM-640-AES	9,616	9,720	1.929	1.048	1.064

Table 1: Key exchange algorithm communication size and runtime

Algorithm	Public key (bytes)	Signature (bytes)	Sign (ms)	Verify (ms)
ECDSA NIST P-256	64	64	0.031	0.096
Dilithium2	1,184	2,044	0.050	0.036
qTESLA-P-I	14,880	2,592	1.055	0.312
Picnic-L1-FS	33	34,036	3.429	2.584

Table 2: Signature scheme communication size and runtime

https://eprint.iacr.org/2019/1447.pdf

이것만은 기억하자

- 양자컴퓨터가 유의미한 수준으로 상용화되면 기존 암호는 멸망한다

이것만은 기억하자

- 양자컴퓨터가 유의미한 수준으로 상용화되면 기존 암호는 멸망한다

- 양자 암호 최적화 잘 된 건 그다지 느리지 않다

이것만은 기억하자

- 양자컴퓨터가 유의미한 수준으로 상용화되면 기존 암호는 멸망한다

- 양자 암호 최적화 잘 된 건 그다지 느리지 않다

- Harvest Now Decrypt Later를 방지하자