NIST 경량암호 공모 최종 후보 양자회로 구현 동향

오유진* 장경배* 임세진* 양유진* 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Survey on Quantum Circuit Implementations for NIST Lightweight Cryptography Standardization Finalist Algorithms

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

Yu-Jin Yang* Hwa-Jeong Seo**

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

사물인터넷의 발전으로 초소형 스마트 기기의 보안성 문제가 대두되면서 이를 위해 경량 암호 기술에 대한 연구가 활발하게 이루어지고 있다. NIST에서는 AEAD형태의 경량 암호 표준화 공모전을 주최하였으며 최종적으로 10개의 후보군이 선정되었다. 또한 현재 암호시스템은 양자 컴퓨터의 발전으로 위협받고 있으며 이를 위해 양자 회로 상에서의 암호 구현 및 공격 비용 평가에 관한 연구가 활발하게 진행되고 있다. 이에 본 논문에서는 NIST 경량암호 표준화 공모전에 선정된 암호 중 ASCON, Sparkle, Grain-128AEAD에 대한 양자 회로 구현 동향과 공격 비용에 대해 살펴본다.

I. 서론

사물인터넷(Internet of Things, IoT)의 발전으로 초소형 스마트 기기의 보안성 문제가 대두되고 있다. 이러한 기기는 다양한 리소스가 제한된 환경에서 사용되며 이를 위해 경량 암호 기술에 대한 연구가 활발하게 이루어지고 있다. 미국 국립표준기술연구소(The National Institute of Standard and Technology, NIST)에서는 경량암호 표준화 공모전을 주최하였으며 특히 AEAD (Authenticated Encryption with Associated Data) 형태의 암호를 제출받았다. 최종적으로 10개의 후보군이 선정되었다.

또한 현재의 암호시스템은 양자 컴퓨터의 발전으로 위협받고 있다. 양자 알고리즘인 Shor 알고리즘[1]으로 공개키가 다항 시간 내에 공격될 수 있으며 Grover 알고리즘[2]으로 대칭 키 또한 키 전수 조사를 루트만큼 감소시킬 수 있다.

이에 본 논문에서는 NIST 경량암호 표준화 공모전에 선정된 암호 중 ASCON[3], Sparkle[4], Grain-128AEAD[5]에 대한 양자 회로 구현 동향에 대해 살펴보고 공격 비용을 비교한다.

II. 관련연구

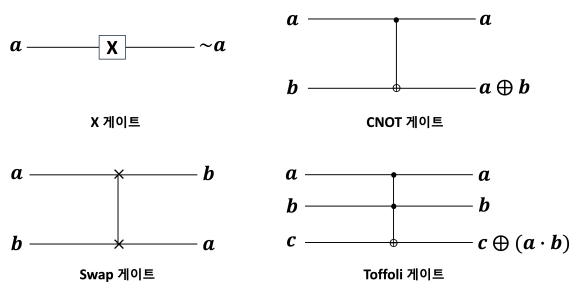
2.1 NIST 양자 후 보안 레벨

NIST는 양자 후 보안 강도 평가를 위해 AES에 대한 양자 공격 비용을 기반으로 보안 레벨(Level 1,3,5)을 수립하였다. 이를 위해 Grassl et al.에 의한 AES 양자 회로 구현[6]을 기반으로 Grover 공격 비용을 추정하였으며 이러한 공격 비용은 총 게이트 수 x 깊이로 계산된다. 보안 레벨 1,3,5는 각각 AES-128, 192, 256에 대한 공격 비용이며 각각 2^{170}, 2^{233}, 2^{298}이다.

그러나 최근 AES에 대한 최적화 연구가 진행됨에 따라 NIST도 AES에 대한 공격 비용을 조정하였으며 [7]를 기반으로 새롭게 보안 레벨을 수립하였다. 그리하여 현재 수립된 보안 레벨 1,3,5에 대한 공격 비용은 각각 2^{157}, 2^{221}, 2^{285} 이다.

2.2 양자 게이트

양자 컴퓨터에서는 고전 컴퓨터의 논리 게이트와 유사하게 양자 게이트를 사용하여 큐비트의 상태를 제어한다. 대표적인 양자 게이트에는 X, CNOT, Swap, Toffoli 게이트가 있으며 [그림 1]과 같다.



[그림 1] 양자 게이트

X 게이트는 큐비트의 상태를 반전 시키며 고전 컴퓨터 상에서의 NOT 연산과 동일하다. CNOT 게이트는 control 큐비트(a)가 1일 때 target 큐비트(b)의 값이 반전되는 게이트로 XOR 연산과 동일하다. Swap 게이트는 두 큐비트의 상태를 교환한다. Toffoli 게이트는 2개의 control 큐비트를 사용한다. 두 개의 control 큐비트(a,b)가 모두 1일 경우에만 target 큐비트(c)의 값을 반전 시키며 AND 연산과 동일하다.

III. NIST 경량암호 공모 최종 후보 양자 회로 구현 동향

3.1 ASCON

Ascon은 순열 함수 기반의 암호로, AEAD와 Hash 총 두가지 버전이 존재하며 AEAD에는 ASCON-128, Ascon-128a 버전이 존재한다. Ascon의 핵심 연산은 320비트 순열이며 상수 XOR, 5-비트 S-box, 64-비트 선형연산으로 구성된다. Ascon AEAD의 두 가지 버전은 순열의 라운드 수와 블록 크기만 다르며 내부 연산은 동일하게 진행된다.

[8]에서는 ASCON 계열 중 Ascon-128에 대한 양자 회로를 구현하였다. 특히, 순열 연산 내의 치환 계층과 선형 계층에서 최적화를 진행하였다. 치환 계층에서 사용되는 64개의 S-box를 320 (5 x64)개의 보조 큐비트 할당을 통해 병렬로 구현함으로써 최적화를 하였다. 또한, 역연산을 수행하여 320개의 보조 큐비트를 매 라운드마다 재사용하였다. 선형 계층에서는 [9]에 구현된 방법 중 naive한 구현을 진행하였다. 큐비트 수를 줄이는 대신 출력 값을 저장할 큐비트들을 할당하여 병렬로 구현함으로써 깊이 측면에서 최적화를 하였다. 또한 [linear]의 naive한 구현과 비교했을 때, CNOT 게이트 순서를 정렬함으로써 depth를 3으로 줄였다.

3.2 Sparkle SCHWAEMM

Sparkle은 경량 블록 암호 SPARX를 변형한 순열 함수 기반 암호이며, AEAD인 SCHWAEMM과 해시 함수인 ESCH가 존재한다. Sparkle의 핵심연산인 순열 연산은 64-비트 S-box로 구성된 Alzette 함수와 파이스텔 구조의 선형 레이어로 구성된 diffusion layer로 구성되어 있다.

[10]에서는 128비트 키를 가지는 Sparkle SCHWAEMM를 양자 회로로 구현하였다. 순열 과정 중 Alzette 단계에서 리플-캐리 모듈 덧셈기인 CDKM 양자 덧셈기를 사용하여 한 개의 보조 큐비트만을 사용하였다. 또한, Sparkle의 순열 함수에는 4개의 Alzette 함수가 작동하는데, 이를 병렬로 구현함으로써 depth측면에서 최적화를 하였다. 함수 내부의 사용되는 덧셈기를 병렬로 구현하기 위해 4개의 보조 큐비트를 할당하여 이를 통해 depth를 크게 줄였다.

3.3 Grain-128AEAD

Grain-128AEAD는 Grain 스트림암호에 AEAD를 결합한 암호로 스트림 암호 중 유일하게 최종 후보에 선정된 암호이다. 128비트

NFSR과 LFSR이 결합되어있는 형태이며 둘의 초기값은 128비트 키와 96비트 넌스로 설정된다.

[11]에서는 3 큐비트 및 4 큐비트에 대한 토폴리 게이트를 구현하기 위해 compute-copy-uncompute 방법을 사용하였다. 각각 2개, 3개의 보조 큐비트를 사용하여 결과 값을 복사함으로써 3 큐비트 및 4 큐비트에 대한 AND 연산을 수행하였다. 또한 초기화 단계와 키 스트림 생성 단계를 동시에 구현함으로써 최적화를 진행하였다.

IV. 성능평가

암호	#X	#CNOT	#Toffoli	depth	Qubits
ASCON-128	21243	69600	9600	304	20064
Sparkle-SCHWAEMM	35951	102976	29280	8598	612
Grain-128AEAD	127	13624	18116	13068	531

[표 1] NIST 경량암호 공모 최종 후보 양자회로 비용

[표 1]은 앞서 언급한 Ascon-128, Sparkle SCH, Grain-128AEAD에 대한 양자 회로 구현 비용을 나타낸다.

Grover 알고리즘은 oracle과 확산 연산자의 반복으로 이루어져 있다. 확산 연산자의 경우 오버헤드가 매우 적기 때문에 oracle에 비해 무시된다. 그 결과, Grover 공격의 비용 추정은 주로 oracle에서 이루어지며, oracle에서 양자 회로가 두 번 실행되기 때문에 비용은 양자 회로의 구현 비용에 2를 곱한 것으로 추정한다. 따라서 ASCON, Sparkle, Grain-128AEAD의 Grover 공격 비용은 [표 1] x 2 x $[\frac{\pi}{4}\sqrt{2^k}]$ 이며 [표 2]에서 볼 수 있다.

V. 결론

암호	Total gates	Total detph	Cost	Qubits
ASCON-128	$1.180 \cdot 2^{83}$	$1.574 \cdot 2^{73}$	$1.856 \cdot 2^{156}$	20065
Sparkle-SCHWAEMM	$1.732 \cdot 2^{83}$	$1.431 \cdot 2^{80}$	$1.239 \cdot 2^{164}$	613
Grain-128AEAD	$1.724 \cdot 2^{82}$	$1.820 \cdot 2^{80}$	$1.569 \cdot 2^{163}$	532

[표 2] NIST 경량암호 공모 최종 후보에 대한 양자 공격 비용

암호 공격 비용이 NIST에서 제시하는 비용보다 높을 경우 해당 암호는 양자 컴퓨터 공격으로부터 안전하다고 판단할 수 있으며 그와 반대로 NIST에서 제시하는 비용보다 현저히 낮을 경우 양자 컴퓨터 공격으로부터 보안성이 붕괴될 수 있다고 판단할 수 있다.

본 논문에서는 NIST 경량암호 표준화 공모전에 선정된 암호 중 ASCON, Sparkle, Grain-128AEAD에 대한 양자 회로 구현 동향에 대해 살펴보고 공격 비용을 비교하였다. ASCON, Sparkle, Grain-128AEAD에 대한 공격 비용은 2^{157} 이상이거나 그와 비슷한 것을 확인할 수 있으며 이에 보안 레벨 1을 달성한 것을 확인 할 수 있다.

VI. Acknowledgment

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] Shor, Peter W. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." SIAM review 41.2 (1999): 303-332.

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

[3] Dobraunig, Christoph, et al. "Ascon v1. 2." Submission to the CAESAR Competition 5.6 (2016): 7.

[4] Beierle, Christof, et al. "Schwaemm and esch: lightweight authenticated encryption and hashing using the sparkle permutation family." NIST round 2 (2019).

[5] Hell, Martin, et al. "Grain-128AEADv2-A lightweight AEAD stream cipher." NIST Lightweight Cryptogr. Stand. Process (2019): 1-38.

[6l] Grassl, Markus, et al. "Applying Grover's algorithm to AES: quantum resource estimates." International Workshop on Post-Quantum Cryptography. Cham: Springer International Publishing, 2016.

[7] Jaques, Samuel, et al. "Implementing Grover oracles for quantum key search on AES and LowMC." 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.

[8] Oh, Yujin, et al. "Depth-optimized implementation of ascon quantum circuit." Cryptology ePrint Archive (2023).

[9] Roy, Soham, Anubhab Baksi, and Anupam Chattopadhyay. "Quantum implementation of ascon linear layer." Cryptology ePrint Archive (2023).

[10] Yang, Yujin, et al. "Grover on SPARKLE." International Conference on Information Security Applications. Cham: Springer Nature Switzerland, 2022.

[11] Anand, Ravi, et al. "Resource estimation of Grovers-kind quantum cryptanalysis against FSR based symmetric ciphers." Cryptology ePrint Archive (2020).