국산경량암호 양자 회로 구현 동향

오유진* 장경배* 임세진* 양유진* 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Research Trends on Quantum Circuit Implementation of Korean Lightweight Block Cipher

Yu-Jin Oh* Kyung-Bae Jang* Se-Jin Lim*

Yu-Jin Yang* Hwa-Jeong Seo**

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

양자 컴퓨터는 현재 암호체계에 큰 위협으로 여겨지고 있다. 양자 컴퓨터의 발전으로 Shor알고리즘의 공개키 암호 공격이 다항시간 내에 가능함이 밝혀지면서 NIST에서는 양자 내성 암호 공모전을 진행하였다. 또한 Grover 알고리즘으로 대칭키 암호 공격의 복잡도가 제곱근으로 감소될 수 있으며 이에 따라 대칭키 암호 역시 안전하다고 보기 어렵다. 그리하여, 안전한 양자 후 보안 시스템 구축을 위해 NIST는 양자 후 보안 강도를 추정하며 이에 맞춰 양자 암호 분석 연구가 활발하게 수행되고 있다. 이에 본 논문에서는 국산 경량 암호에 대한 양자 회로 구현 동향을 살펴보고 NIST 보안 강도와 비교하여 평가한다.

I. 서론

양자 컴퓨터의 발전으로 양자 암호 분석 연구가 활발하게 수행되고 있다. 양자 암호 분석으로 사용되는 대표적인 양자 알고리즘은 Shor Grover 알고리즘[1]과 Grover 알고리즘[2]이다. Shor 알고리즘으로 인해 공개키 암호 시스템인 RSA와 ECC가 다항 시간 내 깨질 수 있음이 밝혀졌으며 이에 NIST에서는 양자 내성 암호 표준화 공모전을 진행하였다. Grover 알고리즘은 대칭키 암호 알고리즘 전수조사 복잡도를 제곱근만큼 감소 시켜준다. Grover 알고리즘에 의한 대칭키 공격은 공개키 암호 공격에 비해 상대적으로 보안 위협이 적지만, 암호 구조에 따라 보안 취약점을 가질 수 있다.

이에 본 논문에서는 국산 경량 암호에 대한 양자 회로 구현 동향을 살펴보고 NIST 보안 강도와 비교하여 평가한다.

II. 관련연구

2.1 NIST 양자 후 보안 레벨

암호와 관련된 양자 공격에 대해 NIST는 AES에 대한 양자 공격의 복잡성을 기반으로 사후 양자 보안 기준을 수립하였다[3]. 레벨 1,3,5는 AES-128, 192, 256에 대한 Grover 공격 비용에 의해 결정되며 이 비용은 Grover 공격에 대한 (총 게이트 수 x 깊이)로 계산된다. NIST는 Grassl et al.에 의한 AES 양자 회로 구현[4]에 기초하여 레벨 1,3,5에 대한 비용을 각각 2^{170}, 2^{233}, 2^{298}로 추정하였다. 최근 AES에 대한 양자 회로 최적화가 진행됨에 따라 NIST에서도 AES에 대한 Grover 비용을 조정하였다[5]. 현재 NIST는 [6]에 기반으로 하여 보안 레벨 1,3,5를 2^{157}, 2^{221}, 2^{285}로 새롭게 정의하였다.

III. 국산경량암호 양자 회로 구현 동향

3.1 CHAM

CHAM의 naive 한 키 스케줄 구현은 결과를 저장할 보조 큐비트를 할당하는 기법이다. [7]에서는 라운드 키 생성에 사용되는 보조 큐비트를 줄이기 위해 키 스케줄에 두 가지 선형 레이어 최적화 기법을 적용한다.

첫 번째는 PLU 기법이다. PLU 기법을 활용하여 CNOT 게이트와 Swap 게이트만을 사용한다. 두 번째는 FSE 기법으로 CNOT 게이트만을 사용하고 swap연산은 논리적 swap을 사용한다.

$$RK_i = K_i \oplus (K_i \lll 1) \oplus (K_i \lll 8),$$
$$RK_{(i+k/w)\oplus 1} = K_i \oplus (K_i \lll 1) \oplus (K_i \lll 11)$$

위의 식에서 CHAM - 64/128를 예로 들면, 두 기법 모두 $RK_{0\sim 7}$ 연산 이후 $RK_{8\sim 15}$를 구하기 위해 K_i값을 되돌려야하기 때문에 역연산을 수행한다.

3.2 LEA

[8] 에서는 큐비트 수 절약을 위해 라운드 키를 하나씩 업데이트하여 라운드 함수에 사용하는 on-the-fly 방식을 활용한다. 키 스케줄에서 사용되는 연산들을 병렬로 처리함으로써 깊이 측면에서 최적화한다. 첫 번째 라운드 키 생성 단계에서, 라운드 상수 δ_0와 덧셈기를 사용하여 K[0]~K[3]를 생성한다. 이 과정을 병렬로 처리하기 위해 4개의 δ_0(δ_0[0]~δ_0[3])를 할당한다. 또한 리플-캐리 모듈 덧셈기를 사용하며 덧셈기에서 1개의 캐리 큐비트(c_0)가 사용되기 때문에, 캐리 큐비트 또한 4개(c_0~c_3) 할당하여 K[0]~K[3]의 병렬 덧셈을 수행한다. 결과적으로, 병렬연산을 통해 깊이 측면에서 최적화한다.

3.3 HIGHT

[8]에서는 키 스케줄과 라운드 함수에서 최적화를 진행한다. 라운드 함수에서 4개의 라운드 키(RK)를 사용한 덧셈이 서로 독립적이므로 병렬 덧셈을 수행할 수 있다. 키 스케줄 단계에서,, 라운드 키(RK) 생성 시 사용하는 σ_i는 초기 σ_0값만 할당하면 그 다음 $\sigma_i(1 \le i \le 127)$를 생성할 수 있으며 이로 인해 큐비트 수를 줄일 수 있다. 그러나 σ_0만 할당하여 라운드 키(RK)를 업데이트 하면 라운드 함수에서의 병렬 덧셈이 불가능하다. 따라서 σ_0을 총 4개(σ_0~σ_3) 할당하여 4개의 라운드 키를 병렬적으로 생성하여 깊이를 최적화한다. 또한, 다음 라운드에서 사용할 σ_4~σ_7는 σ_0~σ_3를 재사용하여 큐비트 수 측면에서 최적화한다.

IV. 양자 공격 비용 비교 및 평가

Grover 알고리즘은 oracle + diffusion operator의 반복으로 구성된다. diffusion operator의 경우 oracle에 비교하여 무시될 만큼 오버헤드가 미미하기 때문에, Grover 공격 비용에서 무시된다. 그러므로 oracle에서의 비용만 추정하게 되며, oracle 에서는 양자 회로가 2번 동작하기 때문에 oracle 비용은 양자 회로 구현 비용 x 2 로 추정한다. [표 1]은 앞서 언급한 국산 경량암호 회로 구현을 기반으로 추정한 Grover 양자 공격 비용을 나타낸다. 기존의 NIST 보안 강도와 비교하면 살펴 본 암호 모두 보안 강도를 만족하지 못하지만, 새롭게 정의된 NIST 보안 강도와 비교하면 모두 보안 레벨 1을 달성한다.

<표 1> 국산 경량 블록 암호에 대한 양자 공격 비용

Cipher	Qubits	Total gates	Total depth	Cost
CHAM	409	2^{81}	2^{81}	2^{157}
HIGHT	457	2^{82}	2^{75}	2^{158}
LEA	389	2^{82}	2^{77}	2^{159}

V. 결론

본 논문에서는 국산 경량암호들에 대한 양자 회로 구현 연구에 대해 살펴보고 그에 따른 Grover 양자 공격 비용 및 양자 후 보안 강도를 평가하였다. 안전한 양자 후 보안 시스템 구축을

위해 NIST가 정의한 양자 후 보안 기준을 고려하는 것이 중요하며 국산 경량 암호인 CHAM, HIGHT, LEA 모두 보안 레벨 1을 달성한 것을 확인하였다. 미리 보안 강도를 평가하는 것은 향후 양자 컴퓨터가 실용화되기 전에 보안 시스템을 구축하는 데 도움이 될 것으로 판단된다.

VI. 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, 100%).

[참고문헌]

[1] P. W. Shor, “Polynomial-Time Algorithmsfor Prime Factorization and Discrete Logarithms on a Quantum Computer” SIAMreview, Vol. 41. No. 2. 303-332. 1999.

[2] L.K. Grover, “A fast quantum mechanical algorithm for database search,” Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pp. 212 - 219, 1996.

[3] NIST, “Submission requirements and evaluation criteria for the post-quantum cryptography standardization process,” https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/call-for-proposals-final-dec-2016.pdf

[4] M. Grassl, B. Langenberg, M. Roetteler, and R. Steinwandt, “Applying Grover’s algorithm to AES: quantum resource estimates,” Post-Quantum Cryptography, PQCrypto'16, LNCS, 9606, pp. 29 - 43, 2016.

[5] NIST, “All for additional digital signature schemes for the post-quantum cryptography standardization process” https://csrc.nist.gov/csrc/media/Projects/pqc-dig-sig/documents/call-for-proposals-dig-sig-sept-2022.pdf

[6] JAQUES, Samuel, et al. Implementing Grover oracles for quantum key search on AES and LowMC. In: Advances in Cryptology - EUROCRYPT 2020: 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10 - 14, 2020, Proceedings, Part II 30. Springer International Publishing, 2020. p. 280-310

[7] YANG, Yujin, et al. Optimized implementation and analysis of cham in quantum computing. Applied Sciences, 2023, 13.8: 5156.

[8] JANG, Kyungbae, et al. Parallel quantum addition for Korean block ciphers. Quantum Information Processing, 2022, 21.11: 373.