Cascade 단계에서 고전 채널 오류 발생에 대한 영향 분석

김응준, 최정규, 류중곤, 신유철
㈜ 큐심플러스

{ej_kim, jk_choi, jg_ryu, yc_shin}@qsimplus.com

Impact Analysis of Existing Classic Channel Errors in the Cascade Protocol

Eungjun Kim, Jeongkyu Choi, Joonggon Ryu and Youchul Shin
QSIMPLUS Co., Ltd.

요 약

본 논문은 양자 키 분배의 후처리 단계에서 오류 정정 과정을 진행할 때 활용되는 프로토콜 중 하나인 Cascade 에 대하여, 고전 채널에서 발생하는 송, 수신 간 오류에 대한 영향 분석을 목표로 한다. 본 논문에서 사용된 Cascade 는 한국정보통신기술협회에서 제정한 표준 문서인 TTAK.KO-12.0406 을 참고하여 구현을 진행하였고, 송, 수신 간 오류에 대해 확인하기 위해 송신자가 전송하는 데이터에 변화를 주어 측정을 진행하였다.

Ⅰ. 서 론

Cascade 프로토콜은 양자 키 분배(Quantum Key Distribution, QKD)의 후처리(Post-Processing) 과정 중 오류 정정 단계에서 사용되는 대표적인 프로토콜 중 하나로, 송신자와 수신자가 이진 탐색 알고리즘(Binary Search Algorithm)을 기반으로 고전 채널에서 상호 간 데이터 교환을 통해 최종적으로 동일한 키를 획득하는 것을 목표로 하고 있다. 동일한 키의 획득을 위해서는 각 비트에 대한 정확한 송, 수신 과정이 필수적이며, 이는 키의 보안성을 확보하는 데 핵심적인 역할을 한다.

본 논문에서는 Cascade 의 상호 간 데이터 교환 시, 송신자가 전송하는 데이터인 Parity bit 에 오류 비트(Error bit)를 반영하는 방식으로 다양한 오류 환경을 구성하였고, 이에 따른 성능 변화에 대한 분석을 위해 무작위로 추출된 난수를 이용하는 몬테카를로 시뮬레이션(Mante-Carlo Simulation)을 통해 진행하였다.

Ⅱ. 본론

본 논문에서 사용된 Cascade 프로그램은 TTAK.KO-12.0406 표준 문서[1]에서 제시하는 그림 1 의 Cascade 프로토콜 절차도를 참고하여 구현하였으며, Original Cascade 에서 제안하는 최적의 초기 블록 크기 값인 Ceil(0.73/QBER)을 적용하였고, 반복 횟수는 최적 값으로 제안하는 4 회로 설정하였다.[2] 패리티 계산 단계에서는 전체 키를 여러 블록으로 분할한 후, 각 블록의 패리티를 생성하여 고전 채널을 통해 수신자에게 전송하고, 이진 탐색 단계에서는 수신자가 수신된 패리티 정보를 기반으로 오류 위치 정보를 추정한 뒤 송신자에게 전달하여 오류 수정 절차를 진행한다. 일치성 검사 단계에서 key 를 대체하는 값을 비교하여 일치 여부를 판단하지만, 본 논문에서는 보다 정확한 성능 평가를 위해 송, 수신자의 키를 비트 단위(Bit-by-Bit)로 비교하여 진행하였다. 이때, 1bit 라도 일치하지 않는다면 해당 키는 폐기 처리하였다.

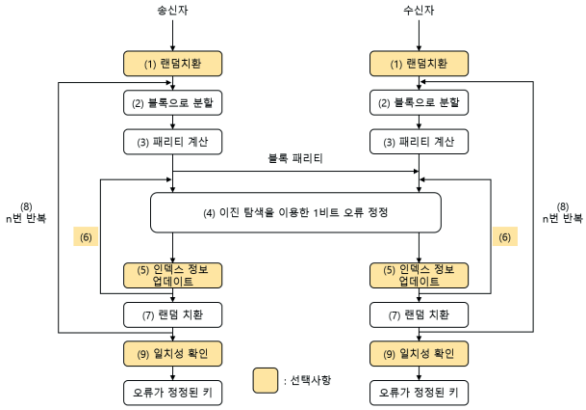

그림 1. Cascade 프로토콜 절차도 [1]

위 과정을 기반으로 폐기된 키의 개수(Frame Error Rete, FER)를 측정하였고, 송신자의 Parity bit 가 정확하게 송신되지 않은 상황에서의 성능 변화를 확인하기 위해 정상적인 상황에서의 성능 측정을 진행한 뒤, 두 결과를 비교하는 방식으로 진행하였다.

시뮬레이션은 총 10,000,000 회로 수행되었으며, 다양한 오류 조건에서 FER 을 측정하였다. 키의 길이가 1,000bit 일 경우에는 0.1% 및 1%의 오류 비트를 삽입하였고, 키의 길이가 10,000bit 일 경우에는 0.01% 및 0.1%의 오류 비트를 삽입하여 측정을 진행하였다.

파라미터 명	파라미터 값
Simulation Repeat Count	10,000,000 회
Key Size	1,000, 10,000 Bit
Initial Block Size	Ceil(0.73 / QBER)
Pass 별 Block size 증가량	이전 블록 크기의 2 배
QBER	1~11 %
Pass (cascade 반복 횟수)	4
Trace Back	ON

표 1. 시뮬레이션 환경 파라미터

표 1 은 시뮬레이션 상황에서 사용된 파라미터들을 정리한 것이다.

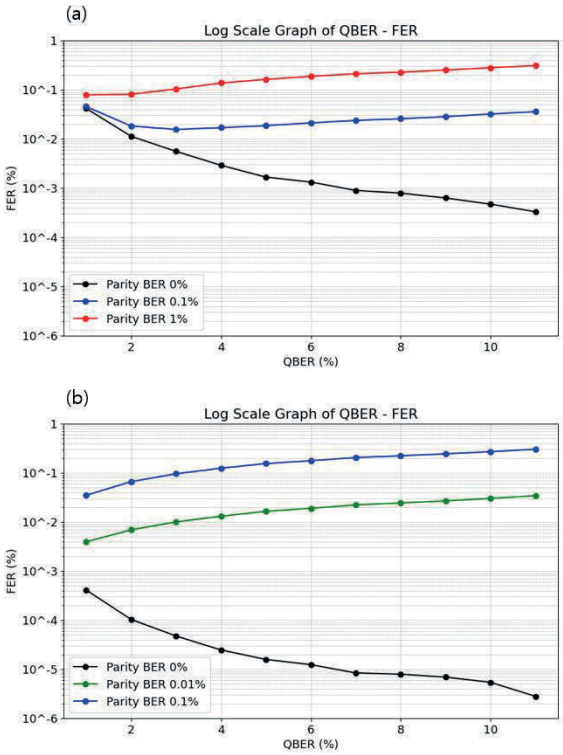

그림 2. QBER 에 따른 FER, (a) 1,000bit, (b) 10,000bit

그림 2 는 QBER 이 증가할 때 FER 변화의 양상을 나타낸 것이다. 오류가 존재하지 않는 경우(Parity BER 0%), QBER 에 따라 FER 이 점진적으로 감소하는 경향을 보인다. 이는 QBER 이 커질수록 초기 블록의 크기가 작아지며, 그에 따라 오류 정정의 효율성이 향상되어 FER 측면에서 성능이 개선되는 것으로 해석할 수 있다. 반면, 송신자의 패리티 비트에 0.1%의 오류 비트가 존재하는 경우(Parity BER 0.1%), QBER 3%를 초과한 이후부터 FER 이 점차 증가하는 현상이 나타난다. 이 경우 약 8 배에서 최대 110 배까지 증가한 것으로 나타났다. 나아가, 패리티 비트에 1%의 오류가 존재할 경우에는, QBER 전 구간에 걸쳐 FER 이 증가하였으며, 이 경우에는 약 1.89 배에서 최대 940 배까지 증가한 것으로 나타났다.

그림 3 은 그림 2 와 동일한 조건에서 키의 길이를 증가시켜 측정한 결과를 나타낸다. 오류 비트가 존재하지 않는 경우, 그림 2 와 마찬가지로 QBER 증가에 따라 FER 이 점진적으로 감소하는 경향을 나타낸다. 그러나 패리티 비트의 0.01%의 오류가 삽입된 경우, 오류가 없는 조건에 비해 FER 성능이 약 10 배에서 최대 1,000 배까지 저하되었으며, 0.1%의 오류가 존재하는 경우에는 약 87.5 배에서 최대 100,000 배까지 증가하는 등 성능 저하가 더욱 뚜렷하게 나타났다. 즉, 고전 채널에서의 오류가 조금이라도 발생하는 경우, FER 성능에 큰 영향이 나타난다.

Ⅲ. 결론

기존의 Cascade 프로토콜에서는 주로 이진 탐색, 패리티 계산, 그리고 오류 위치 정보의 정확한 생성에 초점이 맞춰져 왔다. 그러나 본 측정 결과와 같이, 패리티 비트에 소량의 오류가 삽입된 경우에도 정상적인 패리티를 전송할 때 대비 약 1.89 배에서 최대 100,000 배까지 FER 이 증가하는 현상이 관찰되었으며, 패리티 비트의 신뢰성이 Cascade 프로토콜 전반의 성능에 중대한 영향을 미칠 수 있음을 시사한다. 따라서 향후 Cascade 프로토콜의 성능 평가에 있어 다양한 관점에서의 접근이 필요하며, 경우에는 고전 채널에서의 오류를 고려하는 오류 정정 부호의 도입이 요구될 수 있을 것으로 기대된다.

ACKNOWLEDGMENT

본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학 ICT 연구센터육성지원사업[IITP-2025-2021-0-01810]과 정부(과학기술정보통신부)의 재원으로 한국 연구재단(No. RS-2023-00242396)의 지원을 받아 수행된 연구임

참 고 문 헌

[1] Gilles Brassard and Louis Salvail. Secret-key reconciliation by public discussion. In Advances in Cryptology - EUROCRYPT '93, Workshop on the Theory and Application of Cryptographic Techniques, volume 765 of Lecture Notes in Computer Science, pages 410-423. Springer Berlin Heidelberg, 1994.

[2] Telecommunications Technology Association (TTA),"Security Requirements and Test Methods for Post Processing of Quantum Key Distribution" *TTA Standard TTAK.KO-12.0406*, pp. 1-2, 18-19. Jun. 2024.