블록암호 RC5에 대한 Grover 공격 최적화

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

Optimizing Grover's Attack on Block Cipher RC5

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

양자 컴퓨터가 암호 알고리즘들이 기반하고 있는 수학적 난제들을 효율적으로 모델링하고 검색 복잡도의 어려움을 감소시킴에 따라 최근 양자 알고리즘을 사용한 양자 암호 분석 연구들이 다양하게 제시되고 있다. 공개키 암호의 경우, RSA와 ECC의 보안성이 완전히 붕괴됨에 따라 새로운 양자 내성 암호가 필요한 상황이며, 이에 NIST의 공모전이 주최되었다. 반면 대칭키 암호의 경우 보안성이 감소되는 것으로 그치지만, NIST 공모전의 양자 내성 암호 알고리즘들 내부에서도 대칭키 암호 요소들이 활용됨에 따라 대칭키 암호의 보안 훼손은 안전한 양자 내성 암호의 보안성을 우회할 수도 있다. 이에 AES 암호를 시작으로 다양한 대칭키 암호에 대해 Grover 알고리즘을 사용한 양자 암호 분석 연구들이 수행되고 있다 [1]. Grover 알고리즘이 대칭키 암호의 전수 조사를 가속화함에 따라 보안 강도를 제곱근만큼 감소시킬 수 있지만 [2], 현실적인 공격 난이도가 매우 높음에 따라 양자 회로 최적화를 통한 공격 비용 감소 연구들이 진행되고 있다. 잠재적인 강력한 양자 공격들을 미리 분석하는 것은 안전한 양자 후 암호 시스템을 구축하기 위한 발판이 된다. 이에 본 논문에서는 블록암호 RC5 [3]에 대해 Grover 알고리즘을 사용한 양자 암호 분석을 수행한다. 이를 위해, RC5 암호화 양자 회로를 최적화하고 이를 기반으로 최종 Grover 공격 비용을 평가한다. 최종적으로는, NIST의 양자 후 보안 강도 평가 기준 [4]과 최신 결과들과 함께 RC5에 대한 양자 후 보안 강도를 평가하고자 한다.

2 Grover 알고리즘을 사용한 키 전수 조사[2]

양자 검색 알고리즘인 Grover 알고리즘은 대칭키 암호에 대한 검색 복잡도를 제곱근만큼 감소시킬 수 있다. n-bit 키를 사용하는 블록암호에 대한 고전 전수 조사 복잡도는 $O(2^n)$이지만, 양자 전수 조사는 제곱근으로 감소된 $2^{n/2}$의 복잡도를 가진다. Grover 알고리즘을 사용한 키 복구 공격 프로세스는 수식 (1), (2), (3) 순으로 수행된다. (1)은 Hadamard 게이트를 사용하여 중첩 상태의 n-qubit 키를 준비한다 ($H^{\otimes n}|0\rangle^{\otimes k}$). 중첩 상태의 키는 모든 경우의 키 값을 확률로서 가지게 된다. Grover Oracle $f(x)$ (2)에서는 중첩 상태의 키로 구현된 대상 암호화 양자 회로로 알려진 평문을 암호화하여 중첩 상태의 암호문을 생성한다. 알려진 암호문과 일치하는 경우를 비교하고 일치하는 경우 ($f(x)=1$), 이후 해당 키 값의 부호를 반전시키는 방식으로 oracle은 올바른 키를 반환한다 ($((-1)^{f(x)}|x\rangle|-\rangle$). 마지막으로 Diffusion operator (3)를 통해 Oracle이 반환한 키의 관측 확률을 증가시킨다. Grover 알고리즘은 Oracle과 Diffusion operator를 순차적으로 약 $2^{n/2}$번을 반복함으로써 제곱근의 복잡도만으로 높은 확률의 키 복

구를 성공할 수 있다.

$$H^{\otimes n}|0\rangle^{\otimes n}=\left(\frac{|0>+|1>}{\sqrt{2}}\right)^{\otimes n}=\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}|x\rangle \quad (1)$$

$$f(x)=\begin{cases}1 \text{ if } Enc(key)=Ciphertext\\ 0 \text{ if } Enc(key)\neq Ciphertext\end{cases} \quad (2)$$

$$U_f(|\psi\rangle|-\rangle)=\frac{1}{2^{n/2}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle|-\rangle \quad (3)$$

3. RC5 양자 회로 최적화 구현

RC5 암호는 가변적인 블록 크기(32/64/128 비트), 키 크기(0~2040 비트) 및 라운드 수(0~255 비트)를 가지고 있다. 본 논문에서는 64비트 평문, 128비트 키를 사용하여 총 12 라운드를 진행하였다.

3.1 Rotation 구현

RC5에서는 상수 값이 아닌 중간 값에 따라 좌측으로 로테이션을 하는 과정이 있다. (그림 1)을 보면 해당 비트가 1일 때, 비트자리(i)에 따라 2^i만큼 로테이션을 돌고 Swap 게이트를 사용하여 값을 옮긴다. 본 논문에서는 32비트 배열을 사용하므로 32비트(2^5) 이상 로테이션은 제자리 결과가 됨으로써 하위 5비트까지만 값을 확인해준다.

Algorithm : Left Rotation
Input: $s[i]$, $a\_b[i]$ $(0 \le i < 32)$
Output: $s[i]$
1: for $i=0$ to 5
2: with Control($a\_b[i]$)
3: for $j=0$ to 2^i
4: for $k=0$ to 31
5: SWAP ($s[31-k]$, $s[30-k]$)
6: **return** $s[i]$

(그림 1) 좌측 Rotation 양자 회로 구현

3.2 Encryption

Encryption 부분에서는 덧셈, Rotation 연산이 사용되며 Key schedule 단계에서 생성한 S 배열과 평문을 사용하여 연산을 진행한다. 최적화를 위해 덧셈 연산 구현 시 개선된 ripple carry 덧셈기(CDKM, [5])를 사용한다. Encryption 구현은 (그림 2)와 같다.

Algorithm : Encryption
Input: pt([0],[1]), $S[i]$ $(0 \le i < 823)$
Output: pt([0],[1])
1: CDKM($S[0:32]$,pt[0],c)
2: CDKM($S[32:64]$,pt[1],c)
1: for $i=0$ to 12
2: CNOT32(pt[1],pt[0])
5: left_rotation(pt[0],pt[1])
6: CDKM($S[32\cdot(2\cdot i+2):32\cdot(2\cdot i+3)]$,pt[0],c)
7: CNOT32(pt[0],pt[1])
8: left_rotation(pt[1],pt[0])
9: CDKM($S[32\cdot(2\cdot i+3):32\cdot(2\cdot i+4)]$,pt[1],c)
10: **return** pt[0],pt[1]

(그림 2) Encryption 양자 회로 구현

3.3 Key Schedule

Key schedule 단계에서는 128비트 키를 사용하여 덧셈 및 로테이션 연산을 통해 26개의 원소를 가진 32비트 워드 단위의 배열 S를 생성한다. 키는 32비트씩 연산에 사용되며 총 78번의 반복 문을 돌기 위해 4번마다 키 값을 재사용되고 배열 S 또한 26번마다 재사용된다. 그러한 이유로 키 값과 배열 S의 값이 변경되지 않고 보존되어 있어야한다.

로테이션 연산 이후, 해당 결과를 A와 B에 저장해야 한다. 양자 컴퓨터상에서는 초기화 된 상태에서 게이트를 사용 하는 것으로만 값을 할당 할 수 있기 때문에 배열을 초기화해야 한다. "$B=Key[i]$"와 같이 표현하면 값을 저장하는 개념이 아닌 같은 주소를 공유하는 개념이므로 B값이 달라지면 키 값 또한 달라져 키 값을 보존할 수 없다. (그림 3)을 보면 A의 경우 덧셈 연산 시에 값이 변경되지 않은 반면, B의 경우 덧셈 연산이 B에 저장됨에 따라 값이 변경된다. 그로인해 매 라운드마다 값이 초기화 된 큐비트가 필요하며, 본 논문에서는 매 라운드마다 큐비트를 선언하는 대신 새로운 32비트 new_B를 한 번만 할당하고 뺄셈 연산 및 이전 key값과의 XOR연산을 통해 new_B를 초기화 시킨다. 초기화 된 new_B는 다음 라운드에서 재사용되며 이를 통해 큐비트 수를 감소시켰다.

Algorithm : key expansion
Input: $c, S[i]$, $A[j]$, $B[j]$, $Key[k]$ $(0 \le i < 823), (0 \le j < 32)$ $(0 \le k < 128)$
Output: $S[i]$
1: for $i=0$ to 78
2: CDKM($B, S[(32\cdot(i\%26)):32\cdot((i\%26)+1)], c$)
3: CDKM($A, S[(32\cdot(i\%26)):32\cdot((i\%26)+1)], c$)
4: A=ROTL3($S[(32\cdot(i\%26)):32\cdot((i\%26)+1)]$)
5:
6: CDKM(A, B, c)
7: CDKM($B, Key[(32\cdot(i\%4)):32\cdot((i\%4)+1)], c$)
8: left_rotation($Key[(32\cdot(i\%4)):32\cdot((i\%4)+1)], B$)
9:
10: if($i=0$):
11: copy($Key[(32\cdot(i\%4)):32\cdot((i\%4)+1)]$,new_$B$)
12: else:
13: CDKM_minus(A,new_B,c)
14: copy($Key[32\cdot(((i-1)\%4):32\cdot(((i-1)\%4)+1)]$, new_$B$)
15: copy($Key[(32\cdot(i\%4)):32\cdot((i\%4)+1)]$,new_$B$)
16:
17: B = new_B
18 : **return** $S[i]$

(그림 3) Key schedule 양자 회로 구현

4. 성능 평가 및 RC5 양자 후 보안 강도 분석

본 장에서는 제시하는 RC5 양자 회로 구현에 필요한 양자 자원들을 추정하며, 이를 기반으로 RC5에 대한 Grover 공격 비용을 평가한다. 마지막으로 추정된 비용을 NIST의 양자 후 보안 평가 기준에 따라

RC5의 양자 후 보안 강도를 분석하고자 한다. RC5 양자 회로 구현에 필요한 양자 자원들은 <표 1>과 같다. Clifford + T 게이트 단위의 세부 분석을 위해 Toffoli 게이트는 분해 방법 중 하나인 7개의 T 그리고 8개의 Clifford 게이트, depth는 8로 분해되어 비용에 포함된다.

<표 1> RC5 양자 회로 구현에 사용된 양자 비용

Cipher	Qubits	Clifford gates	T gates	Full depth
RC5	1122	394250	177051	256252

제안하는 RC5 양자 회로를 기반으로 Grover 공격 비용은 다음과 같이 추정된다. Grover 공격은 Oracle과 Diffusion operator의 반복으로 수행되지만, Diffsuion operator의 경우 비용이 무시할 수 있을 정도로 작기 때문에 Oracle 반복에 대한 비용이 공격 비용으로 추정된다. Oracle 내부는 RC5 암호화 회로가 순차적으로 2번 동작한다. 따라서 <표 1>에서 큐비트 수를 제외한 모든 메트릭의 × 2가 한 번의 Oracle에 대한 비용이고 Oracle은 약 2^{64}번 반복된다. 최종적으로 Grover 해킹 비용은 <표 1> × 2 × 2^{64}로 추정되며 <표 2>와 같다.

<표 2> RC5에 대한 Grover 공격 비용 및 보안 강도 평가

Cipher	Total gates	Total depth	Cost	Security
RC5	1.021×2^{84}	1.535×2^{82}	1.567×2^{166}	Not achieved ($2^{166} < 2^{170}$)

NIST는 Grover 공격 비용을 총 게이트 수 × 총 depth로 추정한다. 동일한 방식을 따르면, RC5는 1.567×2^{166}의 비용이 추정되며, AES-128에 대한 공격 비용인 2^{170}보다 낮은 비용이 요구되기 때문에 양자 후 보안 강도 Level 1을 달성하지 못한다.

5. 결론

본 논문에서는 블록암호 RC5에 대한 Grover 알고리즘을 사용한 양자 암호 분석을 수행하였다. Grover 알고리즘의 공격 비용을 감소시키기 위해 Oracle에 자리하는 RC5 암호화 양자 회로를 최적화 구현하였다. 추정된 Grover 공격 비용에 따라 RC5의 양자 후 보안 강도를 평가한 결과, RC5는 128-bit 키 크기에 따른 적정 양자 후 보안 강도 Level 1을 달성하지 못함을 확인하였다.

6. Acknowledgements

This work was partly supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00264, Research on Blockchain Security Technology for IoT Services, 25%) and 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, 50%) 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 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.

[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] Rivest, Ronald L. "The RC5 encryption algorithm." Fast Software Encryption: Second International Workshop Leuven, Belgium, December 14-16, 1994 Proceedings. Berlin, Heidelberg: Springer Berlin Heidelberg, 2005.

[4] NIST, “Submission requirements and evaluation criteria for the post-quantum cryptography standardization process,”, 2016.

[5] Cuccaro, Steven A., et al. "A new quantum ripple-carry addition circuit." arXiv preprint quant-ph/0410184 (2004).