AES S-Box에 대한 양자 회로 구현 동향

장경배[1], 임세진[1], 이민우[1], 서화정[1]
[1]한성대학교 IT융합공학부
starj1023@gmail.com, minunejip@gmail.com, dlatpwls834@gmail.com,
hwajeong84@gmail.com

Research Trend about Quantum Circuit Implementation for AES S-Box

Kyung-Bae Jang[1], Se-Jin Lim[1], Min-Woo Lee[1], Hwa-Jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-sung University

요 약

다가오는 양자 컴퓨터 시대에 대비하여, 양자 컴퓨터상에서의 암호 분석은 활발한 연구 분야 중 하나이다. 양자 알고리즘을 사용한 암호 분석 시, 대상 암호는 반드시 양자 회로로 구현되어 양자 컴퓨터상에서 동작될 수 있어야 한다. 이에 공개키 암호인 RSA, ECC의 핵심 연산 또는 다양한 대칭키 암호들에 대해 양자 회로로 최적화 구현하는 연구들이 발표되고 있다. AES는 고전 컴퓨터상에서 뿐만 아니라, 양자 컴퓨터상에서 활발한 최적화 구현 대상이다. AES의 양자 회로 구현 시, 가장 많은 양자 자원이 필요한 연산은 S-Box이다. 이에 본 논문에서는 다양한 AES 양자 구현에서의 다양한 S-Box 양자 회로 구현에 대해 살펴보고 다양한 최적화 특징에 대해 살펴본다.

1. 서론

고전 컴퓨터의 컴퓨팅 방식과는 달리, 양자 컴퓨터에서는 양자 역학적 특징을 활용한 컴퓨팅이 수행된다. 0 또는 1을 확정적으로 결정하는 고전 비트가 아닌 0과 1이 확률로서 동시에 존재하는 양자 비트인, 큐비트를 양자 컴퓨터에서는 사용한다 (양자 중첩). 이 외에도 상호 작용 했더 큐비트들이 서로 얽혀 하나의 큐비트가 다른 큐비트의 상태에 영향을 주는 양자 얽힘의 특성 등, 다양한 양자 컴퓨팅이 수행된다. 이러한 특징으로 인해, 양자 컴퓨터는 고전 컴퓨터상에서의 특정 난제들을 효율적으로 모델링하거나 빠른 시간 내에 해결할 것으로 기대된다. 이에는 암호 알고리즘들이 기반하는 계산 복잡도 기반의 문제들도 포함 된다. 공개키 암호의 경우, RSA와 Elliptic Curve Cryptography(ECC)에서 기반하고 있는 소인수 분해, 이산 대수 문제를 양자 컴퓨터는 Shor 알고리즘을 사용하여 다항 시간 내에 해결할 수 있다. 안전성이 아예 무너지기 때문에 NIST에서는 RSA와 ECC를 대체할 수 있는 양자 내성 암호 표준화 작업이 진행 중이다. 대칭키 암호의 경우, Grover 알고리즘을 사용하는 양자 컴퓨터는 암호 알고리즘들이 고전 컴퓨터에 대해 주장하던 보안 강도를 제곱근으로 감소시킨다. 즉 n-bit 키를 사용하는 이상적인 암호에 대한 전수 조사 복잡도는 $O(2^n)$이지만, Grover 알고리즘을 사용한 양자 전수 조사는 약 $\sqrt{2^n}$번 만에 높은 확률로 비밀 키를 복구할 수 있다 [1].

Shor 알고리즘과 Grover 알고리즘을 사용한 암호 분석에는 고전 암호화가 아닌 양자 암호화 회로가 요구된다. Grover 알고리즘에서도 $\sqrt{2^n}$의 암호화를 수행해야 하는데, 이 때 분석 대상 암호화 양자 회로가 구현되어야 한다. 따라서 암호화 회로를 얼마나 효율적으로 구현하는지에 따라 양자 암호 분석의 성능 또한 결정되는 것이다. 이에 다양한 암호 알고리즘의 핵심 연산 또는 암호 알고리즘의 암호화를 양자 회로로서 최적화 구현하는 연구들이 제시되고 있다. 이에 본 논문에서는 AES에 대한 양자 회로 구현 중, 가장 핵심이 되는 S-Box에 대한 양자 회로 구현 동향에 대해 살펴본다. S-Box 양자 회로의 경우, AES에서 가장 많은 비용을 차지하는 부분이며, 다양한 최적화 관점에서의 트레이드오프가 존재한다.

2. AES에 대한 S-Box 양자 회로 구현

양자 회로 구현에 대한 최적화 관점에서 중요 요소는 필요 큐비트 수, Toffoli 게이트 수, Toffoli depth, 그리고 회로의 전체 depth로 특정 지을 수 있다. AES S-box의 경우 위의 요소들에 대한 다양한 트레이드오프 구현들이 존재한다.

2.1 Grassl et al.의 S-Box 양자 회로[2]

2016년, PQCrypto에서는 AES에 대한 양자 회로 구현이 최초로 제시되었다. 현 시점에서, 해당 구현에는 높은 비용이 사용되고 있다 평가되고 있다. 가장 큰 이유는 S-Box에 대한 양자 회로 구현 시, 갈루아 필드 $GF(2^8)/(x^8+x^4+x^3+x+1)$에 대한 Inversion 연산이 양자 회로로 구현되었고 이에 대한 양자 비용이 매우 높기 때문이다. 해당 구현에서는 곱셈과 제곱의 조합으로 구현되는 Itoh-Tsujii 기반이 Inversion이 구현되었다. 제곱 연산의 경우, shift에 대한 양자 비용이 없고 modular reduction에 대한 CNOT 게이트만이 사용되기 때문에 상대적으로 비용이 낮다. 하지만 곱셈의 경우, Toffoli 게이트들이 사용되고 양자 회로 구현 시, 상대적으로 많은 비용이 요구된다. 해당 구현에서는 4번의 양자 곱셈이 순차적으로 구현되어 Toffoli 게이트, Toffoli depth가 높고 전체 depth 또한 높다. 하지만 필요 큐비트 수는 상대적으로 낮은 편이다.

2.2 Langenberg의 S-Box 양자 회로[3]

해당 구현에서는, S-Box 양자 회로 구현에 있어, 고전 컴퓨터상에서의 AES S-Box 하드웨어 최적화 구현 연구를 활용하였다. Boyer-Peralta의 S-Box 구현을 사용하였으며, 양자 구현에서의 필요 큐비트 수를 줄이기 위해, reverse 연산을 자주 활용함으로써 temp 변수의 사용 횟수를 줄였다. Grassl et al.의 양자 S-Box보다 훨씬 적은 비용으로 구현이 가능하였으며, 가장 큰 이유는 갈루아 필드 상에서의 Inversion이 비효율적 이였던 것과 동시에 Boyer-Peralta의 S-Box 구현을 채택했다는 것이다. 해당 연구를 기점으로 Boyer-Peralta의 S-Box 구현은 대부분의 AES 양자 회로 구현에서 채택되었으며, 이를 기반으로 변형된 AES S-Box 양자 회로들이 구현되고 있다.

2.3 S. Jaques et al.의 S-Box 양자 회로[4]

이전 양자 구현들에서는 대부분 큐비트를 줄이기 위해 temp 변수의 사용을 줄이는 방식의 양자 회로가 구현되었지만, 해당 구현에서는 Boyer-Peralta의 S-Box 구현이 그대로 양자 회로 상으로 구현되었다. 이유는 해당 AES 구현에서의 최적화 관점이 큐비트 감소가 아닌 depth 감소에 맞추어져 있었기 때문이다. temp 변수의 사용을 줄이기 위한 구현의 경우. 수행했던 연산들을 거꾸로 반복하거나 추가적인 연산들이 요구되지만 해당 구현에서는 이러한 오버헤드가 없기 때문에 큐비트 수는 많지만 낮은 Toffoli depth, 회로 depth로 S-Box 양자 회로가 구현되었다.

2.4 H. Zhenyu et al.의 S-Box 양자 회로[5]

해당 구현에서도 Boyer-Peralta의 S-Box 구현이 활용되었다. S. Jaques et al.의 구현에서는 Boyer-Peralta의 S-Box가 그대로 양자 회로로 구현된 반면, 해당 저자들은 연산 수식을 수정하여 S-Box 양자 회로 구현에서의 Toffoli depth를 감소시켰다. 핵심은 AND 연산의 동기화이다. AND 연산은 양자 회로 구현 시. Toffoli 게이트로 구현되는데, AND 연산의 동기화로 인해 Toffoli 게이트가 병렬로 동작될 수 있도록 하였다. 이를 통해, 기존 구현은 Toffoli depth가 6이였던 반면, 해당 구현에서는 연산 수정을 통해 Toffoli depth 4의 효율적인 S-Box 양자 회로를 구현하였다.

3. 성능 평가 및 분석

본 장에서는, 앞서 살펴본 S-Box 양자 회로들을 구현하고 이에 필요한 양자 자원들을 평가한다. Toffoli 게이트는 사실, 여러 개의 양자 게이트들로 조합되어 구현되며 이에 대한 여러 가지 방법이 존재한다 [?]. 본 논문에서 사용된 분해 방법은 [?]의 7개의 T 게이트와 8개의 Clifford 게이트, T-depth 4, 전체 depth 8의 구현을 사용한다. [표 1]은 해당 분해 방식으로 추정한 AES S-Box 양자 회로 구현에 필요한 양자 자원들을 나타낸다. Inversion이 양자 회로상에서 구현된 [3]의 S-Box는 큐비트 수가 적지만 매우 높은 Toffoli depth, 전체 depth를 보여주며, 하드웨어 기반의 S-Box 구현이 양자 회로상에서 구현되는 경우, 큐비트를 더 많이 사용하지만 상대적으로 낮은 Toffoli depth, 전체 depth만으로 구현됨

을 확인할 수 있다.

<표 1> S-Box 구현에 필요한 양자 자원 비교

Qubits	Total gates	Toffoli depth	Full depth
40	88	88	951
136	6	6	85
136	4	4	72

4. 결론

본 논문에서는 AES의 S-Box 양자 회로 구현들을 살펴보고 이에 대한 필요 양자 자원들을 비교하였다. S-Box는 AES 양자 회로 구현 시, 가장 많은 비용을 차지하기 때문에 효율적인 양자 회로가 요구된다. S-Box 양자 회로의 개선 과정과 몇가지 트레이드오프를 찾아보았으며, 이를 통해 추후 AES 양자 회로 최적화 구현 시, 참조할 수 있을 것으로 기대된다.

5. 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] 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.

[2] 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.

[3] 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.

[4] 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.

[5] H. Zhenyu, and S. Sun. "Synthesizing Quantum Circuits of AES with Lower T-depth and Less Qubits." Cryptology ePrint Archive (2022).