양자 회로 상에서의 SHA2 구현 동향

임세진[1], 장경배[2], 양유진[1], 오유진[3], 서화정[4]
[1]한성대학교 IT융합공학과 석사과정
[2]한성대학교 정보컴퓨터공학과 박사과정
[3]한성대학교 융합보안학과 석사과정
[4]한성대학교 융합보안학과 교수
dlatpwls834@gmail.com, starj1023@gmail.com, yujin.yang34@gmail.com,
oyj0922@gmail.com, hwajeong84@gmail.com

Research Trend about Quantum Circuit Implementation for SHA2

Se-Jin Lim[1], Kyung-Bae Jang[2], Yu-Jin Yang[1], Yu-Jin Oh[3], Hwa-Jeong Seo[4]
[1]Dept. of IT Convergence Engineering, Han-Sung University
[2]Dept. of Information and Computer Engineering, Han-Sung University
[3]Dept. of Convergence Security, Han-Sung University
[4]Dept. of Convergence Security, Han-Sung University

요 약

양자컴퓨터는 큐비트(qubit)의 얽힘(entanglement)과 중첩(superposition) 성질을 통해 동시에 연산을 수행할 수 있어 고전컴퓨터에 비해 연산 속도가 획기적으로 빠르다. 전수조사 연산을 매우 빠르게 수행할 수 있는 양자 알고리즘인 Grover 알고리즘을 사용하면, n-bit 보안강도를 가지는 SHA2와 같은 해시함수를 $n/2$-bit 보안강도로 낮추게 되어 해시함수가 적용되는 분야의 보안을 위협하게 된다. 양자컴퓨터를 통한 해킹에는 많은 양자 자원이 요구되고, 안정적인 구동 환경이 갖춰져야 하기 때문에 실현되기 위해서는 아직까지 상당한 시간이 소요될 것으로 보인다. 이에 연구자들은 필요한 양자 자원을 최소화하는 효율적인 양자 공격 회로를 제시하며 연구를 수행하고 있다. 본 논문에서는 이러한 SHA2 해시함수에 대한 양자 회로 구현 동향에 대해 살펴본다.

1. 서론

양자컴퓨터는 양자 역학의 특성을 활용한 컴퓨터로, 큐비트(qubit)를 기본 연산 단위로 삼는다. 이러한 큐비트는 양자 현상인 얽힘(entanglement)과 중첩(superposition) 성질을 통해 동시에 연산을 수행할 수 있어 고전컴퓨터에 비해 연산 속도가 획기적으로 빠르다. 전수조사 연산을 매우 빠르게 수행할 수 있는 양자 알고리즘인 Grover 알고리즘[1]을 사용하면, n-bit 보안강도를 가지는 해시함수를 $n/2$-bit 보안강도로 낮추게 되어 해시함수가 적용되는 분야의 보안을 위협하게 된다. 해시함수는 전자서명, 메시지 인증 코드, 난수 생성, 키 유도 함수 등에 활용될 수 있으며, SHA2의 경우 현재 상용화되어 있는 SSL의 디지털 인증서 등에 적용되어 사용되고 있다. Grover 알고리즘은 해시함수에 대한 역상 공격(preimage attack)에 사용될 수 있다. 역상 공격은 해시함수의 출력값이 동일하게 나오는 입력값을 찾는 해시 충돌 공격 방식이다. SHA-256은 고전적인 충돌 공격에 대해 128-bit 보안 강도를 가지는데, Grover 알고리즘을 사용하면 이러한 해시함수의 보안 강도가 절반에 해당하는 64-bit로 줄어들게 된다[2]. Grover 알고리즘은 양자컴퓨터 상에서 동작하기 때문에 공격을 수행하기 위해서 공격 대상으로 삼은 해시함수를 양자 회로로 구현해야한다. 양자컴퓨터를 통한 해킹에는 많은 양자 자원이 요구되고, 안정적인 구동 환경이 갖춰져야 하기 때문에 실현되기 위해서는 아직까지 상당한 시간이 소요될 것으로 보인다. 이에 연구자들은 필요한 양자 자원을 최소화하는 효율적인 양자 공격 회로를 제시하며 연구를 수행하고 있다. 본 논문에서는 해시함수 중 SHA2에 대한 양자 회로 구현 동향에 대해 살펴본다.

2. SHA2 해시함수[2,3]

SHA2(Secure Hash Algorithm 2)는 2002년에 NIST(National Institute of Standards and Technology)에서 표준화한 해시함수의 집합으로, 해시 값의 길이에 따라 6개로 구성된다. SHA-224,

SHA-256, SHA-384, SHA-512, SHA-512/224, SHA-512/256이 해당되며, 일부 상수와 라운드 수를 제외하고 구조적으로 동일하다고 볼 수 있다. 표 1에 상세 정보를 정리하였다. 메시지 크기는 원본 메시지의 길이를 말하며, 2^{64}미만은 원본 메시지의 길이가 64비트로 표현되어야함을 의미한다. SHA-256로 해시함수의 동작 방식을 살펴보면 SHA2는 크게 전처리 단계와 해시 연산 단계로 구성된다. 전처리 단계에서는 메시지 패딩 및 파싱을 수행하고 패딩된 메시지의 길이가 512-bit의 배수가 되도록 비트를 추가한다. 해시 값이 생성되는 해시 연산 단계는 패딩된 메시지의 블록 수에 따라 전체 알고리즘을 반복 수행한다.

<표 1> SHA2 상세 정보

Hash Function	Message Size (bits)	Block Size (bits)	Message Digest Size (bits)
SHA-224	$< 2^{64}$	512	224
SHA-256	$< 2^{64}$	512	256
SHA-384	$< 2^{128}$	1024	384
SHA-512	$< 2^{128}$	1024	512
SHA-512/224	$< 2^{128}$	1024	224
SHA-512/256	$< 2^{128}$	1024	256

3. Grover 알고리즘[1]

Grover 알고리즘은 양자 알고리즘으로, N개의 무작위 데이터 집합으로부터 찾고자하는 대상 데이터를 $\sqrt{N}$번 안에 높은 확률로 찾아내는 전수조사 알고리즘이다. 고전컴퓨터에서는 해당 작업에 $O(N)$의 시간복잡도가 소요되지만, 양자컴퓨터상에서는 Grover 알고리즘을 통해 $O(\sqrt{N})$의 시간복잡도를 가지게 된다. 따라서 Grover 알고리즘을 사용하면 대칭키 암호의 키를 찾기 위한 전수조사를 가속화할 수 있으며, 해시함수의 출력값이 동일하게 나오도록 하는 입력값을 찾는 해시 충돌 공격도 가속화할 수 있다.

4. 양자 회로 상에서의 SHA2 구현 동향

필요한 양자 자원을 최소화하여 양자 회로를 구현할 때 고려해야할 요소는 사용되는 큐비트 수를 의미하는 width, Toffoli-gate 수, Toffoli-depth, 전체 회로 depth가 있다. SHA2에서는 많은 덧셈 연산이 수행되기 때문에 효율적인 양자 덧셈기 회로를 사용하여 구현하는 것 또한 고려해야할 중요한 요소이다.

4.1 Kim et al.의 SHA2 양자 회로 구현[4]

[sha2]은 AES 암호, SHA2와 SHA3 해시함수에 대해 효율적인 양자 회로를 구성하여 공격을 수행하였으며, SHA3는 양자 비용 추정이 광범위하여 AES와 SHA2에 대해서만 보안 강도를 측정하였다. SHA2 해시함수 회로 구현에 사용한 양자 덧셈기는 다항 깊이를 가지는 Cuccaro[5] 덧셈기와 대수 깊이를 가지는 Draper[6] 덧셈기를 사용하여 비교하였다. 다항 깊이(poly-depth)를 가지는 덧셈기의 경우 SHA-256 양자 회로 구현에서 1개의 큐비트와 61의 Toffoli-depth를 가지며, 대수 깊이(log-depth)의 덧셈기는 53 큐비트와 22 Toffoli-depth를 가짐을 보였다. 각각 작업 공간 절약 또는 실행 시간 단축의 장점이 있다. 또한 CNOT-gate를 사용하여 해시 연산이 효율적으로 실행되도록 하였다. 최적화 구현을 위해 3가지를 고려했는데, 메시지 스케줄링과 라운드 함수의 병렬화 여부, 덧셈기 선정, $C^{256}NOT$ 구현에 사용할 큐비트 수가 이에 해당한다. 3가지 요소의 유무에 따라 8가지의 회로가 구현될 수 있지만, 개선점을 가지는 6개에 대해 표 2와 같이 SHA-C1부터 SHA-C6까지 명명하여 설계하였다.

<표 2> SHA2의 6가지 회로 설계 방식

Hash Function	Schedule round	Adder	$C^{256}NOT$
SHA-C1	serial	poly-depth	less-qubit
SHA-C2	serial	log-depth	less-qubit
SHA-C3	serial	log-depth	lower-depth
SHA-C4	parallel	poly-depth	less-qubit
SHA-C5	parallel	log-depth	less-qubit
SHA-C6	parallel	log-depth	lower-depth

이 구현에 대한 Grover 알고리즘 공격 비용은 표 3과 같다.

<표 3> 6가지 구현에 대한 Grover 알고리즘 공격 비용

Hash Function	Toffoli-depth	Qubits
SHA-C1	1.568×2^{143}	802
SHA-C2	1.227×2^{142}	854
SHA-C3	1.163×2^{142}	1023
SHA-C4	1.216×2^{143}	835
SHA-C5	1.919×2^{141}	939
SHA-C6	1.792×2^{141}	1023

4.2 Lee et al.의 SHA2 양자 회로 구현[7]

[7]은 앞의 [4]를 개선한 논문으로, SHA2 해시함수는 6가지가 있지만, 구조가 거의 유사하기 때문에 SHA-256에 집중하여 회로를 제시하였다. SHA2는 덧셈 연산이 주로 사용되기 때문에 효율적인 양자 덧셈기를 사용하여 최적화하였다. 또한 T-gate와 T†-gate는 양자컴퓨팅 계산 복잡도 및 성능에 큰 영향을 주기 때문에 T-depth와 T-width를 최소화하는 것도 양자 회로 최적화에서 중요한 부분이다. 따라서 해당 논문은 최적화를 위해 T-gate와 관련된 두 가지 수치를 감소시키는 방법을 제안한다. ripple carry 양자 덧셈기인 TK (Takahashi) 덧셈기[8]의 Toffoli-gate 구조의 특징을 이용하여 일부 T-gate를 제어된 위상 게이트로 대체하여 T-depth를 감소시킨, 개선된 TK 덧셈기를 사용하였다. 결과적으로 이전 덧셈기에 비해 T-depth가 33% 이상 감소하였다. 또한 SHA-256 양자 회로에 사용되는 양자 덧셈기를 3개로 줄였으며, 덧셈기 개선에 사용한 T-depth 감소 기법을 SHA-256의 기능 블록에도 적용하여 최적화하였다.

5. 결론

양자 알고리즘인 Grover 알고리즘을 사용하면, 해시함수의 보안 강도를 절반으로 낮추게 되어 보안을 위협하게 된다. 본 논문에서는 해시함수 SHA2에 대한 Grover 알고리즘의 공격 비용을 줄이기 위한 SHA-256 양자 회로 최적화 구현에 대한 동향을 살펴보았다. 큐비트 수부터, Toffoli-gate, T-gate, depth 등 최적 구현을 위해 고려할 수 있는 요소가 다양하며 어떤 요소에 초점을 맞추느냐에 따라 여러 가지 구현 버전이 제시되는 것을 알 수 있었다. SHA2 해시함수는 다양한 분야에서 사용되므로 해시함수에 보안 강도와 관련된 연구가 더욱 활발히 수행되야할 것으로 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] 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] N. I. of Standards and Technology: Fips Pub 180 4: Secure Hash Standard (Shs) (2012)

[3] Penard, Wouter, and Tim van Werkhoven “On the secure hash algorithm family” Cryptography in context, pp. 1-18, 2008.

[4] Kim, Panjin, Daewan Han, and Kyung Chul Jeong. "Time - space complexity of quantum search algorithms in symmetric cryptanalysis: applying to AES and SHA-2." Quantum Information Processing 17 (2018): 1-39.

[5] Cuccaro, S.A., et al.: A New Quantum Ripple Carry Addition Circuit (2004). arXiv preprint quant ph/0410184

[6] Draper, T.G., et al.: A Logarithmic Depth Quantum Carry Lookahead Adder (2004). arXiv preprint quant ph/0406142

[7] Lee, Jongheon, et al. "T depth reduction method for efficient SHA 256 quantum circuit construction." IET Information Security 17.1 (2023): 46-65.

[8] Takahashi, Y., Kunihiro, N.: A linear size quantum circuit for addition with no ancillary qubits. Quant. Inf. Comput. 5(6), 440 - 448 (2005). https://doi.org/10.26421/qic5.6-2