Simon 기반 알고리즘을 활용한 키 복구 공격 사례 연구

양유진[1], 장경배[1], 임세진[1], 윤세영[1], 서화정[1]
[1]한성대학교 IT융합공학과
yujin.yang34@gmail.com, starj1023@gmail.com, dlatpwls834@gmail.com,
sebbang99@gmail.com, hwajeong84@gmail.com

Key Recovery Attak Case Study Using Simon-Based Algorithm

Yu-Jin Yang[1], Kyung-Bae Jang[1], Se-jin Lim[1],
Se-Young Yoon[1], Hwa-jeong Seo[1]
[1]Dept. of IT Convergence, Han-Sung University

요 약

양자 컴퓨터의 발전과 양자 알고리즘의 등장이 암호 시스템의 위협을 야기함에 따라 양자 알고리즘을 활용하여 기존 암호의 공격 비용을 추정하는 연구가 꾸준히 증가하고 있다. 대칭키 암호에 자주 사용되던 Grover 알고리즘이 가진 단순 양자 완전 탐색의 한계를 보완하기 위하여 최근 Simon 기반의 알고리즘 관련 연구가 등장하였다. 본 논문에서는 두 가지 Simon 기반 알고리즘과 해당 알고리즘을 적용하여 단순한 구조의 암호 키를 복구한 사례에 대해 살펴본다.

1. 서론

양자 컴퓨터의 발전과 Grover, Shor, Simon과 같은 양자 알고리즘의 등장은 기존 암호의 보안에 위협이 될 수 있다. 이에 양자 알고리즘들을 암호에 적용하여 공격 비용을 추정하는 연구가 꾸준히 증가하고 있다. 대칭키 암호에 Grover 알고리즘을 적용하는 사례가 가장 대표적이었는데, 단순 양자 완전 탐색의 한계에 따라 Simon 알고리즘을 비용 추정을 위한 공격에 사용하는 연구가 제안되고 있다. 기존의 Simon 알고리즘의 한계를 보완하기 위하여 Simon 기반의 다양한 알고리즘이 등장하였고 이를 단순한 암호 구조에 실험한 연구들이 등장하였다[1,2,3,4]. 본 논문에서는 두 가지 Simon 기반 알고리즘에 대해 살펴본 후, 해당 알고리즘들을 적용하여 단순한 구조의 암호들의 키를 복구한 사례에 대해 알아본다.

2. 관련연구

2.1 qRAM과 Oracle

양자 정보 저장과 관련이 깊은 qRAM(Quantum Random Access Memory)은 고전 컴퓨터의 RAM처럼 이전에 저장된 양자 정보를 검색할 수 있고 양자 계산 이후에 저장된 정보를 업데이트할 수 있다. 양자 컴퓨터의 개발에 필수적인 요소로 난제를 풀 때 상당히 중요하다[5].

양자 오라클은 단일 연산자로 가역성을 보장한다. Grover, Shor, Simon과 같은 많은 양자 알고리즘 모두 이 오라클 접근이 필요하다. 만약 양자 알고리즘의 오라클 호출이 없을 경우 qRAM이 필요 없다.

2.2 Simon 알고리즘

Simon 알고리즘은 모두 $x \in \{0,1\}^n$인 입력에 대해 $f(x) = f(x \oplus s)$를 만족하는 함수 $f : \{0,1\}^n \rightarrow \{0,1\}^n$의 $s \in \{0,1\}^n$를 찾는 문제인 Simon 문제를 기하급수적인 속도로 풀 수 있게 만들어주는 알고리즘이다[6]. 고전적인 방법으로는 s를 찾기 위해 빅오메가($2^{n/2}$) 쿼리가 발생하지만, Simon 알고리즘을 적용하면 빅오(n) 중첩쿼리만 필요하다. 암호의 비밀 정보를 복구하기 위하여 비트 문자열 입력이 있는 두 함수 간의 숨겨진 이동을 찾아야 하는 작업, 구성 모드에 대한 공격에 많이 사용되었다[1].

2.3 양자 일반 공격 모델

공격자의 능력이 다르다고 가정하였을 때 양자 일반 공격 모델은 Q1과 Q2로 분류할 수 있다. Q1 모델은 공격자가 오프라인 계산을 수행하기 위해 양자 컴퓨터에 접근이 가능하나 고전적인 방식으로만 온라인 쿼리를 수행할 수 있는 경우이다. 공격에 사용될

양자 알고리즘이 매우 제한적이며 Grover 알고리즘을 사용한 단순 양자 완전 탐색 등이 이에 해당한다. 2차적인 속도 향상을 허용하지 않으며 막대한 양자 하드웨어 요구 사항을 충족해야 한다.

Q2 모델은 Q1 모델과 달리 오프라인 양자 계산 외에도 양자 암호화 오라클에 중첩 쿼리 수행이 가능하다. 낮은 비용으로 일부 공격 생성이 가능하기에 simon 알고리즘을 사용하여 공격하며 매우 낮은 복잡성을 달성할 수 있다. 그러나 많은 양의 양자 메모리를 사용해야 하기에 양자 메모리가 더 작은 Q1 모델 공격이 보다 현실적인 공격이라 볼 수 있다[1].

3. 오프라인 Simon 알고리즘

우선, 오프라인 Simon 문제는 $s \in 0,1^n$, $c \in 0,1^n$이고 $f: 0,1^k \times 0,1^n \rightarrow 0,1^m$이고 $E: 0,1^n \rightarrow 0,1^m$인 함수 2개가 있고 $E(x) = f(i_0, x \oplus s) \oplus c$를 충족하는 고유한 $i_0 \in 0,1^k$가 존재할 때, i_0와 s를 찾는 문제이다. 해당 문제를 풀면 함수 $E(x) \oplus f(i_0, x)$가 주기 s를 가지기 때문에 주기 함수를 찾는 문제로 축소된다. 여기서 주어진 함수 $E(x)$는 블록 암호와 같이 고전적으로만 쿼리할 수 있는 비밀 함수이고, $f(x)$는 양자적으로 계산이 가능한 함수이다.

오프라인 Simon 알고리즘은 양자 쿼리를 재사용하여 E에 대한 양자 쿼리 수를 지수에서 다항식으로 줄일 수 있다. 또한 $E(x)$의 모든 값을 알고 있는 경우 중첩 쿼리 계산이 QRAM쿼리를 기존 값으로 만드는 것과 같으므로 양자 상태를 계산할 때, 고전 쿼리를 사용할 수 있다[1].

논문[3]에서는 Simon 알고리즘과 오프라인 Simon 알고리즘을 사용하여 Even-Mansour 암호와 FX 구조의 암호를 공격하였다.

3.1 Even-Mansour 구조의 키 복구

Even-Mansour 스킴은 하나의 치환 함수 $P(x)$와 2개의 n-bit 비밀키 k_1, k_2로 이뤄진 매우 간단한 블록암호이다. 함수로는 $E_{k_1,k_2}(x) = P(x \oplus k_1) \oplus k_2$로 표현할 수 있다[7].

Even-Mansour 스킴은 충돌을 찾아 공격할 수 있고, 모든 오라클에 양자 액세스 권한을 부여하는 완전한 양자 공격에 안전하지 않다. Even-Mansour 암호화를 2^d 쿼리했다고 가정하면, 모든 σ에 대해 스킴 함수 양변에 $P(x \oplus \sigma)$를 XOR한 형식을 계산할 수 있다. 만약 목록에 $x \oplus y \oplus \sigma = k_1$를 만족하는 메시지 x, y가 포함된 경우, XOR의 성질을 이용하여 $P(x \oplus \sigma)$를 $P(y \oplus k_1)$로 바꿀 수 있고 역으로 $P(y \oplus \sigma) = P(x \oplus k_1)$도 만족할 수 있다. 그 결과 충돌이 존재하게 되는 것이다.

Simon 알고리즘을 사용할 경우, 양자 쿼리로 주기 k_1을 가진 함수 $E_{k_1,k_2}(x) \oplus P(x) = P(x) \oplus P(x \oplus k_1) \oplus k_2$에 접근하여 pre-whitening key k_1을 다항시간 내에 복구할 수 있고, post-whitening key k_2도 금방 복구할 수 있다.

2^n개의 고전 쿼리를 필요로 하기에 공격을 직접 적용할 수가 없지만 암호입력을 $(n-u)$bit로 고정하면 주기적인 함수를 얻을 수 있기에 공격 적용이 가능하다. $(n-u)$bit로 고정하여 얻은 주기함수는 $E_{k_1,k_2}(x \| 0^{n-u}) \oplus P(x \| y) = P(x \| y) \oplus P(x \oplus k_1^1 \| k_1^2) \oplus k_2$이다. 해당 주기함수에서 k_1^1은 k_1의 처음 $(n-u)$bit이고, k_1^2는 마지막 u-bit를 의미한다. 이 함수에 고전 쿼리 공격에 적용할 수 있는 오프라인 Simon 알고리즘을 적용하면 $O(2^u)$의 고전 쿼리 비용과 $O(\max(2^u, 2^{(n-u)/2}))$ 양자 시간에 키를 복구 할 수 있다.

3.2 FX 구조의 키 복구

FX 구조는 블록 암호의 키 길이를 확장할 수 있는 간단한 방법이다. 함수는 $FX_{K_1,K,K_2}(x) = E_K(x \oplus K_1) \oplus K_2$이다. FX구조의 양자 공격은 키를 알 경우 Even-Mansour 구조로 축소될 수 있다. FX 함수에서 $i = K$인 경우에만, 주기 K_1을 가지기 때문에 양자 쿼리를 적용할 수 있다. $|K| = k$인 경우 Grover 알고리즘과 Simon 알고리즘을 조합한 Grover-meets-Simon 알고리즘을 적용할 수 있고, $O(2^{k/2})$시간 내에 K와 K_1를 복구할 수 있다.

FX 구조의 주기함수는 오프라인 Simon 문제의 구조와 잘 맞기 때문에 오프라인 Simon 알고리즘을 적용이 가능하다. FX 구조의 k-bit 키에 n-bit의 블록 암호에 오프라인 Simon 알고리즘을 적용하면 2^n개의 고전 쿼리와 $O(\max(2^n, 2^{k/2}))$시간에 공격을 성공할 수 있다.

4. 결론

본 논문에서는 Simon 알고리즘과 발전된 오프라인 Simon 알고리즘에 대해 살펴본 후, 간단한 암호 구조인 Even-Mansour와 FX구조에 Simon 기반의 알고리즘을 적용하여 키를 복구하는 공격을 수행하는

연구에 대해 살펴보았다. 앞으로 다양한 암호들에 소개한 Simon 기반 알고리즘을 적용한 연구와 Simon 알고리즘을 발전시킨 방향의 알고리즘이 계속 제안될 것으로 예상된다.

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] Bonnetain, Xavier, et al. "Quantum attacks without superposition queries: the offline Simon's algorithm." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2019.

[2] Canale, Federico, Gregor Leander, and Lukas Stennes. "Simon's Algorithm and Symmetric Crypto: Generalizations and Automatized Applications." Cryptology ePrint Archive (2022).

[3] Bonnetain, Xavier, and Samuel Jaques. "Quantum period finding against symmetric primitives in practice." arXiv preprint arXiv:2011.07022 (2020).

[4] Bonnetain, X. (2021, October). Tight bounds for Simon's algorithm. In International Conference on Cryptology and Information Security in Latin America (pp. 3-23). Springer, Cham.

[5] Green, A., & Kaplitz, E. (2019). Quantum Random Access Memory.

[6] Vazirani, Umesh, "On the power of quantum computation," Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 356.1743 : 1759-1768

[7] Kim, HongTae. "Simplification on Even-Mansour Scheme Attacks," KOCOSA 16,7(2016):85-91.