차세대 보안을 위한 양자 암호 통신에서 쇼어 알고리즘 공격 강도에 따른 단일 및 이중 QKD 시스템의 방어 성능 비교

심소원, 장용훈, 이욱진, 이상현

고려대학교

lenashim0802@korea.ac.kr, disclose@korea.ac.kr, mekdugi@korea.ac.kr, sanghyunlee@korea.ac.kr

A Comparative Study of Single and Dual QKD Systems under Varying Shor's Algorithm Attack Strengths for Next-Generation Secure Communications

Sowon Shim, Yong Hun Jang, Wookjin Lee, Sang Hyun Lee

Korea University

요 약

양자 컴퓨터의 발전으로 인해 기존 RSA 기반 공개키 암호 체계는 심각한 위협에 직면하고 있다. 특히 쇼어 알고리즘은 소인수분해 문제를 효율적으로 해결할 수 있어, 현재의 보안 시스템을 무력화할 수 있는 강력한 '창'으로 작용한다. 이에 대한 대응책으로 물리적 보안을 제공하는 양자 키 분배(QKD)가 '방패'로서 주목받고 있으나, 공격자의 연산 및 측정 능력이 충분히 발달한 경우 QKD의 오류 감지 메커니즘이 작동하기 전에 키가 노출될 가능성이 존재함을 가정한다. 이를 검증하기 위해, Python 환경에서 쇼어 알고리즘의 연산 능력을 공격 강도로 설정하여 QKD 시스템에 대한 도청 시뮬레이션을 수행하였다. 실험 결과, 단일 QKD 시스템은 특정 공격 강도 구간에서 오류 감지 없이 키가 탈취되는 '무감지 해킹' 현상이 발생한다. 이를 극복하기 위해 본 연구는 서로 다른 두 개의 경로를 활용하는 XOR 연산 기반의 독립적 채널 구성을 통한 'Dual QKD' 시스템을 제안한다.

Ⅰ. 서 론

현대 정보 보안 체계는 소인수분해의 계산 복잡도를 이용하는 RSA와 같은 공개키 암호 알고리즘에 의존하고 있다 [1].그러나 양자 컴퓨팅 기술의 비약적인 발전은 이러한 암호 체계의 근본적인 안전성을 위협하고 있다. 특히 쇼어 알고리즘은 대규모 정수의 소인수분해를 다항 시간 내에 수행할 수 있어, 기존의 고전적 컴퓨팅 환경에서는 사실상 안전하다고 여겨졌던 암호 체계를 무력화할 '창'으로 비유될 수 있다 [2]. 이에 대한 대응책으로, 물리적 법칙에 기반한 보안 기술인 양자 키 분배(Quantum Key Distribution)가 주목받고 있다 [3]. QKD는 양자 상태의 비복제 특성으로 암호 키를 안전하게 나누는 방법으로, 기존 암호 시스템의 계산 복잡성 의존에서 벗어나 안전성을 확보한다 [4]. QKD는 도청 시도가 있을 때 양자 비트 오류율이 상승하는 것을 감지하여 통신을 차단한다. 그러나 공격자의 측정 기술과 계산 자원이 극도로 발달한 상황에서는, QKD의 오류 감지 메커니즘이 항상 충분히 빠르게 작동하는지에 대해 검토한다. 특히 공격자가 QBER이 임계치인 11%에 도달하기 전에 키 복원을 완료할 가능성을 고려한다. 본 연구는 쇼어 알고리즘의 연산 능력을 공격 강도로 설정하고, 공격 강도가 증가함에 따라 QKD 시스템이 어떻게 반응하는지를 확률적 시뮬레이션을 통해 분석한다. 또한, 단일 QKD 시스템이 특정 조건에서 방어 한계에 도달할 경우를 대비하여, 이를 보완할 수 있는 이중 QKD 구조를 제안하고 그 유효성을 실험적으로 검증한다.

Ⅱ. 시스템 모형 및 실험 설정

Google Colab 환경에서 실험을 구성하여 공격 강도별로 100회 시행을 반복하여 실험하였다.

- 공격자(창) 설정: 쇼어 알고리즘 기반 모형

공격자 Eve의 능력을 나타내는 변수 S를 0부터 10까지 설정하였다. S는 양자 컴퓨터의 연산 처리 속도와 도청 시도의 적극성을 복합적으로 나타낸다. S가 증가할수록 공격자가 암호 키가 갱신되기 전에 이를 해독할 확률이 증가하도록 모델링하였다. 공격자가 연산 속도를 높이기 위해서는 양자 상태에 대해 더 빈번한 측정을 수행해야 하므로, S에 비례하여 선형적으로 QBER(Quantum Bit Error Rate)이 상승한다고 설정했다.

- 방어자(방패) 설정: QKD 프로토콜

방어 측 시스템으로는 BB84 프로토콜을 기반으로 하는 QKD 시스템을 모델링하였다. QKD의 보안 상태를 판단하기 위해 QBER을 고려하였다. 통상적으로 QBER이 11%를 초과하면 도청이 발생한 것으로 간주되며, 이 경우 시스템은 보안 위협을 감지하고 통신을 즉시 중단한다. 각 실험 시행의 결과는 다음의 세 가지 중 하나로 분류된다.

- 성공: 공격자의 연산 능력이 부족하여 해독에 실패함
- 차단: 해독 여부와 관계없이 QBER이 보안 임계치인 11%를 초과하여 시스템이 통신을 강제 종료함
- 뚫림: 공격자가 암호 키를 해독했음에도 불구하고, QBER이 11% 미만으로 유지되어 시스템이 이를 감지하지 못함

단일 QKD의 한계를 극복하기 위해 제안하는 이중 QKD는 두 개의 독립된 양자 채널(A, B)을 사용한다. 최종 암호 키는 두 채널의 키를 XOR 연산하여 생성된다. 공격자는 A의 키와 B의 키를 동시에 완벽하게 해독해야만 최종 암호 키를 얻을 수 있으며 두 채널 중 하나라도 QBER이 임계치를 넘으면 통신은 차단된다.

본 연구에서는 고정된 예측값이나 상수를 사용하는 결정론적 접근 대신, 매 시행마다 확률적으로 결과를 도출하는 통계적 접근 방식을 채택하였다. 구체적인 실험 절차는 다음과 같다. Alice가 총 1,000개의 광자를 전송하면, Eve는 공격 강도 S에 비례하는 확률로 각 광자에 대한 도청 여부를 결정한다. 이 과정은 이항 분포를 따르는 확률적 사건으로 모델링된다. Eve가 도청한 광자들에 대해서는 25%의 물리적 오류 확률을 적용하여 실제 오류 발생 개수를 계산하고, 이를 전체 광자 수로 나누어 해당 시행의 실측 QBER을 산출한다. 또한 Eve가 획득한 정보량에 비례

하여 암호 키 해독 성공 여부를 확률적으로 판정한다.

Ⅲ. 실험 결과 및 분석

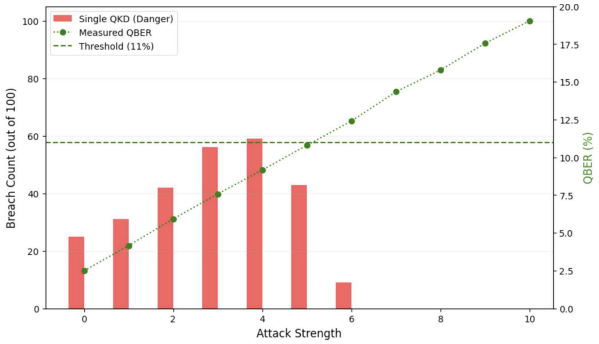

그림1 해킹 성공 횟수와 평균 실측 QBER의 관계

그림1은 단일 QKD 채널에 대해 100회 공격을 수행했을 때 해킹 성공 횟수와 평균 실측 QBER을 나타낸다. 실험 결과, 공격 강도 0~3구간에서 보안 공백이 발견되었다. S=3일 때, 실측 QBER은 약 10%로 임계치(11%)를 넘지 않아 차단 시스템이 작동하지 않았다. 이는 사용자가 공격을 인지하지 못한 채 정보를 지속적으로 탈취당하는 '무감지 해킹' 상태를 의미하며, 단일 QKD만으로는 고성능 양자 컴퓨팅 공격을 방어하는 데 한계가 있음을 시사한다.

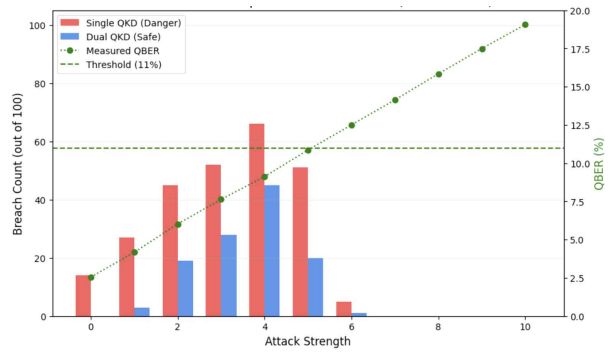

그림2 이중 QKD 시스템의 실험 결과

그림2는 동일한 공격 환경에서 두 개의 독립적인 채널과 XOR 논리를 적용한 이중 QKD 시스템의 실험 결과이다. 단일 QKD와 대비하여 다음과 같은 뚜렷한 보안 성능 향상이 관찰되었다. 단일 QKD가 쉽게 뚫리던 0~3 구간에서 이중 QKD의 해킹 성공 횟수는 현저히 감소하였다. 이는 공격자가 두개의 채널을 동시에 해독해야 하므로, 성공 확률이 급격히 감소하기 때문이다. 공격자가 두 채널을 동시에 뚫기 위해 강도를 S=7 이상으로 높일 경우, 실측 QBER이 즉시 11%를 초과하여 시스템이 차단 모드로 전환되었다. 즉, 정보가 실질적으로 유출되기 이전에 통신이 중단되어 보안성이 유지되었다.

표1 공격 강도에 따른 QKD 시스템의 평균 QBER 및 해킹 성공 확률

공격 강도(S)	평균QBER(%)	단일 QKD (%)	이중 QKD (%)
0	2.49	25	9
1	4.16	31	10
2	5.92	42	19
3	7.58	56	25
4	9.17	69	44
5	10.08	43	18
6	12.41	9	1
7	14.34	0	0
8	15.79	0	0
9	17.56	0	0
10	19.05	0	0

표1은 강도별 실험결과를 요약한 것이다. 가장 위험한 공격 강도인 S=4에서 단일 QKD는 69%가 뚫린 반면, 이중 QKD는 44%만이 뚫리는 데 그쳤다. 이는 이중 QKD 구조가 쇼어 알고리즘기반 공격의 실질적 위협을 감소시킬 수 있음을 실험적으로 보여준다. 이중 QKD는 두 채널 중 하나만이라도 이상 징후인 QBER 〉 11%인 상황이 발견되면 즉시 통신을 차단하므로, 공격 감지 확률이 크게 증가하고, 결과적으로 전체 시스템의 보안성이 구조적으로 강화된다.

공격자 Eve가 이중 QKD 시스템의 두 채널(A, B)을 공격할 때, 각각의 채널에 대해 동일한 공격 강도 S를 투입할 수 있다고 가정한 최악의 시나리오에 기반한다. 실험 결과는 두 채널의 해독 사건을 독립 시행으로 계산하여 도출되었다. 그러나 실제 물리적 환경에서는 공격자가 두 개의 독립된 채널을 동시에 도청하기 위해 한정된 양자 연산 자원을 분산해야 하며, 이는 각 채널에 가해지는 유효 공격 강도를 감소시키거나, 혹은 두 배 이상의 하드웨어 비용을 요구한다. 따라서, 공격자의 자원 분산 효과까지 고려한다면, 실제 환경에서 이중 QKD 시스템이 뚫릴 확률은 본 시뮬레이션에서 제시한 값보다 더욱 낮아질 것으로 판단된다. 결론적으로, 본 연구의 실험 결과는 이중 QKD의 보안성을 가장 보수적인 관점에서 측정한 것이며, 실제 적용 시에는 이보다 더욱 강력한 방어 효과를 기대할 수 있음을 시사한다.

Ⅳ. 결론

본 연구에서는 확률적 몬테카를로 시뮬레이션을 통해 쇼어 알고리즘이라는 '창'과 QKD라는 '방패'의 상호작용을 정량적으로 모사하고, 단일 QKD 구조의 한계와 이를 보완할 수 있는 대안적 구조를 제시하였다. 실험 결과, 단일 QKD 시스템은 공격자의 연산 능력이 QBER 상승에 따른 QKD의 감지 속도보다 미세하게 상회하는 특정 임계 구간에서, 오류 경보 없이 보안이 무력화되는 '무감지 해킹'에 취약함을 확인하였다.

본 연구에서 고려한 이중 QKD 구조는 XOR 논리 결합을 통해 공격자에게 '동시 해독'이라는 확률적 제약을 부과하고, 방어자에게는 '이중 감지'라는 구조적 이점을 제공한다. 그 결과, 공격 성공 확률은 확률곱 형태로 급격히 감소하며, 동시에 QBER 기반 차단 메커니즘의 작동 빈도는 증가하여 실질적인 정보 유출 가능성이 크게 줄어드는 것을 확인하였다. 결론적으로, 다가오는 양자 컴퓨팅 시대의 통신 보안은 단일 알고리즘이나 단일 채널에 의존하는 접근에서 벗어나, 다중 경로와 논리적 결합을 활용한 복합 보안 아키텍처로 진화해야 할 것이다. 이러한 방향성으로서, 이중 QKD 구조가 중요한 설계원칙을 제공할 수 있음을 보여준다.

ACKNOWLEDGMENT

본 논문은 고려대학교 차세대통신학과 진리장학 프로그램의 지원을 받아 작성되었습니다.

참 고 문 헌

[1] Sasaki, Y. (2012). Quantum Computing and number theory. Interdisciplinary Graduate School of Science and Engineering, Kinki University.

[2] 이순칠. (2004). 공개키 암호 체계와 Shor 알고리듬. 정보보호학회지, 14(3), 1-7.

[3] Nielsen, M. A., & Chuang, I. L. (2010). Quantum computation and quantum information: 10th anniversary edition. Cambridge University Press.

[4] 이종민, 심동희, 차대준, 윤민근, 나민수, 최회영. (2019-06-19). 양자키 분배 기술 및 통신망 활용 개요. 한국통신학회 학술대회논문집.