양자회로 상에서 경량 블록암호 구현 동향

IT융합공학부 송경주

Contents

서론

- 시스템에서는 데이터를 보호하기 위해 공개키 암호 및 블록암호를 사용함

- 양자컴퓨터의 성능이 암호 공격에서의 사용으로 제안되면서 현재 암호 체계에 위협이 되고 있음

> **Grover's algorithm :** 대칭키 암호에 대해 **brute-force attack 가속화**
> (n-bit 의 보안 수준을 $\sqrt{n}$-bit 수준으로 줄임)
>
> **Shor's algorithm :** 공개키 암호에 대해 **소인수 분해**를 다항시간 내에 수행

- IoT 환경에서는 많은 정보를 주고받는 만큼 데이터에 대한 보안이 중요
  - 사물인터넷에서 사용하는 저사양 디바이스는 리소스 및 운용에 제한이 있으므로 기존 기기에 사용하는 암호화 방식을 사용하기 어려움

  → 저사양 디바이스를 위한 암호화 방식인 경량암호를 사용

양자 컴퓨터

- **양자 컴퓨터의 가용 자원이(ex. 사용 가능한 큐비트 수) 암호 공격에 필요한 자원에 도달할 때가 곧 암호가 깨질 수 있는 시점으로 봄**

- 양자 알고리즘을 동작하기 위해서 공격 대상이 되는 암호를 양자회로로 구현해야 하며 양자자원을 줄이는 최적화 방식을 통해 공격 시기를 앞당긴다고 예상함

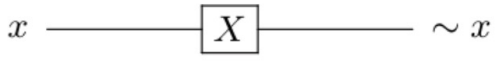
- 앞선 많은 연구들은 post-quantum 강도를 평가하기 위해 공격 대상이 되는 암호를 양자회로로 구현하고 공격 자원을 추정하는 연구들이 꾸준히 진행되고 있음

- **본 논문에서는 사물 인터넷 환경에서 사용하기 위해 설계된 경량블록 암호에 대한 양자회로 구현 동향을 살펴봄**

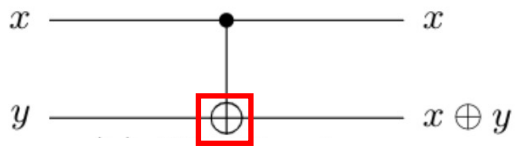
관련연구 - 양자컴퓨터

- 양자컴퓨터는 큐비트의 **중첩** 및 **얽힘**의 양자 상태를 활용하여 계산을 수행
- 큐비트의 **중첩** 성질로 인해 n큐비트로 2^n개의 경우를 한번에 표현하고 연산 가능
- Quantum gate

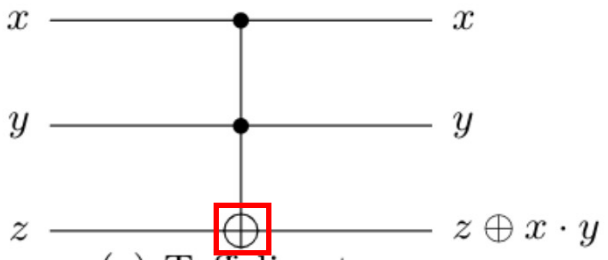
- 양자 컴퓨터에서는 디지털 회로의 디지털 논리 게이트와 유사하게 양자 게이트를 사용하여 큐비트의 상태를 제어
- 큐비트는 양자회로 연산에서 Control 큐비트 과 Target 큐비트로 나눌 수 있음
  - ■**Control 큐비트** : 연산에 영향을 주는 큐비트, 값이 바뀌지 않음 ■ **Target 큐비트** : 연상 대상, 결과 값이 저장됨
- 측정을 제외한 모든 연산에 대하여 **가역적 특성**을 가짐 → inverse 연산 가능
- 대표적인 양자 게이트로는 **Hadamard gate, X gate, CNOT gate, Toffoli gate, Swap gate**가 있음
- 큐비트와 양자 게이트로 구성한 회로를 **양자 회로(Quantum circuit)** 라고 함



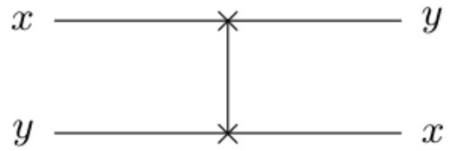
(a) X (NOT) gate



(b) CNOT gate



(c) Toffoli gate



(d) Swap gate

연구동향 - LEA 양자회로

- LEA
  - LEA는 2013년 한국인터넷진흥원에서 제시한 128-bit의 경량 블록암호
  - ARX연산으로 구성되며 128, 192, 256 bit의 키 사이즈를 제공
  - “Optimization of LEA Quantum Circuits to Apply Grover’s Algorithm”[1]의 LEA 양자회로 구현에서는 LEA 경량블록암호의 내부 함수 중 키 스케줄의 상수 덧셈을 최적화 함

<LEA 키 스케줄>

- δ : 정의된 상수
- ROL_i : i-bit의 left rotation을 나타냄

$$\delta[0] = 0xc3efe9db, \quad \delta[1] = 0x44626b02$$
$$\delta[2] = 0x79e27c8a, \quad \delta[3] = 0x78df30ec$$
$$\delta[4] = 0x715ea49e, \quad \delta[5] = 0xc785da0a$$
$$\delta[6] = 0xe04ef22a, \quad \delta[7] = 0xe5c40957$$

$$K[0] = ROL_1(ADD(K[0], ROL_i(\delta[i \bmod 4])))$$
$$K[1] = ROL_3(ADD(K[1], ROL_{i+1}(\delta[i \bmod 4])))$$
$$K[2] = ROL_6(ADD(K[2], ROL_{i+2}(\delta[i \bmod 4])))$$
$$K[3] = ROL_{11}(ADD(K[3], ROL_{i+3}(\delta[i \bmod 4])))$$
$$RK_i = (K[0], K[1], K[2], K[3], K[1])$$

<키 스케줄링 함수>

[1] Jang, K. B. et al. (2021) “Optimization of LEA Quantum Circuits to Apply Grover’s Algorithm,” KIPS Transactions on Computer and Communication Systems. 한국정보처리학회, 10(4), pp. 101 –106. doi: 10.3745/KTCCS.2021.10.4.101.

연구동향 - LEA 양자회로

- LEA
  - 이전의 LEA 양자회로 “Grover on Korean Block Ciphers”[2]에서는 로테이션 된 δ와 K의 덧셈을 수행하기 위해 상수 $\delta[0], \delta[1], \delta[2], \delta[3]$ 의 값을 저장하기 위한 큐비트를 할당하여 사용함
  - 32-bit 의 δ의 값을 저장하기 위해서는 $32\text{bit} \times 4(\delta$ 개수) = 128 개의 큐비트를 사용해야함 (LEA-192 : 192개, LEA-256 : 256개 사용)

  - “Optimization of LEA Quantum Circuits to Apply Grover’s Algorithm” [1]의 LEA 양자회로 구현 논문에서는 여러 개의 상수 δ (최대 8개)에 대해 하나의 δ 크기의 큐비트를 할당하여 재사용 하였음

  - 사용되는 δ의 값과 순서는 정해져 있으므로 연산에 필요한 δ의 값을 X게이트를 사용하여 생성함

[1] Jang, K. B. et al. (2021) “Optimization of LEA Quantum Circuits to Apply Grover’s Algorithm,” KIPS Transactions on Computer and Communication Systems. 한국정보처리학회, 10(4), pp. 101 –106. doi: 10.3745/KTCCS.2021.10.4.101.
[2] K. B. Jang, S. J. Choi, H. D. Kwon, H. J. Kim, J. H. Park, and H. J. Seo, “Grover on Korean Block Ciphers,” Applied Sciences, Vol.10, No.18, pp.6407, 2020.

연구동향 - LEA 양자회로

- LEA 양자회로의 양자자원 추정 결과
  - **[1]에서 제안한 양자회로 자원추정 결과 <표 1>**는 큐비트 최적화 방식을 통해 이전의 LEA 양자회로 구현 결과[2] <표 2>보다 할당 큐비트를 각각 LEA 128에서 96개, LEA192에서 160개, LEA256에서 224개를 감소시킴

<표 1> LEA 양자 자원 추정 결과 [1]

	Quantum gates			
	Toffoli	CNOT	X	Qubit
LEA 128	10,416	28,080	352	289
LEA 192	15,624	39,816	398	353
LEA 256	17,856	45,504	465	417

<표 2> LEA 양자 자원 추정 결과 [2]

	Quantum gates			
	Toffoli	CNOT	X	Qubit
LEA 128	10,416	28,080	68	385
LEA 192	15,624	39,816	100	513
LEA 256	17,856	45,504	130	641

[1] Jang, K. B. et al. (2021) “Optimization of LEA Quantum Circuits to Apply Grover’s Algorithm,” KIPS Transactions on Computer and Communication Systems. 한국정보처리학회, 10(4), pp. 101 –106. doi: 10.3745/KTCCS.2021.10.4.101.
[2] K. B. Jang, S. J. Choi, H. D. Kwon, H. J. Kim, J. H. Park, and H. J. Seo, “Grover on Korean Block Ciphers,” Applied Sciences, Vol.10, No.18, pp.6407, 2020.

연구동향 – SIMON 양자회로

- SIMON

- SIMON은 2013년 National Security Agency (NSA)에서 공개한 경량암호
- Feistel 구조의 블록 암호이며 다양한 키 사이즈를 제공
- SIMON은 두 개의 내부 함수인 라운드 함수화 키 확장 함수로 구성됨
- 그림 2는 SIMON에 대한 라운드 함수를 보여주며 수식 (1)은 라운드 함수 F에 대한 수식을 나타냄
- $S^i(x)$는 i-bit 만큼의 left rotation을 수행하며 k_i는 i번째 라운드 키를 의미

$$F(x,y) = (y \oplus S^1(x)S^8(x) \oplus S^2(2) \oplus k, x) \quad (1)$$

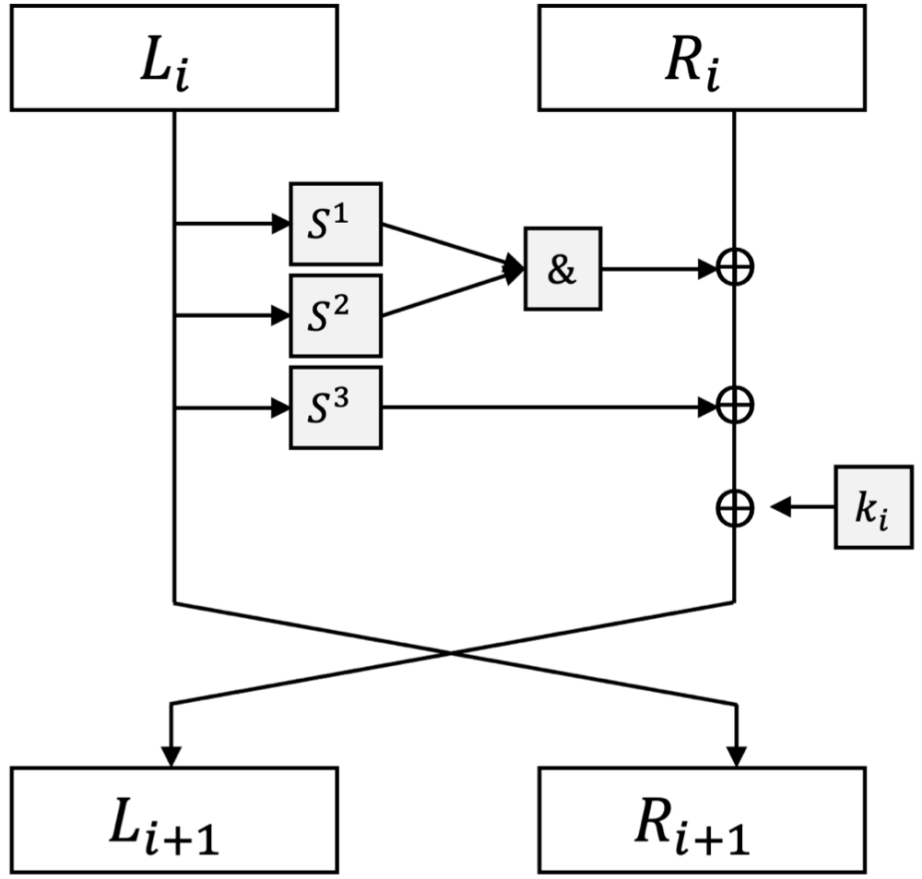


그림 2. SIMON 라운드 함수

[3] Anand, Ravi, Arpita Maitra, and Sourav Mukhopadhyay. "Grover on SIMON" Quantum Information Processing 19.9 (2020): 1-17.

연구동향 – SIMON 양자회로

- SIMON 양자회로[2]
  - "Grover on SIMON" [3]에서는 SIMON에 대한 가역 양자회로를 설계하고 그루버 알고리즘 공격에 필요한 양자 게이트를 제시함
  - 논문에서는 키 K에 대해 k-큐비트가 할당되어 있으며 L과 R에 대해 각각 n개의 큐비트가 할당되어 있다고 가정하여 다음과 같은 식을 나타냄

$$R_2(i) = L_1(i) = R_0(i) \oplus K_0(i) \oplus L_0((i+1) \bmod (n/2)) \\ \oplus L_0((i+8) \bmod (n/2)) \oplus L_0((i+2) \bmod (n/2))$$

  - SIMON 2라운드에서 R_2의 각 비트는 R_0, $F(L_2)$, K_0와 XOR 됨
  - SIMON 2라운드에서 L_2의 각 비트는 L_0, $F(R_2)$, K_1와 XOR 됨
    - 이때, $F(x) = S^1(x)S^8(x) \oplus S^2(x)$
  - 이와 같은 연산을 통해 추가적인 큐비트를 사용하지 않도록 하였으며 키 확장에서 ancilla 큐비트를 사용하지 않고 상수를 적절한 X게이트를 사용하여 회로를 구현함

[3] Anand, Ravi, Arpita Maitra, and Sourav Mukhopadhyay. "Grover on SIMON" Quantum Information Processing 19.9 (2020): 1-17.

연구동향 - LEA 양자회로

- SIMON 양자회로의 양자자원 추정 결과[2]
  - <표 3>은 SIMON (블록 크기)/(키 길이)에 대한 양자 자원 추정 결과를 보여줌
  - brute-force attack 수행에는 Grover's algorithm 내부의 Oracle 반복만큼 암호화를 진행 : $2 \times$ <표 3> $\times \left\lfloor \frac{\pi}{4} \times \sqrt{2^{key\ length}} \right\rfloor$ 의 양자 자원 필요

<표 3> SIMON 양자 자원 추정 결과 [3]

	Quantum gates			
	X	CNOT	Toffoli	Depth
SIMON 32/64	448	2,816	512	946
SIMON 48/72	792	3,312	864	1,062
SIMON 48/96	768	4,800	864	1,597
SIMON 64/96	1,248	5,184	1,344	1,674
SIMON 64/128	1,216	7,396	1,408	2,643
SIMON 128/256	4,352	26,624	4,608	8,848

[3] Anand, Ravi, Arpita Maitra, and Sourav Mukhopadhyay. "Grover on SIMON" Quantum Information Processing 19.9 (2020): 1-17.

결론

- 본 논문에서는 저사양 디바이스에서 사용하기 위해 설계된 경량암호에 대한 양자회로 구현 동향을 살펴보았음

- 경량암호에 대한 post-quantum 보안 강도를 평가하기 위해서는 대상 암호에 대해 양자회로로 구현하고 그루버 알고리즘에 필요한 양자자원을 추정해야 함

- 살펴본 LEA, SIMON 경량암호 양자구현에서는 대상 암호에 대해 최적화 방식으로 양자회로를 구현하고 양자자원 추정 결과를 제시함

Q & A