경량 블록 암호 post-quantum 보안 강도 확인
https://youtu.be/Yc0Rxge-AQc

송경주

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

양자 알고리즘

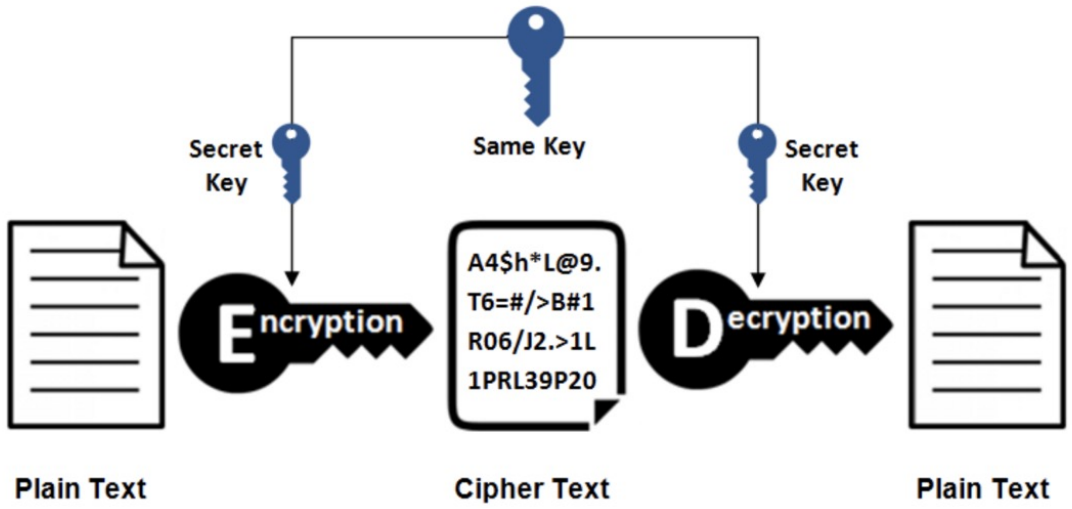
SPN, ARX 구조 경량암호

강도 평가

Quantum algorithm

- Grover algorithm

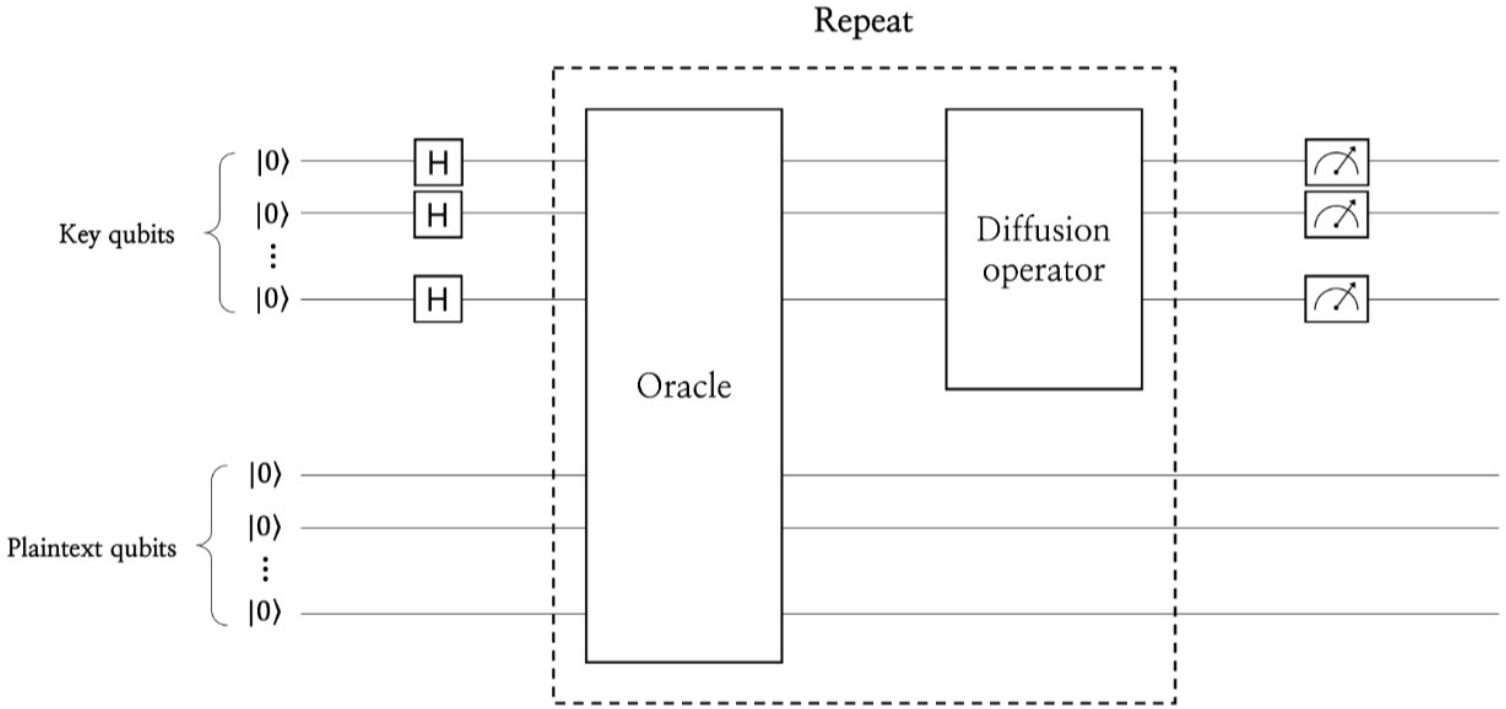
- 중첩 상태의 key를 이용하여 대칭키 암호에 대하여 brute-force attack을 수행하는 알고리즘.
- Block cipher 에 대한 brute-force attack 을 빠르게 수행 가능.
- 하지만 현재 양자컴퓨터의 성능 한계(qubit 수, 오류 등)로 실제 양자컴퓨터로 동작은 불가능.
- 양자 컴퓨터의 가용 자원이(ex. 사용 가능한 qubit 수) 암호 공격에 필요한 자원에 도달할 때가 곧 암호가 깨질 수 있는 시점.
- 양자 자원이 한정되어 있으므로 최적화된 구현(ex. 적은 양의 qubit, quantum gate)은 양자컴퓨터의 실제 실행 시기와 연관되어 있음.

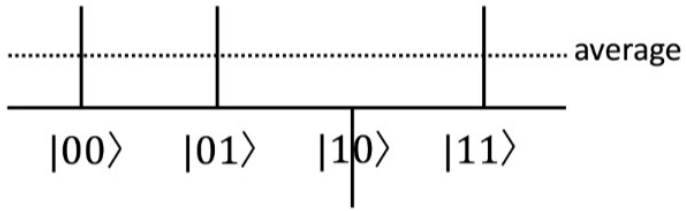


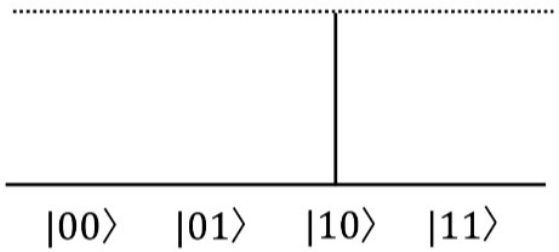
Quantum algorithm

- Grover algorithm
  - **Oracle** : 주어진 평문-암호문 쌍에 대한 키를 찾음, 이때, 대상이 되는 암호가 양자 회로로 구현되어야 함.
  - **Diffusion operator** : Oracle에서 찾은 키의 진폭을 증폭시켜 관측 확률 증가
  - n-bit 키의 대칭키 암호에 대해 Oracle과 Diffusion operator를 $\left\lfloor \frac{\pi}{4}\sqrt{2^n} \right\rfloor$번 반복. (약 $\sqrt{2^n}$번)

Key search : Classic computer : 2^n번, Quantum computer : $2^{\frac{n}{2}}$ 번

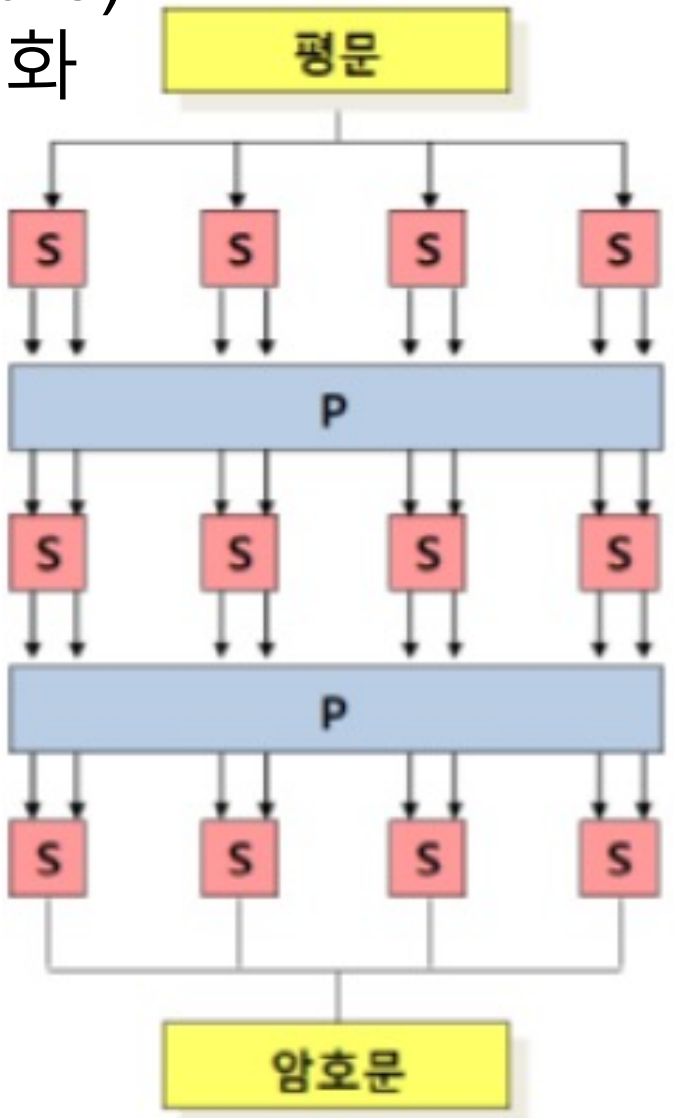






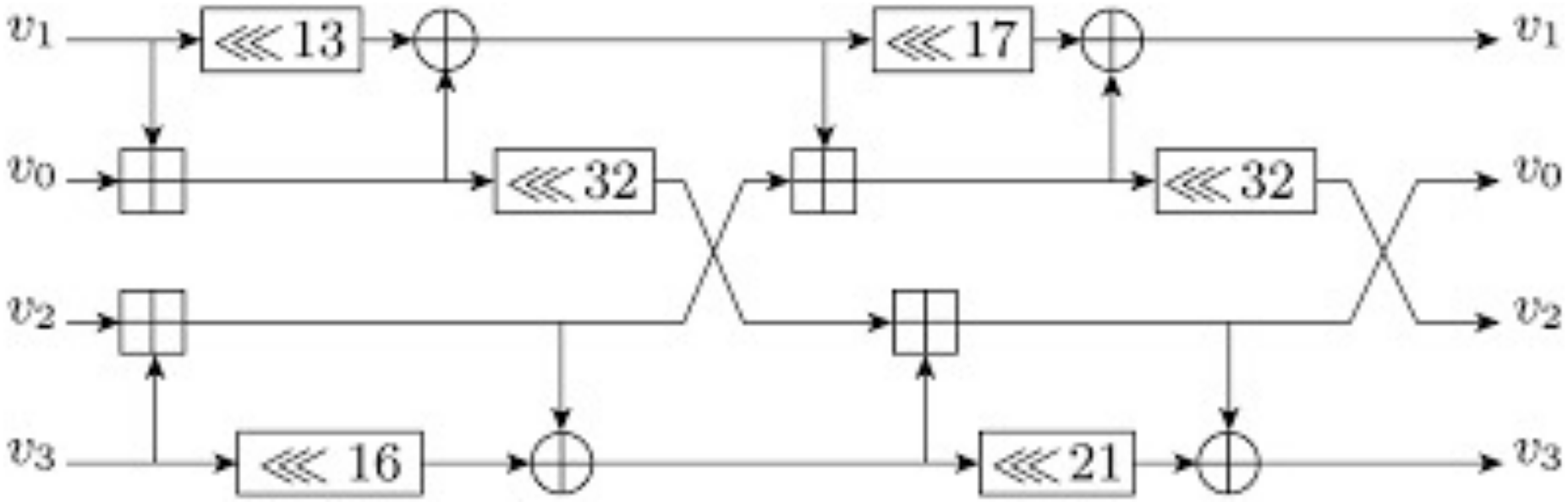
SPN 구조

- SPN 구조 (Substitution Permutation Network Structure)
  - Substitution + Permutation 연산의 반복으로 암호화
  - 병렬 연산이 가능
  - 복호화, 암호화 알고리즘이 다름.
  - Ex) PRESENT, GIFT, PIPO ..



ARX 구조

- ARX 구조
  - Addition, Rotation Shift, XOR 연산의 반복으로 암호화
  - 양자컴퓨터에서는 ARX의 Addition 연산에 많은 양자 자원이 필요함 (SIMON은 예외적으로 Addition이 아닌 Add를 사용)
  - Ex)HIGHT, LEA, SIMON, CHAM



양자 자원 확인

- SPN구조와 ARX 구조의 양자 자원 확인
- ARX 구조의 암호에서 Addition 연산에 많은 양자 자원을 사용하므로 SPN 구조의 암호보다 추정 자원이 높다.
- Add연산을 사용하는 SIMON은 예외적으로 적은 양자자원으로 구현되었다.

<SPN 구조 경량 암호의 그루버 알고리즘 적용 자원 추정>

Cipher	gates			Depth
	T	Clifford	Total	
GIFT 64-128 [2]	$1.2 \cdot 2^{78}$	$1.76 \cdot 2^{79}$	$1.18 \cdot 2^{80}$	$1.41 \cdot 2^{74}$
PIPO 64-128 [4]	$1.67 \cdot 2^{78}$	$1.31 \cdot 2^{79}$	$1.07 \cdot 2^{80}$	$1.52 \cdot 2^{73}$
PIPO 64-256 [4]	$1.09 \cdot 2^{144}$	$1.71 \cdot 2^{144}$	$1.4 \cdot 2^{145}$	$1.98 \cdot 2^{138}$

<ARX 구조 경량 암호의 그루버 알고리즘 적용 자원 추정>

Cipher	gates			Depth
	T	Clifford	Total	
SIMON 64-128 [5]	$1.32 \cdot 2^{77}$	$1.23 \cdot 2^{76}$	$1.94 \cdot 2^{77}$	$1.52 \cdot 2^{75}$
HIGHT 64-128 [6]	$1.05 \cdot 2^{81}$	$1.69 \cdot 2^{81}$	$1.37 \cdot 2^{82}$	$1.57 \cdot 2^{79}$
CHAM 64-128 [6]	$1.61 \cdot 2^{79}$	$1.52 \cdot 2^{80}$	$1.16 \cdot 2^{81}$	$1.49 \cdot 2^{78}$
CHAM 64-256 [6]	$1.99 \cdot 2^{143}$	$1.92 \cdot 2^{144}$	$1.45 \cdot 2^{145}$	$1.14 \cdot 2^{143}$

강도평가

- NIST에서는 post-quantum security strength에 대한 기준을 제시함.
  - **Level 1** : 128-bit key의 블록암호는 AES-128에서 사용하는 quantum resource 를 기준으로 평가.
  - **Level 3** : 192-bit key의 블록암호는 AES-192에서 사용하는 quantum resource 를 기준으로 평가.
  - **Level 5** : 256-bit key의 블록암호는 AES-256에서 사용하는 quantum resource 를 기준으로 평가.

Level 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)**
Level 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)**
Level 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)**

강도평가

- Post-quantum security strength평가에 필요한 quantum resource 계산.

quantum resource = total gates × total depth

→ quantum resource 기준 : AES-128 = 2^{170}, AES-196 = 2^{233}, AES-256 = 2^{298}

- 양자회로를 이용하여 Grover algorithm에 필요한 quantum resource 계산
- 계산한 quantum reosource 를 사용하여 post-quantum 보안 강도 확인

강도평가

- Block cipher strength evaluation

- NIST에서 제시한 기준에 따라 post-quantum security strength를 평가.
  - 평가결과

    일반적으로 128-bit 키를 가지는 경량암호들은 모두 기준 level에 도달하지 못함.
    예외적인 경우(SIMON)을 제외하고 SPN 구조의 경량암호가 양자 컴퓨터에 더 취약함.
    같은 암호에 키 길이를 증가시키면 기준 level에 도달하는 결과를 보임.

- 양자컴퓨터에서 보안을 유지하기 위해서는 키 길이를 증가시키는 방법을 고려할 수 있음.

<SPN 구조 경량 암호 강도평가>

Cipher	Quantum resource (Total gates × Total depth)	Level
GIFT 64-128[2]	$1.66 \cdot 2^{154}$	-
PIPO 64-128[4]	$1.62 \cdot 2^{153}$	-
PIPO 64-256[4]	$1.38 \cdot 2^{284}$	Level 3

ARX구조 경량 암호 강도평가>

Cipher	Quantum resource (Total gates × Total depth)	Level
SIMON 64-128[5]	$1.47 \cdot 2^{153}$	-
HIGHT 64-128[6]	$1.07 \cdot 2^{162}$	-
CHAM 64-128[6]	$1.72 \cdot 2^{160}$	-
CHAM 64-256[6]	$1.65 \cdot 2^{288}$	Level 3

Q & A