Post-Quantum Cryptography (양자 내성 암호)

정유수 202312810

PQC

01 양자 컴퓨터의 발전

02 양자 컴퓨터의 위협

03 PQC란?

04 PQC 종류

05 PQC 전환

06 PQC 활용 사례

양자 컴퓨터의 발전

아시아경제 산업·IT | [과학을 읽다]막오

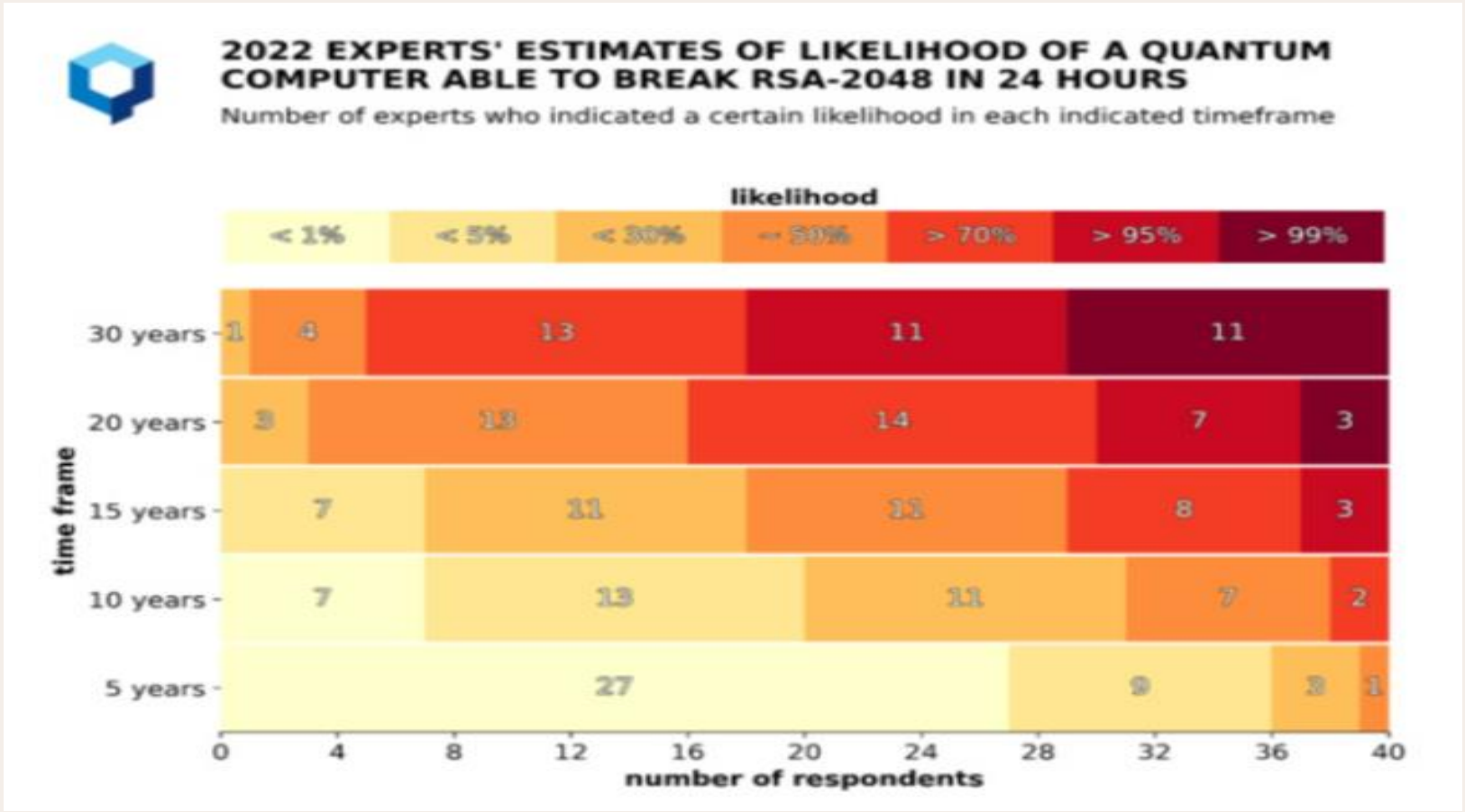
현재의 컴퓨터들은 0과 1로 구성된 이진법을 계산에 사용한다. 이에 반해 양자컴퓨터는 양자역학에 기반해 0과 1을 동시에 다룰 수 있어 연산 속도와 처리 용량이 급격히 치솟는다. 미국 마이크로소프트(MS)가 오픈AI와 함께 생성형 AI에 주력했다면 컴퓨터의 시조격인 IBM은 양자컴퓨터에 주력해왔다. IBM이 지난 4일 공개한 신형 양자컴퓨터는 이목을 끌기에 충분했다는 평이다. 이 양자컴퓨터의 연산속도가 1121큐비트에 달했기 때문이다. IBM은 2022년 433큐비트의 속도로 가장 빠른 양자컴퓨터라는 기록을 세웠지만 1년 만에 속도를 배 이상 끌어 올렸다.

이는 지난 10월 양자컴퓨터 스타트업인 아톰컴퓨팅의 양자컴퓨터가 기록한 연산속도 1180큐비트보다는 소폭 느리지만 1000큐비트를 돌파했다는 점에서 중요한 이정표라는 분석이다. 아톰컴퓨팅은 IBM이 지난해 발표한 1000큐비트 달성 목표를 한 달 앞서 추월하는 성과를 올렸다.

양자 컴퓨터의 위협

Cryptographic Algorithm	Scheme	Type	Pre-quantum Security Level	Post-quantum Security Level
Symmetric-Key Cryptographic Algorithm	AES-128	Block cipher	128	64 (Grover)
	AES-256	Block cipher	256	128 (Grover)
	Salsa20	Stream cipher	256	128 (Grover)
	GMAC	MAC	128	128 (No impact)
	Poly 1305	MAC	128	128 (No impact)
Hash Function	SHA-256	Hash function	256	128 (Grover)
	SHA-3	Hash function	256	128 (Grover)
Public-Key Cryptographic Algorithm	RSA-3072 [27]	Encryption	128	Broken (Shor)
	RSA-3072 [27]	Signature	128	Broken (Shor)
	DSA-3072 [27]	Signature	128	Broken (Shor)
	ECDSA-256	Signature	128	Broken (Shor)
	DH-3072 [27]	Key exchange	128	Broken (Shor)
	ECDH-256 [27]	Key exchange	128	Broken (Shor)

양자 컴퓨터의 위협


2022 EXPERTS' ESTIMATES OF LIKELIHOOD OF A QUANTUM COMPUTER ABLE TO BREAK RSA-2048 IN 24 HOURS
Number of experts who indicated a certain likelihood in each indicated timeframe
likelihood
< 1%
< 5%
< 30%
~ 50%
> 70%
> 95%
> 99%
time frame
30 years
20 years
15 years
10 years
5 years
1
8
13
11
11
3
18
14
7
3
7
11
11
8
3
7
13
11
7
2
27
9
3
1
0
4
8
12
16
20
24
28
32
36
40
number of respondents

PQC란?

• PQC(양자 내성 암호)는 양자 컴퓨터의 공격 시도에도 안전하다고 여겨지는 암호 알고리즘입니다. 양자 컴퓨터도 풀어내는 데 수십억 년이 걸리는 수학 알고리즘을 사용합니다.

• PQC는 수학적 난제에 따라 다변수 기반(Multivariate-based), 코드 기반(Code-based), 격자 기반(Lattice-based), 아이소제니 기반(Isogeny-based), 해쉬 기반(Hash-based) 5가지 유형으로 나뉩니다.

PQC 종류

다변수 이차식 문제 기반

다변수 이차식 시스템의 해를 구하는 문제

해시 함수 기반

해시 함수 H, H(x)=H(x')를 만족하는 값 x, x'를 찾는 문제

격자 문제 기반

가장 짧은 길이의 벡터를 찾는 문제

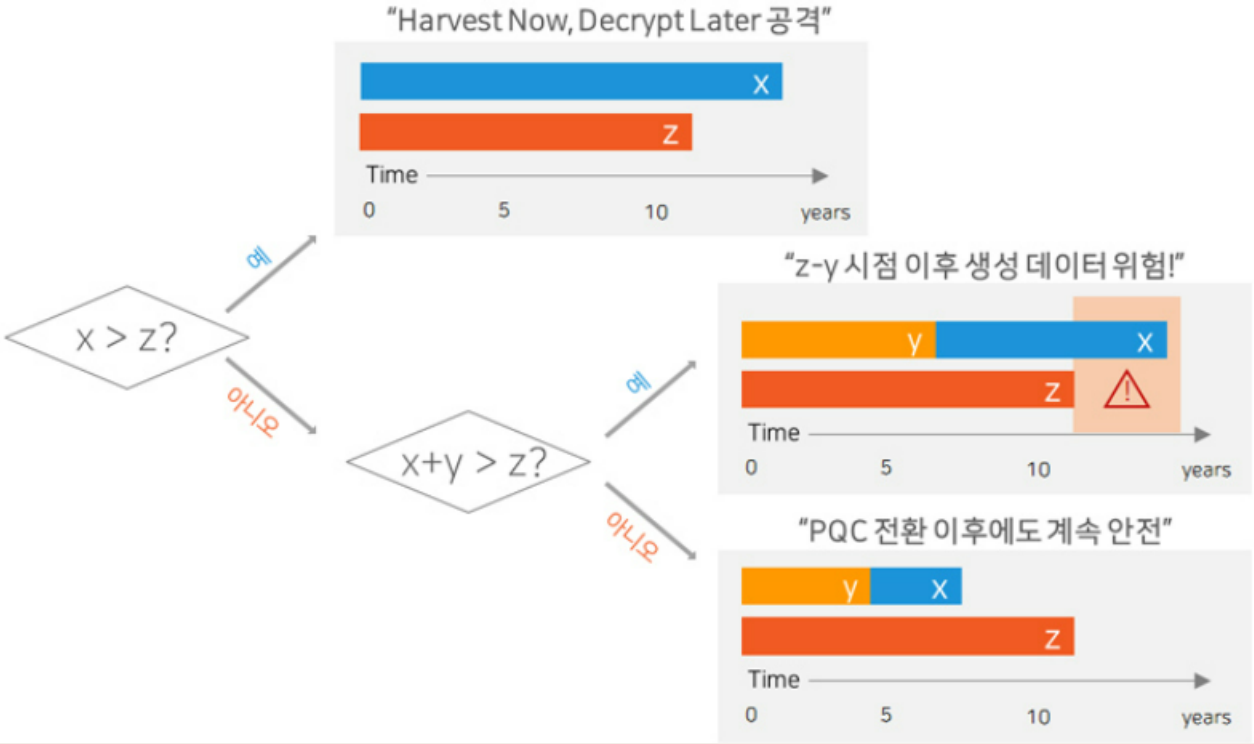
코드 문제 기반

Syndrome Decoding problem

Supersingular isogeny 문제 기반

Supersingular 타원곡선에서 isogeny를 찾는 문제

PQC전환



- x: Shelf-life Time
- y: Migration Time
- z: Threat Timeline

PQC 활용 사례

SK브로드밴드는 지난 8월 SW 업데이트를 통해 PQC-VPN 설치를 완료하고 미국, 일본, 싱가폴 등 해외에서 네트워크 테스트를 성공적으로 완료했다고 설명했다.

PQC-VPN은 VPN 네트워크의 보안 강화를 위해 PQC 공개키 암호화, 키분배, 전자서명 알고리즘을 적용했다.