양자내성암호 전환

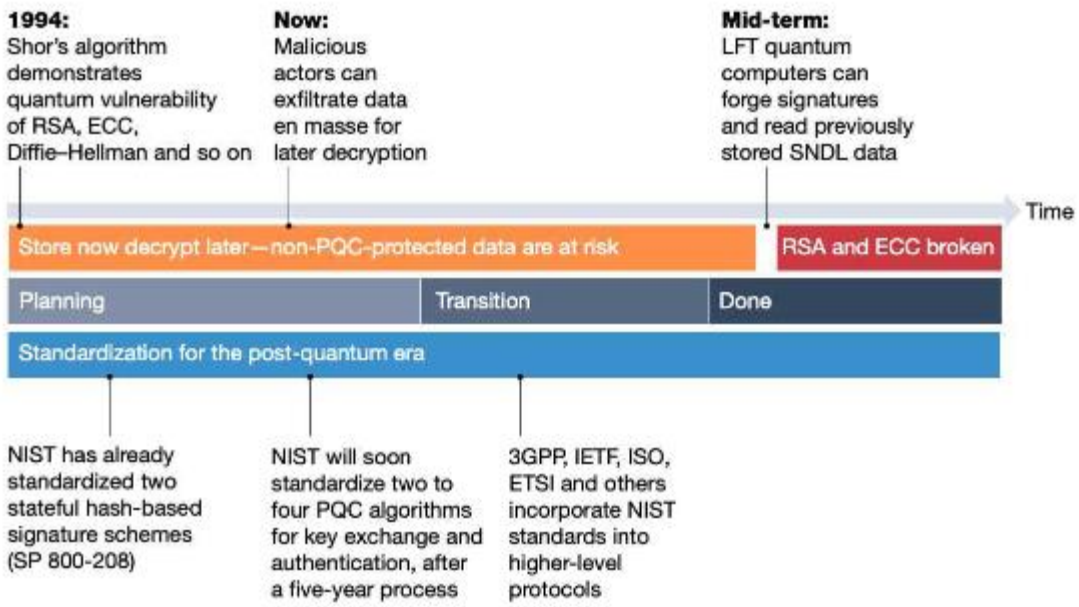
정보컴퓨터공학과 권혁동

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

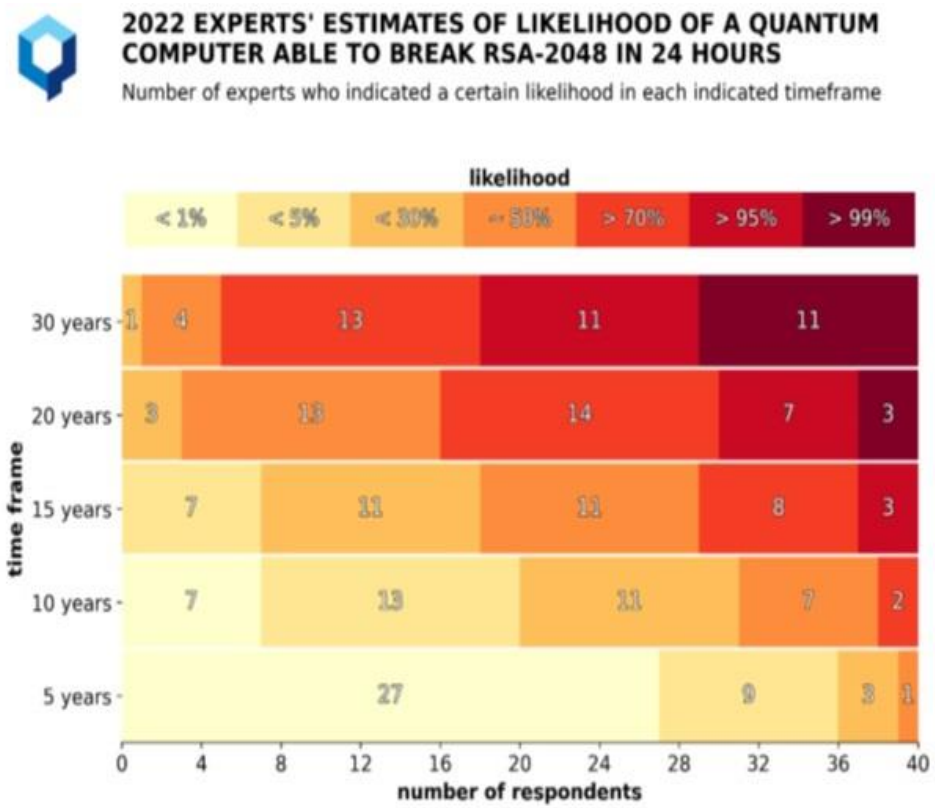
양자내성암호의 필요성

- 양자컴퓨터의 등장으로 현대 암호 체계의 붕괴가 우려됨
  - **특히 공개키 암호는 거의 사용이 불가**
- 전 세계에서 양자내성암호로 전환을 위해 노력이 진행 중
  - 미국의 NIST에서는 양자내성암호 표준화 공모전 개최
  - 한국의 양자내성암호연구단에서도 한국의 양자내성암호 표준 선정 중



양자내성암호의 필요성

- 양자컴퓨터는 정말로 위협적인가?
  - 캐나다의 Global Risk Institute에서 설문 조사
  - **5년 내로 등장할 것이다 → 회의적**
  - **15년 내로 등장할 것이다 → 반반**

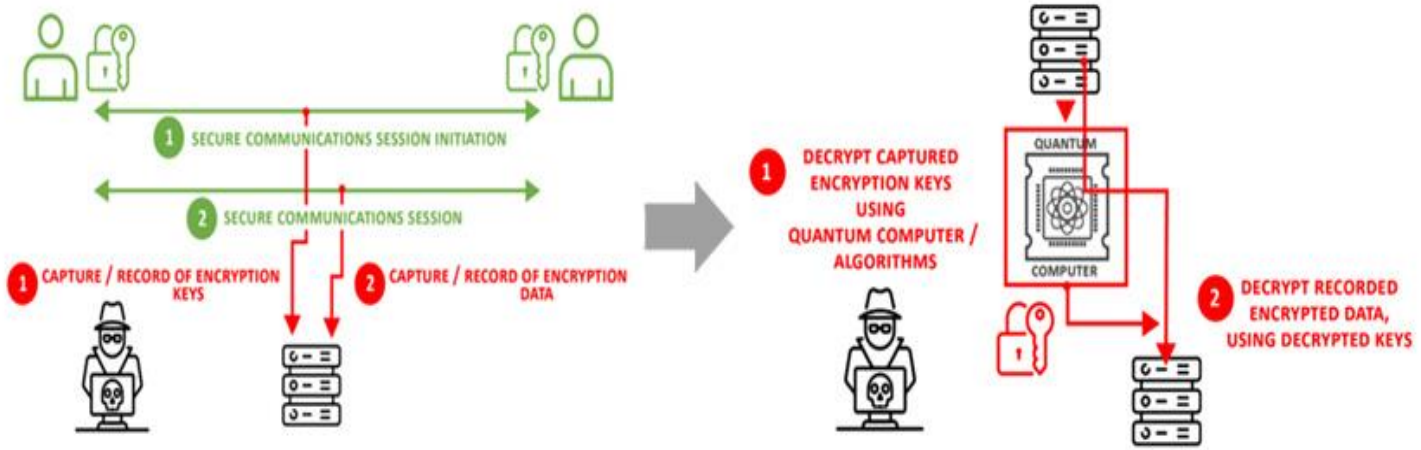


- 양자컴퓨터가 나오기 전에 전환해야 하는가?
  - Mosca의 정리
  - 비밀 데이터 유지 기간 X
  - 암호 알고리즘이 유효한 기간 Y
  - 양자컴퓨터 상용화까지 남은 기간 Z
  - **X + Y > Z일 경우 위험**

양자내성암호의 필요성

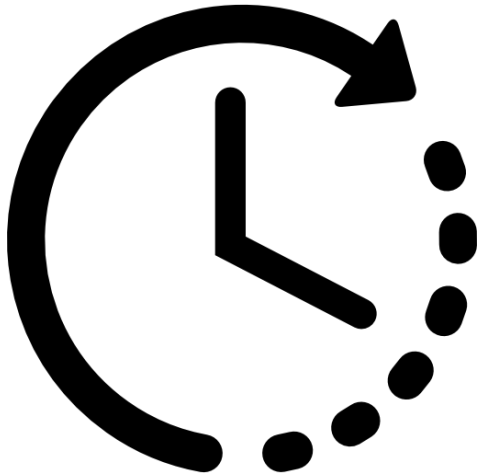
- Harvest Now Decrypt Later
  - **통념과는 다르게 양자컴퓨터가 없는 현재에도 빠른 전환이 필요한 이유**
- 비밀 데이터를 지금 획득하고 **나중에 분석**하는 공격 기법
  - 현재는 양자컴퓨터가 없기에 데이터가 안전함
  - 그러나 **암호화 된 데이터를 탈취(Harvest Now)**하는 것은 가능
  - 양자컴퓨터 등장 이후 **탈취해둔 데이터를 복구(Decrypt Later)**

→ 비밀 정보 획득

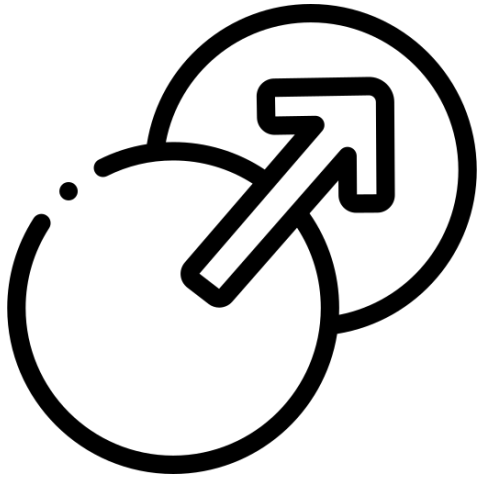


양자내성암호 전환

- **양자내성암호 표준은 이미 나와있음**
  - Kyber / Dilithium, Falcon, SPHINCS+
  - 그리고 추가 표준도 등장할 예정
  - 그러나 표준이 있다고 해서 **전환이 되는 것은 아님**



- 고려해야 할 두 가지 요소
  1. 전환에 걸리는 시간?
  2. 전환 하는 방법?



양자내성암호 전환

- 전환에 얼마나 시간이 걸리는가?
  과거의 암호 전환 기록을 통해 현재 전환을 예상해보기

DES → AES	SHA-1 → SHA-2, SHA-3	ECC
• 90년대 표준 DES, 3DES • 2001 Rijndael을 AES 표준 지정 • DES, 3DES → AES 전환 시작 • 그러나 일부 시스템에 3DES 잔존 • 여전히 **전환이 진행 중**	• SHA-1은 95년에 발표된 해시함수 • 2011년 SHA-1의 취약성 인정 • SHA-2, SHA-3로 전환 권고 • 2030년 말 SHA-1의 모든 지원 중단 • **약 20년가량 소요**	• ECC는 1978년에 발표 되어 지정됨 • 이후 교체된 적 없음 • RSA는 ECC보다 매개변수가 큼 • **RSA 전환은 어려울 것으로 예상**

양자내성암호 전환

- 전환은 어떻게 해야하는가?
  1. 암호화 민첩성(Crypto Agility): 전환하고자 하는 알고리즘과의 호환성
  2. 암호화 인벤토리(Crypto Inventory): 사용중인 암호 알고리즘의 목록

- 완전한 알고리즘 전환은 현 시점에서 불가능
  - 민첩성 문제 → 완전한 호환이 되지 않음
  - 인벤토리 문제 → 어디서 무슨 알고리즘을 사용하는지 알고있지 않음

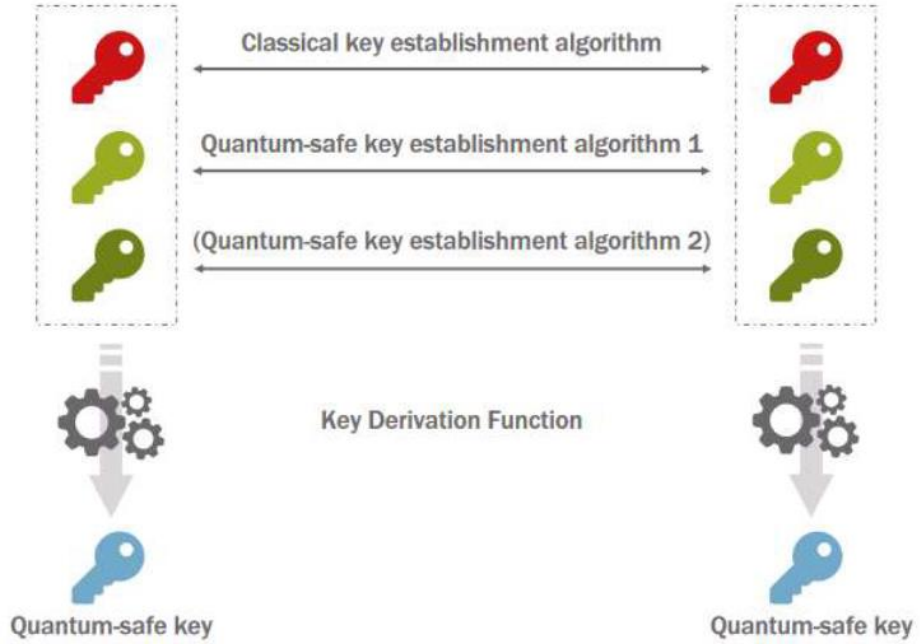
양자내성암호 전환

- 하이브리드 솔루션
  - 현대 암호를 완벽하게 전환할 수 없다면? **둘 다 쓰자**
  - 평문 → 현대 암호 → 양자내성암호
- 장점
  - **당장 양자내성암호 적용이 가능함**

    →암호화 민첩성과 관계 없이 적용 가능
  - 양자컴퓨터가 등장할 때까지 임시로 버틸 수 있음
- 단점
  - 완벽한 전환은 아니기에 결국 현대 암호를 포기해야 하는 시기가 옴

양자내성암호 전환

- KDF(Key Derivation Function)에 적용
  - 현대 암호를 사용한 키 설정
  - 양자내성암호를 통한 추가 키 생성
  - 필요에 따라서는 양자내성암호를 더 사용
- 효과
  - HNDL 공격으로 기존 암호 키를 탈취 가능
  - 그러나 양자내성암호 키는 복구 불가



양자내성암호 전환

- 전자서명에 적용
  - 위조와 분리불가 특성을 가지도록 설계
  - 위조: 현대 암호, 양자내성암호 모두 알아야 가짜 서명 생성 가능
  - 분리불가: 기존 서명과 양자내성서명을 분리할 수 없음
  - 메시지를 양자내성암호로 서명
  - 메시지와 서명 값을 기존 알고리즘으로 추가 서명