ARTIFICIAL INTELLIGENCE 5

박규민

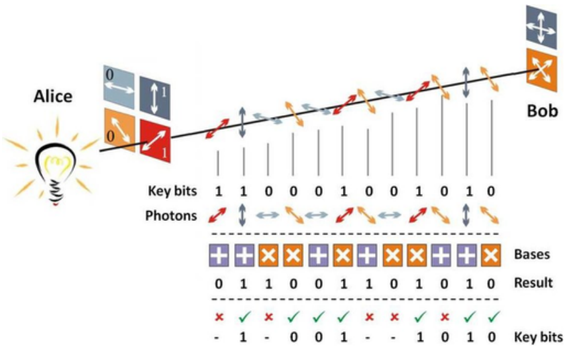
QSIM+

01. 진공 상태가 필요한 이유

QKD의 목표

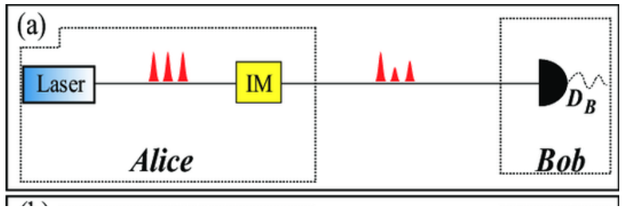
QKD의 목표

물리 법칙 기반의
무조건적인 보안 보장



디코이 상태 방법

PNS 공격 방어를 위해 μ,ν,0
세 가지 강도 사용
(k∈{μ,ν,0})



QUESTION

왜 k=0을 ν보다 작은
아주 작은 세기 k=δ>0로
대체할 수 없는가?

k=0만이 엄격한 보안을 위한 통계적 계산의 기준점을 제공
하며, δ>0는 이 기준점의 물리적 확실성을 훼손하기 때문

QSIM+

순수한 물리적 기준점

비밀 키 길이(ℓ)를 계산하려면, 실제 광자 수율(Y_1)과
순수한 배경 잡음 수율(Y_0)의 기여도를 엄격하게 분리해야 함

1. 진공 상태($k=0$)는 광자를 방출하지 않음을 보장하는 물리적 기반을 제공함.
따라서 $k=0$에서 관측된 사건은 오직 순수한 잡음만을 반영

2. $\delta>0$인 펄스는 포아송 통계상 **1개 이상의 광자를 포함**할 수 있으므로,
해당 관측값은 잡음과 광자 신호가 섞인 결과

3. 따라서, $k=0$이 아니면 Y_0와 Y_1을 엄격하게 분리할 수 없어,
QKD 보안의 핵심 매개변수 추정 과정 전체가 흔들림

관측값과 통계적 엄격성 원칙

진공 상태(k=0)는 디코이 상태 방법에서 널리 사용되며,
이와 관련된 관측된 사건 수 n_Z0는 통계적 변수 x에 해당하고 그 값이 매우 작음

1. 우리는 관측된 **x(n_Z0)**로부터 보안에 필요한 진공 사건 수의
엄격한 하한 **x*(s_Z0*)**을 추정해야 함 $\underline{x}^* = x - \frac{\beta}{2} - \sqrt{2\beta x + \frac{\beta^2}{4}}$

2. x가 매우 작을 때, **하한 x***를 계산하는 수학적 공식은 음수 결과를 도출할 위험이 가장 높음

3. x*는 물리적 사건 수이므로 음수일 수 없으므로, 계산 결과가 음수이더라도 무조건 0으로 설정되어야 함 **(x*≥0)**
이는 무조건적인 보안을 위한 보수적이고 필수적인 안전장치

4. k=0 (진공 상태)가 제공하는 가장 작은 관측값(x)을 이용하여 **x*≥0** 원칙을 엄격히 적용함으로써
성능(SKR 수율)보다 엄격한 통계적 하한을 보장하는 필수적인 물리적 기준점

최종 보안 하한 확립

최종 비밀 키 길이(ℓ)는 엄격하게 추정된 매개변수들의 하한에 의존

$$\ell = \underline{s}_0^Z + \underline{s}_1^Z \left[1 - h\left(\overline{\phi}_1^Z\right)\right] - \lambda_{\mathrm{EC}} - \log_2 \frac{2}{\varepsilon_{\mathrm{cor}}} - 6\log_2 \frac{23}{\varepsilon_{\mathrm{sec}}},$$

1. ℓ 계산에 필수적인 진공 사건 수의 하한 **s_Z0***은 오직 **k=0**에서 얻은 엄격한 **n_Z0***을 통해서만 계산됨

$$\underline{s}_0^{Z^*} \geq (e^{-\mu} p_\mu + e^{-\nu} p_\nu) \frac{p_z \underline{n}_0^{Z^*}}{p_0},$$

2. 따라서 **k=0**만이 **Y_0**에 대한 순수한 물리적 기준점과 통계적 분석에서 가장 보수적인 원칙을 강제할 수 있는 가장 작은 관측값을 제공하며, 이는 QKD의 구성 가능한 보안을 확립하는 데 절대적으로 필수

02. 성능 비교

수정 전

L = 100km

최적화된 GA 파라미터

crossover_type: single_point,
mutation_type: adaptive,
parent_selection_type: sss,
sol_per_pop: 102,
num_parents_mating: 22,
keep_parents: 21,
keep_elitism: 9,
crossover_probability: 0.650933611086074,
mutation_percent_genes: [0.5, 0.05]

최적 SKR 값: 9.883606e-06

mu(강도 파라미터): 0.879389
nu(약한 강도 파라미터): 0.181233
vac(진공 상태 파라미터): 0.136371
p_mu(mu 상태 확률): 0.013206
p_nu(nu 상태 확률): 0.911127
p_vac(진공 상태 확률): 0.094369
p_X(X 기저 확률(Alice)): 0.10079
q_X(X 기저 확률(Bob)): 0.086119

수정 후

L = 100km

최적화된 GA 파라미터

crossover_type: uniform,
mutation_type: random,
parent_selection_type: sss,
sol_per_pop: 223,
num_parents_mating: 219,
keep_parents: 216,
keep_elitism: 20,
crossover_probability: 0.4520234912146035 6,
mutation_probability: 0.018366799686118797,
K_tournament: 8

최적 SKR 값: 1.348981e-05

mu(강도 파라미터): 0.521068
nu(약한 강도 파라미터): 0.236871
vac(진공 상태 파라미터): 0.034389
p_mu(mu 상태 확률): 0.252630
p_nu(nu 상태 확률): 0.862988
p_vac(진공 상태 확률): 0.090949
p_X(X 기저 확률(Alice)): 0.163874
q_X(X 기저 확률(Bob)): 0.209120

VAC=0

L = 100km

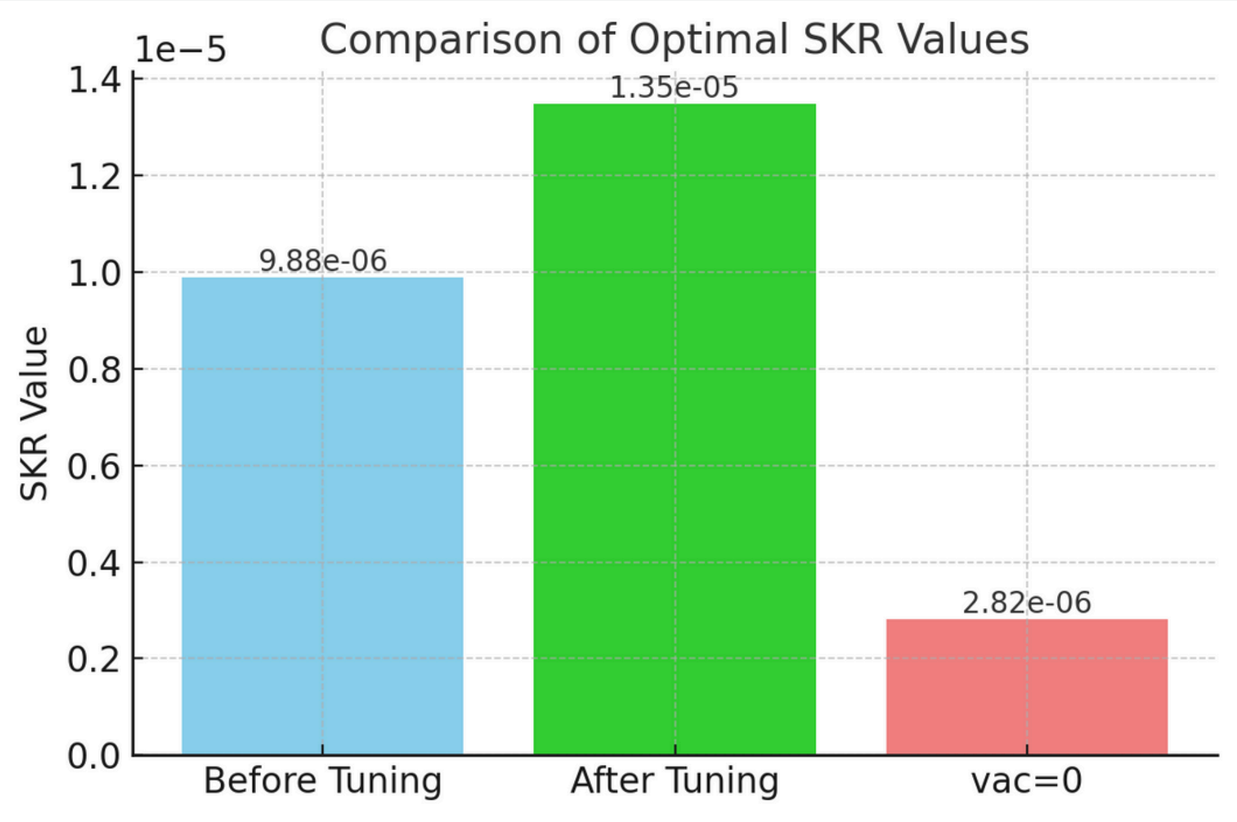
최적화된 GA 파라미터

crossover_type: two_points,
mutation_type: adaptive,
parent_selection_type: tournament,
sol_per_pop: 239,
num_parents_mating: 125,
keep_parents: 107,
keep_elitism: 12,
crossover_probability: 0.724853932736994 6,
mutation_percent_genes: [0.3, 0.1],
K_tournament: 71

최적 SKR 값: 2.821089e-06

mu(강도 파라미터): 0.399478
nu(약한 강도 파라미터): 0.167165
vac(진공 상태 파라미터): 0.000000 (고정)
p_mu(mu 상태 확률): 0.563898
p_nu(nu 상태 확률): 0.912773
p_vac(진공 상태 확률): 0.141586
p_X(X 기저 확률(Alice)): 0.332250
q_X(X 기저 확률(Bob)): 0.363639

비교


Comparison of Optimal SKR Values
1e−5
SKR Value
1.4
1.2
1.0
0.8
0.6
0.4
0.2
0.0
9.88e-06
1.35e-05
2.82e-06
Before Tuning
After Tuning
vac=0

감사합니다

박규민

QSIM+