Grover 알고리즘을 사용한 대칭키 암호 공격 동향

장경배[1], 오유진[2], 김덕영[2], 서화정[3]
[1]한성대학교 정보컴퓨터공학과 박사과정
[2]한성대학교 IT 융합보안학과 석사과정
[3]한성대학교 IT 융합보안학과 교수
starj1023@gmail.com, oyj0922@gmail.com, dudejrdl123@gmail.com,
hwajeong84@gmail.com

Symmetric Key Cryptographic Attack Trend Using Grover's Algorithm

Kyung-Bae Jang[1], Yu-Jin Oh[2], Duk-Young Oh[2], Hwa-Jeong Seo[3]
[1]Dept. of Computer Information Engineering, Hansung University
[2]Dept. of Convergence Security, Hansung University
[3]Dept. of Convergence Security, Hansung University

요 약

양자 컴퓨터가 현대 암호 시스템의 보안성을 위협하고 있음에 따라, 최근 잠재적인 양자 공격들에 대한 분석 연구들이 다수 발표되고 있다. 공개키 암호인 RSA와 ECC의 경우, Shor 알고리즘에 의해 다항시간 내에 해결됨으로써 보안성이 완전히 붕괴되는 반면, 대칭키 암호는 Grover 알고리즘에 의해 보안 강도가 제곱근으로 감소하기 때문에 키 길이를 증가시킴으로써 기존 보안성을 복구할 수 있다. 이론적으로 Grover 알고리즘은 보안성을 훼손시키지만, 현실적인 공격 난이도가 매우 높음에 따라 대상 암호에 대한 양자 회로 최적화 구현이 중요하다. 이에 본 논문에서는 블록암호 RC5를 양자 회로 상에서 최적화하고 이를 기반으로 Grover 공격 비용을 추정한다. 마지막으로, 추정한 비용을 NIST의 양자 후 보안 강도 평가와 함께 비교함으로써 RC5에 대한 양자 암호 분석을 수행한다.

1. 서론

다가오는 양자 컴퓨터 시대에 있어, 안전한 양자 후 암호 시스템 구축을 위한 다양한 양자 암호 분석 연구들이 수행되고 있다. 공개키 암호인 RSA와 ECC의 경우, Shor 알고리즘 [1]을 통해 다항 시간 내에 해결되기 때문에 새롭게 대체할 양자 후 내성 암호가 필요한 상황이다. 이에 NIST는 양자 내성 암호 공모전을 주최하였으며, 현재 4개의 표준화 암호 알고리즘이 Key Encapsulation Mechanism (KEM)과 전자 서명 분야에 선정된 상태이다, 표준화 이후, Round 4를 진행 중이며, Round 4 이후 몇 개의 암호 알고리즘들이 추가로 표준화 될 예정이다. 양자 컴퓨터의 공격으로 인해 공개키 암호는 보안성이 완전히 붕괴되지만, 다행히도 대칭키 암호의 경우는 그렇지 않다.

Grover 알고리즘은 대칭키 암호의 보안성을 감소시킬 수 있는 양자 알고리즘이다 [2]. 검색을 가속화 시키는 양자 알고리즘이며, 이를 통해 대칭키 암호에 대한 전수 조사를 가속화 시킬 수 있다. 이에 대칭키 암호 AES를 시작으로 다양한 대칭키 암호들에 대한 양자 암호 분석 연구들이 수행되고 있다. 이에 본 논문에서는 Grover 알고리즘을 사용한 대칭키 암호 분석 연구들을 살펴보고자 한다.

2. 관련 연구

2.1 Grover 알고리즘

Grover 알고리즘은 검색하고자 하는 모든 경우의 수를 중첩 상태의 큐비트를 통해 확률로서 저장한다. Grover oracle을 통해 원하는 데이터를 찾고, Grover diffusion operator를 통해 해당 데이터의 관측 확률을 증가시킨다. Grover 알고리즘은 범위에 n-bit 검색 범위에 대해 oracle + diffusion operator를 순차적으로 $2^{n/2}$번 반복 수행함으로써 매우 높은 확률로 원하는 데이터를 찾아낸다. 따라서 Grover 알고리즘을 사용한 전수 조사의 경우, n-bit 키를 사용하는 경우 고전 컴퓨터는 $O(2^n)$의 검색 복잡도가 요구되지만, Grover 알고리즘을 사용한 검색은 $2^{n/2}$의 복잡도가 요구된다. 즉, 고전 컴퓨터상으로 주장하던 보안 강도가 제곱근만큼 감소하게 된다.

Grover 알고리즘은 높은 반복 횟수로 인한 극심한 양자 비용이 사용된다. 따라서 비용을 감소시키는 것이 중요한데, 이는 공격 대상이 되는 암호 알고리즘의 양자 회로가 얼마나 효율적인지에 따라 결정된다.

2.2 NIST 양자 후 보안 강도 평가 [3]

NIST는 AES에 대한 Grover 공격 비용을 기준으로 하여 암호 알고리즘의 양자 후 보안 강도를 평가하고 있다. 이론적으로 Grover 알고리즘은 모든 대칭키 암호의 보안 강도를 제곱근만큼 감소시킨다. 하지만, 현실적으로 현재는 물론 가까운 미래에 개발될 양자 컴퓨터의 성능으로는 Grover 알고리즘의 극심한 양자 자원을 감당할 수 없다. 때문에 공격에 필요한 양자 비용이 너무 높다면, 해당 암호 알고리즘은 현실적으로 Grover 알고리즘을 사용한 양자 공격에 내성을 가지고 있다고 판단할 수 있다. NIST는 이 양자 비용에 대한 기준점을 AES-128, 192, 256에 필요한 Grover 공격 비용으로 삼아 Level 1, 3, 5를 산정하였다. 예를 들어, 특정 암호에 대한 양자 공격 비용이 Level 1에 해당하는 AES-128에 대한 양자 공격 비용보다 낮다면, 해당 암호는 양자 후 보안 강도 Level 1을 획득할 수 없다. 반대로 해당 암호를 공격하는데 더 많은 양자 비용이 필요하다면, Level 1을 달성하게 된다.

3. AES에 대한 양자 회로 최적화 구현 동향

3.1 Grassl et al. AES 양자 회로 구현 [4]

2016년, Grassl et al.은 AES-128, 192, 256에 대한 양자 회로 구현을 최초로 제시하였다. 해당 연구는 PQCrypto에서 발표되었으며, NIST가 추정한 AES에 대한 양자 공격 비용은 해당 연구를 참조하고 있다. AES 양자 회로 구현의 경우, 대부분의 양자 비용이 SubBytes의 S-box들과 키 스케줄의 S-box들에 소모된다. 해당 구현에서는 S-box를 양자 회로로 구현하는데 있어 S-box 내부 연산인 $\mathbb{F}_{2^8}/(x^8+x^4+x^3+1)$ 역치 연산을 그대로 구현하였다. 역치에 해당하는 지수 승을 계산하기 위해 곱셈과 제곱의 연속으로 구성되는 양자 회로를 구현하였다. 그런데 곱셈의 경우, 양자 컴퓨터에서 매우 높은 비용을 차지한다. 그 결과 현 시점에서 보았을 때, Grassl et al.의 AES 양자 회로 구현은 매우 높은 양자 비용이 사용되었다고 평가된다. 비록 양자 게이트와 회로 depth가 높기는 하지만, 저자들은 큐비트 수를 줄이는데 초점을 맞추었다. Zig-zag 구조의 AES 양자 회로 아키텍처를 제시함으로써 큐비트 수를 줄였다. AES의 경우 S-box의 출력을 저장하기 위해 매 라운드 128-qubit이 사용되어야 한다. 저자들은 매 라운드 128-qubit을 새롭게 할당하는 것이 아닌, 이 전 라운드에서 할당했던 128-qubit을 0으로 초기화시키고 해당 라운드의 출력을 저장하는 방식의 Zig-zag 아키텍처를 구현하였다. 이전 라운드의 128-qubit을 0으로 되돌리기 위해, 이전 라운드의 연산들을 거꾸로 한 번 더 수행하는 리버스 연산들이 수행됨으로써 양자 게이트와 depth 는 증가하였지만, 큐비트 수를 절약할 수 있었다.최근 AES 양자 회로 구현들은 해당 Zig-zag 아키텍처를 개선하여 큐비트 수를 더욱 줄이는 추세이다.

3.2 Jaques et al. AES 양자 회로 구현 [5]

2020년, Jaques et al.은 가장 낮은 비용의 AES 양자 회로 구현을 제시하였다. 해당 구현에서는 Boyer-Peralta의 S-box 구현을 양자 회로 상으로 옮겨 구현하였다. 양자 곱셈을 구현하는 것이 아닌, 하드웨어 최적화된 Boyer-Peralta의 Boolean function 기반의 S-box를 구현함으로써 낮은 depth를 가지도록 최적화 되었다. 또한 회로 아키텍처를 설계하는데 있어 Pipeline 구조를 선택하였는데, 이는 매 라운드 S-box의 출력을 새로운 큐비트에 저장함으로써 큐비트 사용은 증가하였지만, 게이트와 depth는 크게 감소하였다. 그 결과, 큐비트-depth의 트레이드오프를 평가해보았을 때, 가장 높은 성능의 AES 양자 회로가 제시되었다. 하지만 이 후, 해당 논문의 AES 양자 회로 비용이 과소하게 추정되었다는 오류가 보고되었다. 저자들은 양자 회로를 구현하고 비용을 추정하는데 있어 Microsoft의 Q#을 사용하였는데, Q#의 리소스 추정기의 큐비트-depth의 불일치 오류로 인해 낮은 비용이 보고된 것이다.

3.3 Jang et al.의 AES 양자 회로 구현 [6]

2021년, Jang et al.은 Jaques et al.의 구현 오류를 수정함으로써 해당 구현의 올바른 양자 비용을 추정하였다. 보고된 큐비트 수를 유지할 때, 얼마만큼의 depth가 나와야 하는지 분석하였으며 기존 보고된 depth보다 훨씬 높은 depth가 추정되었다. 또 한 Jang et al.은 새로운 AES 양자 회로 구현을 제시하였다. 해당 구현은 큐비트 수를 많이 사용하지만, 가장 적은 양자 게이트와 가장 낮은 depth 성능을 제

공한다. 해당 저자들은 큐비트를 추가적으로 사용하기는 하지만 큐비트-depth의 트레이드오프를 적절히 고려하는 개선된 Pipeline 아키텍처를 제시하였다. 그 결과, 양자 회로의 성능을 나타내는 지표인 큐비트 수 × depth의 메트릭에서 높은 성능을 제공한다. Grover 공격 비용을 측정하는데 있어 총 양자 게이트 수 × depth 메트릭을 사용하고 있는데, 해당 논문에서 추정한 Grover 공격 비용은 현재까지 AES에 대해 Grover 공격 비용들 중 가장 낮다.

4. 대칭키 암호에 대한 최적화 구현 동향

추정된 공격 비용을 기반으로 NIST의 평가 지표와 비교함으로써 해당 암호의 양자 후 보안 레벨을 평가하는 방식으로, AES 뿐만이 아닌 다양한 대칭키 암호들을 양자 회로로 최적화 구현하고 공격 비용을 추정하는 연구들이 발표되고 있다. 현재 NIST가 추정한 양자 후 보안 레벨별 공격 비용과 최근 [6]이 최적화한 공격 비용은 [표 1]과 같다.

<표 1> NIST 양자 후 보안 강도 평가 지표

Security	NIST	[6]
Level 1 (AES-128)	2^{170}	2^{157}
Level 3 (AES-192)	2^{233}	2^{222}
Level 5 (AES-256)	2^{298}	2^{286}

다양한 대칭키 암호들에 대한 Grover 공격 비용이 추정되고 있지만, NIST의 추정 비용과 비교 시, 같은 키 사이즈 기준, AES보다 훨씬 더 적은 비용으로 공격이 가능하다. 이는 NIST가 추정한 비용이 Grassl et al.의 AES 양자 공격 비용을 기반으로 하고 있기 때문이다. 해당 구현은 현 시점에서 보았을 때, 매우 높게 추정되었고 최신 양자 회로 구현들은 이보다 훨씬 적은 비용으로 구현되고 있다. 결론적으로, NIST 기준과 비교 시, 대부분의 암호들이 키 사이즈 별 적정 보안 레벨을 획득하지 못하게 된다. 하지만 NIST가 공격 비용을 구체적으로 추정하긴 하였지만, AES에 대한 상대적인 공격 비용을 기준으로 하기 때문에 최신 공격 비용이 줄어들 시, 해당 기준으로 보안 레벨을 평가해야 한다. 만약 [6]의 추정 비용과 비교 시, 해당 AES 구현은 최적화가 높은 수준으로 달성되었기 때문에 대부분의 암호들이 키 사이즈별 적정 보안 레벨을 달성할 수 있다.

5. 결론

본 논문에서는 대칭키 암호에 대한 Grover 공격 동향에 대해 살펴보았다. AES 공격 비용이 양자 후 보안 레벨의 기준점이 되기 때문에 AES를 양자 회로 상에서 최적화하기 위한 몇 가지 연구들을 분석하였다. 또한 NIST의 기준과 최신 AES 공격 비용과 비교하여 다양한 대칭키 암호들의 양자 후 보안 강도가 어떻게 평가되어야 하는지에 대해 살펴보았다. 본 논문을 통해 대칭키 암호에 대한 양자 공격의 흐름과 결과가 어떠한 방식으로 도출되어야 하는지에 대해 도움이 될 수 있을 것이라 사료된다.

6. Acknowledgements

This work was partly 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, 75%) and this work was partly supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices, 25%).

참고문헌

[1] Shor, Peter W. “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” SIAM review 41.2, pp. 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,” [internet], 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, R. Steinwandt, “Applying Grover’s algorithm to AES: quantum resource estimates,” Post-Quantum Cryptography, PQCrypto'16, LNCS, 9606, pp. 29 - 43, 2016.
[5] S. Jaques, M. Naehrig, M. Roetteler, 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.
[6] K. Jang, A. Baksi, H. Kim, G. Song, H. Seo, A. Chattopadhyay, “Quantum analysis of aes,”. Cryptology ePrint Archive. 2022.