AES 양자 회로 구현 동향

장경배[1], 김현지[1], 송경주[1], 양유진[1], 임세진[1], 서화정[1]
[1]한성대학교 IT융합공학부
starj1023@gmail.com, khj1594012@gmail.com, thdrudwn98@gmail.com,
yujin.yang34@gmail.com, dlatpwls834@gmail.com, hwajeong84@gmail.com

Research Trends on AES Quantum Circuit Implementation

Kyung-bae Jang[1], Hyun-ji Kim[1], Gyeong-ju Song[1], Yu-jin Yang[1], Se-jin Lim[1], Hwa-jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-Sung University

요 약

특정 문제를 효율적으로 모델링하고 해결할 수 있는 자체적인 특성을 가지고 있는 양자 컴퓨터는 다양한 컴퓨팅 분야에서 강세를 보일 것으로 기대된다. 이러한 양자 컴퓨터는 가까운 미래에 암호학계에 다가올 가장 큰 위협으로 여겨지고 있다. 공개키 암호와는 달리 대칭키 암호에서 기반하고 있는 문제들은 양자 컴퓨터에 대해 아직은 안전할 것으로 여겨지지만, 안전한 양자 후 보안 시스템을 구축하기 위해 이에 대한 파급력을 확인하는 연구들이 수행되고 있다. NIST는 대칭키 암호 AES에 대한 상대적인 양자 공격 비용에 따라 양자 후 보안 강도를 추정하고 있으며, 이에 본 논문에서는 AES에 대한 양자 회로를 구현하고 공격 비용을 추정하는 다양한 연구들에 대해 살펴본다.

1. 서론

IBM, Google, Microsoft 등의 국제 대기업이 양자 컴퓨터 개발에 적극적인 투자를 진행 중이다. 특정 문제를 효율적으로 모델링하고 해결할 수 있는 양자 컴퓨터는 인공지능, 시뮬레이션과 같은 분야에서 뛰어난 컴퓨팅 능력을 보여줄 것으로 예상되지만, 또 다른 측면으로는 암호 학계에 다가올 가장 큰 위협으로 여겨지고 있다.

공개키 암호 시스템의 경우, 현재 널리 사용되고 있는 RSA, ECC(Elliptic Curve Cryptography)가 기반하고 있는 인수분해, 이산대수 문제들이 Shor 알고리즘[1]이 동작 가능한 규모의 양자 컴퓨터로 다항 시간 내에 해결될 것이기 때문에 새로운 양자 내성 암호가 필요한 상황이다. 이러한 보안 위협에 대응하여 NIST(National Institute of Standards and Technology)는 양자내성암호 표준화 공모전을 주최하였으며, 현재, 몇 개의 최종 후보 알고리즘들로 간추려진 상황이다.

대칭키 암호의 경우, 공개키 암호에 비해 보안 위협이 적을 것으로 평가되고 있지만 암호 시스템의 구조에 따라 심각한 보안 취약점을 가질 수 있다. 양자 검색 알고리즘인 Grover 알고리즘은 비밀키를 찾기 위한 고전 공격들의 복잡도를 제곱근으로 감소시킬 수 있다[2]. 전수 조사의 경우, Grover 알고리즘을 사용하면 n-bit 비밀키를 사용하는 대칭키 암호에 대해 약 $\sqrt{2^n}$번의 검색만으로 비밀키를 높은 확률로 복구할 수 있다. 이러한 대칭키 암호에 대한 보안 위협은 단일 대칭키 암호 시스템뿐만이 아니라 NIST 양자내성암호 표준화 공모전에서도 발견된다. 후보 알고리즘들은 핵심 암호화 요소들은 양자 컴퓨터로부터 안전하다고 여겨지는 문제들을 기반으로 하지만, 내부적으로 일부 암호화 요소에 대칭키 암호를 사용하고 있기 때문에 공격자는 대칭키 암호 요소만을 공격하여 전체적인 보안을 우회할 수 있다.

이에 2016년 NIST는 대칭키 암호에 대한 양자 후 보안 요구 사항들을 제시하였다[3]. NIST는 AES-128, 192, 256에 필요한 공격 복잡도에 따라 상대적으로 Level 1, 3, 5의 보안 레벨을 정의하였다. 공격 복잡도를 측정하는 메트릭에는 양자 공격을 수행하기 위한 양자 회로의 크기를 채택하고 있다. Grover 알고리즘이 동작 가능하다면 보안 훼손이 발생하지만 이 공격에는 엄청난 반복으로 인한 대규모의 양자 회로를 동작시키는 것은 매우 어렵기 때문이다. NIST는 상대적인 보안 레벨을 정의함과 동시에 AES-128, 192, 256에 대한 Grover 공격 회로 비용

을 추정하였다. 비용 추정에는 2016년 Grassl et al.의 최초 AES에 대한 Grover 공격 비용 추정 연구[4]를 인용하였다. NIST는 추후 복잡도를 크게 감소시키는 양자 공격이 제시되는 경우, 추정한 비용은 보수적으로 평가되어야 한다고 언급하였다.

이에 반응하여, AES 양자 회로를 효율적으로 구현하는 다양한 연구들이 제시되었다. 본 논문에서는 AES 양자 회로 구현 동향에 대해 분석하고 이와 관련하여 NIST의 대칭키 암호 보안 요구사항에 대해 살펴본다.

2. NIST 양자 후 보안 레벨

NIST는 표 1과 같이 상대적인 AES에 대한 공격 복잡도에 대해 보안 레벨을 지정함과 동시에 2016년 Grassl et al.의 AES 양자 회로 구현 연구를 인용하여 구체적인 공격 비용을 추정하였다. [표 1] 비용은 전체 Grover 공격 회로의 (양자 게이트 수 × 회로 Depth)로 계산된다. 양자 구현에서 중요 요소인 큐비트 수는 비용 계산에서 제외 되었는데, 이는 큐비트 수가 Grover 알고리즘의 극심한 반복에 영향을 받지 않지만 양자 게이트와 회로 depth는 심각하게 증가하기 때문이다.

<표 1> 대칭키 암호에 대한 NIST 양자 후 보안 레벨

Security	Attack Complexity	Cost
Level 1	Any attack that breaks the relevant security definition must require computational resources comparable for key search on a block cipher with a 128-bit key (e.g. AES128)	2^{170}
Level 3	Any attack that breaks the relevant security definition must require computational resources comparable for key search on a block cipher with a 128-bit key (e.g. AES128)	2^{233}
Level 5	Any attack that breaks the relevant security definition must require computational resources comparable for key search on a block cipher with a 128-bit key (e.g. AES128)	2^{298}

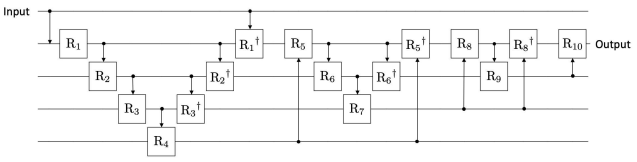
3. AES 양자 회로 구현 동향

Grover 알고리즘을 사용하는 양자 비용은 공격 대상의 암호화 양자 회로를 얼마나 효율적으로 구현하는지에 따라 결정된다. 본 장에서는 Grassl et al.의 최초의 AES 양자 회로부터 이후 제시된 다양한 AES에 대한 양자 회로 구현 특징들에 대해 살펴본다.

3.1 Grassl et al.의 AES 양자 회로[4]

최초의 AES 양자 회로 구현인 만큼 해당 구현에는 많은 양자 자원들이 사용되었다. 특히 대부분의 비용이 AES의 Sbox를 구현하는데 사용된다. Sbox 구현에 있어 사전 테이블을 활용하는 방식은 고전 컴퓨터에서는 일반적인 선택이지만 양자 컴퓨터에서는 그렇지 않다. 모든 입력 값에 대한 출력 값을 한 번에 계산하는 양자 중첩의 특성을 활용해야 하기 때문이다. 따라서 입력 값에 따라 출력 값을 계산되는 Sbox 내부 연산을 양자 게이트로 구현해야 한다. 해당 연구에서는 Itoh-Tsujii 알고리즘을 기반으로 하여 AES의 Sbox 유한체 역연산에 대해 곱셈과 제곱의 조합 양자 회로를 구현하였다. 곱셈은 양자 컴퓨터상에서 많은 양자 자원을 필요로 하기 때문에 Grassl et al.의 AES 양자 회로 구현은 매우 높은 양자 자원들이 사용되었다고 평가된다.

저자들은 회로 아키텍처를 설계하는 데 있어 큐비트 수를 줄이기 위한 Zig-zag 방식을 제시하였다. Zig-zag 아키텍처는 [그림 1]과 같이 이전에 수행한 라운드의 reverse 연산들을 수행하여 큐비트를 재사용할 수 있으며 헤딩 아키텍처는 향후 연구들에서 채택되거나 개선되고 있다.



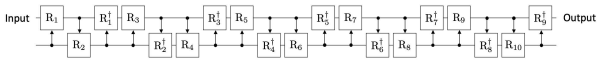
[그림 1] Zig-zag 아키텍처

3.2 Langenberg et al.의 AES 양자 회로[5]

해당 연구에서는 Sbox 양자 회로 구현에 필요한 양자 자원들을 크게 줄였다. Grassl et al.의 구현과는 달리, 하드웨어 친화적인 구현으로 잘 알려진 Boyar-Peralta의 AES Sbox 구현을 채택하였다. 해당 구현 방식을 단순 양자 회로로 이식하는 것만으로도 극적인 성능 향상을 제공할 수 있지만 해당 연구에서는 해당 Sbox 구현의 수식을 변경하여 큐비트를 더욱 절약하였다. 회로 아키텍처는 이전 연구에서 사용된 Zig-zag 방식을 그대로 사용하였다.

3.3 Zou et al.의 AES 양자 회로[6]

ASIACRYPT'20에서는 기존 Zig-zag 아키텍처를 개선함으로써 큐비트 수를 크게 감소시켰다. 특히 개선된 Zig-zag 아키텍처를 위해 해당 연구에서는 출력 값에서 입력 값을 계산하는 $Sbox^{-1}$ 양자 회로가 사용 되었다. [그림 2]는 개선된 Zig-zag 아키텍처를 나타내며 기존 Zia-zag 방식보다 회로 depth는 증가하지만 큐비트를 절약할 수 있다. Sbox 양자 회로 구현에 있어 Langenberg et al.의 구현과 동일하게 Boyer-Peralta의 Sbox를 기반으로 하지만 큐비트를 더욱 절약할 수 있도록 개선하였다.



[그림 2] 개선된 Zig-zag 아키텍처

3.4 Jaques et al.의 AES 양자 회로[7]

선행 연구들에서는 모두 큐비트를 줄이는데 집중하였지만 EUROCRYPT'20의 AES 양자 회로 연구에서는 양자 게이트와 회로 depth를 줄이는데 초점을 두었다. 이를 위해 Zig-zag 아키텍처를 선택하는 것이 아닌 reverse 연산을 수행하지 않고 큐비트를 지속적으로 할당하는 pipeline 아키텍처를 선택하였다. Sbox 양자 회로 구현 또한 이전 연구들은 큐비트를 절약하기 위해 게이트 및 회로 depth가 증가한 반면 해당 구현에서는 Boyer-Pelta의 Sbox 구현[?]을 그대로 양자 회로로 이식함으로써 낮은 게이트 및 회로 depth만이 사용되었다. 그 결과, 추정한 공격 비용은 AES-128 기준 2^{170}으로 가장 좋은 구현 결과를 제시하였다. 하지만 추후 해당 구현에서 사용된 양자 프로그래밍 툴인 Microsoft Q#의 자원이 하한으로 추정된다는 오류가 보고됨에 따라 올바른 수치가 아닌 것으로 평가되었다.

4. AES에 대한 양자 공격 복잡도 비교

Grover 알고리즘을 사용한 대칭키 암호에 대한 공격 비용 추정 방식은 다음과 같다. Grover 알고리즘 회로는 oracle + diffusion operator의 반복으로 구성되지만 diffusion operator의 오버헤드는 oracle에 비해 매우 적기 때문에 일반적으로 oracle에 대한 비용만을 추정한다. oracle이 한 번 동작하는데 필요한 비용은 공격 대상 암호화 양자 회로가 2번 동작하는데에 필요한 비용으로 추정한다. 따라서 (AES 양자 회로 비용 X 2)가 oracle에 대한 비용이며 AES-128의 경우 oracle이 약 2^{64}번 반복되는데 사용되는 양자 자원들이 최종 공격 비용으로 계산된다. [표 2]는 다양한 AES-128 양자 회로 구현을 기반으로 추정한 공격 비용을 나타낸다.

<표 2> AES-128에 대한 양자 공격 비용 비교

Source	Qubits	Total gates	Total depth	Cost
NIST, [3]	-	-	-	2^{170}
Grassl, [4]	984	2^{87}	2^{81}	2^{168}
Langenberg, [5]	864	2^{82}	2^{79}	2^{161}
Zou, [6]	512	-	-	-
Jaques, [7]	1,785	2^{82}	2^{75}	2^{157}

5. 결론

NIST의 양자 후 보안 요구사항에서 명시된 공격 비용을 감소시키기 위한 다양한 AES 양자 회로 구현 연구들이 수행되어 왔으며 본 논문에서는 다가오는 양자 컴퓨터시대에 대비하여 다양한 AES 양자 회로 구현 및 공격에 대한 연구 동향에 대해 살펴보았다. 특정 암호 알고리즘에 대한 양자 공격 시, NIST에서 제시한 상대적인 공격 비용보다 높은 비용이 소모된다면 해당 암호 알고리즘은 양자 컴퓨터의 공격으로부터 내성을 가지고 있다고 평가할 수 있다. 반면 요구되는 공격 비용이 NIST에서 제시한 공격 비용보다 현저히 낮을 경우, 그만큼 쉽게 양자 컴퓨터의 공격에 노출되어 안전성이 훼손되기 쉽다는 것을 의미한다. 양자 컴퓨터라는 최고의 암호 분석 도구가 등장할 것으로 기대되며, 이에 대한 파급력을 미리 확인하는 것은 향후 안전한 양자 후 보안 시스템을 구축하는데 기여할 수 있을 것으로 사료된다.

6. Acknowledgement

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 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 al gorithm for database search," Proceedings of t he twenty-eighth annual ACM symposium on T heory of computing, pp. 212 - 219, 1996.
[3] NIST, "Submission requirements and evalua tion criteria for the post-quantum cryptograph y standardization process," [internet], https://c src.nist.gov/CSRC/media/Projects/Post-Quantu m-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-Quan tum Cryptography, PQCrypto'16, LNCS, 9606, p p. 29 - 43, 2016.
[5] B. Langenberg, H. Pham, and R. Steinwandt, "Reducing the cost of implementing AES as a quantum circuit." Technical report, Cryptology ePrint Archive, Report 2019/854, 2019.
[6] J. Zou, Z. Wei, S. Sun, X. Liu, and W. Wu, "Quantum circuit implementations of AES with fewer qubits," International Conference on the Theory and Application of Cryptology and Information Security, Springer, pp. 697-726, 2020.
[7] S. Jaques, M. Naehrig, M. Roetteler, and F. Virdia, "Implementing Grover oracles for quantum key search on AES and LowMC." Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, pp. 280 - 310, 2020.