

Performance of the BB84 protocol without decoy states under varying announcement structures

Zhiyao Wang^{*,†}, Aodhán Corrigan^{*,‡} and Norbert Lütkenhaus[§]

Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada



(Received 6 April 2026; accepted 12 August 2026; published 14 September 2026)

In phase-randomized weak coherent pulse (WCP) implementations of the quantum key distribution (QKD) BB84 protocol, the decoy method is often used to compensate BB84's vulnerability against photon number splitting attacks. However, this typically introduces extra complexities and requirements on experimental devices. In this paper, we are therefore interested in phase-randomized WCP implementations without the decoy method. We examine the performance of three QKD protocols with different classical announcement structures, namely, BB84, SARG04, and No Public Announcement of Basis (NPAB) BB84, using numerical security proof techniques. Key rates are computed using the OPENQKD SECURITY software [J. Burniston *et al.*, software OPENQKDSECURITY, ver. 2.0.2 (2024)]. We compare secure key rates of the three protocols in asymptotic and finite-size regimes for lossy and noisy channels. The three protocols show different relative advantages depending on the channel behavior. Canonical BB84 shows robustness against errors and depolarization, SARG04 demonstrates resilience against high-loss channels, and NPAB BB84 shows potential advantages against physical misalignment between QKD devices.

DOI: [10.1103/ybl1-j3td](https://doi.org/10.1103/ybl1-j3td)

I. INTRODUCTION

In the original BB84 protocol [1], it is assumed that the sender, Alice, sends out single-photon states. However, true single-photon sources are not accessible with today's technology. In actual implementations, phase-randomized weak coherent pulse (WCP) sources are used as they mostly emit single-photon signals with a relatively small probability of emitting multiphoton signals. However, the use of WCP sources opens the door for eavesdroppers. In the photon number splitting (PNS) attack [2,3], an adversary siphons off photons from multiphoton signals, revealing some information about the secret key. This information leakage is greatest in the BB84 protocol as Alice and the receiver, Bob, explicitly announce their basis choices. This results in multiphoton pulses being completely insecure and, as a consequence, the long-range performance of BB84 is severely limited.

One solution to this problem is to use the decoy-state method [4–6], where Alice decides the pulse intensities randomly before she encodes and transmits the signal. After Bob measures all signals, she announces her choices of intensities. In this way, the attacks by the adversary on multiphoton signals can be detected by estimating how the photon number statistics have changed through the transmission channel. However, the decoy-state method

requires additional hardware to modulate the intensities on a round-by-round basis according to a random sequence, which introduces additional side channels and requires extra effort to close the loopholes [7].

Another potential solution is to use modified announcement structures. We make use of two such protocols. The first is the SARG04 protocol [8], wherein Alice implicitly announces the basis encodings and requires Bob to combine the announcements and his detection outcomes to deduce Alice's encoding bases, while still using the physical BB84 hardware. We further propose a second, different protocol which we call No Public Announcement of Basis (NPAB) BB84, where we forgo basis sifting altogether in key generation rounds.¹ The different basis announcement structures of these protocols reduce the efficiency of PNS attacks and enable us to extract secret keys from multiphoton signals, without the need for decoy states. Furthermore, BB84, NPAB BB84, and SARG04 can be implemented using the same BB84 hardware as they all simply require Alice to send computational and conjugate basis states, with Bob actively measuring in these bases. In this work, we investigate the performance of the BB84, NPAB BB84, and SARG04 protocols under lossy and noisy channels with the same device setups to understand the impact of announcement structure on the key rate. Our proof framework allows for the extraction of secret keys from multiphoton signals and we illustrate the resulting performance improvements that are achieved by explicitly including these contributions in the analysis for NPAB and SARG04. This paper is organized as follows. In Sec. II, we describe a generic QKD protocol and we further detail the specific protocols investigated in this paper. In Sec. III, we briefly describe our mathematical model

*These authors contributed equally to this work.

†Contact author: z2425wan@uwaterloo.ca

‡Contact author: aodhan.corrigan@uwaterloo.ca

§Contact author: lutkenhaus.office@uwaterloo.ca

¹To the best of our knowledge, there is no existing literature that mentions NPAB BB84. If any reader is aware of relevant references, please feel free to contact the authors.

for simulating the protocol. In Sec. IV, we detail the resulting protocol performance under various model assumptions such as varying channel loss, channel alignment, and error rates. Finally, in Sec. V, we provide some concluding remarks.

II. PROTOCOL DESCRIPTIONS

A. General QKD protocol description

We begin by describing a generic, variable-length QKD protocol.

1. Signal preparation

In each round, Alice decides with probability p_{gen} whether the sent signal will be used for a key generation or testing round. She stores the positions of test (key generation) rounds in a string $T_{\text{test}}(T_{\text{gen}})$. Alice then picks a signal state from a set of d_A states, $\{\rho_x\}_{x=1,\dots,d_A}$, with associated probabilities $\{q_x\}_{x=1,\dots,d_A}$, from which she then prepares the signal with intensity μ in phase-randomized WCP, sent to Bob through a quantum channel $\mathcal{E}$. She stores the label corresponding to x in a classical register X_i .

2. Measurement phase

Bob measures the incoming states with positive operator-valued measure (POVM) elements $\{\Gamma_y^B\}_{y=1,\dots,d_B}$, where the index y runs over all possible measurement outcomes,² and stores his information in a classical register Y_i . The signal and measurement phases are repeated N times.

3. Announcement and testing phase

Alice and Bob process their data by using public announcements through an authenticated classical channel and sifting their resulting bits. Alice and Bob make public announcements C_A and C_B , respectively. Announcements include whether a round is used for testing or for generation. In the subset m selected testing, Alice and Bob announce the states X_i and full measurement outcomes Y_i , where $i \in T_{\text{test}}$, to obtain observed statistics $\bar{F}^{\text{obs}}$. The remaining $n = N - m$ rounds are used for key generation. Announcements for key generation rounds can include click or no-click outcomes, basis choices, or sets of possible signal states depending on the specific protocol.

4. Key generation and privacy amplification

For key generation rounds, Alice maps her register X_i (for $i \in T_{\text{gen}}$) to a raw key register R_i , using a key map $g: \mathcal{X} \times \mathcal{C}_A \times \mathcal{C}_B \rightarrow \mathcal{Z} \cup \{\perp\}$, where $\mathcal{X}$, $\mathcal{C}_A$, $\mathcal{C}_B$, and $\mathcal{Z}$ denote the alphabets for the respective registers. This function implements key mappings and sifting of signals depending on the previous classical announcements. Sifted signals, denoted by the label $\perp$, are removed from the final key and can include vacuum detections, inconclusive measurements, or more depending on the type of protocol. For the purposes of computing the key rate, we denote the number of signals

surviving sifting by n_{sift} . The two parties then perform error correction, leaking some bits of information, and then apply a two-universal hash function to their raw keys in order to generate a common secret key.

B. The BB84 hardware

BB84, NPAB BB84, and SARG04 can be implemented using the same physical hardware, as well as the same *signal preparation* (up to different choices of source settings and basis choices) and *measurement phase*. We now explain the setup and the parameters that Alice and Bob are free to change in this section.

(1) *Signal preparation*. Alice can choose the intensity μ of the phase-randomized WCP before the protocol begins, which fixes the intensity for all rounds in the protocol. For each round (for both key generation rounds and test rounds), she decides to encode in the Z (X) basis with probability p_Z (p_X). In the Z (X) basis, she randomly chooses the encoding $\{H, V\}$ ($\{D, A\}$) with equal probability. Since Alice prepares the outgoing states, she has the choice to misalign the outgoing basis states with respect to the two canonical bases by introducing some rotation angle θ .

(2) *Measurement phase*. Bob has an active detection setup. He measures in the Z (X) basis with the same probability p_Z (p_X) that Alice uses to choose the basis encoding. While this is a choice, it maximizes the probability of bases matching between the two.

(3) *Announcement and testing phase*. For testing rounds, Alice and Bob reveal the encodings and measurement outcomes. For key generation rounds, different protocols have different announcement structures, as we will explain in the next section.

We make use of polarization encoding $\{H, V, D, A\}$ using a phase-randomized WCP source.³ Although we pick this specific encoding, we do not expect major changes in the following analysis for encoding using other nonorthogonal states such as $\{R, L\}$ or other degrees of freedom such as time-bin encoding.

C. Specific protocols

We now describe the details of the BB84, NPAB BB84, and SARG04 protocols in this section (see Table I for a concise summary).

1. BB84 protocol

In the BB84 protocol, Alice randomly decides on sending a bit encoded in either $\{H, V\}$ (Z basis) or $\{D, A\}$ (X basis) polarizations with probability p_Z and p_X . Effectively, she picks a signal state from the set $\{\rho_H, \rho_V, \rho_D, \rho_A\}$ (phase-randomized WCP with polarization encoding) with probability $\{\frac{p_Z}{2}, \frac{p_Z}{2}, \frac{p_X}{2}, \frac{p_X}{2}\}$. The signal state choices are stored in the string $X_1^N = X_1, \dots, X_N$. She also generates a string $X_1'^N$ from X_1^N to store the basis choices. These states, generated by the string $X_1'^N$, are sent through an insecure but authenticated quantum channel $\mathcal{E}$. Bob measures the incoming

²The POVM corresponds to the one after the postprocessing map, if there is any. Further note that these elements may, in general, depend on the basis chosen for active detection setups.

³Since we use a phase-randomized WCP source, the output state is a mixed state.

TABLE I. Summary for all three protocols considered in this work.

Protocol	BB84	NPAB BB84	SARG04
Postprocessing map	Double-click ^a $\mapsto \begin{cases} H \vee D, & \text{probability } 1/2 \\ V \vee A, & \text{probability } 1/2 \end{cases}$, depending on basis		
Testing round	Reveal the full details of measurement outcomes X_i, Y_i		
Key generation round announcements	Alice announces basis choice string X'_i . Bob announces basis choice string Y'_i and no-click outcomes.	Bob announces no-click outcomes.	Alice announces nonorthogonal pairs $S_x := \{\rho_x, \rho_{x'}\}$. ^b Bob announces “conclusive” vs “inconclusive”.
Alice’s key map	$\perp$ if $X'_i \neq Y'_i \vee \text{no-click}$ 0 if $X'_i = Y'_i \wedge X_i \in \{H, D\}$ 1 if $X'_i = Y'_i \wedge X_i \in \{V, A\}$	$\perp$ if no-click 0 if $X_i \in \{H, D\}$ 1 if $X_i \in \{V, A\}$	$\perp$ if inconclusive 0 if $X_i \in \{H, V\}$ 1 if $X_i \in \{D, A\}$
Bob’s measurement map	$\perp$ if $X'_i \neq Y'_i \vee \text{no-click}$ 0 if $X'_i = Y'_i \wedge Y_i \in \{H, D\}$ 1 if $X'_i = Y'_i \wedge Y_i \in \{V, A\}$	$\perp$ if no-click 0 if $Y_i \in \{H, D\}$ 1 if $Y_i \in \{V, A\}$	$\perp$ if inconclusive 0 if $Y_i \in \{D, A\}$ 1 if $Y_i \in \{H, V\}$

^aMapping double-clicks to one of the results inside that basis is a prerequisite for our squashing model. For more details, we refer to Sec. III and Ref. [13].

^bFor more details, we refer to Sec. II C 3 and Ref. [8].

state using Z-basis (X -basis) measurements with probability $p_Z(p_X)$. In particular, he maps double-click outcomes to one of the possible single-click outcomes in the current measurement basis. Bob stores his basis choices in the string Y'^N_1 and the measurement outcomes in Y^N_1 . After all signals are measured, Alice and Bob announce all information in the m testing rounds. For key generation rounds, Alice announces the basis encodings X'_i and Bob announces measurement bases Y'_i . An extra announcement is made on Bob’s side to inform Alice of the no-click outcomes. Alice applies the key map on the remaining n bits to sift out rounds with basis mismatch and no-click outcomes and obtain the raw key.

2. No public announcement of basis (NPAB) BB84

NPAB BB84 differs from regular BB84 in the announcement and testing phase and is used to strengthen BB84 against PNS attacks by limiting public basis announcements. If a round is decided for testing, then Alice and Bob proceed exactly as in the BB84 protocol; Alice’s encoding choices and Bob’s measurement outcomes are fully revealed. During key generation rounds, the only announcements made are whether

Bob measured a click or a no-click outcome (Fig. 1). This allows Alice and Bob to sift out no-click outcomes in the key map. The remaining steps occur as in the case of BB84 to extract a secret key. This protocol differs from previous reduced-public-announcement BB84 variants [9–12] in that no secret information is required to be shared between the two parties ahead of time.

3. SARG04

SARG04 also differs from regular BB84 in the classical announcement phase [8]. During the quantum communication rounds, Alice still sends $\rho_x \in \{\rho_H, \rho_V, \rho_D, \rho_A\}$ with equal probability. Rather than announce the polarization encoding basis, Alice randomly picks one of the two states that are not orthogonal to ρ_x .⁴ We call this new state $\rho_{x'}$. She then announces the set $S_x := \{\rho_x, \rho_{x'}\}$. If Bob has measured a state orthogonal to $\rho_{x'}$ (or ρ_x), he can conclude the correct signal is ρ_x (or $\rho_{x'}$). Otherwise, he discards the round. For example, in one particular round, Alice sends an ρ_H state. In the announcement phase, she can then announce the pair $\{\rho_H, \rho_D\}$. If Bob measures an outcome with polarization A , he can exclude the state ρ_D to deduce that Alice has sent the ρ_H state and this round is kept for key generation. Otherwise, he discards it. He also discards no-click outcomes. Bob later announces the label “conclusive” (“inconclusive”) for kept (discarded) rounds without revealing the details of the measurement outcomes. For key maps, Alice maps $\{\rho_H, \rho_V\}$ to key bit 0 and maps $\{\rho_D, \rho_A\}$ to key bit 1.

III. METHODS

In this section, we describe the essential methods we use to numerically calculate key rates. The full details are described in Appendix A.

To numerically represent Bob’s measurement, we use a postprocessing map that randomly assigns double-click out-

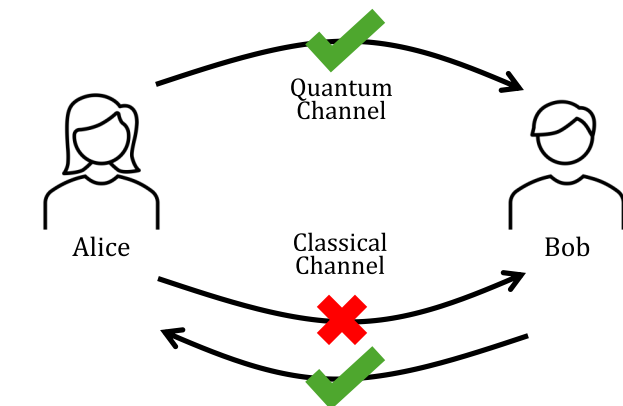


FIG. 1. In NPAB BB84, the only sifting done is Bob announcing no-click/click.

⁴Two states $\rho_x, \rho_{x'}$ are orthogonal if $\rho_x \rho_{x'} = \rho_{x'} \rho_x = 0$, which generalizes the notion of orthogonality to mixed states.

comes to one of the outcomes on Bob's side. This random bit assignment is required to prove the existence of a squashing map for active detectors [13]. Following this, we apply a squashing map which allows us to consider an equivalent QKD protocol where Bob's previously infinite-dimensional measurements are reduced to three-dimensional (qubit plus loss) measurements. Given this, the asymptotic, independent and identically distributed (i.i.d.) key rate formula [[14], Eqs. (50)–(54)] can be numerically computed as the optimization problem,

$$R_\infty = \min_{\rho_{AB} \in \mathcal{S}} D\{\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})]\} - f_{\text{EC}} \delta_{\text{leak}} \quad (1)$$

$$=: \min_{\rho_{AB} \in \mathcal{S}} f(\rho_{AB}) - f_{\text{EC}} \delta_{\text{leak}}, \quad (2)$$

where $\mathcal{S}$ is a predetermined feasible set constraining channel behavior, $D(\cdot || \cdot)$ is the quantum relative entropy, $\mathcal{G}$ and $\mathcal{Z}$ are maps that model measurements, sifting, and key maps, and δ_{leak} is the cost for classical error correction with weighting f_{EC} .

When we consider finite-size effects, the total security of the protocol decomposes into several terms, $\varepsilon_{\text{sec}} = \varepsilon_{\text{EV}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{AT}}$, where the ε 's are security parameters for error verification (ε_{EV}), privacy amplification (ε_{PA}), and acceptance testing (ε_{AT}). Using the postselection security proof technique, the key length can be shown to be lower bounded against coherent attacks by ([15], Eq. (49) of [16] with $t = 0$)

$$\begin{aligned} \ell_{\text{finite}} \geq n_{\text{sift}} \min_{\rho_{AB} \in \mathcal{V}(\vec{F}^{\text{obs}})} \frac{1}{P(\text{sift} \wedge \text{gen})} f(\rho_{AB}) - f_{\text{EC}} \delta_{\text{leak}} n_{\text{sift}} \\ - \sqrt{n_{\text{sift}}} (\alpha - 1) \log_2(\dim A + 1) - \log_2 \left(\frac{2}{\varepsilon_{\text{EV}}} \right) \\ - \frac{\alpha}{\alpha - 1} \left[\log_2 \left(\frac{1}{2\varepsilon_{\text{PA}}} \right) + \frac{2}{\alpha} \right], \end{aligned} \quad (3)$$

where N is the total number of signals, n_{sift} is the number of signals surviving sifting, $\mathcal{V}(\vec{F}^{\text{obs}})$ is the constraint set generated by the observations, and α is the Rényi entropy parameter. Whether a signal survives sifting [and therefore the probability $P(\text{sift}|\text{gen})$] is determined by Alice and Bob's observed statistics and classical announcements. The testing rounds are used to estimate the error rate of the raw key and are used to compute the asymptotic error correction cost per sent signal δ_{leak} .⁵

IV. RESULTS

We present an overview of the numerical results. We make use of the OPENQKDSECURITY software package [17] to simulate the channels and compute key rates. Our findings can be summarized as follows:

⁵The Shannon entropy H_2 of Alice's raw key string to Bob's raw key string is the asymptotic cost of error correction and can be upper bounded by n_{sift} times the binary entropy of the bit error rate. We use testing rounds to estimate the error rate, and in order to account for a realistic error correction protocol on finite blocks of data, we make use of the efficiency factor f_{EC} . In actual implementations, the error correction cost will be dependent on the code that is used.

(1) *Announcements have significant effect.* We show that different announcement structures can dramatically change the performance of QKD protocols using the same hardware and can allow for extracting secret keys from higher photon (≥ 3) states, even in the finite-size regime.

(2) *Misalignment.* The case where Alice and Bob's devices are perfectly aligned is not optimal for NPAB BB84. In other words, the key rate performance is better when we intentionally misalign Alice and Bob's device by some angle θ , in order to maximize the probability of matching bits, rather than states.

(3) *Multiphoton contribution.* For NPAB BB84 and SARG04, the use of numerical proof techniques allows us to extract secret information from multiphoton signals, which are typically assumed to be insecure in BB84. We show that allowing Alice and Bob to distill key bits from two-photon and three-photon signals does indeed improve secret key rates, expanding on existing results in Refs. [8, 18].

(4) *Channel parameter resilience.* We show that the three protocols have different regimes in which they show their respective advantages. We consider asymptotic and finite key rates for lossy, misaligned, and depolarizing channels.

In Table II, we list parameters that are set in our simulations. We specify if this parameter is optimized for the given channel settings. Note that we do not specify channel parameters here. We introduce a new parameter K labeling the photon number cutoff in our simulation, where we assume all photon pulses containing more than K photons are completely leaked to the adversary. We refer to Sec. IV B for more details.

A. Misalignment angle θ^* for NPAB BB84

One possible source of error in implementations of QKD protocols is physical misalignment in the quantum channel. In BB84 or any protocol with basis announcements, the optimal angles are $\theta = 0$ and $\pi/2$, as any nontrivial angle introduces some error in distinguishing between encoded key bits. In the case of BB84, distinguishing between encoded key bits is aided by basis sifting. After basis sifting, the probability of correctly matching bits is simply the probability of measuring the appropriate one of the two orthogonal states. Unlike canonical BB84, NPAB BB84 does not sift bases and so performance may be increased by instead minimizing the cost of error correction across all signal detections by optimizing the probability of bits matching across all bases, keeping in mind that the polarization encodings $\{H, D\}$ are both mapped to bit "0" and $\{V, A\}$ to bit "1." This can be achieved by Alice intentionally rotating her prepared states by some angle θ , and can therefore be thought of as part of the protocol. We present a detailed calculation for the qubit case in Appendix E. For the photonic case, we scanned numerical parameters and found that the optimal θ^* closely agrees with the qubit case (see the increased key rate for nonzero θ in Fig. 3). We ascribe differences between the optimal angle for the qubit and photonic cases to the fact that the optimization routine also tries to minimize other parameters, such as double-click outcomes, whose probability does slightly increase with the misalignment angle. For the remainder of this work, NPAB BB84 results will be simulated with a fixed but nonzero misalignment angle $\theta^* = 0.055$ rad (meaning scanning over

TABLE II. Plotting parameters in Sec. IV.

Parameter	Symbol	Value
Mean photon number	μ	Globally optimized in all plots. ^a
Photon number cutoff	K	Scanned in Fig. 4. Fixed $K = 3$ (including 3) otherwise.
Channel misalignment	θ	Scanned in Figs. 3, 13, and 14. Fixed $\theta = 0$ for BB84, SARG04 otherwise. Fixed $\theta = \theta^* \approx 0.055$ for NPAB BB84 otherwise.
Channel loss	η	Scanned in Figs. 5, 8, 9, 10 and associated μ plots. Fixed $\eta \approx 0.36$ in Fig. 4; fixed $\eta = 0.1$ otherwise.
Channel visibility angle	φ	Scanned in Figs. 7, 11, and 12. Fixed $\varphi = 0$ otherwise.
X-basis probability	p_X $p_Z = 1 - p_X$	Fixed $p_X = 0.9$ for BB84, NPAB BB84. Fixed $p_X = 0.5$ for SARG04.
Testing probability	p_{test}	Fixed $p_{\text{test}} = 0.15$. ^b
Security parameters	ε_i	Fixed $\varepsilon_{\text{AT}} = \frac{1}{4} 10^{-9}$, $\varepsilon_{\text{EC}} = \frac{1}{2} 10^{-9}$, and $\varepsilon_{\text{PA}} = \frac{1}{4} 10^{-9}$.
Error correction efficiency	f_{EC}	Fixed $f_{\text{EC}} = 1$ for asymptotic plots; fixed $f_{\text{EC}} = 1.2$ for finite-size plots.
Rényi parameter	α	Fixed $\alpha = 1 + \sqrt{\log_2(1/\varepsilon_{\text{PA}})/n_{\text{sift}}/\log_2(d_A + 1)}$. ^c

^aOptimized using `fminbnd` subroutine in MATLAB. The optimal μ value from the previous simulation point is used as the optimization's starting μ value for the current point since the optimum does not change much over small parameter ranges. The built-in global optimization does, however, cause numerical instability in high-loss regions and the optimal choice of intensity. We believe that the nonsmooth behavior comes from the limited precision of the global optimization routine.

^bWhen a large amount of signals is sent, a smaller fraction of signals is needed to estimate the quantities. While as N tends to infinity the optimal value of p_{test} tends to zero, we find that p_{test} fixed to 0.15 works well for all regimes considered in this work.

^cHere, n_{sift} denotes the number of rounds surviving sifting and d_A denotes the dimension of Alice's registers, X_i . See Ref. [14].

misalignment angles is *in addition* to θ^*) chosen in order to boost protocol performance, with the value taken from Fig. 3. We justify this by the fact that the misalignment minimizes the cost of error correction (see Appendix E), which is independent of loss, mean photon number, and the number of signals sent after Alice and Bob discard no-click events. In order to consider this intentional channel misalignment as part of the protocol, this may be equivalently modeled as Alice preparing misaligned states via source map arguments (for a schematic illustration, see Fig. 2). Source map arguments allow us to prove security considering the case where signal states without misalignment are prepared and Eve implements the rotation, thus simplifying the analysis [19]. In both the asymptotic and finite-size regimes, NPAB BB84 is more resilient to physical misalignment and is capable of outperforming both BB84 and SARG04 in the finite-size regime (Figs. 3, 13, and 14).

B. Inclusion of multiphoton signals

For NPAB and SARG04, multiphoton signals contribute to the key rates due to bases not being announced and we can

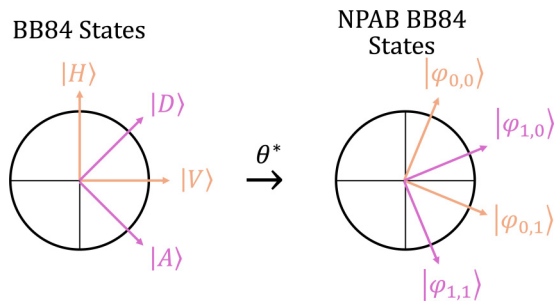


FIG. 2. Optimized NPAB BB84 protocol states are shifted relative to bases.

choose to include those signals in our analysis. The key rate contribution from signals with photon number greater than 3 is small (Fig. 4). We further scanned for other parameter regimes and observed the same trend. Intuitively, this is because higher photon number nonorthogonal states have less overlap, allowing Eve to unambiguously discriminate them with higher success probability. Since the increase in key rates from $K = 3$ to $K = 4$ is relatively small, and it takes much more computer resources to calculate key rates when increasing K , we include up to $K = 3$ photon number contributions in the key rates' calculation for NPAB and SARG04 and flag the remaining signals. For mathematical details, see Appendix A 2.

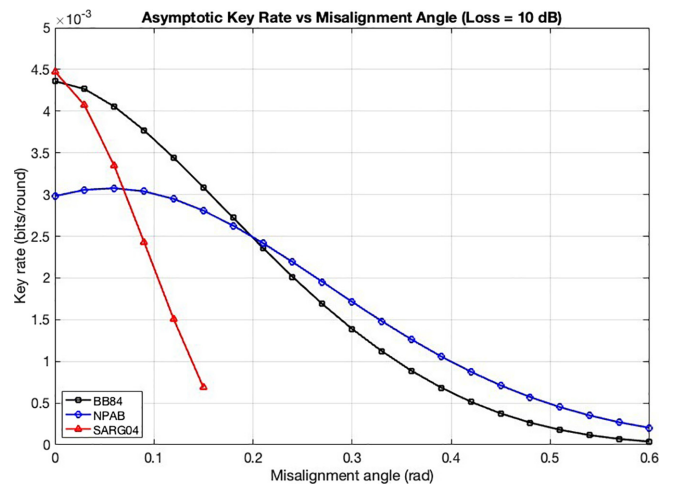


FIG. 3. Performance of BB84, SARG04 and NPAB BB84 at 10 dB channel loss when introducing physical misalignment θ between detectors in the limit $N \rightarrow \infty$. The signal intensity is optimized. Note that NPAB BB84's absolute misalignment angle starts at 0 in this plot.

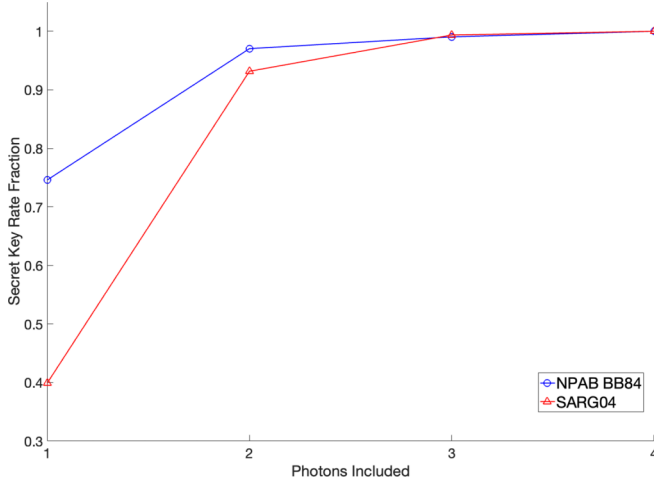


FIG. 4. Key rate vs number of photons used for key calculation in a given pulse (the photon cutoff K). Protocols are simulated in the asymptotic limit $N \rightarrow \infty$ with 5 dB quantum channel loss and we optimize the choice of intensity of the phase-randomized WCP (mean photon number μ).

C. Asymptotic key rates

In this section, we explore the performance of BB84, SARG04, and NPAB BB84 in the asymptotic regime using the framework in [20] (see Appendix A 5, A 7 a) in which we assume Alice sends infinitely many signals, allowing for exact bounds on channel statistics.

We first investigate the performance of a loss-only channel. We find that SARG04 is more resilient to high loss, allowing for higher key rates in that regime. These results agree with a previous analytic study on SARG04 and BB84 [21]. Note, however, that this previous work only included a cutoff of two photons in its analysis, whereas our work can include an arbitrary number of photons. In addition, NPAB BB84 does not show any advantage against the other two protocols (Fig. 5). The announcement structure of SARG04 allows

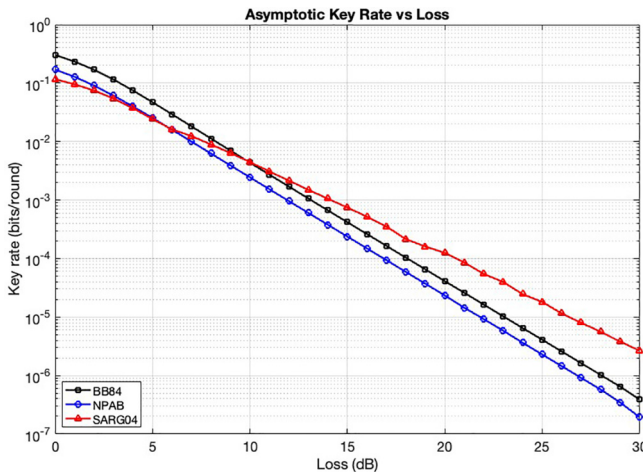


FIG. 5. Secret key rate per signal in a loss-only channel for protocols in the asymptotic limit $N \rightarrow \infty$ total signals sent. The signal intensity is optimized. We take loss = $-10 \log_{10} \eta$ in dB.

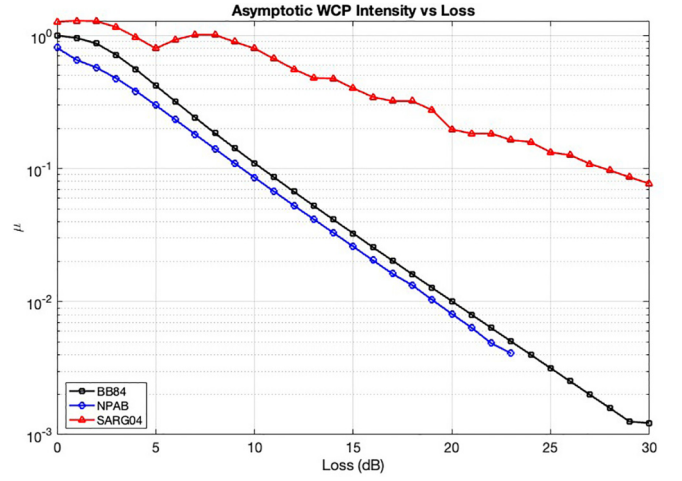


FIG. 6. Optimal pulse intensity (mean photon number) vs loss in dB in a loss-only channel for asymptotic key rates.

for a higher signal intensity and mean photon number, with $\mu_{\text{SARG04}}^{\text{opt}} \sim 10^{-1}$ between 0 and 35 dB (Fig. 6). Note that the key rate of BB84 and NPAB BB84 scales as $O(\eta^2)$, which is in line with known results in the literature. Similarly, the key rate of SARG04 scales as $O(\eta^{3/2})$ [18]. We further remark that this is still sublinear, in contrast to decoy-state BB84 which scales as $O(\eta)$. We also highlight the change in SARG04's behavior around 7 dB seen in Figs. 5 and 6, which has previously been observed at 10 dB [8]. We ascribe the difference to the fact that we optimize the signal intensity at each point. Next, we introduce depolarization error into the channel (see Appendix A 7 c). The advantage of SARG04 vanishes quickly as error increases due to its announcement structure. This also agrees with previous results indicating SARG04 is not robust against depolarization error [21]. Again, however, NPAB BB84 shows no significant advantage compared to BB84, though it does perform better than SARG04 (Fig. 7).

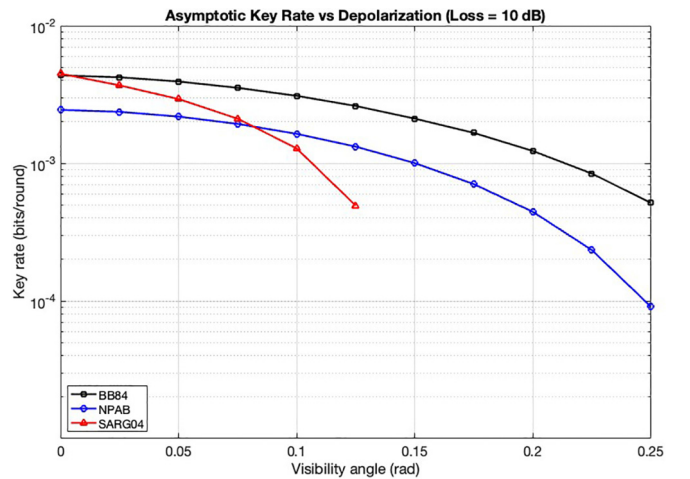


FIG. 7. Secret key rate per signal in a quantum channel with depolarizing noise and fixed 10 dB loss for protocols in the asymptotic limit $N \rightarrow \infty$ total signals sent.

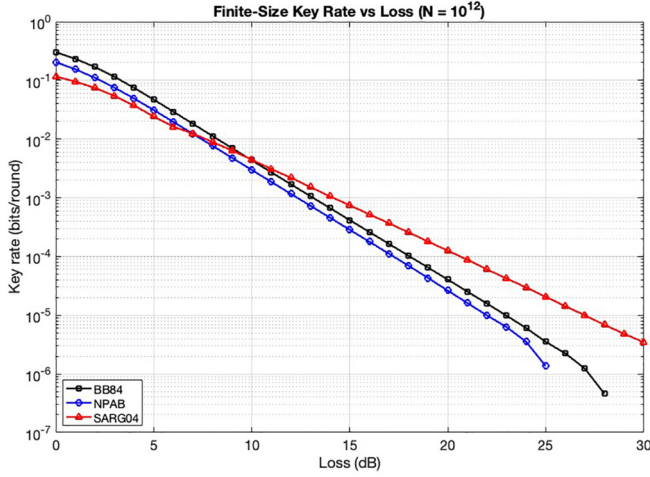


FIG. 8. Secret key rate per signal for a loss-only quantum channel for protocols with $N = 10^{12}$ total signals sent. The signal intensity is optimized.

D. Finite-size key rates

We repeat the previous section's investigation while introducing finite-size effects (see Appendix A 6). We specifically investigate the case for $N = 10^{12}$, $N = 10^9$, and $N = 10^6$ total signals, corresponding to 1000 seconds, 1 second, and 1 millisecond with a 1 GHz clock rate, respectively, representing current and near-future technical capabilities, respectively [22]. As before, we begin with investigating the behavior of the protocols in a loss-only channel. As was the case in the asymptotic formulation, a loss-only protocol implementation with $N = 10^{12}$ total signals and $p_{\text{gen}} = 0.85$ demonstrates that SARG04 is much more resilient to loss, with the relative scaling between the three protocols being similar (Fig. 8). Limiting the total number of signals to $N = 10^9$ and $N = 10^6$ introduces much more prevalent finite-size effects. We observe that the general behavior is similar in the asymptotic case, with SARG04 having stronger performance with high

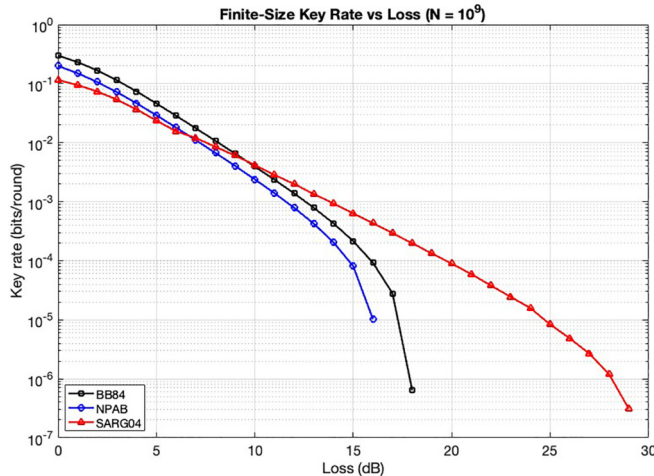


FIG. 9. Secret key rate per signal in a loss-only quantum channel for protocols with $N = 10^9$ total signals sent. The signal intensity is optimized.

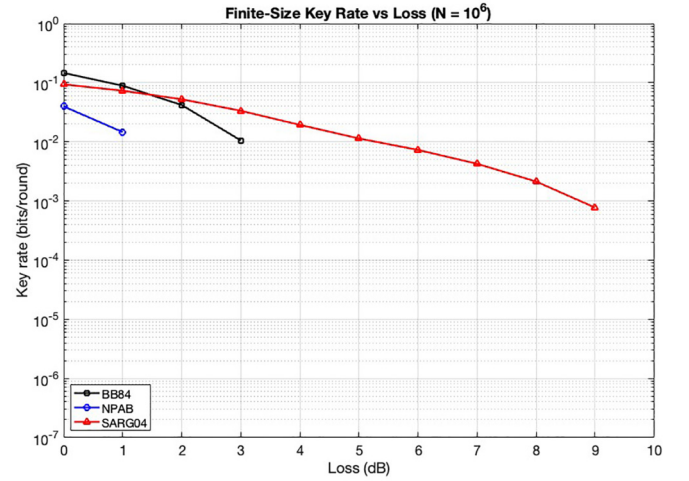


FIG. 10. Secret key rate per signal in a loss-only quantum channel for protocols with $N = 10^6$ total signals sent. The signal intensity is optimized.

loss. Due to the finite-size effects, expected key rates die out at a quicker rate (Figs. 9 and 10). Compared to $N = 10^{12}$ signals, which behaves close to the asymptotic limit, key rates cannot tolerate as much loss and the protocols are unable to produce key rates past 15 to 20 dB.

Introducing misalignment and depolarizing noise into the channel leads to similar behavior as before in the asymptotic regime. We observe that BB84 and NPAB BB84 behave similarly (see Figs. 13 and 14). The optimal misalignment angle θ^* shifts towards zero as one decreases the number of signals sent. Since the cost of error correction is invariant under the number of signals sent, we ascribe this difference to finite-size effects in the optimization set. SARG04 is more susceptible to depolarization errors, while BB84 and NPAB BB84 manage higher key rates with error (Figs. 11 and 12). We do not include calculations for $N = 10^6$ for misalignment and depolarization because most of the key rates vanish.

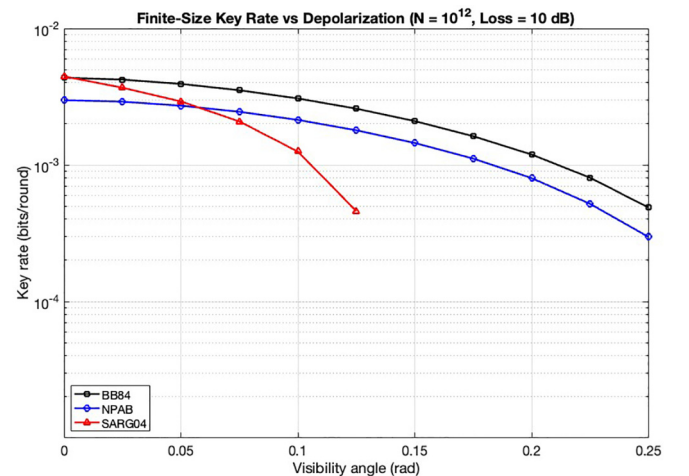


FIG. 11. Secret key rate per signal in a quantum channel with depolarizing noise and fixed 10 dB loss for protocols in the case of $N = 10^{12}$ total signals sent.

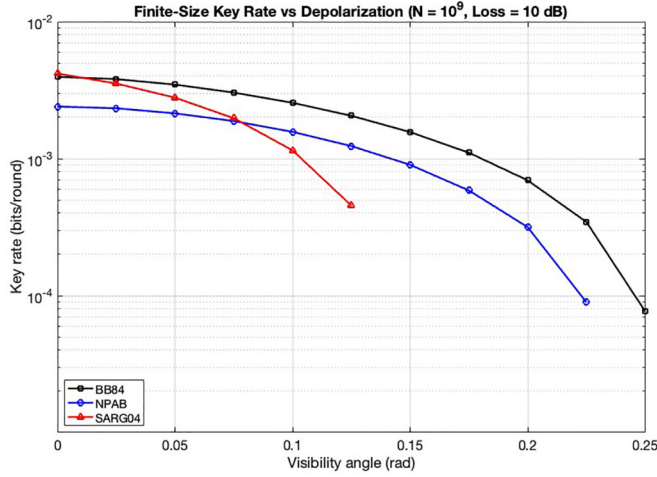


FIG. 12. Secret key rate per signal in a quantum channel with depolarizing noise and fixed 10 dB loss for protocols in the case of $N = 10^9$ total signals sent.

V. CONCLUSION

We use a numerical security analysis to characterize the performance of three quantum key distribution protocols, i.e., BB84, NPAB BB84, and SARG04, with phase-randomized WCP implementations without using the decoy method. In general, in the case where we do not have decoy states, BB84 is still more robust than NPAB BB84 and SARG04 when considerable loss and noise are present. We have also shown that NPAB BB84 outperforms the other protocols when we consider physical misalignment and that SARG04 can produce more secret key when in a high-loss but noiseless channel.

Further points of interest could include comparing a larger variety and complexity of announcement structures in order to best take advantage of each protocol's specific strengths, as well as changing the physical protocol setups.

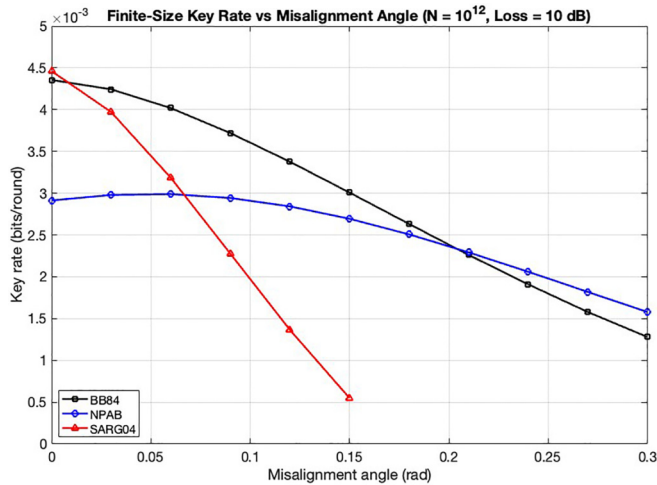


FIG. 13. Secret key rate per signal in a quantum channel with physical misalignment and fixed 10 dB loss for protocols in the case of $N = 10^{12}$ total signals sent.

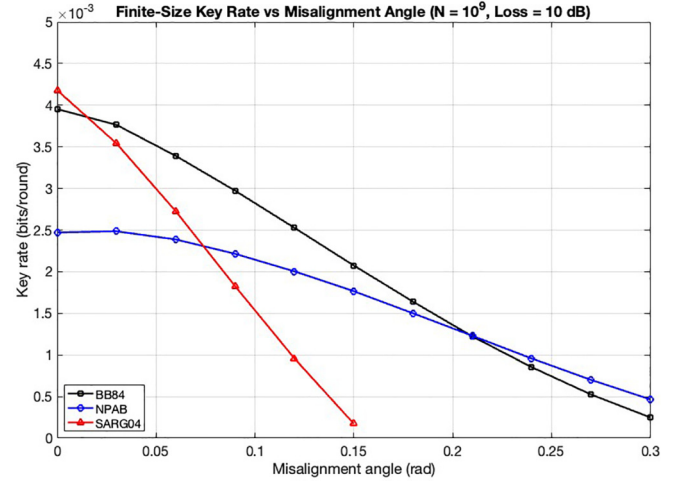


FIG. 14. Secret key rate per signal in a quantum channel with physical misalignment and fixed 10 dB loss for protocols in the case of $N = 10^9$ total signals sent.

ACKNOWLEDGMENTS

This research is supported by NSERC (through the NSERC Discovery program and NSERC Alliance project) and QUINT (Qeyssat User INvestigation Team). The authors would like to thank John Burniston for his help in implementing the protocols using OPENQKDSecurity [17]. They further extend thanks to Lars Kamin and Devashish Tupkary for their knowledge of the theoretical aspect of QKD protocols.

DATA AVAILABILITY

This work made use of the OPENQKDSecurity framework (see Ref. [17]). The source code for this specific publication may be found in Ref. [23].

APPENDIX A: MATHEMATICAL MODEL

1. State preparation

We make use of the source-replacement scheme to model a prepare-and-measure protocol with an entanglement-based one [24,25]. Each round in a prepare-and-measure protocol consists of Alice sending some signal state $|s_x\rangle$ with probability q_x . Through the source-replacement scheme, this is equivalent to Alice preparing and sending the entangled state

$$|\psi\rangle_{AA'} = \sum_x \sqrt{q_x} |x\rangle_A |s_x\rangle_{A'}, \quad (\text{A1})$$

where the set $\{|x\rangle_A\}_{x=1,\dots,d_A}$ is an orthonormal basis for Alice's register of output states and the register A' is the signal system before the action of the channel. The shield system [26], which is necessary if Alice uses a phase-randomized source, allows us to write a purification of phase randomized Fock states as

$$|\psi\rangle_{A_s A A'} = \sum_{n=0}^{\infty} \sqrt{p_n} |n\rangle_{A_s} \sum_x \sqrt{q_x |n|} |x\rangle_A |s_{x,n}\rangle_{A'}, \quad (\text{A2})$$

where $p_n \equiv P_\mu(n) = e^{-\mu} \mu^n / n!$ is the Poisson distribution for the photon number $n \in \mathbb{N}_0$ and the signal states are defined in terms of the creation operators [27] as

$$|s_{x,n}\rangle = \frac{1}{\sqrt{n!}} (a_{h(x)}^\dagger)^n |0\rangle, \quad (\text{A3})$$

where h is a bijective map, $h: \{1, 2, 3, 4\} \rightarrow \{H, V, D, A\}$. Finally, Alice sends the signal system through a quantum channel $\mathcal{E}$, after which Alice and Bob share the state

$$\rho_{A_S A_B} = \mathbb{1}_{A_S A} \otimes \mathcal{E}_{A' \rightarrow B}(|\psi\rangle\langle\psi|_{A_S A A'}). \quad (\text{A4})$$

2. Tagging source and squashing model

In order to numerically represent this system with finite matrices, we model the incoming phase-randomized state up to some photon number cutoff [28]. In our calculation, we pick $K = 3$. Past this cutoff, we tag those states with orthogonal states $\{|f_x\rangle\}_{x=1,\dots,d_A}$, leaving Eve with full knowledge of the tagged states. The shared density matrix is then

$$\rho_{A_S A A'} = |\Psi\rangle\langle\Psi|_{A_S A A'}, \quad (\text{A5})$$

where

$$\begin{aligned} |\Psi\rangle_{A_S A A'} &= \sum_{n=0}^K \sqrt{p_n} |n\rangle_{A_S} \otimes \sum_x \sqrt{q_{x|n}} |x\rangle_A \otimes |s_{x,n}\rangle_{A'} \\ &+ \sqrt{p_{n>K}} |K+1\rangle_{A_S} \otimes \sum_x \sqrt{q_{x|K+1}} |x\rangle_A \otimes |f_x\rangle_{A'}. \end{aligned} \quad (\text{A6})$$

On Bob's side, we use the simple squashing map [13] after postprocessing, which randomly assigns double-click events to one of the detection outcomes. This squashing model also allows us to represent Bob's measurements in the qubit and vacuum subspace [13].

3. Measurements

Following the framework of [14,20], in the prepare-and-measure implementation, Alice's choice of signal state is equivalent to performing a measurement on $\rho_{A_S A}$ with POVM defined by elements

$$\Gamma_x^A \in \left\{ \sum_{n=0}^{K+1} |n\rangle\langle n| \otimes |x\rangle\langle x| \right\}_{x=1,\dots,d_A}. \quad (\text{A7})$$

Accordingly, Bob's measurements are represented as basic qubit and vacuum measurements, with POVM

$$\Gamma_y^B \in \{|y\rangle\langle y|\}_{y=0,1,\perp} \text{ or } \{|y\rangle\langle y|\}_{y=+,-,\perp}, \quad (\text{A8})$$

depending on the choice of basis (where these operators act on the qubit and vacuum space $\mathbb{C}^2 \oplus \mathbb{C}$).

4. Kraus operators and key map

In the framework of [14], we use a set of Kraus operators, $K_{a,b} := K_a^A \otimes K_b^B$, to incorporate Alice and Bob's announcements and the key map, where the indices a, b run over Alice and Bob's possible announcements. Let R be the key register, X a register of Alice's measurement outcomes, Y a register of Bob's measurement outcomes, $C = C_A \times C_B$ a register of the joint announcements, $\mathcal{X}_a$ the set of Alice's

measurement outcomes associated with announcement α , and $\mathcal{Y}_b$ the set of Bob's measurement outcomes with announcement b . Let $g: \mathcal{X} \times \mathcal{C} \rightarrow \mathcal{Z} \cup \{\perp\}$ be the key map, which takes in announcements and Alice's measurement outcome (postsifting, stored in alphabets $\mathcal{C}$ and $\mathcal{X}$, respectively) and outputs a raw key (with alphabet $\mathcal{Z}$, or an abort symbol). $\Gamma_{a,x}^A$ and $\Gamma_{b,y}^B$ are the POVM elements corresponding to the announcement.⁶ Then the joint Kraus operator is defined as

$$\begin{aligned} K_{\alpha,\beta} &= \Pi_{RXYABC}^{\text{sift}} \sum_{\substack{x \in \mathcal{X}_\alpha \\ y \in \mathcal{Y}_\beta}} |g(x, \alpha, \beta)\rangle_R \otimes |x\rangle_X \otimes |y\rangle_Y \\ &\otimes \sqrt{\Gamma_{\alpha,x}^A} \otimes \sqrt{\Gamma_{\beta,y}^B} \otimes |\alpha, \beta\rangle_C, \end{aligned} \quad (\text{A9})$$

where

$$\Pi_{RXYABC}^{\text{sift}} = \mathbb{1}_{RXYAB} \otimes \Pi_C^{\text{sift}}. \quad (\text{A10})$$

The map $\Pi_{RXYABC}^{\text{sift}}$ performs sifting of signals based on C , sifting out testing, vacuum, and, in the case of BB84, basis-mismatched signals. We are left with surviving Kraus operators, explicitly described in the following sections, which define a map we denote by $\mathcal{G}$. Furthermore, we define the $\mathcal{Z}$ map by

$$\mathcal{Z}(\rho) = \sum_r P_r \rho P_r^\dagger, \quad (\text{A11})$$

where

$$P_r = |r\rangle\langle r|_R \otimes \mathbb{1}_{XYABC}. \quad (\text{A12})$$

5. Asymptotic key rates

We compute asymptotic key rates using the framework developed in [14] and improved in [20]. In this formulation, the key rate formula is

$$\begin{aligned} R_\infty &= \min_{\rho_{AB} \in \mathcal{S}} D\{\mathcal{G}(\rho_{AB}) || \mathcal{Z}[\mathcal{G}(\rho_{AB})]\} - f_{\text{EC}} \delta_{\text{leak}} \\ &=: \min_{\rho_{AB} \in \mathcal{S}} f(\rho_{AB}) - f_{\text{EC}} \delta_{\text{leak}}, \end{aligned} \quad (\text{A13})$$

where $\mathcal{S}$ is a set constraining the system's density matrix, D is the quantum relative entropy, and the $\mathcal{G}$ and $\mathcal{Z}$ maps model measurements, announcements, sifting, and key maps. The parameter f_{EC} is a choice characterizing the efficiency of error correction ($f_{\text{EC}} = 1$ is the Shannon limit). In our calculation, we pick $f_{\text{EC}} = 1$ for the asymptotic key rate and $f_{\text{EC}} = 1.2$ for the finite-size key rate.

6. Finite-size and variable-length key rates

In order to compute key rates while accounting for finite-size effects (i.e., given some finite N signals sent between Alice and Bob), new correction terms are needed [15,16]. Variable-length key rates can be used to compute the hash length of the secret key after the run of the protocol and after

⁶The announcements a do not change Alice's measurement, though we use this notation for consistency with previous works [14]. It does, however, decide which POVM is used for Bob's measurement (since his POVM is different depending on whether basis X or basis Z is chosen for measurement).

test statistics have been established. We compute variable-length key rates for the case that the channel behaves as expected, such that the observed statistics $\vec{F}^{\text{obs}}$ are equal to the expected channel output $\vec{F}$. In other words, we simulate honest channel implementations (although still allowing Eve to have any purification and perform any attack compatible with the observed statistics). This, however, is not restrictive and one could simulate data via other simulation means or make use of experimental results. Given a protocol with $\varepsilon_{\text{sec}} = \varepsilon_{\text{EV}} + \varepsilon_{\text{PA}} + \varepsilon_{\text{AT}}$ security, the key length is lower bounded by

$$\begin{aligned} \ell_{\text{finite}} \geq n_{\text{sift}} \min_{\rho_{AB} \in \mathcal{V}(\vec{F}^{\text{obs}})} \frac{1}{P(\text{sift} \wedge \text{gen})_{\rho_{AB}}} f(\rho_{AB}) - f_{\text{EC}} \delta_{\text{leak}} \\ - \sqrt{n_{\text{sift}}} (\alpha - 1) \log_2^2(\dim A + 1) - \log_2 \left(\frac{2}{\varepsilon_{\text{EV}}} \right) \\ - \frac{\alpha}{\alpha - 1} \left[\log_2 \left(\frac{1}{2\varepsilon_{\text{PA}}} \right) + \frac{2}{\alpha} \right], \end{aligned} \quad (\text{A14})$$

where N is the total number of signals, n_{sift} is the number of generation signals surviving sifting, $\mathcal{V}(\vec{F}^{\text{obs}})$ is a constraint set

accounting for statistical fluctuations in the finite-size regime, and α is the Rényi entropy order with optimal value

$$\alpha^{\text{opt}} = 1 + \sqrt{\frac{\log_2(1/\varepsilon_{\text{PA}})}{\log_2(\dim A + 1)n_{\text{sift}}}}. \quad (\text{A15})$$

The feasible set is defined as [[16], Lemma 7]

$$\begin{aligned} \mathcal{V}(\vec{F}^{\text{obs}}) = \{ \rho \in S_{\circ} \mid \text{Tr}_B(\rho) = \rho_{A_S A}, \\ \text{Tr}(\Gamma_k \rho) \in \{ F_k^{\text{obs}} - \tilde{\kappa}_k^L, F_k^{\text{obs}} + \tilde{\kappa}_k^U \} \forall k \in \Sigma \}, \end{aligned} \quad (\text{A16})$$

where $S_{\circ}$ denotes the set of all density matrices over Alice and Bob's systems, $\rho_{A_S A}$ is the fixed state in Alice's laboratory, $\Gamma_k = \Gamma_x^A \otimes \Gamma_y^B$ for $k = (x, y)$, and $\Sigma = \Sigma_{\text{test}} \cup \{\text{sift} \wedge \text{gen}, \perp\}$ is the set of all possible pairs of announcements in union with the events that Alice and Bob abort a given round or not. For test rounds, we define

$$\begin{aligned} \tilde{\kappa}_k^L = F_k^{\text{obs}} - B\left(\frac{\varepsilon_{\text{AT}}}{2\text{card}(\Sigma)}; N_{\text{test}} F_k^{\text{obs}}, N - N_{\text{test}} F_k^{\text{obs}} + 1\right), \\ \tilde{\kappa}_k^U = -F_k^{\text{obs}} + B\left(1 - \frac{\varepsilon_{\text{AT}}}{2\text{card}(\Sigma)}; N_{\text{test}} F_k^{\text{obs}} + 1, N - N_{\text{test}} F_k^{\text{obs}}\right), \end{aligned} \quad (\text{A17})$$

where $\text{card}(\cdot)$ denotes the alphabet's cardinality, and $B(p; a, b)$ is the p th quantile of the beta distribution with shape parameters a, b . Through this formalism, we also simplify the optimization problem by upper bounding the relative entropy prefactor in (A14) by

$$\min_{\rho_{AB} \in \mathcal{V}(\vec{F}^{\text{obs}})} \frac{1}{P(\text{sift} \wedge \text{gen})_{\rho_{AB}}} f(\rho_{AB}) \geq \frac{1}{F_{\text{sift} \wedge \text{gen}}^{\text{obs}} + \tilde{\kappa}_{\text{sift} \wedge \text{gen}}^U} \min_{\rho_{AB} \in \mathcal{V}(\vec{F}^{\text{obs}})} f(\rho_{AB}), \quad (\text{A18})$$

where $F_{\text{sift} \wedge \text{gen}}^{\text{obs}}$ is the observed frequency of bits chosen for generation rounds surviving sifting, and $\tilde{\kappa}_{\text{sift} \wedge \text{gen}}^U$ is defined as in (A17), except with all generation rounds $N_{\text{sift} \wedge \text{gen}}$ instead of $N_{\text{test}} F_k$. We stress that the key rate in Eq. (A14) is valid for any observed statistics $\vec{F}^{\text{obs}}$, and that we simply choose our simulation to output observed statistics equal to the expected honest channel behavior. The tolerances in the statistics given by Eqs. (A17) are a consequence of the security proof and are required even in the case of an honest channel implementation in order to account for finite-size statistical fluctuations.

7. Modeling the channel

a. Loss

We simulate loss by attenuating the mean photon number of Alice's prepared state. Given a loss of λ (in dB), the channel transmittance is defined as

$$\eta = 10^{-\lambda/10}. \quad (\text{A19})$$

In order to model lost signals due to a lossy quantum channel, we perform the following map to the phase-randomized weak

coherent pulse:

$$\frac{1}{2\pi} \int_0^{2\pi} |\mu e^{i\theta}\rangle \langle \mu e^{i\theta}| d\theta \mapsto \frac{1}{2\pi} \int_0^{2\pi} |\eta \mu e^{i\theta}\rangle \langle \eta \mu e^{i\theta}| d\theta, \quad (\text{A20})$$

effectively attenuating the mean photon number from μ to $\mu' = \eta \mu$ [29].

b. Misalignment angle

In order to model physical rotations, we act on the incoming state $|\psi\rangle$ by a unitary rotation about the y axis as our protocols of interest use Z and X basis polarizations. This yields the map

$$\Phi^\theta(\rho) = e^{-i\theta \vec{a}^\dagger \sigma_Y \vec{a}} \rho e^{i\theta \vec{a}^\dagger \sigma_Y \vec{a}}, \quad (\text{A21})$$

where σ_Y is the Y Pauli matrix, θ is the physical misalignment angle [30], and $\vec{a}^\dagger = [\hat{a}_H^\dagger, \hat{a}_V^\dagger]$.

c. Depolarization and visibility

In the qubit case, one can simulate errors caused by misalignment in random directions by depolarization. Specifically, let $|\psi\rangle$ be some general qubit state. We can assume that

it has real entries in measurement basis $\{|0\rangle, |1\rangle\}$ if we only encode signals in the Z and X bases. It then follows that

$$\begin{aligned}\rho &= \frac{1}{2}[\Phi^\theta(\rho_0) + \Phi^{-\theta}(\rho_0)] \\ &= \frac{1}{2}(e^{i\theta\sigma_Y}\rho_0 e^{-i\theta\sigma_Y} + e^{-i\theta\sigma_Y}\rho_0 e^{i\theta\sigma_Y}) \\ &= \rho_0(\cos^2\theta - \sin^2\theta) + \sin^2\theta \mathbb{1} \\ &= \rho_0(1 - 2\sin^2\theta) + \frac{2\sin^2\theta}{2}\mathbb{1},\end{aligned}$$

where $\rho_0 = |\psi\rangle\langle\psi|$ and Φ^θ is defined in Appendix A 7b. Note that here the rotation is reduced to the rotation on the Bloch sphere for the qubit case. We obtain the standard depolarization channel on the qubit with depolarization probability $p_{\text{error}} = 2\sin^2\theta$. Therefore, in order to simulate a multiphoton analogy to visibility and loss of coherence [21], we simulate two separate channel observations with some physical misalignment angle of φ and another with physical misalignment of $-\varphi$ to generate observations

$$\vec{F}^{\text{obs}} = \frac{1}{2}(\vec{F}_{+\varphi} + \vec{F}_{-\varphi}). \quad (\text{A22})$$

In the qubit case, depolarization is characterized by channel visibility $V \in [0, 1]$. The probability of introducing an error in a signal is then $p_{\text{error}} = \frac{1-V}{2}$. Here, we inherit this idea and define the angle

$$\varphi = \frac{1}{2} \arccos(V). \quad (\text{A23})$$

Our construction of $\vec{F}^{\text{obs}}$ reduces to the usual depolarized observations with channel visibility V for qubits.

APPENDIX B: KRAUS OPERATORS FOR BB84

We compute the Kraus operators from Appendix A 4. In general, Alice's POVM elements are

$$\begin{aligned}\Gamma_{Z,0}^A &= \Gamma_1^A = \sum_{n=0}^{K+1} |n\rangle\langle n| \otimes |1\rangle\langle 1| \\ \Gamma_{Z,1}^A &= \Gamma_2^A = \sum_{n=0}^{K+1} |n\rangle\langle n| \otimes |2\rangle\langle 2| \\ \Gamma_{X,0}^A &= \Gamma_3^A = \sum_{n=0}^{K+1} |n\rangle\langle n| \otimes |3\rangle\langle 3| \\ \Gamma_{X,1}^A &= \Gamma_4^A = \sum_{n=0}^{K+1} |n\rangle\langle n| \otimes |4\rangle\langle 4|\end{aligned} \quad (\text{B1})$$

Note that the PNS attack allows Eve to gain full information of signals with multiphoton components. Therefore, in BB84, we set the photon number cutoff to be $K = 1$. Bob's POVM elements, as they lie in the $n \leq 1$ photon space, are

$$\begin{aligned}\Gamma_{Z,0}^B &= \Gamma_H^B = p_Z |0\rangle\langle 0| = p_Z \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\ \Gamma_{Z,1}^B &= \Gamma_V^B = p_Z |1\rangle\langle 1| = p_Z \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix},\end{aligned}$$

$$\begin{aligned}\Gamma_{X,0}^B &= \Gamma_+^B = p_X |+\rangle\langle +| = \frac{1-p_Z}{2} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\ \Gamma_{X,1}^B &= \Gamma_-^B = p_X |-\rangle\langle -| = \frac{1-p_Z}{2} \begin{pmatrix} 1 & -1 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \\ \Gamma_\perp^B &= |\perp\rangle\langle \perp| = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.\end{aligned} \quad (\text{B2})$$

Note that we discard basis mismatched announcements and vacuum signals. We apply isometries to eliminate redundant registers. The resulting Kraus operators are

$$\begin{aligned}K_Z &:= K_{\alpha=Z, \beta=Z} = (|0\rangle_R \otimes \sqrt{\Gamma_{Z,0}^A} + |1\rangle_R \otimes \sqrt{\Gamma_{Z,1}^A}) \\ &\quad \otimes \sqrt{p_Z}(\mathbb{1}_{2 \times 2} \oplus 0)_B \otimes |0\rangle_C\end{aligned} \quad (\text{B3})$$

and

$$\begin{aligned}K_X &:= K_{\alpha=X, \beta=X} = (|0\rangle_R \otimes \sqrt{\Gamma_{X,0}^A} + |1\rangle_R \otimes \sqrt{\Gamma_{X,1}^A}) \\ &\quad \otimes \sqrt{p_X}(\mathbb{1}_{2 \times 2} \oplus 0)_B \otimes |1\rangle_C,\end{aligned} \quad (\text{B4})$$

where C is a two-dimensional register, resulting in a $\mathcal{G}$ map,

$$\mathcal{G}(\rho) = K_Z \rho K_Z^\dagger + K_X \rho K_X^\dagger. \quad (\text{B5})$$

APPENDIX C: KRAUS OPERATORS FOR NPAB BB84

Alice and Bob perform the same measurements and so the resulting POVM elements are the same as in Appendix B. However, only a single announcement is made announcing the signal that is detected. The Kraus operator is thus

$$\begin{aligned}K_N &:= K_{\beta=\text{detect}} \\ &= (|0\rangle_R \otimes |0\rangle_X \otimes \sqrt{\Gamma_{Z,0}^A} + |1\rangle_R \otimes |0\rangle_X \otimes \sqrt{\Gamma_{Z,1}^A} \\ &\quad + |0\rangle_R \otimes |1\rangle_X \otimes \sqrt{\Gamma_{X,0}^A} + |1\rangle_R \otimes |1\rangle_X \otimes \sqrt{\Gamma_{X,1}^A}) \\ &\quad \otimes (\mathbb{1}_{2 \times 2} \oplus 0)_B,\end{aligned} \quad (\text{C1})$$

where the register X now encodes Alice's basis choice, and the register C is one dimensional and thus trivial. The resulting $\mathcal{G}$ map is

$$\mathcal{G}(\rho) = K_N \rho K_N^\dagger. \quad (\text{C2})$$

APPENDIX D: KRAUS OPERATORS FOR SARG04

Alice and Bob again perform the same measurements and so the resulting POVM elements are the same as in Appendix B. The announcement structure of SARG04 yields multiple Kraus operators for the $\mathcal{G}$ map. As only the $\beta = 1$

announcement survives sifting, the Kraus operators are

$$\begin{aligned}
 K_1 := K_{\alpha=1} &= \left(|0\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{Z,0}^A \otimes \sqrt{1-p_Z} |-\rangle \langle -|_B + |1\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{X,0}^A \otimes \sqrt{p_Z} |1\rangle \langle 1|_B \right) \otimes |1\rangle_C, \\
 K_2 := K_{\alpha=2} &= \left(|0\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{Z,1}^A \otimes \sqrt{1-p_Z} |-\rangle \langle -|_B + |1\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{X,0}^A \otimes \sqrt{p_Z} |0\rangle \langle 0|_B \right) \otimes |2\rangle_C, \\
 K_3 := K_{\alpha=3} &= \left(|0\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{Z,1}^A \otimes \sqrt{1-p_Z} |+\rangle \langle +|_B + |1\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{X,1}^A \otimes \sqrt{p_Z} |0\rangle \langle 0|_B \right) \otimes |3\rangle_C, \\
 K_4 := K_{\alpha=4} &= \left(|0\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{Z,0}^A \otimes \sqrt{1-p_Z} |+\rangle \langle +|_B + |1\rangle_R \otimes \sqrt{\frac{1}{2}} \Gamma_{X,1}^A \otimes \sqrt{p_Z} |1\rangle \langle 1|_B \right) \otimes |4\rangle_C.
 \end{aligned} \tag{D1}$$

The resulting $\mathcal{G}$ map is

$$\mathcal{G}(\rho) = \sum_{i=1}^4 K_i \rho K_i^\dagger. \tag{D2}$$

Note that each of Alice's POVMs has an additional $\frac{1}{2}$ to indicate the fact that given Alice is sending a particular polarization, Alice randomly chooses one of the two different equal probable announcements and associates it with this signal.

APPENDIX E: OPTIMAL MISALIGNMENT ANGLE FOR LOSSLESS QUBIT NPAB BB84

The NPAB BB84 protocol's performance can be increased by introducing intentional misalignment between Alice and Bob's devices, relative to an honest implementation. In this appendix, we argue that the form of the cost of error correction implies the existence of an optimal misalignment angle which is nonzero in the qubit case, with the intuition developed here holding in the photonic implementation. Assuming an asymptotic protocol such that the Devetak-Winter formula [14,31] holds,

$$R_\infty = \min_{\rho \in \mathcal{S}} [H(R|E)_\rho - H(R|Y)_\rho], \tag{E1}$$

where R is Alice's key register, E is Eve's side information, and Y is Bob's postmeasurement and postsifting register. Note that for NPAB BB84, Y is a register on Bob's full measurement alphabet $\mathcal{Y} = \{0, 1, +, -\}$. Under channel rotation, we observe that the privacy amplification term $H(R|E)$ is constant, while the error correction cost $H(R|Y)$ varies as the channel misalignment θ varies⁷ (Fig. 15). This is because, unlike depolarizing noise, a simple misalignment does not change how much Eve can learn about a sent state. As a result, the asymptotic constraint set $\mathcal{S}$ still contains the same set of states. The state ρ_{RYE} comes from Alice and Bob implementing their measurements and classical announcements on the joint state ρ_{ABE} . This state can be thought of as Eve

acting on the source-replaced state in Eq. (A2), which in the single-photon subspace may be written as

$$\begin{aligned}
 |\psi\rangle_{AA'} &= \sqrt{\frac{p_Z}{2}} (|00\rangle_{AA'} + |01\rangle_{AA'}) + \sqrt{\frac{p_X}{2}} (|2+\rangle_{AA'} \\
 &\quad + |3-\rangle_{AA'}),
 \end{aligned} \tag{E2}$$

where $\mathcal{H}_A \cong \mathbb{C}^4$, $\mathcal{H}_{A'} \cong \mathbb{C}^2$ and we have neglected $\mathcal{H}_{A_S} \cong \mathbb{C}$. We consider a four-dimensional Alice system since this protocol is equivalent and analytically easier to work with. It is known from the literature that unitary transformations of the signal states do not provide more information about the choice of bit to Eve, with Alice and Bob being able to eliminate attacks from the full fine-grained statistics [32]. In other words, even though unitary operations on the outgoing states changes the constraining values forming $\vec{F}^{\text{obs}}$, the underlying constraint set $\mathcal{S}$ constructed from them contains the same set of states. This matches what we observe in our results. Given this, for the remainder of the appendix, we focus on the error correction of the key rate.

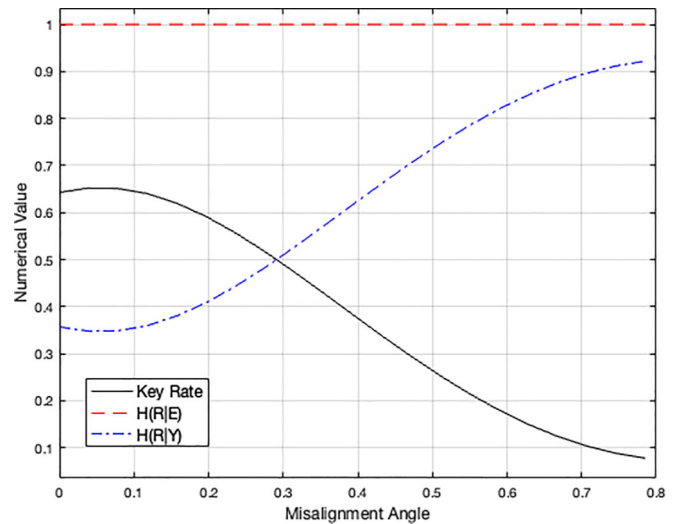


FIG. 15. Numerically evaluated asymptotic key rate for qubit NPAB BB84. Note that the cost of error correction $H(R|Y)$ varies, but has a nontrivial optimal.

⁷We observe the same trend at different loss regimes for photonic implementations as well. We omit these plots since they only complicate the analysis.

TABLE III. Joint probability distribution function for classical registers R , Y and their associated random variables $\mathbf{R}$, $\mathbf{Y}$.

	$\mathbf{Y} = "0"$	$\mathbf{Y} = "1"$	$\mathbf{Y} = "+"$	$\mathbf{Y} = "-"$
$\mathbf{R} = "0"$	$\frac{p_Z(p_Z \cos 2\theta - p_X \sin 2\theta + 1)}{4}$	$\frac{p_Z(p_X \sin 2\theta - p_Z \cos 2\theta + 1)}{4}$	$\frac{p_X(p_X \cos 2\theta + p_Z \sin 2\theta + 1)}{4}$	$\frac{p_X(-p_X \cos 2\theta - p_Z \sin 2\theta + 1)}{4}$
$\mathbf{R} = "1"$	$\frac{p_X(p_X \sin 2\theta - p_Z \cos 2\theta + 1)}{4}$	$\frac{p_Z(p_Z \cos 2\theta - p_X \sin 2\theta + 1)}{4}$	$\frac{p_X(-p_X \cos 2\theta - p_Z \sin 2\theta + 1)}{4}$	$\frac{p_X(p_X \cos 2\theta + p_Z \sin 2\theta + 1)}{4}$

θ dependence of error correction

We now examine how the cost of error correction does change as one introduces misalignment in the quantum channel or if Alice prepares rotated states. For the sake of argument, we will suppose the statistics are generated from Eve's attack channel being the identity operation

$$\mathcal{E}_{A'E \rightarrow BE} = \text{id}_{A' \rightarrow B} \otimes \text{id}_E. \quad (\text{E3})$$

In this case, given that we know the state $|\rho\rangle_{ABE}$ exactly allows for a simple calculation to develop intuition. Recall

that we model a misalignment channel via the unitary operation Φ^θ defined in Eq. (A21). On the single-photon subspace ($a_H^\dagger|\text{vac}\rangle \cong (1, 0) \cong |0\rangle$, $a_V^\dagger|\text{vac}\rangle \cong (0, 1) \cong |1\rangle$), the mapping takes on the simple form of⁸ [30]

$$\Phi^\theta : \rho \mapsto R_\theta \rho R_\theta^\dagger; R_\theta := \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}. \quad (\text{E4})$$

With R_θ defined, we may compute the source-replaced state after misalignment to be

$$\begin{aligned} |\psi_\theta\rangle_{AA'} = & \sqrt{\frac{p_Z}{2}} [|0\rangle_A (\cos \theta |0\rangle_{A'} + \sin \theta |1\rangle_{A'}) + |1\rangle_A (-\sin \theta |0\rangle_{A'} + \cos \theta |1\rangle_{A'})] + \sqrt{\frac{p_X}{2}} \left\{ \frac{1}{\sqrt{2}} |2\rangle_A [(\cos \theta - \sin \theta) |0\rangle_{A'} \right. \\ & \left. + (\cos \theta + \sin \theta) |1\rangle_{A'}] + \frac{1}{\sqrt{2}} |3\rangle_A [(\cos \theta + \sin \theta) |0\rangle_{A'} + (-\sin \theta + \cos \theta) |1\rangle_{A'}] \right\}, \end{aligned} \quad (\text{E5})$$

which we suppose is then transmitted through the honestly implemented channel (i.e., $\mathcal{E}_{A' \rightarrow B} = \text{id}_{A' \rightarrow B}$, $\mathcal{H}_{A'} \cong \mathcal{H}_B$). After measuring their respective systems with the POVMs,

$$\Gamma^A = \{|i\rangle\langle i|\}_{i=0}^3, \Gamma^B = \{p_b |\psi_{b,i}\rangle\langle \psi_{b,i}|\}_{b=X,Z, i=0,1}, \quad (\text{E6})$$

the two parties induce the joint probability distribution $p(x, y)$, which Alice then coarse grains ($x = 0, 2 \mapsto r = 0$ and $x = 1, 3 \mapsto r = 1$) in order to generate the distribution $p(r, y)$. A tedious but straightforward calculation yields the probability distribution listed in Table III, from which one may calculate the cost of error correction. Since the register R is two dimensional, the entropy takes on the simple form of

$$\begin{aligned} H(R|Y)_\rho &= - \sum_y p(y)_\rho H(R|Y = y)_\rho \\ &= \sum_y [p(0, y) + p(1, y)] h\left(\frac{p(0, y)}{p(0, y) + p(1, y)}\right), \end{aligned} \quad (\text{E7})$$

where $h(x) := -x \log_2 x - (1 - x) \log_2 (1 - x)$, and we have dropped the subscript ρ . We find that the expression then simplifies to

$$\begin{aligned} H(R|Y) = & \frac{p_Z}{2} [h(1/2(p_Z \cos 2\theta - p_X \sin 2\theta + 1)) \\ & + h(-1/2(p_Z \cos 2\theta - p_X \sin 2\theta - 1))] \\ & + \frac{p_X}{2} [h(1/2(p_X \cos 2\theta + p_Z \sin 2\theta + 1)) \\ & + h(-1/2(p_X \cos 2\theta + p_Z \sin 2\theta - 1))], \end{aligned} \quad (\text{E8})$$

which simplifies to

$$\begin{aligned} H(R|Y) = & p_Z h[1/2(p_Z \cos 2\theta - p_X \sin 2\theta + 1)] \\ & + p_X h[1/2(p_X \cos 2\theta + p_Z \sin 2\theta + 1)]. \end{aligned} \quad (\text{E9})$$

One may then analytically solve for the roots

$$\frac{\partial}{\partial \theta} H(R|Y)|_{\theta^*} = 0 \quad (\text{E10})$$

using software such as MAPLE to find

$$\theta^* = 1/2 \arctan(p_Z/p_X). \quad (\text{E11})$$

For our simulation parameters of $p_Z = 0.1$, we find that $\theta^* \approx 0.055$. This coincides with the numerically evaluated values we find in Fig. 3 in the asymptotic regime. For Figs. 13 and 14 in the finite-size regime, we observe that the optimal angle shifts towards zero as the number of signals that are used decreases. Since the cost of error correction is independent of loss, we ascribe this to finite-size effects enlarging the constraint set $\mathcal{V}(\bar{F}^{\text{obs}})$.

⁸Note that this is not a Bloch sphere (logical) rotation, but a physical rotation. For this reason, we do not use $\theta/2$.

- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.
- [2] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Quantum cryptography with coherent states, *Phys. Rev. A* **51**, 1863 (1995).
- [3] N. Lütkenhaus and M. Jähma, Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack, *New J. Phys.* **4**, 44 (2002).
- [4] W.-Y. Hwang, Quantum key distribution with high loss: Toward global secure communication, *Phys. Rev. Lett.* **91**, 057901 (2003).
- [5] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, *Phys. Rev. Lett.* **94**, 230504 (2005).
- [6] X.-B. Wang, Beating the photon-number-splitting attack in practical quantum cryptography, *Phys. Rev. Lett.* **94**, 230503 (2005).
- [7] V. Zapatero, Á. Navarrete, K. Tamaki, and M. Curty, Security of quantum key distribution with intensity correlations, *Quantum* **5**, 602 (2021).
- [8] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations, *Phys. Rev. Lett.* **92**, 057901 (2004).
- [9] W. Y. Hwang, I. G. Koh, and Y. D. Han, Quantum cryptography without public announcement of bases, *Phys. Lett. A* **244**, 489 (1998).
- [10] S. Lin and X.-F. Liu, A modified quantum key distribution without public announcement bases against photon-number-splitting attack, *Intl. J. Theor. Phys.* **51**, 2514 (2012).
- [11] Y. Kurochkin, Quantum cryptography with floating basis protocol, in *Quantum Informatics 2004* (SPIE, 2005), Vol. 5833, pp. 213–221.
- [12] A. S. Trushechkin, P. A. Tregubov, E. O. Kiktenko, Y. V. Kurochkin, and A. K. Fedorov, Quantum-key-distribution protocol with pseudorandom bases, *Phys. Rev. A* **97**, 012311 (2018).
- [13] O. Gittsovich, N. J. Beaudry, V. Narasimhachar, R. R. Alvarez, T. Moroder, and N. Lütkenhaus, Squashing model for detectors and applications to quantum-key-distribution protocols, *Phys. Rev. A* **89**, 012325 (2014).
- [14] A. Winick, N. Lütkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [15] D. Tupkary, E. Y.-Z. Tan, and N. Lütkenhaus, Security proof for variable-length quantum key distribution, *Phys. Rev. Res.* **6**, 023002 (2024).
- [16] L. Kamin, D. Tupkary, and N. Lütkenhaus, Improved finite-size effects in quantum key distribution with applications to decoy-state protocols, *Phys. Rev. Res.* **8**, 013332 (2026).
- [17] J. Burniston, W. Wang, L. Kamin, J. Lin, P. Coles, E. Metodieva, I. George, N. K. H. Li, K. Fang, M. Chemtov, Y. Zhang, C. Böhm, A. Winick, T. van Himbeec, S. Johnstun, S. Nahar, D. Tupkary, S. Pan, Z. Wang, A. Corrigan, *et al.*, Open QKD security [Computer software] Zenodo, 2024, <https://doi.org/10.5281/zenodo.14262569>.
- [18] C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Security of two quantum cryptography protocols using the same four qubit states, *Phys. Rev. A* **72**, 032301 (2005).
- [19] S. Nahar, T. Upadhyaya, and N. Lütkenhaus, Imperfect phase randomization and generalized decoy-state quantum key distribution, *Phys. Rev. Appl.* **20**, 064031 (2023).
- [20] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, *Phys. Rev. X* **9**, 041064 (2019).
- [21] B. Kraus, C. Branciard, and R. Renner, Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses, *Phys. Rev. A* **75**, 012316 (2007).
- [22] D. A. Vajner, L. Rickert, T. Gao, K. Kaymazlar, and T. Heindel, Quantum communication using semiconductor quantum dots, *Adv. Quantum Technol.* **5**, 2100116 (2022).
- [23] See <https://github.com/Optical-Quantum-Communication-Theory/VaryingAnnouncementStructuresWithWCP> for the source code used in this paper.
- [24] A. Ferenczi and N. Lütkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, *Phys. Rev. A* **85**, 052310 (2012).
- [25] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a precondition for secure quantum key distribution, *Phys. Rev. Lett.* **92**, 217903 (2004).
- [26] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, General paradigm for distilling classical key from quantum states, in *IEEE Transactions on Information Theory* (IEEE, 2009), Vol. 55, pp. 1898–1929.
- [27] N. Lütkenhaus, Generalised measurements and quantum cryptography, Ph.D. thesis, University of Strathclyde, 1996.
- [28] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Security of quantum key distribution with imperfect devices, [arXiv:quant-ph/0212066](https://arxiv.org/abs/quant-ph/0212066).
- [29] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Security aspects of practical quantum cryptography, in *Advances in Cryptology—EUROCRYPT 2000*, edited by B. Preneel (Springer, Berlin, 2000), pp. 289–299.
- [30] U. Leonhardt, *Essential Quantum Optics: From Quantum Measurements to Black Holes* (Cambridge University Press, Cambridge, 2010).
- [31] I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states, *Proc. R. Soc. A* **461**, 207 (2005).
- [32] W. Wang and N. Lütkenhaus, Numerical security proof for the decoy-state BB84 protocol and measurement-device-independent quantum key distribution resistant against large basis misalignment, *Phys. Rev. Res.* **4**, 043097 (2022).