Cascade 프로토콜의 오류정정 확률 분석

원희정[1], 류지은[1], 안진우[2], 강주성[1]*, 염용진[1]
국민대학교[1] / ㈜에잇바이트[2]
{hiijng1220, ofryuji, jskang*, salt}@kookmin.ac.kr, jinwoo.an@8byte.co.kr

Probability Analysis of the Cascade Error Correction Protocol

Heejeong Won[1], Jieun Ryu[1], Jinwoo An[2], Ju-Sung Kang[1]*, Yongjin Yeom[1]
Kookmin University[1], 8BYTE,INC.[2]

요 약

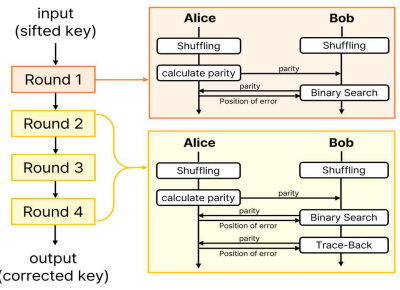
본 논문은 대표적인 QKD 오류정정 프로토콜 중 하나인 Cascade 프로토콜의 변형 프로토콜에 대한 확률적 분석을 수행한다. 변형 프로토콜을 대상으로 1, 2라운드에서 정정되는 오류 개수의 기댓값을 확률 계산을 통해 도출하고, 시뮬레이션한 결과를 실제 QKD 장치로 실험한 결과와 비교하여 확률 모델의 타당성을 검증한다. 기존 Cascade와 달리 변형 프로토콜은 엄밀한 확률 분석이 가능하며, 실제 QKD 환경에서 변형 프로토콜은 Cascade와 유사한 성능을 갖기 때문에 현실적으로 사용할 수 있을 것으로 예상된다.

Ⅰ. 서 론

양자 키 분배(Quantum Key Distribution, 이하 QKD)는 정보 이론적으로 안전한 비밀키를 공유하는 기술이다. QKD의 실용화를 위해 송수신자가 양자 채널을 통해 공유한 원시 키를 조정하고 가공하는 과정인 후처리 과정이 필수적이며, 이 중 오류정정 프로토콜은 양자 채널의 여러 요인으로 인해 발생하는 비트 불일치를 제거하는 핵심 과정이다[1]. 본 논문은 대표적인 QKD 오류정정 프로토콜인 Cascade 프로토콜의 성능 향상을 위해 제안된 변형 Cascade 프로토콜을 대상으로 확률적 분석을 수행한다. 기존의 Cascade 프로토콜의 오류정정률은 근사적 접근으로 계산되었다. 본 연구에서는 변형 프로토콜에 대한 정확한 확률 계산을 통해 1, 2라운드에서 정정되는 오류 개수의 기댓값을 유도하는 확률 모델을 제시한다. 또한 이를 시뮬레이션 결과와 실제 QKD 장치에서의 실험 결과를 비교함으로써 확률 모델의 타당성을 확인한다.

Ⅱ. Cascade 오류정정 프로토콜

QKD 시스템에서는 양자 채널의 잡음 및 측정 오차 등의 영향으로 송신자와 수신자 간 공유된 원시 키 내의 비트 불일치가 발생한다. 동일한 위치에서 일치하지 않는 비트를 오류비트라고 하며, 해당 오류비트들은 QKD 후처리 과정 중 오류정정 프로토콜을 통해 제거한다. Cascade 프로토콜은 1993년 Brassard와 Salvail에 의해 제안된 QKD 오류정정 프로토콜로, [그림 1]과 같이 인증된 공개 채널에서 송수신자의 패리티 교환과 이진 탐색을 기반으로 키 내부의 오류를 정정한다[2].



[그림 1] Cascade 오류정정 프로토콜

Ⅲ. Cascade 변형 프로토콜에 대한 확률적 분석

저자들은 Cascade 오류정정 프로토콜의 성능 저하 요인 중 하나인 통신량을 감소시키는 것을 목표로 TraceBack2First라는 이름의 변형된 Cascade 오류정정 프로토콜을 제안했다[3]. 기존 Cascade의 Trace-Back 알고리즘은 이전 모든 라운드에 대해 백트래킹을 수행하며 추가적인 오류를 정정하는 반면, 본 연구의 대상인 변형 프로토콜은 백트래킹 대상을 첫 번째 라운드로만 제한한다. 변형 프로토콜의 구체적인 동작 과정은 선행 연구에서 제시되었으므로, 본 장에서는 확률적 분석에 집중한다.

ⅰ. Notation

본 논문에서 사용하는 변수 및 표기법에 대해 다음과 같이 정의한다.

r	라운드의 반복 횟수 ($r=1,2,3,4$)
N	전체 키 길이
k_r	r라운드의 블록 크기
n_r	r라운드의 블록 개수
p_r	r라운드의 비트당 오류율
$p_{odd}^{(r)}$	r라운드 진입 시 한 블록에 홀수 개의 오류가 존재할 확률 $\left(p_{odd}^{(r)}=\frac{1-(1-2p_r)^{k_r}}{2}\right)$
$p_{even}^{(r)}$	r라운드 진입 시 한 블록에 짝수 개의 오류가 존재할 확률 $\left(p_{even}^{(r)}=\frac{1+(1-2p_r)^{k_r}}{2}\right)$
$X_i^{(r)}$	r라운드 진입 시 i번째 블록에 홀수 개의 오류가 존재할 확률 $p_{odd}^{(r)}$을 모수로 하는 베르누이 확률변수 ($i=1,2,...,n_r$)
$Y^{(r)}$	r라운드에서 Binary Search를 통해 정정되는 오류 개수
$W^{(r)}$	r라운드에서 Trace-Back을 통해 정정되는 오류 개수

ⅱ. 변형 프로토콜에 대한 확률적 분석

1) 1라운드($r=1$):

p_1은 QKD 장치의 양자비트 오류율(Quantum Bit Error Rate)에 따라 결정되는 값으로, 1라운드 진입 시 샘플링을 통해 추정한 값을 사용한다. 추정한 p_1을 통해 k_1, n_1을 다음과 같이 설정한다.

$$k_1=\left\lfloor\frac{0.73}{p_1}\right\rfloor,\ n_1=\frac{N}{k_1}$$

1라운드 시작 시 Shuffling을 수행하여 균등하게 만든 각 오류비트의 분포는 $B(N,p_1)$을 따르며, 1라운드 오류정정 수행 전 오류 개수의 기댓값은 Np_1이다. 오류비트가 독립이므로 각 블록이 독립임을 가정하고 모든 n_1개의 블록에 대해 독립인 확률변수 $X_i^{(1)}$을 다음과 같이 정의한다.

$$X_i^{(r)}:=\begin{cases}1 & (i\text{번째 블록의 오류가 정정되는 경우})\\ 0 & (i\text{번째 블록의 오류가 정정되지 않는 경우})\end{cases}$$

Binary Search 알고리즘은 홀수 개의 오류를 갖는 블록에서 1개의 오류를 정정하므로 블록 내 1개의 오류비트가 Binary Search를 통해 정정될 확률은 $p_{odd}^{(r)}$와 같다. 이를 통해 $X_i^{(1)}$의 분포를 추정하면 다음과 같다.

$$\mathrm{P}(X_i^1 = x) = \begin{cases} p_{odd}^{(1)} & (x=1) \\ p_{even}^{(1)} & (x=0) \end{cases}$$

1라운드에서 Binary Search를 통해 정정되는 오류 개수를 확률변수 $Y^{(1)}$라고 할 때, $X_i^{(1)}$을 이용하여 이항분포를 따르는 $Y^{(1)}$의 기댓값을 구할 수 있다.

$$Y^{(1)} = X_1^1 + X_2^1 + \ldots + X_{n_1}^1 \ (Y^{(1)} = 0,1,\ldots,n_1)$$
$$Y^{(1)} \sim \mathrm{B}(n_1, p_{odd}^{(1)})$$
$$EY^{(1)} = n_1 \cdot p_{odd}^{(1)} \simeq \lfloor n_1 \cdot p_{odd}^{(1)} \rfloor = m_1$$

1라운드에서는 Binary Search만 수행하므로 1라운드에서 정정되는 오류 개수의 기댓값은 $EY^{(1)}$이며, 실제로 정정되는 오류 개수는 정수이므로 정수 m_1으로 나타낸다.

2) 2라운드($r=2$):

2라운드 진입 시 Shuffling을 수행하여 잔여 오류의 분포를 다시 균등하게 만든다. 이를 통해 각 오류비트가 독립임을 가정하고 2라운드의 파라미터를 다음과 같이 설정한다.

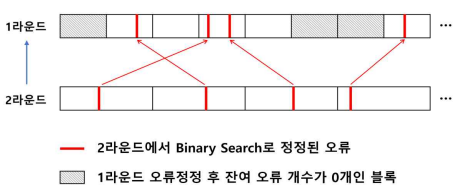
$$p_2 = \frac{Np_1 - EY^{(1)}}{N}, \ k_2 = 2k_1, \ n_2 = \frac{n_1}{2}$$

2라운드에서의 확률변수 $X_i^{(2)}$, $Y^{(2)}$의 분포와 Binary Search로 정정되는 오류 개수의 기댓값 $EY^{(2)}$는 1라운드와 동일한 방식으로 유도된다. $EY^{(2)}$은 이후 Trace-Back에 대한 분석에서 정수 m_2로 대신 사용된다.

$$X_i^{(2)} \sim \mathrm{Ber}(p_{odd}^{(2)})$$
$$Y^{(2)} \sim \mathrm{B}(n_2, p_{odd}^{(2)})$$
$$EY^{(2)} = n_2 \cdot p_{odd}^{(2)} \simeq \lfloor n_2 \cdot p_{odd}^{(2)} \rfloor = m_2$$

1라운드와 달리 2라운드부터는 Binary Search로 정정한 오류비트가 이전 라운드 블록의 패리티 정보에 영향을 미치며, Trace-Back으로 패리티가 변경된 블록의 오류를 추가 정정할 수 있다. 따라서 한 라운드에 정정되는 오류의 개수를 구할 때 Trace-Back으로 추가 정정한 오류의 개수를 계산해야 한다.

Trace-Back을 통해 정정되는 오류 개수를 확률변수 $W^{(2)}$라고 하자. $W^{(2)}$의 기댓값은 [그림 2]와 같이 n_1개의 블록 중 1라운드 수행 후 오류가 남아있지 않은 블록의 개수를 제외한 $\tilde{n_1}$개의 블록에 m_2개의 오류를 무작위로 넣을 때, 홀수 개의 오류가 존재하는 블록의 개수를 세는 것과 같다.



[그림 2] 정정된 오류비트가 이전 라운드의 블록에 영향을 주는 과정

$$\tilde{n_1} := n_1 \cdot (1 - \mathrm{P}(\text{1라운드 후 1라운드의 한 블록에 0개의 오류가 남음}))$$
$$= n_1 \cdot (1 - (\mathrm{P}(\text{1라운드 시작 전 블록 내 오류가 0개 존재}) + \mathrm{P}(\text{1라운드 시작 전 블록 내 오류가 1개 존재})))$$

라고 할 때, $EW^{(2)}$는 다음과 같이 근사된다.

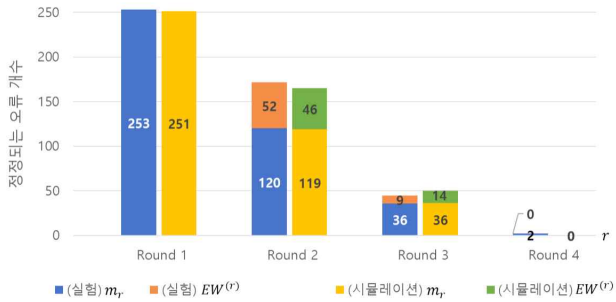
$$EW^{(2)} = \frac{\tilde{n_1}}{2} \cdot \left(1 - \left(1 - \frac{2}{\tilde{n_1}}\right)^{m_2}\right)$$

결론적으로 2라운드에서 정정되는 오류 개수의 기댓값 $EY^{(2)} + EW^{(2)}$을 도출할 수 있다. 변형 프로토콜의 Trace-Back은 백트래킹 대상을 1라운드로만 한정하므로 3, 4라운드에 대한 확률적 분석은 2라운드 과정과 유사하게 진행된다.

iii. 실험 결과

본 절에서는 앞에서 제시한 확률 모델의 시뮬레이션 결과와 실제 QKD 장치를 이용하여 실험을 수행한 결과를 비교하여 설계한 확률 모델이 타당한지 확인한다.

실험에 사용된 QKD 장치는 평균 QBER이 3% 이하인 BB84 프로토콜 기반의 프로그램을 사용한다. 장치로부터 생성한 16,384비트의 걸러진 키 174개로 구성된 데이터 세트를 입력으로 하여 오류정정 프로토콜을 수행하면서 $m_1, m_2, \lfloor EW^{(2)} \rfloor$을 측정한 후, 각 평균을 계산한다. 프로토콜 수행 후 정정된 오류의 개수가 정수이므로 비교 대상을 기댓값의 내림 값으로 사용한다. 걸러진 키 174개의 QBER의 평균값을 기준으로 확률 모델을 시뮬레이션한 결과를 실험 결과와 비교한다.



[그림 3] 라운드별 정정 오류 개수에 대한 실험 및 시뮬레이션 결과

실험에서 사용한 장치처럼 실제 환경에서 사용하는 QKD 장치의 평균 QBER이 대부분 3% 이하이고, 이 경우 변형 프로토콜은 4라운드 내에 기존 Cascade와 거의 유사한 수준으로 오류를 정정한다. 기존 Cascade 프로토콜의 Trace-Back 알고리즘에 대한 명확한 확률 계산은 불가하지만, 단순한 구조를 갖는 변형 프로토콜의 Trace-Back 알고리즘에 대해서는 명확한 확률 계산도 가능할 것으로 예상된다.

Ⅳ. 결론

본 논문에서는 변형된 Cascade 프로토콜에 대해 확률적 분석을 수행하였다. 기존에도 Cascade 프로토콜의 확률 모델에 대한 연구들이 이루어졌으나 Trace-Back 알고리즘의 복잡성으로 인해 이를 독립적으로 분석하지 못했다. 상용 QKD 환경을 고려했을 때 변형 프로토콜은 현실에서 사용할 수 있는 성능을 보이며, 이론적인 분석이 가능한 모델이라는 점에서 유의미하다. 본 연구에서는 단순한 구조의 Trace-Back 알고리즘에 대해 정확한 확률 계산이 가능함을 보였다. 향후 연구에서는 기댓값 기반의 분석을 넘어 확률변수의 분포를 정밀하게 다루는 이론적으로 심화된 확률 모델을 구축할 예정이다.

ACKNOWLEDGMENT

본 연구는 서울시 산학연 협력사업의 지원을 받아 수행된 연구임 (No. QR240013, “일대다(1:N) 구조의 양자암호통신 시스템 구축”)

참 고 문 헌

[1] Y. Luo et al., "An overview of postprocessing in quantum key distribution," Mathematics, vol. 12, no. 14, 2024.

[2] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in EUROCRYPT 1993, T. Helleseth, Ed. Berlin, Heidelberg: Springer, vol. 765, pp. 410 - 423, 1994.

[3] "An Experimental Analysis of Several Variants of CASCADE Protocol for QKD," 2025.