SIMECK에 대한 양자회로 최적화 구현

송경주[1], 장경배[1], 심민주[1], 서화정[1]
[1]한성대학교 IT융합공학부
thdrudwn98@gmail.com, starj1023@gmail.com, minjoos9797@gmail.com,
hwajeong84@gmail.com

Implementation of quantum circuit optimization for SIMECK

Gyeong-Ju Song[1], Kyung-Bae Jang[1], Min-Joo Sim[1], Hwa-Jeong Seo[1]
[1]Dept. of Convergence Engineering, Han-Sung University

요 약

대규모 양자컴퓨터가 등장하면 기존 암호체계가 더 이상 안전하지 않을 것이라 예상한다. 양자 알고리즘인 Grover's 알고리즘은 대칭키 암호에 대한 brute-force attack을 가속화 시켜 보안강도를 감소시킨다. 따라서 양자컴퓨터의 가용 자원이 암호공격에 필요한 자원에 도달했을 때, 공격 대상 암호가 깨지는 시점으로 보고 있다. 많은 선행 연구들은 암호를 양자회로로 구현하여 공격에 필요한 자원을 추정하고 암호에 대한 양자 강도를 확인하였다. 본 논문에서는 이러한 연구동기로 ARX 구조의 SIMECK 경량암호에 대한 양자회로를 처음으로 제안한다. 우리는 SIMECK 양자회로에 대한 최적의 양자회로 구현을 제시하고 각 함수의 동작을 설명한다. 마지막으로 SIMECK 양자회로에 대한 양자자원을 추정하고 SIMON 양자회로와 비교하여 평가한다.

1. 서론

양자컴퓨터의 등장은 기존 암호체계에 위협이 될 것이라 예상한다. 양자 알고리즘인 Grover's algorithm[1]은 대칭키 암호에 대한 brute-force attack을 가속화 시켜 n-bit 블록암호의 보안강도를 $\sqrt{n}$-bit 수준으로 감소시킨다. 현재 사용하는 암호들에 대한 post-quantum 강도를 평가하기 위해서는 공격 대상 암호에 대한 양자회로가 필요하다. 이러한 연구동기로 암호를 양자회로로 최적화 구현하고 양자 알고리즘 공격에 필요한 양자 자원을 추정하는 선행 연구들이 많이 진행되었다.[2-5]

본 논문에서는 SIMON과 SPECK의 장점을 결합하여 설계된 SIMECK 경량암호에 대한 양자회로를 처음으로 제안한다. 우리는 양자 자원을 최소한으로 사용하여 SIMECK 양자회로에 대해 최적화 구현을 진행하였으며 SIMECK 양자회로 자원 추정 결과를 제시하고 SIMON 양자회로와 비교하여 평가한다.

2. 관련 연구

2.1 Quantum computer

양자컴퓨터는 큐비트의 양자역학적인 현상을 이용하여 데이터를 처리하는 컴퓨터이다. 큐비트의 중첩 및 얽힘 성질로 인해 n개의 큐비트로 2^n개의 데이터를 표현하고 처리할 수 있다. 양자컴퓨터에서는 가역적인 특징을 가지는 양자게이트를 사용하여 큐비트를 제어하며 대표적인 양자게이트는 <그림 1>과 같다.

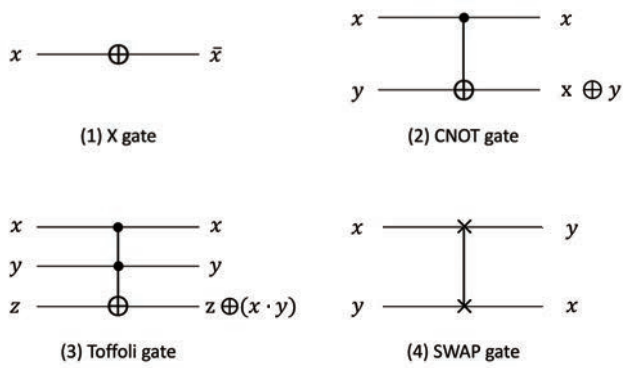

그림 1 양자 게이트

X 게이트는 하나의 입력 큐비트에 대해 상태를 반전시킨다. CNOT 게이트에서는 두 개의 입력 큐비트가 각각 control 큐비트, target 큐비트가 된다. control 큐비트가 1일 때만 target 큐비트가 반전된다. Toffoli 게이트는 세 개의 입력 큐비트 중 두 개

가 control 큐비트가 되며 한 개가 target 큐비트가 된다. 두 개의 control 큐비트가 모두 1일 때만 target 큐비트가 반전된다. Swap 게이트는 두 큐비트의 위상을 서로 바꿔주며 양자비용이 없는 게이트이다.

2.2 SIMECK

SIMECK은 SIMON 과 SPECK 의 장점을 결합하여 설계한 경량암호이다[5]. SIMECK 에서는 SIMON의 라운드 함수를 수정해서 사용하며 SPECK과 유사하게 키 스케줄 함수에서 재사용한다. 경량 암호군인 SIMECK은 SIMECK-2n/mn 으로 표기되며, n은 word 크기를 나타내고 16, 24, 32 중 하나의 값을 가진다. 따라서 2n/mn은 (block size)/(key size)를 나타내며 Feistel 구조의 라운드 함수와 키 스케줄 함수 로 동작한다. 수식 (1)은 SIMECK의 라운드 함수의 동작을 보여준다.

$$R_{k_i}(l_i, r_i) = (r_i \oplus f(l_i) \oplus k_i, l_i) \quad - (1)$$

평문은 두 word l_0, r_0로 나뉘며, 최상위 n비트가 l_0이 되며 최하위 n비트가 r_0이 된다. 두 word는 계속 나뉘어 동작하며 마지막 암호문 출력에서 합쳐진다. 라운드 함수의 내부 함수는 $f(x) = (x \odot (x \lll 5)) \oplus (x \lll 1)$ 로 정의되어 사용한다. 함수의 내부에서는 두 개의 입력 중 첫 번째 입력의 rotation을 통한 AND 값을 두 번째 입력에 XOR하는 연산이 수행된다. 키 스케줄에서 생성된 키는 라운드 함수의 두 번째 입력에 XOR된다. 키 스케줄 함수는 라운드 함수와 같은 내부함수로 동작하고 동작은 다음과 같다 :

$$\begin{cases} k_{i+1} = t_i \\ t_{j+3} = k_i \oplus f(t_i) \oplus C \oplus (z_j)_i \end{cases}$$

3. Simeck 양자회로 구현

본 논문에서는 SIMECK 경량암호에 대한 양자회로 구현을 제시하고 암호 공격에 필요한 양자자원을 추정한다. 양자회로에서 temp 값을 사용할 시 추가 큐비트를 할당해야 하며, temp를 재사용하기 위한 inverse 연산이 추가로 수행되므로 양자 자원 측면에서 매우 비효율적이다. 따라서 제시하는 양자회로에서는 양자자원을 줄이기 위해 temp 값이 생기지 않도록 설계하였다. 우리는 Toffoli 게이트를 사용하여 덧셈 $x \odot x \lll 5$ 중간에 발생하는 temp 값을 따로 저장해 두지 않고 바로 연산 대상 큐비트에 계산되도록 하였다. <Algorithm 1>은 SIMECK 라운드 함수에 대한 양자회로 동작을 보여준다.

Algorithm 1 : SIMECK quantum circuit for round function

Input : l_r, r_r
Output : l_r, r_r, k_r

for i **in range**(length(r_r)):
    $r_r \leftarrow$ **Toffoli**(l_r, $l_r \ggg 11$, r_r)
    $r_r \leftarrow$ **CNOT**($l_r \ggg 15$, r_r)

for i **in range**(length(r_r)):
    $r_r \leftarrow$ **CNOT**(k_r, r_r)

Swap(l_r, r_r)

Algorithm. 1. SIMECK quantum circuit for round function

우리는 시프트 연산에 대해 Swap 게이트의 사용 대신 반복문에서 인덱스를 변경하여 동작한다.

<Algorithm 2>는 SIMECK 키 스케줄을 보여준다. 일반적인 컴퓨터에서는 라운드 함수와 키 스케줄 함수가 동일하게 수행되지만 우리는 사용 양자자원을 줄이기 위해 키 스케줄 함수를 조금 변경하였다. 기존 키 스케줄 함수에서는 key 대신 constant와 CNOT 연산을 진행한다. CNOT 양자게이트를 사용하기 위해서는 constant를 양자자원으로 할당하여 진행해야 하며 constant 업데이트에도 양자 자원이 사용된다. 이에 대해 우리는 constant와 큐비트 간에 quantum to quantum 연산이 아닌 classic to quantum 연산이 진행되도록 하였다. 이러한 방식을 통해 constant를 classic 자원인 정수로 할당하여 큐비트 및 양자게이트를 사용하지 않고 업데이트 한다. 또한, X 게이트가 CNOT 게이트 보다 더 저렴한 양자자원이므로 CNOT 게이트 대신 constant의 비트가 1인 부분에 X 게이트가 동작하도록 하였다.

Algorithm 2 : SIMECK quantum circuit for key schedule

Input : l_r, r_r
Output : l_r, r_r, constant

for i **in range**(length(r_r)):
    $r_r \leftarrow$ **Toffoli**(l_r, $l_r \ggg 11$, r_r)
    $r_r \leftarrow$ **CNOT**($l_r \ggg 15$, r_r)

if constant[i] = 1
    X (r_r)

for i **in range**(length(r_r)):

$r_r \leftarrow \mathbf{CNOT}(k_r,\ r_r)$

$\mathbf{Swap}(l_r,\ r_r)$

Algorithm. 2. SIMECK quantum circuit for key schedule

3. 평가

우리는 projectQ의 양자프로그래밍 툴을 사용하여 SIMECK 양자회로를 구현하고 동작에 필요한 양자자원을 추정하였다. <표 1>은 SIMECK에서 제공하는 모든 (블록 크기)/(키 길이)에 대한 양자회로 자원 추정 결과를 보여준다. 제시하는 양자자원 결과는 암호화가 한번 진행될 때 필요한 양자자원이다. 따라서 SIMECK 암호에 대한 brute-force attack 수행에는 Grover's algorithm 내부의 Oracle 반복만큼 암호화를 진행하므로 총 (<표 1> 양자 게이트)×($\left\lfloor \frac{\pi}{4} \cdot \sqrt{2^{key\ size}} \right\rfloor$)의 양자 자원이 필요하다. 해당 논문은 SIMECK에 대한 첫 번째 양자회로 구현이므로 최적화 결과를 비교하기 위한 SIMECK 양자회로 선행 연구가 없다. 따라서 우리는 [6]에서 제시한 <표 2>의 SIMON 양자자원 추정 결과를 통해 비교하였다. SIMECK과 동일한 (블록 사이즈)/(키 사이즈)를 가지는 SIMON을 비교하였을 때, SIMECK이 훨씬 적은 양자 자원으로 최적화 구현되었다. 해당 결과만으로 비교했을 때, SIMON이 SIMECK 보다 양자강도가 강하다고 평가할 수 있다.

<표 1> SIMECK 양자회로 자원 추정 결과

	Quantum gates			
	X	CNOT	Toffoli	Depth
SIMECK 32/64	465	1,536	1,024	214
SIMECK 48/96	792	2,592	1,728	232
SIMECK 64/128	1,320	4,224	2,816	361

<표 2> SIMON 양자회로 자원 추정 결과

	Quantum gates			
	X	CNOT	Toffoli	Depth
SIMON 32/64	448	2,816	512	946
SIMON 48/96	768	4,800	864	1,597
SIMON 64/128	1,216	7,396	1,408	2,643

3. 결론

본 논문에서는 SIMECK 경량암호를 위한 최적화 양자회로를 제안하였다. 우리는 제안하는 SIMECK 양자회로에서 사용되는 자원을 줄이기 위한 최적화 방법들을 제시하였으며 양자회로 구현을 수도코드로 나타내었다. 마지막으로 SIMECK의 모든 블록, 키 길이에 대한 양자 자원 추정 결과를 제시하고 SIMON 양자회로와 비교하여 평가한다.

4. Acknowledgement

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity).

참고문헌

[1] Lov K Grover. A fast quantum mechanical algorithm for database search. In Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 212- 219, 1996.

[2] Song, Gyeongju, et al. "SPEEDY Quantum Circuit for Grover's Algorithm." Applied Sciences 12.14 (2022): 6870.

[3] Baksi, Anubhab, et al. "Quantum implementation and resource estimates for rectangle and knot." Quantum Information Processing 20.12 (2021): 1-24.

[4] Jang, Kyungbae, et al. "Quantum Analysis of AES." Cryptology ePrint Archive (2022).

[5]Yang, Gangqiang, et al. "The simeck family of lightweight block ciphers." International Workshop on Cryptographic Hardware and Embedded Systems. Springer, Berlin, Heidelberg, 2015.

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