

Composable finite-size security of high-dimensional quantum-key-distribution protocols

Florian Kanitschar^{1,2,*} and Marcus Huber^{1,3}

¹*Vienna Center for Quantum Science and Technology (VCQ), Atominstitut, Technische Universität Wien, Stadionallee 2, 1020 Vienna, Austria*

²*AIT Austrian Institute of Technology, Center for Digital Safety&Security, Giefinggasse 4, 1210 Vienna, Austria*

³*Institute for Quantum Optics and Quantum Information (IQOQI), Austrian Academy of Sciences, Boltzmanngasse 3, 1090 Vienna, Austria*



(Received 8 February 2025; revised 2 September 2025; accepted 17 October 2025; published 10 November 2025)

Practical implementations of quantum key distribution (QKD) extending beyond urban areas commonly use satellite links; however, the transmission of quantum states through the Earth's atmosphere is highly susceptible to noise, restricting its application primarily to nighttime. High-dimensional (HD) QKD offers a promising solution to this limitation by employing high-dimensionally entangled quantum states. Although experimental platforms for HD QKD exist, previous security analyses have been limited to the asymptotic regime and have either relied on impractical measurements or employed computationally demanding convex optimization tasks, restricting the security analysis to low dimensions. In this work, we bridge this gap by presenting a composable finite-size security proof against both collective and coherent attacks for a general HD QKD protocol that uses only experimentally accessible measurements. In addition to the conventional yet impractical “one-shot” key rates, we provide a practical variable-length security argument that yields significantly higher expected key rates. This approach is particularly crucial under rapidly changing and turbulent atmospheric conditions, as encountered in free-space and satellite-based QKD platforms.

DOI: [10.1103/v51y-vkfr](https://doi.org/10.1103/v51y-vkfr)

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] enables two remote parties, commonly called Alice and Bob, to establish cryptographically secure keys without relying on assumptions on the hardness of mathematical problems. Over recent decades, significant advancements in both experimental techniques and security proofs have evolved QKD from an interesting scientific concept toward one of the most developed quantum technologies [3–5], and it is now on the edge of practical use for both private and governmental applications. Implementations range from fiber links [6–10] for urban areas to free-space [11,12] and satellite-based links [13–17] that span countries and even continents. Although the transmission of quantum signals through the atmosphere offers a more favorable loss profile compared to fiber-based systems, it also suffers from

high noise sensitivity, which essentially restricts operation to nighttime hours.

High-dimensional quantum states [18–20] have proven to enhance noise tolerance in entanglement distribution tasks [21], making high-dimensional quantum key distribution (HD QKD) a promising candidate for improving noise robustness in cryptographic tasks. Nonetheless, the security analysis of practically implementable HD QKD protocols is so far rather uncharted. Previous works have primarily focused on asymptotic security, employing either analytical methods [22–26] that leverage symmetry arguments or numerical approaches [27] involving convex optimization [28–30]. Analytical arguments often require 2 or even $d + 1$ mutually unbiased bases measurements, which is impractical, particularly for large dimensions. Numerical methods avoid this but require solving very-high-dimensional convex optimization problems, which are computationally demanding and highly memory intensive, rendering them infeasible even for low to medium dimensions [27]. Our recent work in Ref. [31] has closed the gap between experimentally available setups [32–36] and asymptotic security by providing an efficient semi-analytic method to evaluate key rates for practical HD QKD setups, relying solely on practically implementable

*Contact author: florian.kanitschar@outlook.com

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

measurements. Yet, the security of high-dimensional QKD protocols in the finite-size regime remains an open question.

In this study, we address this issue by presenting a full, composable finite-size security proof for general high-dimensional QKD protocols. We begin by outlining the general HD QKD protocol in Sec. II. Section III details our statistical testing procedure and establishes composable finite-size security against independent and identically distributed (IID) collective attacks. We then apply the postselection technique [37,38] to extend security to coherent attacks. These secure key rates refer to the so-called fixed-length scenario, which is commonly reported in the literature; however, in practical settings, in particular for atmospheric channels, the quantum channel's instability complicates the predefinition of accepted statistics before the execution of the protocol, as required by the security argument. This leads to a high abort rate of the protocol and low effective key rates. To address this, in Sec. IV, we give a variable-length security argument for a variable-length version of our protocol [39], again proving composable finite-size variable-length security against both IID collective and coherent attacks. Finally, in Sec. V, we apply our recent method [31] and present both variable- and fixed-length key rates in Sec. VI.

II. PROTOCOL

We analyze a general high-dimensional, entanglement-based QKD protocol of dimension d , which consists of the following steps:

(1) State generation. A photon source distributes entangled quantum states ρ_{AB} to Alice and Bob.

(2) Measurement. Alice and Bob randomly and independently decide to measure either in their computational bases, represented by positive operator-valued measures (POVMs) $\{A_1^x\}_{x=0}^{d-1}$ and $\{B_1^y\}_{y=0}^{d-1}$, or in one of the test bases, represented by POVMs $\{A_b^x\}_{x=0}^{d-1}$ and $\{B_b^y\}_{y=0}^{d-1}$ for $b \in \{2, \dots, n_{\text{bases}}\}$, where n_{bases} denotes the total number of bases used in the protocol, and record their outcomes in their respective private registers $\bar{A}$ and $\bar{B}$. Practically, this can be implemented either passively via beam splitters or using active switching with random numbers. We denote the probability that basis i is chosen by $p_i \geq 0$, and d is the dimension of the protocol.

Steps (1) and (2) are repeated N times. Once these measurements are complete, Alice may announce a random permutation, which both parties then apply to their data.

(3) Public announcements and sifting. Alice and Bob use the classical authenticated channel to communicate their measurement choice to each other and may discard certain results. Therefore, Bob announces the time stamps of his single clicks, and Alice checks which of those singles lie in her predefined coincidence window. Then, Alice announces her random measurement setting for those

rounds, where she recorded a single in the corresponding window. Other rounds are discarded. Their announcements are stored in their public registers $\tilde{A}$ and $\tilde{B}$.

(4) Acceptance testing. The communicating parties disclose a randomly chosen subset consisting of k_T of their measurement results over the public channel and perform a so-called acceptance test (see Theorem 1). This test helps them to define a set $\mathcal{S}^{\text{AT}}$. They may also announce that they will perform subspace postselection.

(5) Key map. Based on their announcements and their measurement results, one party performs a key map g , which formalizes the process of assigning a logical bit value $\{0, \dots, d-1\}$ to each of the remaining $N - k_T$ rounds as a function of the publicly known announcements and the private measurement data. This step also may allow discarding certain rounds (by assigning the symbol $\perp$ or, more efficiently, by directly shortening the string [39]). If Alice performs the key map, this is called direct reconciliation; if Bob performs it, it is called reverse reconciliation.

(6) Error correction and error verification. On the remaining $N - k_T$ rounds, Alice and Bob perform error correction to reconcile their raw keys X and Y , which leaks some information to an adversary, Eve. This is followed by error verification, where Alice chooses a two-universal hash function that hashes to $\lceil \log_2(1/\epsilon_{\text{EV}}) \rceil$ bits and sends them to Bob, who applies the same hash function and compares them.

(7) Privacy amplification. Finally, they perform privacy amplification, where they map their reconciled key to a shorter one, aiming to decouple Eve from their shared randomness.

III. SECURITY ARGUMENT

In this work, we aim to demonstrate the composable security of a generic high-dimensional QKD protocol against coherent attacks in the finite-size regime. This task, however, presents several challenges compared to the asymptotic analysis carried out in Ref. [31]. Although in the asymptotic regime, the law of large numbers justifies assuming that our measurement outcomes are known with certainty, in the finite-size regime, we need to thoroughly design and perform an acceptance test. The acceptance test carefully compares the observations with the expected channel behavior. If the test passes, the analysis proceeds on the set of all states that are ϵ_{AT} -likely to be compatible with our observations. Instead of considering a plethora of attack strategies that Eve could follow (a nearly impossible task), this allows us to base the security argument solely on the observations made by the communicating parties; however, the direct use of the measured statistics, as is common in discrete-variable QKD, for HD QKD performed in practical measurement setups still requires numerical security arguments. As identified in Ref. [27], these methods suffer

from serious limitations due to complexity issues, which motivated the development of a semianalytic security argument for practical HD-QKD setups in Ref. [31]. This work avoids the use of full statistics, allowing for direct solutions and bypassing highly demanding numerical convex optimization routines; however, it also means that we have to construct the acceptance set based on suitable coarse-grained statistics. Additionally, we need to take into account that all subroutines used for the QKD protocol may fail with a certain probability, such as error verification failing to align the keys between Alice and Bob or privacy amplification failing to decouple Eve from the final key. Each of these contributions has to be carefully taken into account in a composable security argument. Proving composable finite-size security against coherent attacks is inherently challenging, as most available arguments rely on an assumed IID structure of the underlying quantum states. Consequently, a lift from collective IID to coherent attacks is required.

We address these issues as follows. Initially, we consider collective IID attacks, where Eve prepares a fresh ancilla state that interacts identically with each protocol round. She may then store this ancilla state in her quantum memory and wait until Alice and Bob have finished executing their QKD protocol, including their announcements, before measuring her quantum memory. Mathematically, this implies that different rounds are uncorrelated and that Alice's and Bob's shared state has the tensor-product structure $\rho = \rho_{AB}^{\otimes N}$. We then adapt an argument by Refs. [40,41] to our needs and formulate an acceptance test with nonunique acceptance criteria. Based on this test, we prove composable security within Renner's ϵ -security framework [42]. Finally, we apply the postselection technique [37,38] to lift our collective IID key rates to secure key rates against coherent attacks, thereby completing the proof.

A. Security against IID collective attacks

The first goal of our security argument is to prove the security of the considered protocol against coherent attacks. We aim to tackle this task in two steps: we first prove security against IID collective attacks, and we then lift our proof to coherent attacks. For our collective-attacks argument, we follow the ϵ -security framework by Renner [42]. Thus, for now, let us assume IID collective attacks; i.e., Alice's and Bob's shared quantum state after N rounds of transmission has the tensor-product structure $\rho_{AB} = \tau_{AB}^{\otimes N}$. Let $\rho_{ABE} = \tau_{ABE}^{\otimes N}$ be a purification of this state, held by Eve. Alice and Bob then randomly select k_T of those rounds for statistical testing.

Formally, this means we need to construct a set of ϵ_{AT} -filtered states [40,42], which is a set $(\mathcal{S}^{AT})^c$ of quantum states σ leading to an accepted statistics with probability less than ϵ_{AT} , $\Pr[\text{accept}|\sigma] \leq \epsilon_{AT}$. In other words, our goal

is to define a set $\mathcal{S}^{AT}$ such that all states in its complement $(\mathcal{S}^{AT})^c$ could have generated the accepted statistics only with probability less than ϵ_{AT} . Intuitively, this allows us to split the set of all quantum states into two subsets: the set of states that are very unlikely to have produced the observed statistics, and the set of states that have potentially caused our observations. We formalize this notion in Theorem 1, which is an adapted version of Theorem 3 in Ref. [41].

Theorem 1 (Acceptance test [41]). Let Θ be the set of Alice's and Bob's observables. Let $\mathbf{r} \in \mathbb{R}^{|\Theta|}$ and $\mathbf{t} \in \mathbb{R}_{\geq 0}^{|\Theta|}$, where $|\Theta|$ denotes the cardinality of Θ and choose $\epsilon_{AT} > 0$. Define the set of accepted statistics as

$$\mathcal{O} := \{\mathbf{v} \in \mathbb{R}^{|\Theta|} : \forall X \in \Theta, |v_X - r_X| \leq t_X\}, \quad (1)$$

and the corresponding acceptance set as

$$\mathcal{S}^{AT} := \{\sigma \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) : \forall X \in \Theta, |\text{Tr}[\sigma X] - r_X| \leq \mu_X + t_X\}, \quad (2)$$

where r_X is the X th element of the vector $\mathbf{r}$ and likewise for t_X . For every $X \in \Theta$, let

$$\mu_X := \sqrt{\frac{2x^2}{m_X} \ln\left(\frac{2}{\epsilon_{AT}}\right)},$$

where $x := \|X\|_\infty$ and m_X is the number of tests for the observable X . If $\rho \notin \mathcal{S}^{AT}$, then the probability of accepting the statistics generated by the IID measurements of $\rho^{\otimes n}$ is bounded above by ϵ_{AT} . That is, the complement of $\mathcal{S}^{AT}$ consists of all ϵ_{AT} -filtered states.

Let us denote the event of the acceptance test passing by $\mathcal{P}$. Note that we never actually know which state Alice and Bob received but only use the measurement results and the testing procedure to determine how to proceed with the protocol. Thus, we face four different cases:

- (a) $(\tau_{AB} \in \mathcal{S}^{AT}) \wedge \mathcal{P}_{AT}$ —the test passes for an input state in $\mathcal{S}^{AT}$,
- (b) $(\tau_{AB} \in \mathcal{S}^{AT}) \wedge \mathcal{P}_{AT}^c$ —the test fails for an input state in $\mathcal{S}^{AT}$,
- (c) $(\tau_{AB} \notin \mathcal{S}^{AT}) \wedge \mathcal{P}_{AT}$ —the test passes for an input state not in $\mathcal{S}^{AT}$,
- (d) $(\tau_{AB} \notin \mathcal{S}^{AT}) \wedge \mathcal{P}_{AT}^c$ —the test fails for an input state not in $\mathcal{S}^{AT}$.

While cases (a) and (d) correspond to the desired behavior of the test, note that in case (b), although the protocol erroneously aborts, it is nevertheless secure. By design of the acceptance-testing theorem, the probability that (c) occurs is bounded by ϵ_{AT} . Additionally, we denote the event that

the error-verification routine passes by $\mathcal{P}_{\text{EV}}$ and abbreviate the event of both passing by $\mathcal{P}$.

Composable security builds upon the following Gedankenexperiment [43]. The adversary is given the output of both the real and an idealized version of the QKD protocol and aims to distinguish between both protocols without having access to Alice's and Bob's private data. The ideal output is uniformly distributed and completely decoupled from Eve, $\rho_{\text{ideal}} := \pi_{K_A K_B} \otimes \rho_E$, where $\pi_{K_A K_B} := 1/|\mathcal{K}| \sum_{k \in \mathcal{K}} |k\rangle\langle k| \otimes |k\rangle\langle k|$. The output of the real protocol shall be denoted by $\rho_{K_A K_B E} := \Phi(\rho_{ABE})$, where Φ denotes the map representing the action of the protocol (which will be detailed on in Sec. VB). Then, we aim to bound the distinguishing advantage of an adversary,

$$\frac{1}{2} \left\| \rho_{K_A K_B E} - \pi_{K_A K_B} \otimes \rho_E \right\|_1 \leq \epsilon. \quad (3)$$

Since the protocol aborts and is trivially secure when the acceptance test fails [cases (b) and (d)], there is no distinguishing advantage for Eve in that case. Thus, we can focus on the cases where the test passes,

$$\begin{aligned} & \frac{1}{2} \left\| \rho_{K_A K_B E} - \pi_{K_A K_B} \otimes \rho_E \right\|_1 \\ &= 0 + \frac{1}{2} \left\| \rho_{K_A K_B E \wedge \mathcal{P}} - \pi_{K_A K_B} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \\ &\leq \frac{1}{2} \left\| \rho_{K_A K_B E \wedge \mathcal{P}} - \rho_{K_A K_A E \wedge \mathcal{P}} \right\|_1 \\ &\quad + \frac{1}{2} \left\| \rho_{K_A K_A E \wedge \mathcal{P}} - \pi_{K_A K_B} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \\ &\leq \epsilon_{\text{EV}} + \frac{1}{2} \left\| \rho_{K_A K_A E \wedge \mathcal{P}} - \pi_{K_A K_B} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1, \end{aligned}$$

where we used $\Pr[\mathcal{P}] \sigma_{A|\mathcal{P}} =: \sigma_{A \wedge \mathcal{P}}$. For the first inequality, we applied the triangle inequality, and for the second inequality, we used that the first term is bounded by ϵ_{EV} . To ease notation, we now drop Bob's key register, as it is equal to Alice's. For the second term, we use the fact that the remaining cases (a) and (c) are mutually exclusive, which leads to the upper bound

$$\begin{aligned} & \frac{1}{2} \left\| \rho_{K_A K_B E \wedge \mathcal{P}} - \pi_{K_A K_B} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \\ &\leq \max \left\{ \Pr[\tau_{AB} \in \mathcal{S}^{\text{AT}}] \frac{1}{2} \left\| \rho_{K_A E \wedge \mathcal{P}} - \pi_{K_A} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1, \right. \\ &\quad \left. \Pr[\tau_{AB} \notin \mathcal{S}^{\text{AT}}] \frac{1}{2} \left\| \rho_{K_A E \wedge \mathcal{P}} - \pi_{K_A} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \right\}. \end{aligned}$$

For a state $\tau_{AB} \notin \mathcal{S}^{\text{AT}}$, the distinguishability given that the test passes can be upper bounded by the probability of the test passing on a state that is not in the acceptance set,

which in turn is upper bounded by ϵ_{AT} ,

$$\begin{aligned} & \Pr[\tau_{AB} \notin \mathcal{S}^{\text{AT}}] \frac{1}{2} \left\| \rho_{K_A E \wedge \mathcal{P}} - \pi_{K_A} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \\ &\leq \Pr[\mathcal{P}_{\text{AT}} | \tau_{AB} \notin \mathcal{S}^{\text{AT}}] \leq \epsilon_{\text{AT}}. \end{aligned}$$

While we have now successfully treated cases (b)–(d), we are left with case (a), where Alice's and Bob's shared key is not fully private with respect to Eve. To decouple their key from Eve, the protocol requires Alice and Bob to perform privacy amplification. The leftover hashing lemma (Corollary 5.6.1 in Ref. [42]) relates the length of the hashed key to the security parameter,

$$\begin{aligned} & \frac{1}{2} \left\| \rho_{K_A E \wedge \mathcal{P}} - \pi_{K_A} \otimes \rho_{E \wedge \mathcal{P}} \right\|_1 \\ &\leq 2\tilde{\epsilon} + 2^{-\frac{1}{2} \left(H_{\min}^{\tilde{\epsilon}}(X|EC)_{\Phi^{(n)}(\rho_{ABE}) \wedge \mathcal{P}} - \ell \right)} \leq \epsilon_{\text{sec}}, \end{aligned}$$

where C denotes the transcript of the information-reconciliation phase. Thus, provided that the length of the hashed key satisfies

$$\ell \leq H_{\min}^{\tilde{\epsilon}}(X|EC)_{\Phi^{(n)}(\rho_{ABE}) \wedge \mathcal{P}} + 2 \log_2 (\epsilon_{\text{sec}} - 2\tilde{\epsilon}),$$

the key is secret with secrecy parameter ϵ_{sec} . Next, we use Lemma 10 of Ref. [44], $H_{\min}^{\tilde{\epsilon}}(X|EC)_{\sigma \wedge \mathcal{P}} \geq H_{\min}^{\tilde{\epsilon}}(X|EC)_{\sigma}$, as well as Lemma 6.4.1 of Ref. [42], to remove the information reconciliation transcript from the smooth min-entropy at the cost of introducing a leakage term leak_{IR} and arrive at

$$\ell \leq H_{\min}^{\tilde{\epsilon}}(X|E)_{\Phi^{(n)}(\rho_{ABE})} - \text{leak}_{\text{IR}} + 2 \log_2 (\epsilon_{\text{sec}} - 2\tilde{\epsilon}).$$

Our argument applies to every state in the acceptance set; however, as we are aiming for a reliable bound on the secure key rate, we need to find the worst-case state in this set, which is the state that minimizes the smooth min-entropy. This leads to

$$\begin{aligned} \ell &\leq \min_{\rho_{ABE} \in \mathcal{S}^{\text{AT}}} H_{\min}^{\tilde{\epsilon}}(X|E)_{\Phi^{(n)}(\rho_{ABE})} - \text{leak}_{\text{IR}} \\ &\quad + 2 \log_2 (\epsilon_{\text{sec}} - 2\tilde{\epsilon}). \end{aligned}$$

Let $n := N - k_T$ denote the number of rounds used for key generation. Since the smooth min-entropy of a quantum state is defined as the maximum of the min-entropy over all quantum states in an ϵ -ball around the considered quantum state, we can lower bound $H_{\min}^{\tilde{\epsilon}}(X|E)_{\Phi^{(n)}(\rho_{ABE})} \geq H_{\min}(X|E)_{\Phi^{(n)}(\rho_{ABE})}$ (i.e., set $\tilde{\epsilon} = 0$). Next, we use the fact that the min-entropy is additive for IID copies

(see Table 4.1 of Ref. [45]) and obtain

$$\ell \leq n \min_{\tau_{ABE} \in \mathcal{S}^{\text{AT}}} H(X|E)_{\Phi(\tau_{ABE})} - \text{leak}_{\text{IR}} + 2 \log_2(\epsilon_{\text{sec}}).$$

Thus, we choose $\epsilon_{\text{sec}} = \epsilon_{\text{PA}}$ and obtain a valid lower bound on the secure key rate provided that we choose ℓ such that

$$\ell \leq n \min_{\tau_{ABE} \in \mathcal{S}^{\text{AT}}} H_{\min}(X|E)_{\Phi(\tau_{ABE})} - \text{leak}_{\text{IR}} - 2 \log_2\left(\frac{1}{\epsilon_{\text{PA}}}\right) \quad (4)$$

with total security parameter $\epsilon := \epsilon_{\text{EV}} + \max\{\epsilon_{\text{AT}}, \epsilon_{\text{PA}}\}$. This concludes the security argument for IID collective attacks. We summarize this in Theorem 2.

Theorem 2 (Security statement for collective attacks). Let $\epsilon_{\text{EV}}, \epsilon_{\text{PA}}, \epsilon_{\text{AT}} > 0$. Let N be the total number of quantum signals exchanged, k_T the number of test rounds, and $n := N - k_T$. The general high-dimensional QKD protocol described in Sec. II is $\epsilon_{\text{EV}} + \max\{\epsilon_{\text{AT}}, \epsilon_{\text{PA}}\}$ -secure against IID collective attacks, if, in case the protocol does not abort, the secure key length ℓ is chosen such that

$$\ell \leq n \min_{\tau_{ABE} \in \mathcal{S}^{\text{AT}}} H_{\min}(X|E)_{\Phi(\tau_{ABE})} - \text{leak}_{\text{IR}} - 2 \log_2\left(\frac{1}{\epsilon_{\text{PA}}}\right), \quad (5)$$

where leak_{IR} denotes the leakage due to the information-reconciliation phase and $\mathcal{S}^{\text{AT}}$ is the acceptance set defined by the acceptance test in Theorem 1.

Leaving aside the technical details, for pre-fixed subroutine security parameters $\epsilon_{\text{EV}}, \epsilon_{\text{PA}}$, and ϵ_{AT} this theorem relates the achievable secure key length ℓ under collective attacks to an optimization problem over the set $\mathcal{S}^{\text{AT}}$, which we defined earlier in the acceptance test, along with correction terms due to error correction and privacy amplification. It turns out that the remaining optimization problem can now be solved using the method we introduced in our companion paper [31].

B. Lift to coherent attacks

It remains to lift the proof to coherent attacks, based on the postselection technique of Refs. [37,38]. We follow the notation used in Ref. [38]. This requires some additional notation. Recall that $\Phi : ABE \mapsto K_A K_B E$, where Eve's register E contains all information she gathered during the protocol execution, and define $\Phi^{(\ell)} := \text{Tr}_E \circ \text{Tr}_{K_B} \circ \Phi$, a QKD protocol map that produces a key of length ℓ upon acceptance. Additionally, let $\Phi_{\text{ideal}}^{(\ell)}$ be the corresponding ideal QKD protocol map. Now, in contrast to the first part of the proof, we assume a general $\rho_{ABE} = \rho_{A^n B^n E^n}$ without any known structure, so in particular $\rho_{ABE} \neq \tau_{ABE}^{\otimes n}$. After

splitting off the correctness part, similar to the argument above, the secrecy statement reads

$$\frac{1}{2} \left\| \left(\left(\Phi^{(\ell)} - \Phi_{\text{ideal}}^{(\ell)} \right) \otimes \text{id}_E^n \right) (\rho_{A^n B^n E^n}) \right\|_1 \leq \epsilon_{\text{sec}}. \quad (6)$$

Since we applied a random permutation to the classical data acquired during the protocol execution, for measurements that act only on single rounds, the considered protocol is permutation invariant such that the map $\Phi^{(\ell)} - \Phi_{\text{ideal}}^{(\ell)}$ is also permutation invariant (for a formal definition of permutation invariance of a map, we refer to Refs. [37,38]). For such maps, the postselection theorem (Theorem 1 of Ref. [37]) gives an upper bound on this expression in terms of a purification of so-called de Finetti states.

This allows us to relate the ϵ -secrecy of the QKD protocol for an arbitrary state ρ_{ABE} to the $g_{n,x}\epsilon$ -secrecy of the same protocol if the input is a purification of a probabilistic mixture of IID states. The final step of the postselection method then comprises relating this to the secrecy of an IID state. The (corrected) postselection theorem (Corollary 3.1 in Ref. [38]) states the following: provided that one has proven security of a QKD protocol for IID states, yielding a key of length ℓ

$$\frac{1}{2} \left\| \left(\left(\Phi^{(\ell)} - \Phi_{\text{ideal}}^{(\ell)} \right) \otimes \text{id}_E^n \right) (\tau_{ABE}^{\otimes n}) \right\|_1 \leq \epsilon_{\text{sec}}$$

with security parameter $\epsilon_{\text{sec}} = \max\{\epsilon_{\text{AT}}, \epsilon_{\text{PA}}\}$ (which is what we have just accomplished), the security of the same protocol with a purification of a de Finetti state as input that hashes to a length $\ell' = \ell - 2 \log_2(g_{n,x})$, where $g_{n,x} = \binom{n+x-1}{n}$, is then

$$\frac{1}{2} \left\| \left(\left(\Phi^{(\ell')} - \Phi_{\text{ideal}}^{(\ell')} \right) \otimes \text{id}_R \right) (\sigma_{A^n B^n R}) \right\|_1 \leq \epsilon'_{\text{sec}} \quad (7)$$

secure, with security parameter $\epsilon'_{\text{sec}} = \epsilon_{\text{PA}} + 2\sqrt{2\epsilon_{\text{AT}}}$. Note that the postselection theorem of Ref. [38] straightforwardly extends from prepare-and-measure protocols to entanglement-based protocols.

Combining those findings yields the security statement against coherent attacks, which is summarized in the Theorem 3.

Theorem 3 (Security statement for coherent attacks). Let $\epsilon_{\text{EV}}, \epsilon_{\text{PA}}, \epsilon_{\text{AT}}, \bar{\epsilon} > 0$. Let N be the total number of quantum signals exchanged, k_T be the number of test rounds, and $n := N - k_T$. The objective general high-dimensional QKD protocol is $\epsilon_{\text{EV}} + g_{n,x}(\epsilon_{\text{PA}} + 2\sqrt{2\epsilon_{\text{AT}}})$ -secure against coherent attacks, if, in case the protocol does

not abort, the key is hashed to a length of

$$\ell' \leq n \min_{\tau_{ABE} \in \mathcal{S}^{\text{AT}}} H_{\min}(X|E)_{\Phi(\tau_{ABE})} - \text{leak}_{\text{IR}} - 2 \log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right) - 2 \log_2 (g_{n,x}), \quad (8)$$

where $g_{n,x} = \binom{n+x-1}{n}$ and $\mathcal{S}^{\text{AT}}$ is the acceptance set defined by the acceptance test in Theorem 1.

In this work, we use $g_{n,x} \leq (e(n+x-1)/x-1)^{x-1}$ from Ref. [38] as an upper bound. In nontechnical terms, Theorem 3 allows us to relate the security against general attacks to the security against IID collective attacks, which we established earlier in Theorem 2. While we still can relate the achievable secure key length ℓ' to a similar optimization problem as we found for collective attacks, the stronger security claim comes at a price. To obtain secure key, the additional correction term $\log_2 (g_{n,x})$ tells us that we need to hash our raw key a bit more, while additionally, the total security parameter grows.

When we present our results, we plot secure key rates instead of achievable secure key lengths; thus, we divide both sides by N and obtain

$$\frac{\ell'}{N} \leq \frac{n}{N} \min_{\tau_{ABE} \in \mathcal{S}^{\text{AT}}} H_{\min}(X|E)_{\Phi(\tau_{ABE})} - \delta_{\text{leak}} - \frac{2}{N} \log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right) - \frac{2}{N} \log_2 (g_{n,x}), \quad (9)$$

where $\delta_{\text{leak}} := \text{leak}_{\text{IR}}/N$.

IV. VARIABLE-LENGTH SECURITY

In the previous section, we have proven the security of a high-dimensional QKD protocol that produces a key of fixed length or aborts. The most crucial part of such a fixed-length protocol in reality is to construct an acceptance set, which practically boils down to defining the expected channel behavior (r_X , potentially along with some margin t_X). This is because in many practical applications, the expected channel behavior is not known or can change rapidly, such as in free-space and satellite-based QKD applications, which are two of the prototypical use cases in which high-dimensional QKD can play out its strengths; however, according to the security argument given in Sec. III, the accepted statistics have to be fixed before the run of the protocol, and the abort decision is made by comparing the actual measurement results with the acceptance set. For unknown or rapidly changing values, this would mean that even protocols with nonunique acceptance abort very often (and unique acceptance protocols basically all the time), leading to a low expected key rate [39,41]. The only possible counteraction is increasing the parameters t_X

to enlarge the acceptance set. This, however, diminishes the secure key length, as the reported length has to be compatible with the worst-case state within the given set, while not significantly increasing the acceptance probability for varying channels.

We address this problem by introducing a variable-length version of our protocol and proving security, applying the theory of Ref. [39]. We start by stating the required protocol modifications and introducing some additional notation.

The state-generation, measurement, and announcement and sifting phases, as well as the key map of the protocol stated in Sec. II, representing steps (1)–(3) and (5), remain unchanged, while the main modifications pertain to steps (4), (6), and (7). The modified protocol steps are as follows.

(4') Variable-length decision. The communicating parties disclose a randomly chosen subset consisting of k_T of their measurement results over the public channel and, depending on their observations, determine the required EC and hash length.

(6') Error correction and error verification. On the remaining $N - k_T$ rounds, Alice and Bob perform error correction to reconcile their raw keys X and Y . The size of the error-correction leakage is already fixed by step (4'), where they decided to produce a key of length ℓ_i with EC leakage λ_i^{EC} . As for the fixed-length protocol, they proceed with error verification, where Alice chooses a two-universal hash function that hashes to $\lceil \log_2 (1/\epsilon_{\text{EV}}) \rceil$ bits and sends them to Bob, who performs the same hash function and compares them. If they obtain the same hash values, they proceed.

(7') Privacy amplification. Alice chooses a two-universal random hash function from n to ℓ_i bits to decouple Eve from their shared randomness.

For the fixed-length version of the protocol, the values of ℓ_i and λ_i^{EC} had to be fixed before the execution of the protocol; now this decision is made based on the data. Let $\vec{F}^{\text{obs}} \in \mathbb{R}^{|\Theta|}$ denote the vector containing the experimental observations for all considered observables $X \in \Theta$, and denote $\Phi_X(\rho) := \text{Tr}[\rho X]$.

A. Security against collective attacks

In what follows, we summarize the idea of the variable-length security proof from Ref. [39] and adapt it to the objective high-dimensional QKD protocol. First, based on their observations $\vec{F}^{\text{obs}}$, Alice and Bob need to find a statistical estimator $b_{\text{stat}}(\vec{F}^{\text{obs}})$, which is a high-probability lower bound to the Rényi entropy $H_\alpha(Z^n|C^n E^n)_\rho$ of the underlying quantum state with, where C denotes the register collecting the leaked classical information,

$$\Pr \left[b_{\text{stat}}(\vec{F}^{\text{obs}}) \leq H_\alpha(Z^n|C^n E^n)_\rho \right] \geq 1 - \epsilon_{\text{AT}}. \quad (10)$$

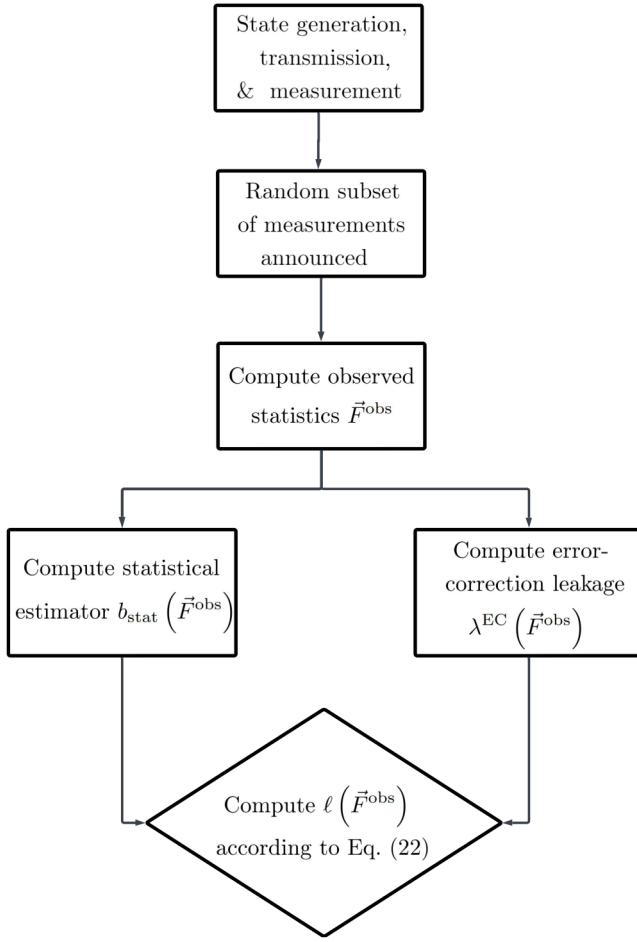


FIG. 1. Flowchart illustrating the variable-length decision. The length of the key is now a function of the observed statistics $\vec{F}^{\text{obs}}$.

Intuitively, this estimator provides a high-probability lower bound on Eve's information about the key, based on the observed statistics $\vec{F}^{\text{obs}}$. Finding such an estimator requires the construction of a set $V(\vec{F}^{\text{obs}})$ that contains the (unknown) quantum state responsible for Alice's and Bob's observations with high probability, i.e., $\Pr[\tau_{AB} \in V(\vec{F}^{\text{obs}})] \geq 1 - \epsilon_{\text{AT}}$. Based on this estimator and the public announcements, Alice and Bob determine the information leakage $\lambda^{\text{EC}}(\vec{F}^{\text{obs}})$, which is an integer between 0 and $\lambda_{\text{max}}^{\text{EC}}$ quantifying how many bits of the key Eve learns by listening to Alice's and Bob's communication over the classical channel. An illustration of the variable-length decision can be found in Fig. 1.

This allows calculating the secure key length as the difference between the statistical estimator and the error correction leakage, along with some additional lower-order correction terms:

$$\ell(\vec{F}^{\text{obs}}) := \max \left\{ 0, \left\lfloor b_{\text{stat}}(\vec{F}^{\text{obs}}) - \lambda^{\text{EC}}(\vec{F}^{\text{obs}}) - \theta(\alpha, \epsilon_{\text{PA}}, \epsilon_{\text{EV}}) \right\rfloor \right\}. \quad (11)$$

In the fixed-length scenario, the acceptance test was built by defining expected statistics and finding the set of density matrices that could have produced these statistics only with some small probability; the complement of this set was the set $\mathcal{S}_{\text{AT}}$. In the variable-length scenario, the construction of the acceptance set follows a slightly different logic. A fixed but otherwise unknown quantum state gives rise to observed statistics $\vec{F}^{\text{obs}}$, which is a random variable. Based on this observation, we aim to construct a set $V(\vec{F}^{\text{obs}})$ such that $\Pr[\tau_{AB} \in V(\vec{F}^{\text{obs}})] \geq 1 - \epsilon_{\text{AT}}$. Since we are using observables, we adapt the argument from Ref. [39]. Let Θ denote the set of observables used in the protocol, and let $x := \|X\|_{\infty} = \|X\|_{\infty} \|\rho\|_1 \geq \|X\rho\|_1$ for $X \in \Theta$. For each $X \in \Theta$, Hoeffding's inequality [46] tells us

$$\Pr[|F_X^{\text{obs}} - \mathbb{E}[X]| \geq \mu_X] \leq 2e^{-\frac{2m_X \mu_X^2}{4x^2}} =: \epsilon_X, \quad (12)$$

where m_X is the number of rounds used for testing observable X . We apply Hoeffding's inequality to every observable $X \in \Theta$ and combine them, using Boole's inequality,

$$\begin{aligned} \Pr \left[\bigcup_{X \in \Theta} \mathbb{E}[X] \notin [F_X^{\text{obs}} - \mu_X, F_X^{\text{obs}} + \mu_X] \right] \\ \leq \sum_{X \in \Theta} \epsilon_X =: \epsilon_{\text{AT}}. \end{aligned} \quad (13)$$

In reverse, this means

$$\Pr \left[\bigcap_{X \in \Theta} \mathbb{E}[X] \in [F_X^{\text{obs}} - \mu_X, F_X^{\text{obs}} + \mu_X] \right] \geq 1 - \epsilon_{\text{AT}}, \quad (14)$$

and thus

$$\Pr[\rho \in V(\vec{F}^{\text{obs}})] \geq 1 - \epsilon_{\text{AT}}, \quad (15)$$

where $\vec{F}^{\text{obs}}$ is defined as the vector containing F_X^{obs} in its X th component. This leads to

$$\begin{aligned} V(\vec{F}^{\text{obs}}) &:= \{\sigma \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E) : \\ &\forall X \in \Theta, |\text{Tr}[\sigma X] - r_X| \leq \mu_X\}. \end{aligned} \quad (16)$$

Note that in the present case, despite the different argument, the main difference from the acceptance set for the fixed-length scenario is the decomposition of ϵ_{AT} as a sum of the single-observable epsilons ϵ_X . This, however, arises from using Hoeffding's inequality and can differ more significantly for other sampling arguments.

Theorem 4 (Variable-length security statement for collective attacks). Let $\epsilon_{\text{EV}}, \epsilon_{\text{PA}}, \epsilon_{\text{AT}} > 0$. Let N be the total

number of quantum signals exchanged, k_T be the number of test rounds, and $n := N - k_T$. Let Θ be the set of observables considered for the objective protocol and $\vec{F}^{\text{obs}} \in \mathbb{R}^{|\Theta|}$ be the vector containing the observations corresponding to Θ . Based on $\vec{F}^{\text{obs}}$, define the statistical estimator

$$b_{\text{stat}}(\vec{F}^{\text{obs}}) := n \min_{\tau_{AB} \in V(\vec{F}^{\text{obs}})} H_{\min}(X|E)_{\Phi_{\text{var}}(\tau_{ABE})} - n(\alpha - 1) \log_2^2(\dim(X) + 1), \quad (17)$$

where $1 < \alpha < 1 + \frac{1}{\log_2(2 \dim(X) + 1)}$ and $V(\vec{F}^{\text{obs}})$ is such that it contains the state that produced $\vec{F}^{\text{obs}}$ at least with probability $1 - \epsilon_{\text{AT}}$.

Then, the variable-length protocol, conditioned on obtaining $\vec{F}^{\text{obs}}$ during acceptance testing and on passing the error-verification step, that hashes to length

$$\ell(\vec{F}^{\text{obs}}) := \max \{0, b_{\text{stat}}(\vec{F}^{\text{obs}}) - \lambda^{\text{EC}}(\vec{F}^{\text{obs}}) - \theta(\alpha, \epsilon_{\text{PA}}, \epsilon_{\text{EV}})\}. \quad (18)$$

where

$$\theta(\alpha, \epsilon_{\text{PA}}, \epsilon_{\text{EV}}) := \frac{\alpha}{\alpha - 1} \left(\log_2 \left(\frac{1}{4\epsilon_{\text{PA}}} + \frac{2}{\alpha} \right) + \left\lceil \log_2 \left(\frac{1}{\epsilon_{\text{EV}}} \right) \right\rceil \right),$$

using $\lambda^{\text{EC}}(\vec{F}^{\text{obs}})$ bits for error correction, is ϵ_{EV} -correct and $\epsilon_{\text{AT}} + \epsilon_{\text{PA}}$ -secure.

Intuitively, Theorem 4 states that we can obtain a qualitatively similar security claim as we obtained in the fixed-length scenario (see Theorem 2) even if we construct our statistical analysis around the observed rather than the expected measurement outcomes; however, as outlined before the statement, this requires a different security argument and leads to different correction terms.

B. Security of variable-length HD-QKD protocols against coherent attacks

Similarly to the fixed-length protocol, we can define a protocol map $\Phi_{\text{var}}^{\ell_1, \dots, \ell_M}$ that describes the action of the variable-length protocol hashing to keys of lengths $\ell_1, \dots, \ell_M$, where M is the number of possible different key lengths. Furthermore, let $\Phi_{\text{var,ideal}}^{\ell_1, \dots, \ell_M}$ be its ideal counterpart. According to Theorem 4, the variable-length protocol was shown to be secure against collective attacks,

$$\frac{1}{2} \left\| \left(\Phi_{\text{var}}^{\ell_1, \dots, \ell_M} - \Phi_{\text{var,ideal}}^{\ell_1, \dots, \ell_M} \right) (\rho_{A^n B^n E^n}) \right\|_1 \leq \epsilon_{\text{PA}} + \epsilon_{\text{AT}}, \quad (19)$$

and ϵ_{EV} -correct. By a similar argument as in the previous section, exploiting the permutation invariance of the

objective high-dimensional QKD protocol (see Ref. [38] for details), one can show that, provided the protocol is secure against collective attacks with security parameter $\epsilon_{\text{PA}} + \epsilon_{\text{AT}}$, the protocol that hashes keys to length $\ell'_i := \ell_i - 2 \log_2(g_{n,x}) - 2 \log_2(1/\tilde{\epsilon})$ instead of length ℓ_i upon Ω_i has security parameter $g_{n,x}(\sqrt{8(\epsilon_{\text{PA}} + \epsilon_{\text{AT}})} + \tilde{\epsilon}/2)$,

$$\frac{1}{2} \left\| \left(\Phi_{\text{var}}^{(\ell'_1, \dots, \ell'_M)} - \Phi_{\text{var,ideal}}^{(\ell'_1, \dots, \ell'_M)} \right) (\rho_{A^n B^n E^n}) \right\|_1 \quad (20)$$

$$\leq g_{n,x} \left(\sqrt{8(\epsilon_{\text{PA}} + \epsilon_{\text{AT}})} + \frac{\tilde{\epsilon}}{2} \right), \quad (21)$$

where $\Phi_{\text{var}}^{(\ell'_1, \dots, \ell'_M)}$ is identical to $\Phi_{\text{var}}^{(\ell_1, \dots, \ell_M)}$, except that it hashes to a shorter key and is ϵ_{EV} -secret. We summarize these findings in Theorem 5.

Theorem 5 (Variable-length security statement for coherent attacks). Let $\epsilon_{\text{EV}}, \epsilon_{\text{PA}}, \epsilon_{\text{AT}}, \tilde{\epsilon} > 0$. Let N be the total number of quantum signals exchanged, k_T be the number of test rounds, and $n := N - k_T$. Provided that the objective high-dimensional variable-length QKD protocol is secure against collective attacks according to Theorem 4 with security parameter $\epsilon_{\text{PE}} + \epsilon_{\text{AT}}$ and correctness parameter ϵ_{EV} , conditioned on obtaining $\vec{F}^{\text{obs}}$ during acceptance testing and passing the error-verification, the protocol is secure against coherent attacks with security parameter $g_{n,x}(\sqrt{8(\epsilon_{\text{PE}} + \epsilon_{\text{AT}})} + \tilde{\epsilon}/2)$, if the key is hashed to a length of

$$\begin{aligned} \ell(\vec{F}^{\text{obs}}) &:= \max \{0, b_{\text{stat}}(\vec{F}^{\text{obs}}) - \lambda^{\text{EC}}(\vec{F}^{\text{obs}}) - \theta(\alpha, \epsilon_{\text{PA}}, \epsilon_{\text{EV}}) \\ &\quad - 2 \log_2(g_{n,x}) - 2 \log_2\left(\frac{1}{\tilde{\epsilon}}\right)\}, \end{aligned} \quad (22)$$

where

$$\theta(\alpha, \epsilon_{\text{PA}}, \epsilon_{\text{EV}}) := \frac{\alpha}{\alpha - 1} \left(\log_2 \left(\frac{1}{4\epsilon_{\text{PA}}} + \frac{2}{\alpha} \right) + \left\lceil \log_2 \left(\frac{1}{\epsilon_{\text{EV}}} \right) \right\rceil \right)$$

and $g_{n,x} = \binom{n+x-1}{n}$ for $x = d_A^2 d_B^2$, using $\lambda^{\text{EC}}(\vec{F}^{\text{obs}})$ bits for error correction.

Similar to the variable-length statement for collective attacks, Theorem 5 presents a variable-length version for the achievable secure key length against coherent attacks, which builds the statistical analysis around the observed rather than the expected behavior of the channel. The core message is that we obtain a qualitatively similar security statement to the fixed-length case, even if we build our security argument upon the observed rather than the expected statistics.

V. SECURITY PROOF METHOD

Having discussed the security for two different attack scenarios and both the fixed- and variable-length scenarios, it remains to find a way to evaluate the given expressions; however, as discussed earlier and in Ref. [27], widely available convex optimization methods [29,30] cannot handle high-dimensional QKD protocols. On the other hand, less computationally demanding methods [22,24] rely on hard-to-implement measurements, which are not available in most practical setups. Instead, we employ a recent technique developed in Ref. [31] that provides lower bounds on the secure key rate without high computational demands, solely relying on available measurements.

A. Key-rate evaluation

While this method computes asymptotic key rates, the formulation of our composable finite-size key-rate-finding problems derived in Secs. III and IV in terms of the min-entropy already allows us to directly apply this framework. The basic idea of this method is as follows [41]. It is well known that the min-entropy can be expressed as the negative binary logarithm of Eve's probability of guessing Alice's key string correctly, $H_{\min}(X|E)_\rho = -\log_2(p_{\text{guess}})$. This allows us to recast the minimization of the min-entropy over $\mathcal{S}^{\text{AT}}$ as a maximization over all possible measurements Eve might carry out to guess Alice's outcomes. Applied to our finite-size optimization problem, this turns into

$$p_{\text{guess}} = \max_{\substack{\rho_{ABE} \\ \{E^l\}_{l=0}^{d-1}}} \sum_{l,k} \text{Tr}[\rho_{ABE} A_1^l \otimes B_1^k \otimes E^l]$$

subject to

$$\begin{aligned} \sum_l E^l &= \mathbb{1}, \\ \text{Tr}[\rho_{ABE}] &= 1, \\ \langle \hat{W}_0 \rangle - \mu_0 &\leq \text{Tr}[(\hat{W}_0 \otimes \mathbb{1}_E) \rho_{ABE}] \\ &\leq \langle \hat{W}_0 \rangle + \mu_0, \\ \text{Tr}[(\hat{W}_j^{(i)} \otimes \mathbb{1}_E) \rho_{ABE}] &\leq \langle \hat{W}_j \rangle + \mu_j, \\ E^l &\geq 0, \\ \rho_{ABE} &\geq 0, \end{aligned} \quad (23)$$

for $j \in \{1, \dots, N_W\}$ and $l \in \{0, \dots, d-1\}$. The observables $\hat{W}_j$ are detailed in Sec. VI. The numerical values of μ_j are calculated according to Theorem 1. Instead of solving this semidefinite program directly, the method derives

its dual

$$\begin{aligned} \min_{y_0, z_0^L, z_0^U, \{z_j\}_{j=1}^{N_W}} & y_0 + z_0^U (\langle \hat{W}_0 \rangle + \mu_0) - z_0^L (\langle \hat{W}_0 \rangle - \mu_0) \\ & + \sum_{j=1}^{N_W} z_j (\langle \hat{W}_j \rangle + \mu_j) \\ \text{subject to} & y_0 \geq \lambda_{\max}(M_\ell) \quad \forall \ell = 0, \dots, d-1, \\ & z_0^L, z_0^U, z_j \geq 0 \quad \forall j = 1, \dots, N_W, \\ & y_0 \in \mathbb{R}, \end{aligned} \quad (24)$$

which reduces the problem to a rather simple minimization problem subject to a constraint that depends on the maximal eigenvalue of a matrix, which is a function of the chosen observables $M_\ell := |\ell\rangle\langle\ell| \otimes \mathbb{1}_d - (z_0^U - z_0^L) \bar{W}_0 - \sum_{j=1}^{N_W} z_j^U \bar{W}_j$.

Thus, the crucial task was reduced to finding experimentally accessible observables. This can be significantly simplified by extending the set of accessible operators using a matrix-completion technique [20,47]. For further details, and a discussion about the complexity scaling, we refer the reader to Ref. [31].

B. Formalization of the protocol

For illustration purposes, we apply our method to a high-dimensional temporal-entanglement setup using a Franson interferometer, analyzed in Protocol 1 of Ref. [27]. A source prepares polarized photon pairs of the form $|\Psi_1\rangle = |\text{DD}\rangle \otimes 1/\sqrt{d} \sum_{k=0}^{d-1} |kk\rangle$, which are distributed to the communicating parties. With probability p_1 , each party performs a time-of-arrival (ToA) measurement, represented by $\{A_1^x\}_{x=0}^{d-1}$ and $\{B_1^y\}_{y=0}^{d-1}$, respectively, and with probability $1 - p_1$, each of them performs a temporal superposition (TSUP) measurement of not necessarily neighboring time bins, represented by $\{A_2^x\}_{x=0}^{d-1}$ and $\{B_2^y\}_{y=0}^{d-1}$, respectively. We start by deriving the protocol map representing the action of this protocol, specifying the map Φ introduced in Sec. III, following the formalism in Refs. [48, 49].

For each round, Alice and Bob may store a measurement outcome α_i and β_i and make a public announcement a_i and b_i , where the measurement outcomes are drawn from the sets $\mathcal{X}_A$ and $\mathcal{X}_B$ and the announcements from the set $\mathcal{A}_A$ and $\mathcal{A}_B$ for Alice and Bob, respectively. In our case, these announcements are the choice of measurement, i.e., a number b related to the label of the POVM measurement performed. For the analyzed protocol, $b = 1$ corresponds to time-of-arrival measurements, labeled ToA, while $b = 2$ refers to superposition measurements of neighboring time bins, labeled TSUP. They store their measurement outcomes in their private registers $\bar{A}$ and $\bar{B}$ and their announcements in their public registers $\bar{A}$

and $\tilde{B}$. Since we perform direct reconciliation, the key map g saves the outcome of the map $g : \mathcal{X}_A \times \mathcal{A}_A \times \mathcal{A}_B \rightarrow \{0, \dots, d-1, \perp\}$ to the key register Z . In more detail, since the protocol only generates a key when both Alice and Bob measure ToA, the key map for our protocol is trivial and simply copies Alice's measurement outcome contained in her private register $\tilde{A}$ to the key register Z . This sets the stage for introducing the formal protocol map. Let ρ_{AB} be Alice's and Bob's shared quantum state after the generation and distribution of the high-dimensional entangled state, and let ρ_{ABE} denote Eve's purification. Furthermore, since Alice's and Bob's announcements are public, Eve has access to them. We use the short notation $[E]$ to label Eve's register, including all available public information. Eve's goal is to perform some (to us unknown) POVM measurement, aiming to gain as much information as possible about Alice's measurement outcome. Since Alice and Bob only generate a key if both measure the time

of arrival, we obtain the following map representing their measurement and announcement steps:

$$\begin{aligned} \Phi_{M\&A}(\rho_{ABE}) &= \sum_{ij} |\text{ToA}\rangle\langle\text{ToA}|_{\tilde{A}} \otimes |i\rangle\langle i|_{\tilde{A}} \otimes |\text{ToA}\rangle\langle\text{ToA}|_{\tilde{B}} \otimes |j\rangle\langle j|_{\tilde{B}} \\ &\otimes \left[\left(\sqrt{A_1^i} \otimes \sqrt{B_1^i} \otimes \sqrt{E^i} \right) \rho_{ABE} \left(\sqrt{A_1^i} \otimes \sqrt{B_1^i} \otimes \sqrt{E^i} \right)^\dagger \right], \end{aligned} \quad (25)$$

and the key-map isometry reads

$$V = \sum_k |k\rangle_Z \otimes |\text{ToA}\rangle\langle\text{ToA}|_{\tilde{A}} \otimes |\text{ToA}\rangle\langle\text{ToA}|_{\tilde{B}} \otimes |k\rangle\langle k|_{\tilde{A}}. \quad (26)$$

Thus, the final state $\sigma_{Z,[E]}$ is obtained by

$$\sigma_{Z,[E]} = \text{Tr}_{A\tilde{B}\tilde{B}} [V \Phi_{M\&A} V^\dagger]. \quad (27)$$

Nonetheless, since the announcements for this protocol are trivial, they do not give any additional information. Hence, after inserting the expressions for Alice's and Bob's key measurement POVM and tracing out the announcement registers, we obtain

$$\sigma_{ZE} = \sum_{ij} |i\rangle\langle i|_Z \otimes \text{Tr}_{AB} \left[\left(\sqrt{|i\rangle\langle i|} \otimes \sqrt{|j\rangle\langle j|} \otimes \sqrt{E^i} \right) \rho_{ABE} \left(\sqrt{|i\rangle\langle i|} \otimes \sqrt{|j\rangle\langle j|} \otimes \sqrt{E^i} \right)^\dagger \right] \quad (28)$$

$$= \sum_{ij} |i\rangle\langle i|_Z \text{Tr}_{AB} \left[(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes E^i) \rho_{ABE} \right] \quad (29)$$

$$=: \Phi(\rho_{ABE}). \quad (30)$$

The last line defines the final protocol map Φ . For this Φ , the objective function of the optimization in Eq. (23) we use to calculate $H_{\min}(X|E)_{\Phi(\rho)} = -\log_2(p_{\text{guess}})$ becomes

$$\begin{aligned} p_{\text{guess}} &= \max_{\substack{\rho_{ABE} \\ \{E^i\}_{i=0}^{d-1}}} \text{Tr}_{ZE} \left[\sum_{ij=0}^{d-1} \text{Tr}_{AB} \left[(|i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes E^i) \rho_{ABE} \right] \right] \\ &= \max_{\substack{\rho_{ABE} \\ \{E^i\}_{i=0}^{d-1}}} \sum_{i=0}^{d-1} \text{Tr} \left[(|i\rangle\langle i|_A \otimes \mathbb{1}_B \otimes E^i) \rho_{ABE} \right], \end{aligned} \quad (31)$$

which then translates to the dual given in Eq. (24).

VI. RESULTS

In this section, we demonstrate our method by deriving composable finite-size key rates for the high-dimensional temporal entanglement protocol and setup analyzed in Ref. [27]. While this is one illustrative example, our method applies to general high-dimensional protocols in a very similar fashion. The underlying data can be found in Ref. [50].

In accordance with Ref. [31], we chose $d-1$ observables $\hat{W}_k := q_0 \sum_{i=0}^{d-1} |i, i\rangle\langle i, i| + \sum_{z=1}^{d-1} \sum_{i=0}^{d-1} q_{z,i} (|i, i\rangle\langle i+z, i+z| + |i+z, i+z\rangle\langle i, i|)$ and $\hat{W}_0 := \sum_{i \neq j}^{d-1} p |i, j\rangle\langle i, j|$, where $p = 1$. We chose the $q_{z,i}$ such that the k th operator acts only on the k th off-diagonal, which allows us to include the optimal choice of relative weights between the witnesses in the optimization problem. More details regarding this choice and the intuition behind it can be found in Appendix D of Ref. [31].

First, we cover the fixed-length scenario, which best suits theoretical discussions of achievable “one-shot” key rates, followed by a discussion of variable-length key rates under specific noise models. In all examples given, we use r_S to refer to the splitting ratio of the beam splitters in Alice’s and Bob’s labs that passively choose the measurement setting (ToA or TSUP). For example, a splitting ratio of $r_S = 1\%$ means that 1% of the photons are directed to the TSUP measurement apparatus, while the remaining 99% are measured in the ToA setup. Thus, they obtain $r_S^2 N$ rounds of aligned TSUP measurements and $(1 - r_S)^2$ rounds of aligned ToA measurements. Given that $8(d - 1)$ different click events are combined into W_1 , we obtain $m_{W_1} := r_S^2 N / 8(d - 1)$. Additionally, we choose $m_{W_2} = m_{W_1}$ such that $n := N(1 - r_S)^2 - Nr_S^2 = N(1 - 2r_S)$, since the click elements required for W_2 are obtained from ToA measurements.

For demonstration purposes, if not mentioned otherwise, we assume an isotropic noise model $\rho = v |\Psi_1\rangle\langle\Psi_1| + \frac{(1-v)}{d^2} \mathbb{1}_{d^2}$; however, we want to emphasize that our method applies independently of the chosen noise model, and the noise model is solely required to simulate the observations for key rate plots. The security analysis is general and does not require any assumptions about the state or the noise model.

Also, note that the leakage in the information-reconciliation phase leak_{IR} appearing in the key rate formulas given in Sec. III is the sum of the error-correction leakage leak_{EC} and the length of the hash used for error verification, $\log_2(2/\epsilon_{\text{EV}})$. If not stated otherwise, we assume ideal error correction.

A. Fixed-length key rates

We start with fixed-length keys, also called “one-shot” key rates, corresponding to key rates usually reported in the literature. Recall that for the definition of the acceptance set (see Theorem 1), one may choose to extend the set of accepted statistics by choosing the parameters $t_X > 0$ (for each observable X). Intuitively, this extends the set of accepted statistics from a point to a (hyper-) rectangle with sides t_X for $X \in \Theta$. To simplify notation and to describe the choices for the acceptance test with a single parameter, we measure the chosen t_X for the different observables in multiples of their respective μ_X by introducing a factor t_F , $t_X = t_F \mu_X$. In the whole subsection discussing the results for the fixed-length scenario, we fix $t_F = 1$. The choice of t_F influences the one-shot key rate (a larger t_F extends the set of feasible states, thus lowering the key rate) and the acceptance probability of the acceptance test (the larger t_F , the higher the acceptance probability). We discuss the influence of t_F in more detail in Sec. VIB, when we compare fixed-length to variable-length key rates.

Since the choices for the epsilons can have an influence on the secure key rates, we discuss our considerations in

more detail in Appendix B, where we express the security epsilons as functions of two real, positive parameters $r, s > 0$. While we did not optimize our choices to the full extent, as this would go beyond the scope of this paper and is best discussed for real experiments, we categorize the different epsilons by their impact on the key rate and choose them accordingly. For the whole section, we set $r = \frac{1}{1000} = s$.

For the collective attack scenario, this leads to $\epsilon_{\text{AT}} = 9.99 \times 10^{-11}$, $\epsilon_{\text{PA}} = 9.99 \times 10^{-11}$, and $\epsilon_{\text{EV}} = 1 \times 10^{-13}$, resulting in a total security parameter of $\epsilon = 1 \times 10^{-10}$. In Fig. 2(a), we examine the key rates for varying N and compare the obtained finite-size key rates with the asymptotic rates for $N \rightarrow \infty$. We fixed the protocol dimension to $d = 16$ and the splitting ratio to $r_S = 1\%$. This means that for passive choice settings, r_S^2 of the rounds are available for TSUP measurements on both sides, and $(1 - r_S)^2 =$

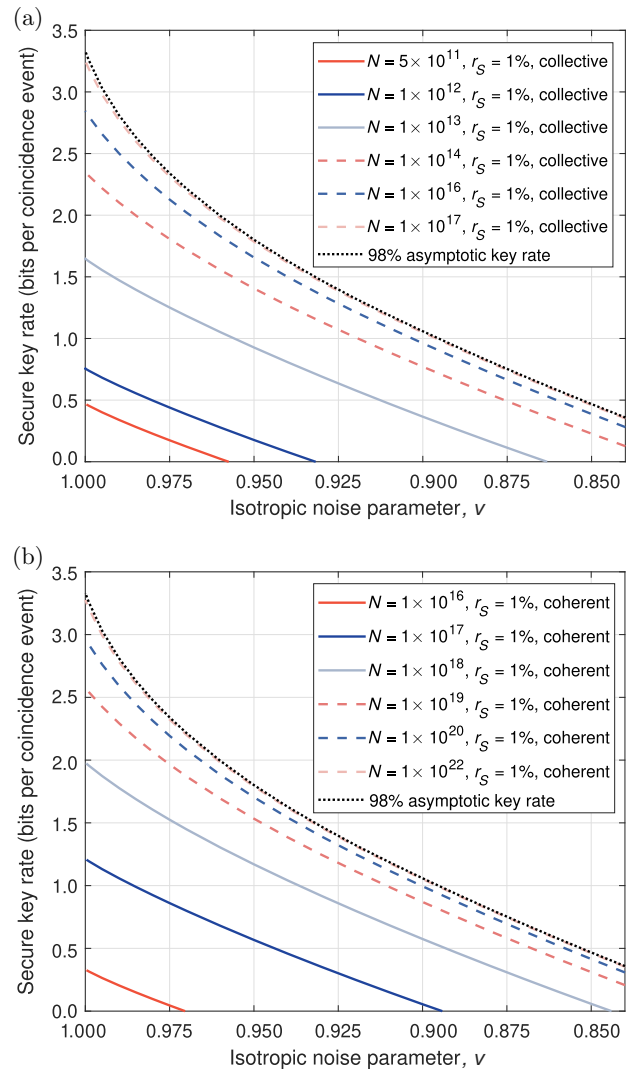


FIG. 2. Composable secure key rates against (a) IID collective attacks and (b) coherent attacks for different block sizes N and constant splitting ratio of 1%. The system dimension was fixed to $d = 16$ and we used the witness KH1.

0.9801 of the rounds are measured in ToA by both parties. Given our choice of $m_{W_1} = m_{W_2}$, $(1 - 2r_S) = 98\%$ of all rounds are available for key generation. Note that the comparable asymptotic key rates refer to $N \rightarrow \infty$, where the testing fraction can be chosen to be infinitesimally small. Thus, to ensure a fair comparison, we need to adjust the asymptotic rates by a factor of 0.98 to take the testing into account. We plot secure key rates for $N \in \{5 \times 10^{11}, 1 \times 10^{12}, 1 \times 10^{13}, 1 \times 10^{14}, 1 \times 10^{16}, 1 \times 10^{17}\}$ and observe convergence to the adjusted asymptotic-key-rate curve, as expected. We obtain nonzero finite-size key rates for block sizes of $N = 5 \times 10^{11}$ and above. For $N = 10^{17}$, our finite-size results effectively reassemble the asymptotic key rates. We note that the comparably high number of rounds required to obtain a nonzero key is due to the low testing ratio, which we chose to examine asymptotic behavior (as asymptotic rates only require infinitesimal testing). We will examine higher testing ratios for realistic block sizes later.

For coherent attacks, the security parameters scale according to Theorem 3. We discuss the detailed scaling in terms of the security parameters in Appendix B. For the presented results, we chose $r = \frac{1}{1000} = s$. We aim to maximize ν_{AT} at the expense of reducing the other security parameters.

Therefore, we aim to keep ν_{AT} as large as possible at the cost of lowering the other security parameters more. We choose $\nu_{AT} = 9.98 \times 10^{-11}$, $\nu_{PA} = 9.99 \times 10^{-14}$, and $\nu_{EV} = 1 \times 10^{-13}$ such that they add up to a total adjusted security parameter of $\nu = 10^{-10}$. The corresponding epsilon parameters can be obtained by scaling according to the security statement in Theorem 3.

In Fig. 2(b), we plot the obtained secure key rates vs visibility and examine the asymptotic behavior for large N of the secure key rates against coherent attacks. We fix the dimension again to $d = 16$ and the splitting ratio $r_S = 1\%$ and plot the curves for $N \in \{1 \times 10^{16}, 1 \times 10^{17}, 1 \times 10^{18}, 1 \times 10^{19}, 1 \times 10^{20}, 1 \times 10^{22}\}$. We obtain nonzero key rates for $N = 10^{17}$ and above and observe convergence to the adjusted asymptotic rate $N \rightarrow \infty$ for large N . Again, we note that we chose the low splitting ratio to examine the asymptotic behavior. Since the asymptotic rate does not take testing into account, we again rescale by the corresponding factor of 0.98. We obtain nonzero key rates for significantly lower N for higher splitting ratios.

Next, we examine the behavior with respect to loss for different block sizes N , splitting ratios r_S , and different noise levels. We use the noise model from Ref. [27] and choose the production rate $c_{\text{prod}} = 0.1$ per time frame for a time-frame length of $T = 5.4 \times 10^{-9}$. The dark-count rate was assumed to be 100 s^{-1} , and the detection efficiency $\eta_D = 0.90$. In Fig. 3, we plot the obtained secure key rates (in bits per pair sent) versus loss. Curves in different shades of blue correspond to $N = 10^{10}$ with a splitting ratio of $r_S = 20\%$, and curves in different shades of red correspond

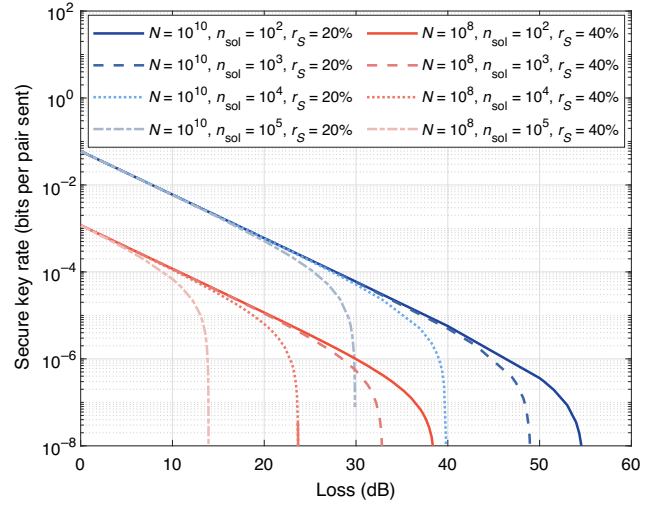


FIG. 3. Composable secure key rates against IID collective attacks versus loss for different block sizes N , splitting ratios r_S , and noise levels, parametrized by the number of solar photons n_{sol} . The system dimension was fixed to $d = 16$.

to $N = 10^8$ with a splitting ratio of $r_S = 40\%$. Different line styles (solid, dashed, dotted, and dot-dashed) indicate different solar photon rates $n_{\text{sol}} \in \{10^2, 10^3, 10^4, 10^5\}$. We observe that for $N = 10^{10}$ and $n_{\text{sol}} = 10^2$, corresponding to almost absolute darkness, we achieve a nonzero key rate up to about 51-dB channel attenuation, which is just shy of the asymptotic rates. For $N = 10^8$, the tolerable loss decreases to 38.5 dB. While the achievable loss decreases with increasing solar photon rate, in both cases, we still obtain a nonzero key for $n_{\text{sol}} = 10^5$, corresponding to sunrise [51]. Increasing the splitting ratio r_S can improve the noise tolerance even further. This demonstrates that high-dimensional QKD can play a crucial role in overcoming noise in loss regimes present in satellite-based QKD.

As shown in Fig. 4, already for $N = 10^{10}$, the collective attack key rates (solid blue curve) are only slightly below the asymptotic rates (solid black curve) in terms of tolerable loss and less than half an order of magnitude lower in terms of achievable secure key rate. Additionally, we compare our results with the key rates from Ref. [27] obtained for the same setup, using the same noise model, but relying on a convex optimization Gauss-Radau method [30]. While Ref. [27] only reports asymptotic rates, similar finite-size corrections are expected, so the comparison of asymptotic curves allows similar conclusions about finite-size results. In Ref. [27], the maximum dimension feasible on a standard computer was $d = 8$ (and $d = 12$ using a cluster), with the $d = 8$ curve (dashed orange) requiring several days of computation. By contrast, our method produces the $d = 16$ curve (solid black) within minutes. Already at $d = 16$, our method outperforms the numerical $d = 8$ result in both key rate and tolerable loss, thereby overcoming the apparent drawback of using H_{min} instead

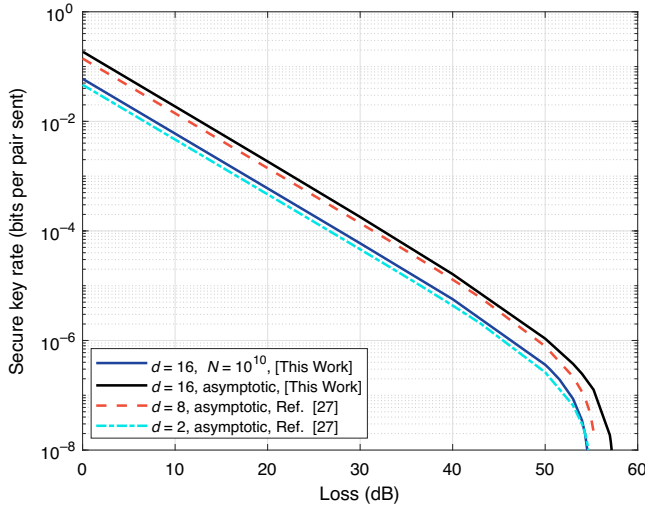


FIG. 4. Comparison of our results with asymptotic behavior and numerical key-rate curves according to Ref. [27]. The splitting ratio was fixed to $r_S = 20\%$ and the noise level, parametrized by the number of solar photons, was chosen to be $n_{\text{sol}} = 10^2$. The system dimension varies and is given in the legend.

of the von Neumann entropy. This highlights the clear advantage of our method, which unlocks the use of genuine high dimensions without substantial compromises on the secure key rate.

B. Variable-length key rates

Next, we come to the variable-length scenario. To illustrate the advantage of finite-size key rates, we need to employ a noise model that translates certain physical parameters of the devices used, such as the pair-production rate of the source, the dark-count rate and efficiency of the detector, and channel parameters like loss and the number of environmental photons (for example, solar photons) into coincidence click matrices. The latter can be used to derive the observations for our witness operators (observables). For illustration purposes, we use the noise model developed in Ref. [27], although, of course, the arguments apply to any noise model. Additionally, one needs to simulate natural channel fluctuations, as they appear under realistic conditions. In Appendix C, we discuss and model two different types of channels that may appear in real experiments. We call the first one the “statistically fluctuating channel,” which refers to a well-characterized, stable channel with channel parameters—the probability of photon loss p_L and a number of excess (solar) photons n_{sol} —that follow a normal distribution around certain characterized means. This represents a stable atmospheric channel under constant weather conditions. The second channel is called the “rapidly fluctuating channel” and describes an atmospheric channel under unstable weather conditions, such

as cloudy or foggy nights, or changing brightness, e.g., due to the rising sun. We apply a simplified model and assume that randomly one out of nine statistically fluctuating channels with different means μ_{sol} and μ_{loss} manifests. This is, of course, only for demonstration purposes; in reality, a plethora of conditions may apply. While the second scenario is more realistic, the first one already suffices to demonstrate the clear advantage of variable-length protocols. Throughout this section, we fix the dimension to $d = 16$. We direct the interested reader to Appendix B for details about our choices for the security parameters. In this section, we set $r = \frac{1}{1000} = s$, which turns out to be a sufficiently good choice.

We start our discussion by reviewing the notion of acceptance testing for fixed-length protocols. There, before the protocol is executed, one has to determine and fix an expected channel behavior by determining expected observations for the witness operators. This is usually a single data point. In this case, of course, every tiny deviation from the expected behavior leads to a deviation from the observed statistics. During the acceptance test, one compares these observed statistics with the expected statistics and aborts if they do not match. Therefore, under this “unique-acceptance” scenario, one would abort the protocol almost all the time, making it secure but essentially useless. We can fix this problem by introducing some margin to extend the set of accepted statistics (see parameter t_X in Theorem 1). As elaborated on earlier, by doing so, we build a multidimensional interval centered on our original expected statistics, which increases the probability of acceptance. This, however, comes at the cost of extending the set of states that pass the acceptance set, hence the set of states that potentially produced the observed statistics, and thus lowers the key rate. To ease the illustration, we parametrize t_X for each observable $X \in \Theta$ by a positive real number t_F , $t_X = t_F \mu_X$. In contrast, the variable-length security argument is built around the observed statistics and *not* around the expected statistics, and it adapts the secure key length to the quality of the observations. Therefore, for variable-length key rates, we can set $t_F = 0$. As derived in Sec. IV, the acceptance-testing security parameter ϵ_{AT} differs between the fixed- and variable-length scenarios, where ϵ_{AT} is the sum of the acceptance-testing epsilons ϵ_X for each single observable $X \in \Theta$. To simplify application for the variable-length scenario, from now on, we require that all the ϵ_X are equal, hence $\epsilon_{\text{AT}} = |\Theta| \epsilon_X$ and $\mu_X = \sqrt{(x^2/2m_X) \ln(2/\epsilon_X)}$.

Let us begin by developing an intuition for those two different notions of key rates on fluctuating channels. In Fig. 5(a), we simulate 100 runs of the statistically fluctuating channel with the channel parameters $\mu_{\text{sol}} = 2 \times 10^4$, $\sigma_{\text{sol}} = 1 \times 10^4$, $\mu_{\text{loss}} = 0.99$, and $\sigma_{\text{loss}} = 0.005$. The pair-production rate was set to 0.1 per time frame, the detection efficiency was assumed to be $\eta_D = 0.90$, and the dark-count rate was assumed to be 100 s^{-1} . Furthermore,

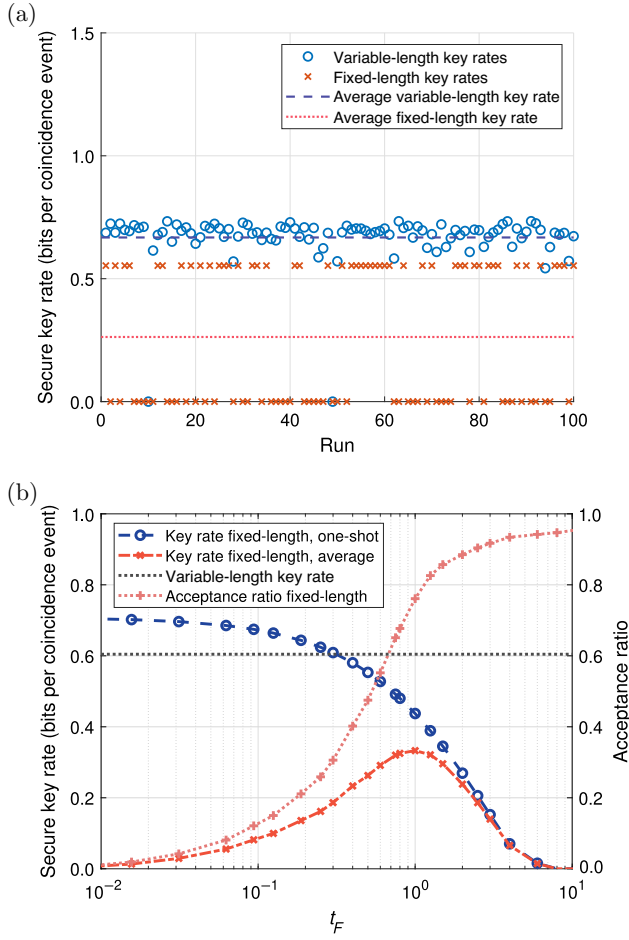


FIG. 5. Variable-length key rates for the statistically fluctuating channel. The system dimension was fixed to $d = 16$. (a) Comparing variable- and fixed-length key rates for 100 simulated runs. (b) Key rate vs t_F .

we set $t_F = 0.5$. We plot the secure key rate for each run, for both the fixed- and variable-length protocols. While the fixed-length protocol either produces a key of fixed length or aborts, it can be readily seen how the key lengths for the variable-length protocol adapt to the observed data, while it only fails for two out of 100 data points, yielding zero key. In the case of acceptance, the difference in key rate between the fixed- and variable-length cases is (in this example) about 20%; however, since more than half of the runs are not accepted in the fixed-length scenario, this results in the average variable-length key rates being roughly 2.5 times higher than the fixed-length key rates.

In real scenarios, the channel parameters are usually unknown; as such, for the present example, we chose t_F heuristically. This leaves the question of whether, if the behavior of the channel—including its statistical parameters—were known, one could find the optimal t_F for the fixed-length scenario and close the gap in performance. We are going to explore this question in what follows.

In Fig. 5(b), we examine the key rates for the fixed-length protocol and its acceptance ratio for different values of t_F . Again, we assumed a statistically fluctuating channel with the channel parameters mentioned above and simulated 1000 runs for each data point. The blue dashed line represents the one-shot fixed-length key rates, which are the fixed-length key rates upon acceptance, while the light-red dotted curve shows the associated ratio of accepted rounds. The dot-dashed red curve represents the average fixed-length key rate for each data point (which is the product of the one-shot value with the acceptance ratio). For comparison, we also plot the (average) variable-length key rate (black dotted line). Note that the variable-length key rate does not require $t_F > 0$ and thus remains constant with t_F . One can see that in this example, the one-shot fixed-length key rates are higher than the variable-length key rates for $t_F < 0.25$; however, due to the low acceptance ratio, the expected fixed-length key rates always remain significantly lower than the variable-length rates. For higher values of t_F , the acceptance rate slowly converges toward 1 while at the same time, the one-shot key rate drops, resulting overall in a decreasing average key rate. The highest fixed-length key rate is observed for $t_F = 1$; however, the exact location of the maximum depends on the channel parameters. Thus, even if one manages to determine the optimal t_F *a priori*, the obtained average fixed-length key rates would still be significantly below the variable-length rates.

Already in the case of stable channels with parameters fluctuating statistically around fixed mean values, variable-length key rates outperform their fixed-length equivalents in every aspect. If, in addition, the mean values fluctuate rapidly, the fixed-length acceptance test will only pass in a tiny fraction of all runs, leading to an expected key rate of nearly zero, while the variable-length key adapts to the observed statistics and will produce a nonzero

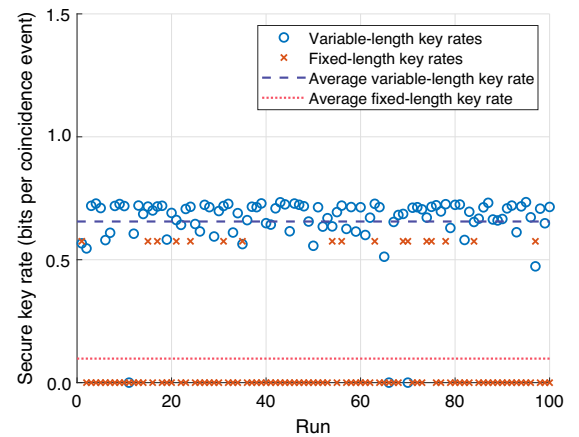


FIG. 6. Comparing variable- and fixed-length key rates for the rapidly fluctuating channel. The system dimension was fixed to $d = 16$.

key in many of those cases. We illustrate this in Fig. 6, where we present the results of simulations of the chaotic channel with parameters $(p_{\text{loss}}, n_{\text{sol}}) \in \{0.97, 0.98, 0.99\} \times \{1 \times 10^4, 2 \times 10^4, 1 \times 10^5\}$ (see Appendix C for details), where each channel parameter is chosen randomly according to a uniform distribution and $t_F = 0.5$. As expected, the fixed-length protocol aborts in the majority of all cases, yielding zero key. In contrast, the variable-length protocol produces a non-negative key for most runs. The average variable-length rates are now about 6.7 times higher than the average fixed-length key rate. This illustrates that, in real free-space channels, the advantage of the variable-length security argument will be even more striking.

VII. DISCUSSION

In recent years, the development of implementations for high-dimensional QKD on the one side and security analyses on the other side has proceeded at vastly different paces. While highly entangled states have been produced in various degrees of freedom [18–20, 33–36, 52–55], theoretical analyses have lagged behind, either relying on practically infeasible measurements [22, 24] or using computationally intensive convex optimization methods [27] that are limited to very low dimensions, despite taking hours to days to compute. While this problem was solved in the asymptotic regime by Ref. [31], the practically relevant finite-size regime for HD QKD was still missing.

In this work, we close this gap by proving the first composable finite-size security argument for a general high-dimensional QKD protocol against both collective and coherent attacks. The obtained rates converge to the corresponding asymptotic rates [31] in the limit of large N . We obtain non-negative key rates already for practically achievable block sizes of $N = 10^8$ under viable conditions. This shows that HD QKD is suitable for the loss and noise regimes [56, 57] present in free-space and low-Earth-orbit satellite QKD links. Additionally, we demonstrate that our method provides key rates comparable to those obtained by state-of-the-art numerical convex optimization techniques. While the latter are computationally intense and thus limited to low double-digit dimensions even on clusters [27], our semianalytic method unlocks genuine high dimensions, providing key rates that surpass existing results in terms of both achievable key rate and maximum tolerable loss.

In addition to common fixed-length key rates, we provide more practically useful variable-length key rates, which build the composable argument around the observed statistics rather than the expected statistics, significantly improving both the practicality and key rates of the protocol. We discuss and compare these two different notions of security to illustrate the advantages of variable-length key rates.

While we used a time-bin implementation for demonstration purposes, our work is general and can be applied to a variety of platforms with little to no adaptation. In summary, this work provides the missing tool for the full security analysis of general high-dimensional QKD protocols and unlocks the practical use of high-dimensionally entangled states in quantum key distribution. The obvious next steps consist of the application to real implementations and further improvements in the key rate.

ACKNOWLEDGMENTS

F.K. thanks Devashish Tupkary for inspiring discussions and precious feedback on an earlier version of this manuscript, Ian George for insightful discussions, and Shlok Nahar and Matej Pivoluska for valuable comments on an earlier version of the manuscript. This work has received funding from the Horizon Europe research and innovation program under Grant Agreement No. 101070168 (HyperSpace). The authors acknowledge TU Wien Bibliothek for financial support through its Open Access Funding Programme. F.K. gratefully acknowledges support from the Dieberger-Skalicky foundation.



Co-funded by
the European Union

DATA AVAILABILITY

The data that support the findings of this article are openly available [50].

APPENDIX A: CONSTRUCTION OF THE SET $V(\vec{F}^{\text{obs}})$

In the fixed-length scenario, the acceptance test was built upon defining expected statistics and finding the set of density matrices that could have produced these statistics only with some small probability; the complement of this set was $\mathcal{S}_{\text{AT}}$. In the variable-length scenario, the construction of the acceptance set follows a slightly different logic. A fixed but otherwise unknown quantum state gives rise to observed statistics $\vec{F}^{\text{obs}}$, which is a random variable. Based on this observation, we aim to construct a set $V(\vec{F}^{\text{obs}})$ such that $\Pr[\tau_{AB} \in V(\vec{F}^{\text{obs}})] \geq 1 - \epsilon_{\text{AT}}$. We are using observables; thus, we have to slightly adapt the argument from Ref. [39]. Let Θ denote the set of observables used in the protocol and let $x := \|X\|_{\infty} = \|X\|_{\infty} \|\rho\|_1 \geq \|X\rho\|_1$ for $X \in \Theta$. For each $X \in \Theta$, Hoeffding's inequality [46] tells us

$$\Pr[|F_X^{\text{obs}} - \mathbb{E}[X]| \geq \mu_X] \leq 2e^{-\frac{2m_X \mu_X^2}{4x^2}} =: \epsilon_X, \quad (\text{A1})$$

where m_X is the number of rounds used for testing observable X . We apply Hoeffding's inequality to every

observable $X \in \Theta$ and combine them using Boole's inequality,

$$\Pr \left[\bigcup_{X \in \Theta} \mathbb{E}[X] \notin [F_X^{\text{obs}} - \mu_X, F_X^{\text{obs}} + \mu_X] \right] \leq \sum_{X \in \Theta} \epsilon_X = \epsilon_{\text{AT}}. \quad (\text{A2})$$

In reverse, this means

$$\Pr \left[\bigcap_{X \in \Theta} \mathbb{E}[X] \in [F_X^{\text{obs}} - \mu_X, F_X^{\text{obs}} + \mu_X] \right] \geq 1 - \epsilon_{\text{AT}}, \quad (\text{A3})$$

and thus

$$\Pr [\rho \in V(\vec{F}^{\text{obs}})] \geq 1 - \epsilon_{\text{AT}}, \quad (\text{A4})$$

where $\vec{F}^{\text{obs}}$ is defined as the vector containing F_X^{obs} in its X th component.

To simplify application, from now on, we require that all ϵ_X are equal; hence, $\epsilon_{\text{AT}} = |\Theta|\epsilon_X$ and $\mu_X = \sqrt{(x^2/2m_X) \ln(2/\epsilon_X)}$.

APPENDIX B: IMPLEMENTATION DETAILS

In this section, we give details about the implementation and parameter choices used to illustrate our security argument, in particular our choices for the ϵ scaling for the lift to coherent attacks. After a general discussion, we start with the fixed-length scenario, followed by the more complex variable-length scenario.

Recall the different security statements in Sec. III, which compose a total security parameter ϵ from various sub-epsilon parameters such as ϵ_{EV} , ϵ_{PA} , ϵ_{AT} , and $\tilde{\epsilon}$. The first two, ϵ_{EV} and ϵ_{PA} , are security parameters related to classical subroutines of the QKD protocol. It is comparably “cheap” to make them almost arbitrarily small, as they scale roughly as $\mathcal{O}(2^{-b})$, where b is the hash length, which is the cost in key rate. The third epsilon, ϵ_{AT} , refers to the acceptance test. As can be seen in Theorem 1, the smaller this parameter, the larger the μ -balls defining the acceptance set. As optimizing over a larger set may significantly lower the key rate, the cost of making ϵ_{AT} small is high. Finally, $\tilde{\epsilon}$ is a “virtual” parameter that does not correspond to any subroutine of the QKD protocol; however, as can be seen by inspecting their corresponding correction terms in Eqs. (5) and (22), its impact on the key rate scales comparably to ϵ_{PA} and ϵ_{EV} .

We denote the target total security parameter for collective attacks by ϵ and the target total security parameter for coherent attacks by ν to avoid confusion. Keeping the discussed impacts of the different epsilons on the key rate

in mind, we aim to maximize the acceptance-testing security parameter at the cost of making all the other epsilons small. To allow for parametrized statements without having to choose numerical values right away, we introduce the parameters $r, s \in [0, 1]$.

1. Fixed-length collective attacks

Recall from Sec. III that the fixed-length ϵ -security statement against collective attacks provides a total security parameter of $\epsilon = \epsilon_{\text{corr}} + \epsilon_{\text{sec}}$, where $\epsilon_{\text{corr}} = \epsilon_{\text{EC}}$ and $\epsilon_{\text{sec}} = \max\{\epsilon_{\text{AT}}, \epsilon_{\text{PA}}\}$. Let r describe how the total security epsilon is split between correctness and secrecy, $\epsilon_{\text{corr}} = r\epsilon$ and consequently $\epsilon_{\text{sec}} = (1-r)\epsilon$. Then, to exploit the maximum in the secrecy statement, we choose $\epsilon_{\text{AT}} = \epsilon_{\text{PA}}$. Furthermore, for simplicity, we choose $\epsilon_{\text{PA}} = \tilde{\epsilon} = (1-r)\epsilon$. This leads to

$$-2 \log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right) = -2 \log_2 \left(\frac{1}{(1-r)\epsilon} \right).$$

Finally, for the error-verification term, we simply obtain

$$-\frac{1}{N} \log_2 \left(\frac{2}{\epsilon_{\text{EV}}} \right) = -\frac{1}{N} \log_2 \left(\frac{2}{r\epsilon} \right),$$

and

$$\mu = \sqrt{\frac{2x^2}{k_T} \ln \left(\frac{2}{\epsilon_{\text{AT}}} \right)} = \sqrt{\frac{2x^2}{k_T} \ln \left(\frac{2}{(1-r)\epsilon} \right)}.$$

2. Fixed-length coherent attacks

We used a similar strategy for the coherent attack scenario. To ensure comparability, we again aim for a total (adjusted) security parameter of $\nu = 10^{-10}$; however, due to the corrections listed in Theorem 3, $\nu_{\text{corr}} = \epsilon_{\text{EV}}$ and $\nu_{\text{sec}} = g_{n,x}(\epsilon_{\text{PA}} + 2\sqrt{2\epsilon_{\text{AT}}})$, we follow a slightly different strategy. Let us discuss this in more detail and denote the scaled security parameters of the subprotocols by ν . While $\nu_{\text{EV}} := \epsilon_{\text{EV}} = r\nu$ remains untouched and we still have $\nu_{\text{sec}} = (1-r)\nu$, let us define $\nu_{\text{PA}} := g_{n,x}\epsilon_{\text{PA}}$ and $\nu_{\text{AT}} := 2g_{n,x}\sqrt{2\epsilon_{\text{AT}}}$. Now we make use of the other parameter s to describe the splitting between the different contributions in the secrecy epsilon. Let $\nu_{\text{PA}} = s\nu_{\text{sec}} = (1-r)s\nu$ and $\nu_{\text{AT}} = (1-s)\nu_{\text{sec}} = (1-r)(1-s)\nu$. As already discussed, this was motivated by the following observation. Despite the apparently massive correction factor of $g_{n,x} = \binom{n+x-1}{n}$, since ϵ_{PA} scales inverse exponentially with the number of hash bits, this can be compensated at the very moderate cost of shortening the key by only $\log_2(g_{n,x})$,

$$\begin{aligned} -\frac{2}{N} \log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right) &\mapsto -\frac{2}{N} \log_2 \left(\frac{g_{n,x}}{\nu_{\text{PA}}} \right) \\ &= -\frac{2}{N} \log_2 \left(\frac{1}{(1-r)s\nu} \right) - \frac{2}{N} \log_2(g_{n,x}); \end{aligned}$$

however, while we can compensate the correction for ϵ_{AT} as well, this increases μ_X , hence enlarging the feasible set, which significantly affects the key rate,

$$\mu = \sqrt{\frac{2x^2}{k_T} \ln\left(\frac{2}{\epsilon_{\text{AT}}}\right)} \mapsto \mu' = \sqrt{\frac{2x^2}{k_T} \ln\left(\frac{16g_{n,x}^2}{v_{\text{AT}}^2}\right)} = \sqrt{\frac{2x^2}{k_T} \left(\log_2\left(\frac{16}{(1-r)^2(1-s)^2v^2}\right) + 2\log_2(g_{n,x}) \right)}.$$

Finally, for the error-verification term, we simply obtain

$$-\frac{1}{N} \log_2\left(\frac{2}{\epsilon_{\text{EV}}}\right) \mapsto -\frac{1}{N} \log_2\left(\frac{2}{rv_{\text{EV}}}\right).$$

3. Variable-length collective attacks

This leads us to the variable-length scenario. Again, we start with the collective-attacks security statement, where $\epsilon_{\text{corr}} = \epsilon_{\text{EV}} = r\epsilon$ and $\epsilon_{\text{sec}} = \epsilon_{\text{PA}} + \epsilon_{\text{AT}} = (1-r)\epsilon$. Similar to before, we set $\epsilon_{\text{PA}} = s\epsilon_{\text{sec}} = (1-r)s\epsilon$ and consequently $\epsilon_{\text{AT}} = (1-s)\epsilon_{\text{sec}} = (1-r)(1-s)\epsilon$. Then, we obtain

$$\alpha = 1 + \frac{\sqrt{\log_2\left(\frac{1}{\epsilon_{\text{PA}}}\right)}}{\log_2(d+1)\sqrt{n}} = 1 + \frac{\sqrt{\log_2\left(\frac{1}{r\epsilon}\right)}}{\log_2(d+1)\sqrt{n}},$$

$$\theta = \frac{\alpha}{\alpha-1} \left(\log_2\left(\frac{1}{4\epsilon_{\text{PA}}} + \frac{2}{\alpha}\right) \right) + \left\lceil \log_2\left(\frac{2}{\epsilon_{\text{EV}}}\right) \right\rceil = \frac{\alpha}{\alpha-1} \left(\log_2\left(\frac{1}{4(1-r)s\epsilon} + \frac{2}{\alpha}\right) \right) + \left\lceil \log_2\left(\frac{2}{r\epsilon}\right) \right\rceil,$$

and

$$\mu = \sqrt{\frac{2x}{k_T} \ln\left(\frac{2}{\epsilon_{\text{AT}}}\right)} = \sqrt{\frac{2x}{k_T} \ln\left(\frac{2}{(1-r)(1-s)\epsilon}\right)}.$$

4. Variable-length coherent attacks

Finally, we come to the variable-length coherent attack scenario. Here, according to Theorem 5, the scaled security statement consists of $v_{\text{corr}} = \epsilon_{\text{EV}}$ and $v_{\text{sec}} = g_{n,x}(\sqrt{8(\epsilon_{\text{PA}} + \epsilon_{\text{AT}})} + \tilde{\epsilon}/2)$. Again, we start with $v_{\text{corr}} = rv$ and $v_{\text{sec}} = (1-r)v$, which we are going to use below.

Next, we set $g_{n,x} \frac{\tilde{\epsilon}}{2} = s v_{\text{sec}} = (1-r)s v$, which yields

$$-2 \log_2\left(\frac{1}{\tilde{\epsilon}}\right) \mapsto -2 \log_2\left(\frac{2(1-r)s}{v}\right) - 2 \log_2(g_{n,x})$$

and leaves us back with $g_{n,x} \sqrt{8\sqrt{\epsilon_{\text{PA}} + \epsilon_{\text{AT}}}} = (1-s)v_{\text{sec}} = (1-r)(1-s)v$. Additionally, we set

$$\epsilon_{\text{PA}} = s \frac{(1-s)^2 v_{\text{sec}}^2}{8g_{n,x}^2} = s \frac{(1-s)^2 (1-r)^2 v^2}{8g_{n,x}^2},$$

and consequently

$$\epsilon_{\text{AT}} = (1-s) \frac{(1-s)^2 v_{\text{sec}}^2}{8g_{n,x}^2} = \frac{(1-r)^2 (1-s)^3 v^2}{8g_{n,x}^2}.$$

This now allows us to discuss the first term of θ ,

$$\begin{aligned} \theta &= \frac{\alpha}{\alpha-1} \left[\log_2\left(\frac{1}{4\epsilon_{\text{PA}}} + \frac{2}{\alpha}\right) \right] + \left\lceil \log_2\left(\frac{2}{\epsilon_{\text{EV}}}\right) \right\rceil \\ &\mapsto \theta' := \frac{\alpha}{\alpha-1} \left[\log_2\left(\frac{8g_{n,x}^2}{4s(1-s)^2 v_{\text{sec}}^2} + \frac{2}{\alpha}\right) \right] + \left\lceil \log_2\left(\frac{2}{rv}\right) \right\rceil \end{aligned}$$

$$\begin{aligned}
&= \frac{\alpha}{\alpha-1} \left[\log_2 \left(\frac{2g_{n,x}^2}{(1-r)^2 s(1-s)^2 v^2} + \frac{2}{\alpha} \right) \right] + \left\lceil \log_2 \left(\frac{2}{rv} \right) \right\rceil \\
&= \frac{\alpha}{\alpha-1} \left[\log_2 \left(g_{n,x}^2 \left(\frac{2}{(1-r)^2 s(1-s)^2 v^2} + \frac{2}{\alpha g_{n,x}^2} \right) \right) \right] + \left\lceil \log_2 \left(\frac{2}{rv} \right) \right\rceil \\
&= \frac{\alpha}{\alpha-1} \left[2 \log_2 (g_{n,x}) + \log_2 \left(\left(\frac{2}{(1-r)^2 s(1-s)^2 v^2} + \frac{2}{\alpha g_{n,x}^2} \right) \right) \right] + \left\lceil \log_2 \left(\frac{2}{rv} \right) \right\rceil \\
&\leq \frac{\alpha}{\alpha-1} \left[2 \log_2 (g_{n,x}) + \log_2 \left(\left(\frac{2}{(1-r)^2 s(1-s)^2 v^2} + \frac{2}{\alpha} \right) \right) \right] + \left\lceil \log_2 \left(\frac{2}{rv} \right) \right\rceil.
\end{aligned}$$

It remains to discuss the scaling of μ ,

$$\mu = \sqrt{\frac{2x}{k_T} \ln \left(\frac{2}{\epsilon_{\text{AT}}} \right)} \mapsto \sqrt{\frac{2x}{k_T} \ln \left(\frac{16g_{n,x}^2}{(1-s)^3 v_{\text{sec}}^2} \right)} = \sqrt{\frac{2x}{k_T} \left[\ln \left(\frac{16}{(1-r)^2 (1-s)^3 v^2} \right) + 2 \ln (g_{n,x}) \right]}.$$

Note that we may choose α freely, in particular according to the security parameters after the lift. Thus, we have

$$\alpha = 1 + \frac{\sqrt{\log_2 \left(\frac{1}{\epsilon_{\text{PA}}} \right)}}{\log_2(d+1)\sqrt{n}} = 1 + \frac{\sqrt{\log_2 \left(\frac{1}{r\epsilon} \right)}}{\log_2(d+1)\sqrt{n}}.$$

APPENDIX C: SIMULATION OF THE ATMOSPHERIC CHANNEL

To demonstrate the advantages of a variable-length security argument, we simulate secure key rates for two different channel behaviors. First, we consider a statistically fluctuating channel, followed by a rapidly fluctuating channel. Both simulations use the noise model from Ref. [27] to relate the following experimental quantities to click matrices: the pair-production rate c_{prod} , dark-count rate d_{dark} , detection efficiency η_d , channel loss probability p_L , and number of environmental (solar) photons n_{sol} . For details regarding this noise model, we refer interested readers to Ref. [27].

1. Statistically fluctuating channel

For this scenario, we assume that both the setup and the channel behavior are relatively well known in advance. The system is characterized by a fixed pair-production rate c_{prod} , a fixed dark-count rate d_{dark} , and a fixed detection efficiency η_d . The channel loss and the number of environmental photons entering the detection device are assumed to follow a normal distribution with means μ_{loss} and μ_{sol} and standard deviations σ_{loss} and σ_{sol} . For our simulation, we then sample n_{sim} -times $p_L \mathcal{N}(\mu_{\text{loss}}, \sigma_{\text{loss}})$, and $n_{\text{sol}} \mathcal{N}(\mu_{\text{sol}}, \sigma_{\text{sol}})$ while keeping all other parameters

fixed. In the fixed-length scenario, within the frame of the acceptance test, the observables ($\hat{W}_1$ and $\hat{W}_2$) are compared to the values w_1^U and w_2 . If they lie within a t -box around those values, the protocol accepts, and we obtain a key of length l ; otherwise, it aborts (and we do not obtain the key). In the variable-length scenario, each run may potentially yield a secure key, although the length differs and depends on the observed values.

2. Rapidly fluctuating channel

For this scenario, we proceed assuming that the system is well characterized. That is, the pair-production rate c_{prod} , the dark-count rate d_{dark} , and the detection efficiency η_d remain fixed and constant. At the same time, we do not know much about the channel. Thus, neither the loss nor the number of environmental photons is known in advance, as they change rapidly. To ease simulation, we nevertheless assume that the conditions only change rapidly between a discrete number of scenarios. In more detail, we model three brightness levels (“pitch dark,” “dark,” and “dawn”), as well as three loss levels (“no clouds,” “slightly cloudy,” and “cloudy”), leading to a total of nine combined scenarios, described by pairs of parameters. If honest channel behavior is known in advance, secure keys could be generated in each of those scenarios; in case of rapid changes—e.g., if a cloud moves into the direct line of sight between transmitter and receiver—the fixed-length protocol aborts in eight out of those nine cases, failing to produce a key. This is because the acceptance test aborts. For simplicity, we assume each of those nine scenarios occurs with the same probability.

In contrast, the variable-length protocol attempts to generate keys in any of those nine scenarios and adapts the secure key length to the measured results.

- [1] C. H. Bennett, and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, India, 1984), p. 175.
- [2] A. K. Ekert, Quantum cryptography based on Bell's theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, *Rev. Mod. Phys.* **81**, 1301 (2009).
- [4] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, Advances in quantum cryptography, *Adv. Opt. Photonics* **12**, 1012 (2020).
- [5] V. C. Usenko, A. Acín, R. Alléaume, U. L. Andersen, E. Diamanti, T. Gehring, A. A. E. Hajomer, F. Kanitschar, C. Pacher, S. Pirandola, and V. Pruneri, Continuous-variable quantum communication, *ArXiv:2501.12801*.
- [6] P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, Long-distance quantum key distribution in optical fibre, *New J. Phys.* **8**, 193 (2006).
- [7] M. Peev *et al.*, The SECOQC quantum key distribution network in Vienna, *New J. Phys.* **11**, 075001 (2009).
- [8] D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, R. J. Hughes, A. E. Lita, S. W. Nam, and J. E. Nordholt, Long-distance decoy-state quantum key distribution in optical fiber, *Phys. Rev. Lett.* **98**, 010503 (2007).
- [9] C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Experimental long-distance decoy-state quantum key distribution based on polarization encoding, *Phys. Rev. Lett.* **98**, 010505 (2007).
- [10] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussi eres, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, Secure quantum key distribution over 421 km of optical fiber, *Phys. Rev. Lett.* **121**, 190502 (2018).
- [11] T. Schmitt-Manderbach, H. Weier, M. F urst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Experimental demonstration of free-space decoy-state quantum key distribution over 144 km, *Phys. Rev. Lett.* **98**, 010504 (2007).
- [12] A. Kr i i  *et al.*, Towards metropolitan free-space quantum networks, *Npj Quantum Inf.* **9**, 1 (2023).
- [13] R. Haber, D. Garbe, S. Busch, W. Rosenfeld, and K. Schilling, Qube - A CubeSat for Quantum Key Distribution Experiments, <https://www.semanticscholar.org/paper/Qube-A-CubeSat-for-Quantum-Key-Distribution-Haber-Garbe/d3da9d85ef68c90ea8a1a1be96d047b7c61bf-dab> (2018).
- [14] C.-Y. Lu, Y. Cao, C.-Z. Peng, and J.-W. Pan, Micius quantum experiments in space, *Rev. Mod. Phys.* **94**, 035001 (2022).
- [15] T. Jennewein, C. Simon, A. Foug eres, F. Babin, F. K. Asadi, K. B. Kuntz, M. Maisonneuve, B. Moffat, K. Mohammadi, and D. Panneton, QEYSSat 2.0 – White Paper on Satellite-based Quantum Communication Missions in Canada, *Arxiv:2306.02481v2*.
- [16] J. S. Sidhu, T. Brougham, D. McArthur, R. G. Pousa, and D. K. L. Oi, Finite key performance of satellite quantum key distribution under practical constraints, *Commun. Phys.* **6**, 1 (2023).
- [17] D. Orsucci, P. Kleinpa , J. Meister, I. De Marco, S. H ausler, T. Strang, N. Walenta, and F. Moll, Assessment of practical satellite quantum key distribution architectures for current and near-future missions, *ArXiv:2404.05668*.
- [18] P. G. Kwiat, Hyper-entangled states, *J. Mod. Opt.* **44**, 2173 (1997).
- [19] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Generation of hyperentangled photon pairs, *Phys. Rev. Lett.* **95**, 260501 (2005).
- [20] A. Martin, T. Guerreiro, A. Tiranov, S. Designolle, F. Fr owis, N. Brunner, M. Huber, and N. Gisin, Quantifying photonic high-dimensional entanglement, *Phys. Rev. Lett.* **118**, 110501 (2017).
- [21] S. Ecker, F. Bouchard, L. Bulla, F. Brandt, O. Kohout, F. Steinlechner, R. Fickler, M. Malik, Y. Guryanova, R. Ursin, and M. Huber, Overcoming noise in entanglement distribution, *Phys. Rev. X* **9**, 041042 (2019).
- [22] L. Sheridan, and V. Scarani, Security proof for quantum key distribution using qudit systems, *Phys. Rev. A* **82**, 030301(R) (2010).
- [23] A. Ferenczi, and N. L utkenhaus, Symmetries in quantum key distribution and the connection between optimal attacks and optimal cloning, *Phys. Rev. A* **85**, 052310 (2012).
- [24] M. Doda, M. Huber, G. Murta, M. Pivoluska, M. Plesch, and C. Vlachou, Quantum key distribution overcoming extreme noise: Simultaneous subspace coding using high-dimensional entanglement, *Phys. Rev. Appl.* **15**, 034003 (2021).
- [25] N. Wyderka, G. Chesi, H. Kampermann, C. Macchiavello, and D. Bru , High-dimensional quantum key distribution rates for multiple measurement bases, *ArXiv:2501.05890*.
- [26] T. N. Thomas, and W. O. Krawec, New key rate bound for high-dimensional BB84 with multiple basis measurements, *ArXiv:2504.11315*.
- [27] F. Kanitschar, A. Bergmayr-Mann, M. Pivoluska, and M. Huber, Harnessing high-dimensional temporal entanglement using limited interferometric setups, *Phys. Rev. Appl.* **22**, 054054 (2024).
- [28] P. J. Coles, E. M. Metodiev, and N. L utkenhaus, Numerical approach for unstructured quantum key distribution, *Nat. Commun.* **7**, 11712 (2016).
- [29] A. Winick, N. L utkenhaus, and P. J. Coles, Reliable numerical key rates for quantum key distribution, *Quantum* **2**, 77 (2018).
- [30] M. Ara ujo, M. Huber, M. Navascu es, M. Pivoluska, and A. Tavakoli, Quantum key distribution rates from semidefinite programming, *Quantum* **7**, 1019 (2023).
- [31] F. Kanitschar, and M. Huber, Practical framework for analyzing high-dimensional quantum key distribution setups, *Phys. Rev. Lett.* **135**, 010802 (2025).
- [32] J. Bavaresco, N. H. Valencia, C. Kl ockl, M. Pivoluska, P. Erker, N. Friis, M. Malik, and M. Huber, Measurements in two bases are sufficient for certifying high-dimensional entanglement, *Nat. Phys.* **14**, 1032 (2018).

- [33] X.-M. Hu, W.-B. Xing, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, P. Erker, and M. Huber, Efficient generation of high-dimensional entanglement through multipath down-conversion, *Phys. Rev. Lett.* **125**, 090503 (2020).
- [34] J. Schneeloch, C. C. Tison, M. L. Fanto, P. M. Alsing, and G. A. Howland, Quantifying entanglement in a 68-billion-dimensional quantum state space, *Nat. Commun.* **10**, 2785 (2019).
- [35] M. C. Ponce, A. L. M. Muniz, M. Huber, and F. Steinlechner, Unlocking the frequency domain for high-dimensional quantum information processing, *ArXiv:2206.00969*.
- [36] A. S. Maxwell, L. B. Madsen, and M. Lewenstein, Entanglement of orbital angular momentum in non-sequential double ionization, *Nat. Commun.* **13**, 4706 (2022).
- [37] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, *Phys. Rev. Lett.* **102**, 020504 (2009).
- [38] S. Nahar, D. Tupkary, Y. Zhao, N. Lütkenhaus, and E. Y. Z. Tan, Postselection technique for optical quantum key distribution with improved de Finetti reductions, *ArXiv:2403.11851*.
- [39] D. Tupkary, E. Y.-Z. Tan, and N. Lütkenhaus, Security proof for variable-length quantum key distribution, *Phys. Rev. Res.* **6**, 023002 (2024).
- [40] I. George, J. Lin, and N. Lütkenhaus, Numerical calculations of the finite key rate for general quantum key distribution protocols, *Phys. Rev. Res.* **3**, 013274 (2021).
- [41] F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols, *PRX Quantum* **4**, 040306 (2023).
- [42] R. Renner, *Security of Quantum Key Distribution*, Ph.D. thesis, ETH Zürich, Zürich, Switzerland, 2005, *ArXiv:quant-ph/0512258*.
- [43] C. Portmann, and R. Renner, Security in quantum cryptography, *Rev. Mod. Phys.* **94**, 025008 (2022).
- [44] M. Tomamichel, and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, *Quantum* **1**, 14 (2017).
- [45] M. Tomamichel, A framework for non-asymptotic quantum information theory, *ArXiv:1203.2142*.
- [46] W. Hoeffding, Probability inequalities for sums of bounded random variables, *J. Am. Stat. Assoc.* **58**, 13 (1963).
- [47] A. Tiranov, S. Designolle, E. Z. Cruzeiro, J. Lavoie, N. Brunner, M. Afzelius, M. Huber, and N. Gisin, Quantification of multidimensional entanglement stored in a crystal, *Phys. Rev. A* **96**, 040303(R) (2017).
- [48] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution, *Phys. Rev. X* **9**, 041064 (2019).
- [49] T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, Dimension reduction in quantum key distribution for continuous- and discrete-variable protocols, *PRX Quantum* **2**, 020325 (2021).
- [50] F. Kanitschar, Composable-Finite-Size-Security-of-High-Dimensional-Quantum-Key-Distribution-Protocols, 2025, <https://github.com/fkan95/Composable-Finite-Size-Security-of-High-Dimensional-Quantum-Key-Distribution-Protocols>
- [51] L. Bulla, M. Pivoluska, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, and R. Ursin, Non-local temporal interferometry for highly resilient free-space quantum communication, *Phys. Rev. X* **13**, 021001 (2023).
- [52] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Provably secure and high-rate quantum key distribution with time-bin qudits, *Sci. Adv.* **3**, e1701491 (2017).
- [53] L. Bulla, K. Hjorth, O. Kohout, J. Lang, S. Ecker, S. P. Neumann, J. Bittermann, R. Kindler, M. Huber, M. Bohmann, R. Ursin, and M. Pivoluska, Distribution of genuine high-dimensional entanglement over 10.2 km of noisy metropolitan atmosphere, *Phys. Rev. A* **107**, L050402 (2023).
- [54] K. Sulimany, G. Pelc, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, High-dimensional coherent one-way quantum key distribution, *Npj Quantum Inf.* **11**, 16 (2025).
- [55] F. Bouchard, D. England, P. J. Bustard, K. L. Fenwick, E. Karimi, K. Heshami, and B. Sussman, Achieving ultimate noise tolerance in quantum communication, *Phys. Rev. Appl.* **15**, 024027 (2021).
- [56] S.-K. Liao *et al.*, Long-distance free-space quantum key distribution in daylight towards inter-satellite communication, *Nat. Photonics* **11**, 509 (2017).
- [57] R. Bedington, J. M. Arrazola, and A. Ling, Progress in satellite quantum key distribution, *npj Quantum Inf.* **3**, 30 (2017).