2022
Trends of Information Security

INTERLUDE 12기 한아림

Keyword?

Of 2022 Information Security

양자컴퓨팅

Quantum Computing

특수한 하드웨어에서의 계산을 실행하거나 정교한 병렬 연산을 수행하기 위해 양자 역학을 컴퓨팅에 적용하여 사용하는 것

양자컴퓨팅 보안

Quantum Computing Security

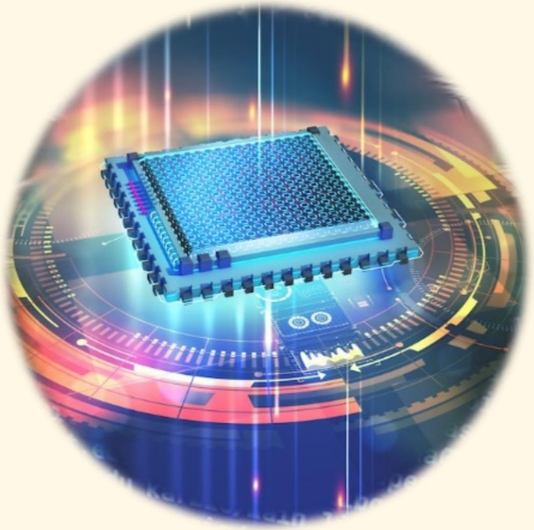
Features
Of Quantum Computing

1

빠른 데이터 처리 속도

2

높은 효율



3

가역적 처리 능력

Security Threats

Caused by high data processing speed

현재 암호 알고리즘의 보안 위협

알고리즘	종류	목적	양자 컴퓨터 대비사항
AES	**대칭키**	**Encryption**	**키 길이 증가 필요 (Larger key sizes needed)**
RSA	**공개키**	**Signatures, Key establishment**	**더 이상 안전하지 않음 (No longer secure)**
SHA-2, SHA-3	-	Hash functions	출력 길이 증가 필요 (Larger output needed)
ECDSA, ECDH (Elliptic Curve Cryptography)	공개키	Signatures, Key exchange	더 이상 안전하지 않음 (No longer secure)
DSA (Finite Field Cryptography)	공개키	Signatures, Key exchange	더 이상 안전하지 않음 (No longer secure)

NIST:미국 국립표준기술연구소(National Institute of Standards and Technology)

- 2019 Google “양자컴퓨터 연산력 > 슈퍼컴퓨터”

- 현 암호 생성 시스템 알고리즘 : 대부분 소인수분해 이용

→ 양자컴퓨팅에 의한 암호 방식 무력화

Ex) Google의 연구 결과 : 129자리 수 소인수분해

“기존 컴퓨터 1600대” -> 8개월

VS

“양자컴퓨터 1대” -> n분

장치 독립적 양자 키 배포 시스템

Device-independent quantum key distribution system

- **영국 인디펜던트의 연구 결과**

: 광자와 같은 양자 입자에 의해 키가 분산되는 시스템.

: 양자 입자가 측정되는 경우 바로 흐트러짐으로써 정보를 안전하게 유지

- **이전 시스템 사용 보류**

: 이런 시스템을 사용하려면 광자 소스 및 검출기와 같은 시스템의 일부 부분에 대한 신뢰가 필요 → 해커가 침투할 수 있는 약점 多

- **단일 광자 대신 엉킨 입자를 사용하여 문제 해결**

: 엉킨 입자의 경우 멀리서도 작용 → 시스템은 양자 입자 생성 및 검출 장치에 대한 신뢰 필요 X

Thank You!

Any Questions?