UNIVERSITY OF LEEDS

This is a repository copy of *Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization*.

White Rose Research Online URL for this paper:
http://eprints.whiterose.ac.uk/165311/

Version: Accepted Version

Article:
Currás Lorenzo, G orcid.org/0000-0003-2096-0036, Wooltorton, L and Razavi, M orcid.org/0000-0003-4172-2125 (2021) Twin-Field Quantum Key Distribution with Fully Discrete Phase Randomization. Physical Review Applied, 15 (1). 014016. ISSN 2331-7019

https://doi.org/10.1103/PhysRevApplied.15.014016

© 2021 American Physical Society. This is an author produced version of an article accepted for publication in Physical Review Applied Uploaded in accordance with the publisher's self-archiving policy.

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Twin-field quantum key distribution with fully discrete phase randomization

Guillermo Currás-Lorenzo,[1,*] Lewis Wooltorton,[1,2] and Mohsen Razavi[1]

[1] *School of Electronic and Electrical Engineering, University of Leeds, Leeds, UK*
[2] *Quantum Engineering Centre for Doctoral Training, H. H. Wills Physics Laboratory and Department of Electrical & Electronic Engineering, University of Bristol, BS8 1FD, UK*

Twin-field (TF) quantum key distribution (QKD) can overcome fundamental secret-key-rate bounds on point-to-point QKD links, allowing us to reach longer distances than ever before. Since its introduction, several TF-QKD variants have been proposed, and some of them have already been implemented experimentally. Most of them assume that the users can emit weak coherent pulses with a continuous random phase. In practice, this assumption is often not satisfied, which could open up security loopholes in their implementations. To close this loophole, we propose and prove the security of a TF-QKD variant that relies exclusively on discrete phase randomization. Remarkably, our results show that it can also provide higher secret-key rates than an equivalent continuous-phase-randomized protocol.

I. INTRODUCTION

Quantum key distribution (QKD) allows two users, Alice and Bob, to generate a shared secret key in the presence of an eavesdropper, Eve, with unlimited computational power. Despite its great potential, QKD has yet to overcome important practical problems before it is ready for widespread use. One of the most important challenges is how to perform QKD at long distances, given that, in optical fibres, the loss increases exponentially with the channel length. Even with a GHz repetition rate, it would take 300 years to successfully send a single photon over 1000 km of standard optical fibres [1]. Another crucial issue is to guarantee that a particular implementation of a QKD protocol is secure. That is, we have to show that QKD implementations satisfy all assumptions made in their corresponding theoretical security proof, or to devise security proofs that match the realities of QKD experiments. In this work, we address the latter issue for twin-field QKD (TF-QKD) [2], one of the key candidates for improving key-rate scaling with distance.

Fundamental bounds show that the key rate of repeaterless QKD protocols scales at best linearly with η [3], where η is the transmittance of the channel connecting Alice and Bob. TF-QKD breaks this limitation, offering a key rate that scales with $\sqrt{\eta}$. The key enabling idea behind the operation of TF-QKD is to effectively generate an entangled state between the two users in the space spanned by vacuum and single-photon states. To do so, we need a repeater node that performs entanglement swapping, using single-photon interference, as well as phase stability across the channel, to make sure the generated state is in the desired superposition form. This approach requires only one photon to survive the path loss over half of the channel, thus the improved scaling with distance. Note that TF-QKD is not the only protocol that achieves this scaling. Other protocols, inspired by quantum repeater structures, can achieve the same key-rate scaling by using quantum memories [4, 5] or quantum non-demolition measurements [6]. However, TF-QKD is, experimentally, in a more advanced state than such alternatives. In fact, certain variants of TF-QKD have already been implemented [7–10], and a distance record exceeding 500 km has already been achieved [11, 12]. The issue of implementation security is crucially relevant for these experiments.

One of the main constraints on a QKD system is given by the type of optical encoder needed in the implementation of the protocol. Its corresponding security proof would then need to address such practical constraints. The single-photon version of TF-QKD has a simple theoretical description [13], but it is difficult to implement in practice. Thus, a significant research effort has focused on developing practical variants [13–16] in which the users encode weak coherent pulses (WCPs). These variants differ in their protocol descriptions and/or security proofs, but, so far, all of them rely on the decoy-state method [17]. That is, they either use decoy states in their key mode [14, 15], i.e., to generate the key, and/or in their test mode [13, 16], i.e., to estimate Eve's side information on the key.

Conventional decoy-state techniques require the emission of phase-randomized coherent states (PRCS), and assume that the users are ideally able to randomize the phase of their pulses *continuously* and *uniformly*. This is, however, difficult to achieve in practice. Experimentally, there are two approaches to randomize the phase of a coherent pulse: passive and active. Passive randomization consists of turning the laser off and then on again to generate the PRCS. In addition to the impracticality of this approach in a high-speed QKD system, it is hard to guarantee experimentally that the generated phase genuinely follows a uniform distribution [18]. In fact, experiments have shown that, in

* g.j.curraslorenzo@leeds.ac.uk

practice, there are phase correlations between adjacent pulses [19, 20]. In an active randomization procedure, a phase modulator is used, in combination with a random number generator. This approach fits the TF-QKD variant of Refs. [13, 16] very well, since one already needs a phase modulator to produce the phase-locked coherent states emitted in the key mode. However, it randomizes the phase over a *discrete*, not *continuous*, set of values. Thus, none of these two approaches necessarily satisfy the assumptions of the decoy-state method, which could open security loopholes in the experimental implementations of TF-QKD.

In this work, we address this security loophole, by proposing and proving the security of a TF-QKD variant that relies exclusively on discrete phase randomization. Note that the use of discrete randomization has already been considered in Ref. [18], in the context of a decoy-state BB84 protocol, where it was treated as a source flaw. Its authors found that, for the decoy-state BB84 protocol, the secret key rate obtainable using discrete randomization is always strictly worse than using continuous randomization, although the former quickly approaches the latter as the number of discrete random phases increases. In fact, in that protocol, one can obtain a performance reasonably close to the continuous case using as few as ten discrete random phases. However, it is not immediately clear whether this behaviour would hold for the TF-QKD variants in [13–16], given that: (i) their security proofs are quite diverse, and some of them very different from that of decoy-state BB84; and (ii) in TF-QKD, both users emit quantum states, and thus the source flaw is present in both users. In fact, recent works have found that the security issue arising from flawed sources that leak information has a much bigger impact in measurement-device-independent (MDI) QKD [21] than in BB84 [22]. In principle, the same could be true for other kinds of source imperfections, such as the use of discrete phase randomization.

The quantum phase of our TF-QKD variant is similar to that of Ref. [13], with the main difference being that we use discrete, not continuous, phase randomization in test mode. However, unlike in the case of decoy-state BB84 [18], we find that our key rate does not simply approach that of Ref. [13] as the number of phase slices increases. Instead, perhaps surprisingly, we can actually obtain *higher* secret-key rates than Ref. [13], with as few as eight discrete random phases. The reason is that discrete randomization allows us to postselect the test-mode rounds in which the users' phase choices exactly *matched*, i.e., they were exactly the same, or their difference was exactly π. As we will see, this postselected data allows for a tighter estimation of the phase-error rate. Intuitively, this is because, in TF-QKD, it is advantageous if the users share the same global phase reference, something that can be equivalently achieved by postselection.

We note that the concept of phase postselection has appeared in other TF-QKD variants [14, 15, 23], although in combination with continuous-phase-randomized signals. Refs. [14, 15] postselect the signals with a *similar*, not *identical*, phase. This introduces challenges in the security analysis, and it is not clear if this approach could be used for the type of TF-QKD variant considered in this work. Ref. [23] assumes that signals with an *identical* phase are postselected. While certainly interesting from a theoretical point of view, this protocol is not implementable in practice, since Alice and Bob will never choose exactly the same phase when using continuous phase randomization.

Similarly to other protocols that rely on discrete randomization [18], we use numerical techniques as part of our security proof. In particular, inspired by the work of Ref. [24], we use semidefinite programming (SDP) techniques to estimate the phase-error rate. We note that, in Ref. [24], the authors already apply their generic numerical technique to prove the security of a TF-QKD protocol with discrete phase randomization. However, in practice, their procedure can only be applied when just a few discrete random phases are used, since the number of constraints grows very quickly as the number of phase values increases. Here, we exploit the particularities of our protocol to introduce an analysis that uses a much smaller number of carefully chosen constraints, and is efficient even with a large number of discrete phases. This allows us to investigate how the key rate improves when increasing the number of phase values.

II. METHODS

A. Protocol description

Our protocol is very similar to that of Refs. [13, 16]. Alice and Bob send quantum signals to an untrusted middle node Charlie, who (ideally) interferes them at a balanced 50:50 beamsplitter, performs a photodetection measurement, and reports the outcome. These signals belong to one of two "modes", key and test, selected at random. Key-mode emissions are used to generate the raw key, while test-mode emissions are used to estimate Eve's side information. In key mode, the users send phase-locked coherent states $\left|\pm\sqrt{\mu}\right\rangle$. In test mode, the users send phase-randomized coherent states of different intensities. Unlike in Refs. [13, 16], the phases of the test-mode states are randomized over a *discrete* set, rather than a continuous range. The detailed protocol steps are the following:

(1) *Preparation*

Alice (Bob) randomly choose the transmission mode, key or test, and

(1.1) If she (he) chooses key mode, she (he) generates a random bit b_A (b_B), prepares an optical pulse in the coherent state $\left|(-1)^{b_A}\sqrt{\mu}\right\rangle$ ($\left|(-1)^{b_B}\sqrt{\mu}\right\rangle$), and sends it to Charlie.

(1.2) If she (he) chooses test mode, she (he) selects a random intensity β_a (β_b) $\in \{\beta_1, \ldots, \beta_{d-2}, \mu, \beta_v\}$, where d is the number of intensities, μ is the same intensity used in key mode, and $\beta_v = 0$ is a vacuum intensity. Then, she (he) selects a random phase θ_a (θ_b) $= \frac{2\pi m}{M}$, where $m \in \{0, 1, 2, \ldots, M-1\}$ and M is the number of random phases, prepares the state $\left|\sqrt{\beta_a}e^{i\theta_a}\right\rangle$ ($\left|\sqrt{\beta_b}e^{i\theta_b}\right\rangle$), and sends it to Charlie.

(2) *Detection*

An honest Charlie interferes Alice and Bob's signals at a 50:50 beamsplitter, followed by threshold detectors D_c and D_d, placed at the output ports corresponding to constructive and destructive interference, respectively. A round is considered successful if exactly one detector clicks, and unsuccessful otherwise. After the measurement, Charlie reports whether or not the round was successful, and, if it was, he reports which specific detector clicked.

(3) *Sifting*

For all successful rounds, Alice and Bob disclose their choices of key mode or test mode, keeping only data from those in which they have used the same mode. Then,

(3.1) They calculate the gain p_{succ} of their key mode rounds, and generate their sifted keys from the values of b_A and b_B corresponding to these rounds. Then, they publicly disclose a small random subset of their sifted keys. With this information, they estimate the fraction of the sifted key, $p_{\text{same}|\text{succ}}$ ($p_{\text{diff}|\text{succ}}$), that originated from emissions in which their phase choices agreed (disagreed). Bob then flips his sifted key bits corresponding to the rounds in which D_d clicked. Based on that, Alice and Bob estimate the bit error rate e_{bit}.

(3.2) For all values of β, Alice and Bob calculate the gains $\{Q_\beta\}$ of the test mode rounds in which they both used intensity β and the same phase $\theta_a = \theta_b$. They also calculate the gains $\{Q_\beta^-\}$ of the rounds in which they both used intensity β and opposite phases $\theta_a = \theta_b \pm \pi$.

(4) *Parameter estimation*

Alice and Bob use the values of $\{Q_\beta\}$ and $\{Q_\beta^-\}$ to estimate the amount of key information I_{AE} that may have been leaked to an eavesdropper.

(5) *Postprocessing*

Alice and Bob perform error correction and privacy amplification to obtain a secret key.

Since this is a discretely-modulated MDI-type protocol, in principle, one could directly use the numerical techniques of Ref. [24] to prove its security. However, the SDP in Ref. [24] requires one constraint, in the form of an inner product, for each combination of emitted states. The number of different states in this protocol can make such an approach infeasible in practice. Namely, since Alice and Bob send $[(d-1)M+1]^2$ different joint states [25], one needs to solve the dual problem of an SDP with $[(d-1)M+1]^4$ inner-product constraints, plus the constraints related to the measurement results of the protocol. Thus, even for $M = 4$ and $d = 3$, the simplest case considered in the numerical results of this paper, one needs to solve a SDP with more than 6561 constraints. For $M = 12$ and $d = 3$, the number of constraints grows to more than 390625. This can make the implementation of such techniques infeasible on conventional computers [26, 27].

In the following, we provide a security analysis that requires to solve the dual problem of two SDPs with only $(d-1)(d-2)M + 2d + M - 1$ constraints each. That is, for the examples considered above, we have SDPs with 17 and 41 constraints, respectively, which can be quickly solved using any commercial off-the-shelf laptop.

B. Security analysis

In our security analysis, we consider the asymptotic scenario in which the users emit an infinite number of signals. Also, for simplicity, we assume collective attacks. We note that, in the asymptotic regime, security against collective attacks implies security against general attacks, thanks to results such as the postselection technique [28].

We consider the virtual protocol in which Alice replaces her key mode emissions by the generation of the state

$$|\psi\rangle_{Aa} = \frac{1}{\sqrt{2}}\left(|0\rangle_A |\sqrt{\mu}\rangle_a + |1\rangle_A |-\sqrt{\mu}\rangle_a\right), \tag{1}$$

where A is a virtual qubit ancilla that she keeps in her lab, and a is the photonic system sent to Charlie; and Bob replaces them by a similarly defined $|\psi\rangle_{Bb}$. We assume that Eve controls not only the quantum channels, but also the untrusted middle node Charlie, and the announcements he makes. As mentioned in the protocol description, for each round, Alice and Bob expect to receive two announcements: whether the round was successful, and, if so, whether Charlie obtained constructive or destructive interference. However, the latter announcement only determines whether or not Bob flips his sifted key bit, which does not affect Eve's side information on Alice's key. Thus, from a security standpoint, we can describe Eve's collective attack as a two-outcome general measurement $\{\hat{M}_{ab}, \hat{M}^f_{ab}\}$ on the photonic systems ab, where $\hat{M}_{ab}$ ($\hat{M}^f_{ab}$) is the Kraus operator corresponding to the announcement of the round as successful (unsuccessful). Conditioned on a successful announcement, Alice and Bob obtain a state,

$$|\Psi\rangle_{AaBb} = \frac{\hat{M}_{ab}\,|\psi\rangle_{Aa}\,|\psi\rangle_{Bb}}{\sqrt{p_{\text{succ}}}}, \tag{2}$$

where $p_{\text{succ}} = \left\| \hat{M}_{ab}\,|\psi\rangle_{Aa}\,|\psi\rangle_{Bb} \right\|^2$ is the probability that Eve announces a key mode round as successful.

In our virtual protocol, after Eve's announcements, Alice and Bob perform the joint measurement $\{\hat{O}_{\text{same}}, \hat{O}_{\text{diff}}\}$, with $\hat{O}_{\text{same}} = |00\rangle\langle 00|_{AB} + |11\rangle\langle 11|_{AB}$ and $\hat{O}_{\text{diff}} = |01\rangle\langle 01|_{AB} + |10\rangle\langle 10|_{AB}$, on the ancillas corresponding to the successful rounds, learning whether they used the same or different phases. Note that this is a valid virtual protocol step, since it commutes with the Z-basis measurement that Alice and Bob would perform to generate their sifted keys. Depending on the result of their joint measurement, they will obtain one of the two post-measurement states

$$|\Psi_{\text{same}}\rangle = \frac{|00\rangle_{AB}\,\hat{M}_{ab}\,|\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b + |11\rangle_{AB}\,\hat{M}_{ab}\,|-\sqrt{\mu}\rangle_a\,|-\sqrt{\mu}\rangle_b}{2\sqrt{p_{\text{succ,same}}}}, \tag{3}$$

$$|\Psi_{\text{diff}}\rangle = \frac{|01\rangle_{AB}\,\hat{M}_{ab}\,|\sqrt{\mu}\rangle_a\,|-\sqrt{\mu}\rangle_b + |10\rangle_{AB}\,\hat{M}_{ab}\,|-\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b}{2\sqrt{p_{\text{succ,diff}}}}, \tag{4}$$

where $p_{\text{succ,same}} = p_{\text{succ}} p_{\text{same|succ}}$ ($p_{\text{succ,diff}} = p_{\text{succ}} p_{\text{diff|succ}}$) is the probability that Alice and Bob use the same (different) phases in a key mode round *and* Eve reports the round as successful. This allows us to define the quantities

$$e_{\text{ph,same}} = \|\,{}_{AB}\langle ++|\Psi_{\text{same}}\rangle\|^2 + \|\,{}_{AB}\langle --|\Psi_{\text{same}}\rangle\|^2, \tag{5}$$

$$e_{\text{ph,diff}} = \|\,{}_{AB}\langle ++|\Psi_{\text{diff}}\rangle\|^2 + \|\,{}_{AB}\langle --|\Psi_{\text{diff}}\rangle\|^2, \tag{6}$$

where $e_{\text{ph,same}}$ ($e_{\text{ph,diff}}$) is the phase-error rate of the successful key mode rounds in which Alice and Bob used the same (different) phases. Eve's side information of the sifted key (per key bit) can now be bounded by

$$I_{AE} \leq p_{\text{same|succ}} h(e_{\text{ph,same}}) + p_{\text{diff|succ}} h(e_{\text{ph,diff}}), \tag{7}$$

where $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the Shannon binary entropy function. The secret key rate that Alice and Bob can distill is

$$R \geq p_{\text{succ}}\left[1 - I_{AE} - f h(e_{\text{bit}})\right], \tag{8}$$

where f is the error correction inefficiency.

The objective of our security analysis is to obtain upper bounds on $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$, using the the data obtained in the test rounds. The procedure is very similar for both terms; we will first explain $e_{\text{ph,same}}$.

1. *Estimation of* $e_{\text{ph,same}}$

First, we rewrite Eq. (3) as

$$|\Psi_{\text{same}}\rangle = \frac{(|++\rangle + |--\rangle)_{AB}\,\hat{M}_{ab}\,|\lambda_{\text{even}}\rangle_{ab} + (|+-\rangle + |-+\rangle)_{AB}\,\hat{M}_{ab}\,|\lambda_{\text{odd}}\rangle_{ab}}{2\sqrt{p_{\text{succ,same}}}}, \tag{9}$$

with $|\lambda_{\text{even}}\rangle_{ab}$ and $|\lambda_{\text{odd}}\rangle_{ab}$ being unnormalized states defined as

$$|\lambda_{\text{even}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b + |-\sqrt{\mu}\rangle_a\,|-\sqrt{\mu}\rangle_b) = \sum_{n\in\mathbb{N}_0}\sqrt{P_{n|\mu}}\,|\lambda_n\rangle_{ab}\,, \tag{10}$$

$$|\lambda_{\text{odd}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a\,|\sqrt{\mu}\rangle_b - |-\sqrt{\mu}\rangle_a\,|-\sqrt{\mu}\rangle_b) = \sum_{n\in\mathbb{N}_1}\sqrt{P_{n|\mu}}\,|\lambda_n\rangle_{ab}\,, \tag{11}$$

where $\mathbb{N}_0$ ($\mathbb{N}_1$) is the set of non-negative even (odd) numbers, $|\lambda_n\rangle_{ab}$ is the n-photon two-mode Fock state defined by

$$|\lambda_n\rangle_{ab} = \frac{1}{\sqrt{2^n n!}}(a^\dagger + b^\dagger)^n |00\rangle_{ab}\,, \tag{12}$$

and

$$P_{n|\mu} = \frac{e^{-2\mu}(2\mu)^n}{n!}, \tag{13}$$

follows a Poisson distribution of average 2μ. Combining Eq. (5) and Eq. (9), we have that

$$e_{\text{ph,same}} = \frac{1}{2p_{\text{succ,same}}} \left\| \hat{M}_{ab} |\lambda_{\text{even}}\rangle_{ab} \right\|^2. \tag{14}$$

Finding a way to estimate the quantity in Eq. (14) is critical for our security proof. One possible approach would be to apply the Cauchy-Schwarz inequality to show that

$$\left\| \hat{M}_{ab} |\lambda_{\text{even}}\rangle_{ab} \right\|^2 \leq \left[\sum_{n\in\mathbb{N}_0} \sqrt{P_{n|\mu} Y_n} \right]^2, \tag{15}$$

where $Y_n = \left\| \hat{M}_{ab} |\lambda_n\rangle_{ab} \right\|^2$ is the yield probability of the state $|\lambda_n\rangle_{ab}$. Let us assume that Alice and Bob used continuous phase-randomization on their test mode emissions, and kept only the data from the events in which they use the same intensity and the same phase. Then, the resulting post-selected state, given that they both chose intensity β, can be expressed as

$$\frac{1}{2\pi}\int_0^{2\pi} d\theta \left|\sqrt{\beta}e^{i\theta}\right\rangle \left|\sqrt{\beta}e^{i\theta}\right\rangle \left\langle\sqrt{\beta}e^{i\theta}\right| \left\langle\sqrt{\beta}e^{i\theta}\right|_{ab} = \sum_{n=0}^{\infty} P_{n|\beta} |\lambda_n\rangle\langle\lambda_n|_{ab}\,, \tag{16}$$

where $P_{n|\beta}$ follows a Poisson distribution and is given by Eq. (13). Then, one could apply the standard decoy-state method to estimate the yield probabilities Y_n, $\forall n \in \mathbb{N}_0$, and plug these in Eq. (15) to estimate $e_{\text{ph,same}}$ in Eq. (14). Essentially, this is the approach of Ref. [23]. However, note that if Alice and Bob use continuous phase-randomization, the probability that they select exactly the same phase θ is zero, and the resulting protocol is not implementable in practice.

Here, we use the same test-mode phase-postselection idea as in Ref. [23], but we employ discrete phase randomization, which results in a protocol that is actually implementable. In this case, Eq. (16) becomes

$$\rho_\beta = \frac{1}{M}\sum_{m=0}^{M-1} \left|\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right\rangle \left|\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right\rangle \left\langle\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right| \left\langle\sqrt{\beta}e^{\frac{2i\pi m}{M}}\right|_{ab} = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} \left|\lambda^{\beta}_{n \bmod M}\right\rangle \left\langle\lambda^{\beta}_{n \bmod M}\right|_{ab}, \tag{17}$$

where ρ_β is the post-selected state when Alice and Bob both used intensity β and the same phase [18]. In Eq. (17), we have that

$$\left|\lambda^{\beta}_{n \bmod M}\right\rangle_{ab} = \sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta}}{P^{\beta}_{n \bmod M}}} |\lambda_{Ml+n}\rangle_{ab}\,, \tag{18}$$

$$P^{\beta}_{n \bmod M} = \sum_{l=0}^{\infty} P_{Ml+n|\beta}. \tag{19}$$

and $P_{n|\beta}$ is given by Eq. (13). Note that for the vacuum intensity β_v, we have

$$\rho_{\beta_v} = \left|\lambda^{\beta_v}_{0 \bmod M}\right\rangle \left\langle\lambda^{\beta_v}_{0 \bmod M}\right|_{ab} = |\lambda_0\rangle\langle\lambda_0|_{ab}\,. \tag{20}$$

Unlike the states $|\lambda_n\rangle$ in Eq. (16), the states $\left|\lambda^{\beta}_{n \bmod M}\right\rangle$ in Eq. (17) have a slight dependence on the intensity β. Thus, their yield probabilities,

$$Y^{\beta}_{n \bmod M} = \left\| \hat{M}_{ab} \left|\lambda^{\beta}_{n \bmod M}\right\rangle_{ab} \right\|^2, \tag{21}$$

are not necessarily equal for two different intensities β_1 and β_2, which prevents us from applying the standard decoy-state method. Instead, we use a similar idea as in Ref. [24], defining the Gram matrix G of the set of Eve's post-measurement states, and constructing a semidefinite program in which the objective function and all the constraints are linear functions of entries of G. In our case, we define G as the Gram matrix of the vector set $\left\{\hat{M}_{ab}\left|\lambda^{\beta}_{n \bmod M}\right\rangle\right\}$, $\forall \beta \in \mathcal{T}$ and $n \in \{0, 1, ..., M-1\}$, where $\mathcal{T}$ is the set of all test-mode intensities, except vacuum. The entries of G are $G_{ij} = \langle i|j\rangle$, where $|i\rangle$ denotes the i-th element of the vector set.

Our objective function is Eq. (14), which we can write as

$$e_{\text{ph,same}} = \frac{1}{2p_{\text{succ,same}}} \langle \lambda_{\text{even}}|\hat{M}^{\dagger}_{ab}\hat{M}_{ab}|\lambda_{\text{even}}\rangle \,. \tag{22}$$

By re-expressing $|\lambda_{\text{even}}\rangle$ and $|\lambda_{\text{odd}}\rangle$ in Eqs. (10) and (11) as

$$\begin{aligned} |\lambda_{\text{even}}\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_0}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, |\lambda^{\mu}_{n \bmod M}\rangle_{ab} \,, \\ |\lambda_{\text{odd}}\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_1}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, |\lambda^{\mu}_{n \bmod M}\rangle_{ab} \,, \end{aligned} \tag{23}$$

it becomes clear that the right-hand side of Eq. (22) is a linear function of elements of G.

Our constraints are the following:

- Taking the norm squared of both sides of Eq. (3), and solving for $p_{\text{succ,same}}$, we obtain

$$p_{\text{succ,same}} = \frac{1}{2} \langle \lambda_{\text{even}}|\hat{M}^{\dagger}\hat{M}|\lambda_{\text{even}}\rangle + \frac{1}{2} \langle \lambda_{\text{odd}}|\hat{M}^{\dagger}\hat{M}|\lambda_{\text{odd}}\rangle \,. \tag{24}$$

- From Eq. (17), we have that

$$Q_{\beta} = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} Y^{\beta}_{n \bmod M}, \tag{25}$$

  where Q_{β} is the measured gain of the state ρ_{β}. Note that $Y^{\beta}_{n \bmod M}$ is a (diagonal) element of G, thus Eq. (25) is a linear function of elements of G.

- Using the trace distance inequality [18], we obtain

$$Y^{\beta_1}_{n \bmod M} - Y^{\beta_2}_{n \bmod M} \leq \sqrt{1 - F^{\beta_1,\beta_2}_{n}}, \tag{26}$$

  where

$$F^{\beta_1,\beta_2}_{n} = \left|\left\langle \lambda^{\beta_1}_{n \bmod M}\middle|\lambda^{\beta_2}_{n \bmod M}\right\rangle_{ab}\right|^2 = \left[\sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta_1}}{P^{\beta_1}_{n \bmod M}}} \sqrt{\frac{P_{Ml+n|\beta_2}}{P^{\beta_2}_{n \bmod M}}}\right]^2 . \tag{27}$$

- Our next constraint is based on the inequality

$$Y^{\beta_1}_{n \bmod M} \leq 1 - Y^{\beta_2}_{n \bmod M} + 2\sqrt{F^{\beta_1,\beta_2}_{n}(1 - F^{\beta_1,\beta_2}_{n})(1 - Y^{\beta_2}_{n \bmod M})Y^{\beta_2}_{n \bmod M}} + F^{\beta_1,\beta_2}_{n}(2Y^{\beta_2}_{n \bmod M} - 1), \tag{28}$$

  which holds when $Y^{\beta_2}_{n \bmod M} \leq F^{\beta_1,\beta_2}_{n}$ [29]. This bound is tighter than the trace distance inequality in Eq. (26), but cannot be directly added to the SDP, since it is a non-linear function of $Y^{\beta_2}_{n \bmod M}$, an element of G. The only exception is the case $n = 0$ and $\beta_2 = \beta_v$, since from Eq. (20), we have that

$$Y^{\beta_v}_{0 \bmod M} = Y_0 = Q_{\beta_v}, \tag{29}$$

and Q_{β_v}, the gain of the vacuum intensity, is directly measurable from the protocol. Thus, substituting $n = 0$, $\beta_1 = \beta$, $\beta_2 = \beta_v$ and $Y^{\beta_v}_{0 \bmod M} = Q_{\beta_v}$ in Eq. (28), we have the inequality

$$Y^{\beta}_{0 \bmod M} \leq 1 - Q_{\beta_v} + 2\sqrt{F_0^{\beta,\beta_v}(1 - F_0^{\beta,\beta_v})(1 - Q_{\beta_v})Q_{\beta_v}} + F_0^{\beta,\beta_v}(2Q_{\beta_v} - 1), \tag{30}$$

which is a linear function of $Y^{\beta}_{0 \bmod M}$. Equation (30) holds when $Q_{\beta_v} \leq F_0^{\beta,\beta_v}$, which should always happen in practice, since $Q_{\beta_v} \approx 0$ and $F_0^{\beta,\beta_v} \approx 1$.

- For our final constraints, we use the fact that $Y^{\beta}_{n \bmod M} \leq 1$, $\forall n, \beta$. To reduce the number of constraints, we only include the case $\beta = \mu$.

Combining everything, we have that our upper-bound on $e_{\text{ph,same}}$ is the solution of the following SDP:

$$\begin{aligned}
&\max_{G} \quad \frac{1}{2p_{\text{succ,same}}} \langle \lambda_{\text{even}} | \hat{M}^\dagger \hat{M} | \lambda_{\text{even}} \rangle \text{ s.t.} \\
&p_{\text{succ,same}} = \frac{1}{2} \langle \lambda_{\text{even}} | \hat{M}^\dagger \hat{M} | \lambda_{\text{even}} \rangle + \frac{1}{2} \langle \lambda_{\text{odd}} | \hat{M}^\dagger \hat{M} | \lambda_{\text{odd}} \rangle ; \\
&Q_\beta = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} Y^{\beta}_{n \bmod M}, \quad \forall \beta \in \mathcal{T}; \\
&Y^{\mu}_{n \bmod M} \leq 1, \quad \forall n \in \{0, ..., M-1\}; \\
&Y^{\beta_1}_{n \bmod M} - Y^{\beta_2}_{n \bmod M} \leq \sqrt{1 - F_n^{\beta_1,\beta_2}}, \quad \forall \beta_1, \beta_2 \in \mathcal{T}, \ n \in \{0, ..., M-1\}; \\
&Y^{\beta}_{0 \bmod M} \leq 1 - Q_{\beta_v} + 2\sqrt{F_0^{\beta,\beta_v}(1 - F_0^{\beta,\beta_v})(1 - Q_{\beta_v})Q_{\beta_v}} + F_0^{\beta,\beta_v}(2Q_{\beta_v} - 1), \quad \forall \beta \in \mathcal{T};
\end{aligned} \tag{31}$$

where $\mathcal{T} = \{\beta_1, \ldots, \beta_{d-2}, \mu\}$ is the set of all test-mode intensities, except vacuum.

2. *Estimation of* $e_{\text{ph,diff}}$

The procedure to estimate $e_{\text{ph,diff}}$ is very similar to that of $e_{\text{ph,same}}$. In this case, we rewrite Eq. (4) as

$$|\Psi_{\text{diff}}\rangle = \frac{(|{+}{+}\rangle - |{-}{-}\rangle)_{AB} \hat{M}_{ab} |\lambda^-_{\text{even}}\rangle_{ab} + (|{-}{+}\rangle - |{+}{-}\rangle)_{AB} \hat{M}_{ab} |\lambda^-_{\text{odd}}\rangle_{ab}}{2\sqrt{p_{\text{succ,diff}}}}, \tag{32}$$

where $|\lambda^-_{\text{even}}\rangle_{ab}$ and $|\lambda^-_{\text{odd}}\rangle_{ab}$ are unnormalized states defined as

$$|\lambda^-_{\text{even}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a |{-}\sqrt{\mu}\rangle_b + |{-}\sqrt{\mu}\rangle_a |\sqrt{\mu}\rangle_b) = \sum_{n+m \in \mathbb{N}_0} c_n c_m |n\rangle_a |m\rangle_b = \sum_{n \in \mathbb{N}_0} \sqrt{P_{n|\mu}} |\lambda^-_n\rangle_{ab}, \tag{33}$$

$$|\lambda^-_{\text{odd}}\rangle_{ab} = \frac{1}{2}(|\sqrt{\mu}\rangle_a |{-}\sqrt{\mu}\rangle_b - |{-}\sqrt{\mu}\rangle_a |\sqrt{\mu}\rangle_b) = \sum_{n+m \in \mathbb{N}_1} c_n c_m |n\rangle_a |m\rangle_b = \sum_{n \in \mathbb{N}_1} \sqrt{P_{n|\mu}} |\lambda^-_n\rangle_{ab}, \tag{34}$$

$|\lambda^-_n\rangle_{ab}$ is the n-photon two-mode Fock state defined by

$$|\lambda^-_n\rangle_{ab} = \frac{1}{\sqrt{2^n n!}} (a^\dagger - b^\dagger)^n |00\rangle_{ab}, \tag{35}$$

and $P_{n|\mu}$ is given by Eq. (13). In this case, the state after post-selecting the test mode emissions in which Alice and Bob both used intensity β and opposite phases $\theta_a = \theta_b \pm \pi = \theta$ is

$$\rho^-_\beta = \frac{1}{M} \sum_{m=0}^{M-1} \left|\sqrt{\beta} e^{\frac{2i\pi m}{M}}\right\rangle \left|{-}\sqrt{\beta} e^{\frac{2i\pi m}{M}}\right\rangle \left\langle \sqrt{\beta} e^{\frac{2i\pi m}{M}}\right| \left\langle {-}\sqrt{\beta} e^{\frac{2i\pi m}{M}}\right|_{ab} = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} \left|\lambda^{\beta,-}_{n \bmod M}\right\rangle\!\left\langle \lambda^{\beta,-}_{n \bmod M}\right|_{ab}, \tag{36}$$

where

$$\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle_{ab} = \sum_{l=0}^{\infty} \sqrt{\frac{P_{Ml+n|\beta}}{P^{\beta}_{n \bmod M}}} |\lambda^-_{Ml+n}\rangle_{ab}, \tag{37}$$

$P_{n|\beta}$ is given by Eq. (13), and $P^{\beta}_{n \bmod M}$ is given by Eq. (19).

Similarly as in the previous subsection, we re-express $|\lambda^{-}_{\text{even}}\rangle$ and $|\lambda^{-}_{\text{odd}}\rangle$ as

$$\begin{aligned} \left|\lambda^{-}_{\text{even}}\right\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_0}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, \left|\lambda^{\mu,-}_{n \bmod M}\right\rangle_{ab}, \\ \left|\lambda^{-}_{\text{odd}}\right\rangle_{ab} &= \sum_{\substack{n=0 \\ n\in\mathbb{N}_1}}^{M-1} \sqrt{P^{\mu}_{n \bmod M}}\, \left|\lambda^{\mu,-}_{n \bmod M}\right\rangle_{ab}, \end{aligned} \tag{38}$$

and define

$$Y^{\beta,-}_{n \bmod M} = \left\| \hat{M}_{ab} \left|\lambda^{\beta,-}_{n \bmod M}\right\rangle_{ab} \right\|^2. \tag{39}$$

This time, we define G as the Gram matrix of the vector set $\left\{\hat{M}_{ab}\left|\lambda^{\beta,-}_{n \bmod M}\right\rangle\right\}$, and follow a similar procedure as in the last subsection to construct the objective function and the constraints. In the end, we have that our upper-bound on $e_{\text{ph,diff}}$ is the solution of the following SDP:

$$\begin{aligned} &\max_{G} \quad \frac{1}{2p_{\text{succ,diff}}} \left\langle \lambda^{-}_{\text{even}} \middle| \hat{M}^{\dagger}\hat{M} \middle| \lambda^{-}_{\text{even}} \right\rangle \text{ s.t.} \\ &p_{\text{succ,diff}} = \frac{1}{2}\left\langle \lambda^{-}_{\text{even}} \middle| \hat{M}^{\dagger}\hat{M} \middle| \lambda^{-}_{\text{even}} \right\rangle + \frac{1}{2}\left\langle \lambda^{-}_{\text{odd}} \middle| \hat{M}^{\dagger}\hat{M} \middle| \lambda^{-}_{\text{odd}} \right\rangle; \\ &Q^{-}_{\beta} = \sum_{n=0}^{M-1} P^{\beta}_{n \bmod M} Y^{\beta,-}_{n \bmod M}, \quad \forall \beta \in \mathcal{T}; \\ &Y^{\mu,-}_{n \bmod M} \leq 1, \quad \forall n \in \{0, ..., M-1\}; \\ &Y^{\beta_1,-}_{n \bmod M} - Y^{\beta_2,-}_{n \bmod M} \leq \sqrt{1 - F^{\beta_1,\beta_2}_{n}}, \quad \forall \beta_1, \beta_2 \in \mathcal{T},\ n \in \{0, ..., M-1\}; \\ &Y^{\beta,-}_{0 \bmod M} \leq 1 - Q^{-}_{\beta_v} + 2\sqrt{F^{\beta,\beta_v}_{0}(1 - F^{\beta,\beta_v}_{0})(1 - Q^{-}_{\beta_v})Q^{-}_{\beta_v}} + F^{\beta,\beta_v}_{0}(2Q^{-}_{\beta_v} - 1), \quad \forall \beta \in \mathcal{T}; \end{aligned} \tag{40}$$

where F^{β_1,β_2}_{n} is given by Eq. (27) and $\mathcal{T} = \{\beta_1, \ldots, \beta_{d-2}, \mu\}$ is the set of all test-mode intensities, except vacuum.

III. NUMERICAL RESULTS

Here, we simulate the secret key rate obtainable as a function of the overall Alice-Bob loss, which includes the inefficiency of Charlie's detectors, for different values of M, the number of random phases. For the sake of our numerical simulations, we assume that there is no eavesdropper, and we only model the imperfections in the system to simulate the values one may obtain in a real experiment. We assume a misalignment error rate of 2%, matching the results of a recent experiment [7], and a dark count probability of 10^{-8} per pulse. In all curves, we assume that Alice and Bob use three different test-mode intensities $\{\beta_1, \mu, \beta_v\}$, where $\beta_v = 0$ is a vacuum intensity and μ is the same intensity used in key mode. We optimize over the value of μ and β_1, with the condition that $\mu, \beta_1 \geq 10^{-4}$. This condition is motivated by the fact that it is experimentally difficult to produce a laser pulse with a very small, but fixed, intensity.

In our channel model, we make the additional assumption that, when Charlie obtains a click on both detectors, he announces the round as successful, and randomly chooses which detector he reports as having clicked. While this is a slight deviation from the protocol described in Section II A, it greatly simplifies all gain and yield formulas, at the cost of introducing some additional errors. In the low-loss regime, when double clicks are relatively common, this assumption slightly lowers the key rate obtainable. At medium to high losses, when the probability of a double click is almost zero, the effect vanishes. Under this assumption, we have that

$$Q_{\beta} = Q^{-}_{\beta} = (1-d)(1 - e^{-2\sqrt{\eta}\beta} + 2de^{-2\sqrt{\eta}\beta}), \tag{41}$$

where d is the dark count probability of each detector, and η is the overall Alice-Bob loss. Moreover, $p_{\text{succ}} = Q_{\mu}$, and $p_{\text{same|succ}} = p_{\text{diff|succ}} = 1/2$, due to the symmetry of the setup. The bit error rate of the sifted key is given by

$$e_{\text{bit}} = \frac{(1-d)e_{\text{mis}} - (e_{\text{mis}} - d)e^{-2\sqrt{\eta}\mu}}{p_{\text{succ}}}, \tag{42}$$

where e_{mis} is the misalignment error probability. To obtain a reliable upper bound on $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$, we need to substitute the above values in Eq. (31) and Eq. (40), and numerically solve the dual problem of each SDP [24, 30]. Note that, due to the symmetry assumed in our channel model, the SDPs in Eq. (31) and Eq. (40) end up being identical; in our simulations, we only solve their dual problem once, since its solution provides an upper-bound on both $e_{\text{ph,same}}$ and $e_{\text{ph,diff}}$. To solve this SDP dual problem, we have written a MATLAB program that uses the CVX toolbox [31], which we run on a commercial laptop.

In Fig. 1, we see that the protocol can overcome the repeaterless bound [3] with as few as four random phases. For the ideal case of $M \to \infty$, we use Eq. (15), assuming that Alice and Bob are somehow able to estimate the exact values of Y_n, $\forall n$, using the data collected in test mode. These values are given by $Y_0 = 2d(1-d)$ and, for $n > 0$,

$$Y_n = (1-d)(1-(1-\sqrt{\eta})^2 + 2d(1-\sqrt{\eta})^n). \tag{43}$$

As explained in the discussion following Eq. (15), the case of $M \to \infty$ is not actually implementable in practice, but it provides an upper-bound on the secret key rate obtainable for finite values of M. Notably, Fig. 1 shows that one can get very close to this ideal scenario with only $M = 12$ random phases.

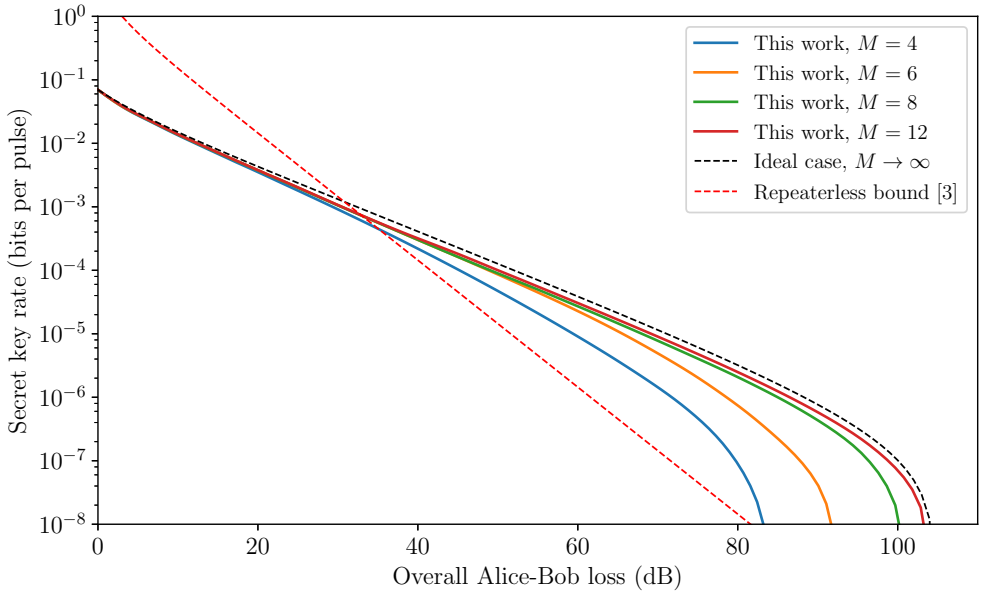

Figure 1. Secret key rate for our discrete-phase-randomized protocol at different values of M, in comparison to fundamental bound for repeaterless QKD systems $-\log_2(1-\eta)$, where η is the overall Alice-Bob transmissivity.

In Fig. 2, we compare the results of our protocol with those of Ref. [13], one of the best performing TF-QKD variants, in both the asymptotic [32] and finite-key [33] regimes. The comparison is interesting because the quantum phase of Ref. [13] is almost identical to ours, the only difference being their use of continuous phase randomization in test mode. Thus, Fig. 2 directly compares the performance of the discrete and continuous randomization approaches. Remarkably, we obtain higher secret-key rates using discrete phase randomization, as long as one uses eight random phases or more. This may sound surprising at first instance, but it is justified by the fact that, for the same value of μ, we can obtain a tighter estimation of the phase-error rate in the discrete-phase version, thanks to the test-mode phase postselection. This can be seen in Fig. 3(a), where we compare the upper-bound on the phase-error rate of the two protocols for a fixed value $\mu = 0.06$. In a practical setting, one would optimize over the value of μ, in which case the two protocols result in similar bounds for the phase-error rate, see Fig. 3(b). But, this will be achieved at a higher value of μ for our protocol, see Fig. 3(c), which results in a higher gain, see Fig. 3(d), and hence a higher secret-key rate.

IV. CONCLUSION AND DISCUSSION

Most previous variants of TF-QKD have relied on the emission of weak laser pulses with a continuous random phase, which is difficult to achieve and certify in practice. Here, we have proposed a practical TF-QKD variant that

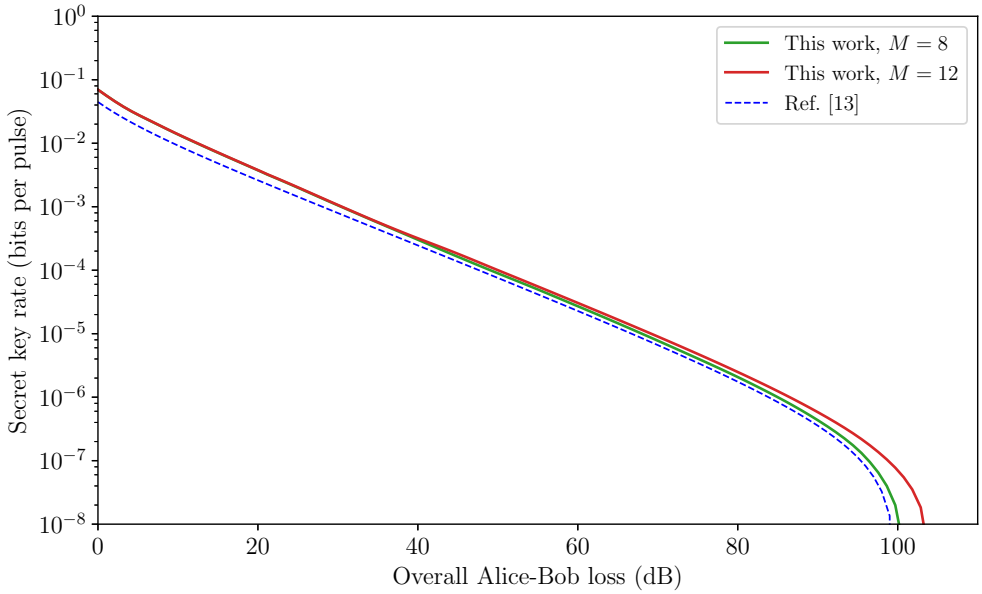

Figure 2. Comparison between the results of this work and those of Ref. [13], which uses continuous phase randomization in its test-mode emissions. For simplicity, to compute the results in [13], we assume that Alice and Bob's test-mode rounds provide perfect estimates of the yield probabilities Y_{nm} for $n + m \leq 4$, while the rest are upper-bounded by one. This is an ideal scenario and, as shown in [13], the results will be slightly worse once one considers the imperfect estimates that result from the use of a finite set of decoy states, as we do for the results in this work.

uses discrete phase randomization instead. Its security proof relies on post-selecting the test-mode rounds in which the users' phase values exactly matched, which is not practically possible with a continuous randomization approach. Consequently, our discretely-randomized protocol can actually result in *higher* key rates than an equivalent protocol based on continuous randomization. This is interesting, given that discrete randomization is usually considered to be a source flaw. In fact, previous analyses of decoy-state QKD with discrete randomization [18] obtained strictly worse results than their continuous counterparts. Our security proof relies on a customised version of numerical techniques for MDI-QKD protocols based on semidefinite programming, which has a substantially reduced complexity as compared with the generic approach.

There are several ways by which we can improve our analysis to account for additional imperfections in a real implementation. For instance, in our analysis, we assume that the users can modulate the phase of their pulses precisely. It would be interesting to find out how they key-rate bounds change when the phase modulator, while fully characterized, is imperfect. Also, we have considered the asymptotic regime in which Alice and Bob run the protocol for infinitely many rounds. It remains an open question whether discrete randomization could still offer an advantage in a finite-key setting. Since state-of-the-art numerical finite-key proofs can only prove security tightly against a restricted class of eavesdropping attacks [34, 35], important developments are needed before we can rigorously answer this question.

We note that, shortly after the first version of this manuscript was uploaded to the arXiv, Zhang et al uploaded another manuscript [36] proposing an alternative TF-QKD protocol with discrete phase randomization. The main difference seems to be that in our protocol, only two phases are encoded in key mode, while in their proposal, M phases are encoded in the key mode, i.e. as many as in the test mode. This symmetry simplifies the phase-error rate formula. However, while the secret key rate of our protocol increases with M, theirs approaches zero as M grows, due to the sifting factor.

ACKNOWLEDGMENTS

We thank Kiyoshi Tamaki, Marcos Curty, Álvaro Navarrete, Margarida Pereira, Zhen-Qiang Yin, and Xiongfeng Ma for valuable discussions. This work was supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement number 675662 (QCALL). L.W. acknowledges the support of of UK EPSRC Grant EP/SO23607/1. All data generated can be reproduced by the equations and the

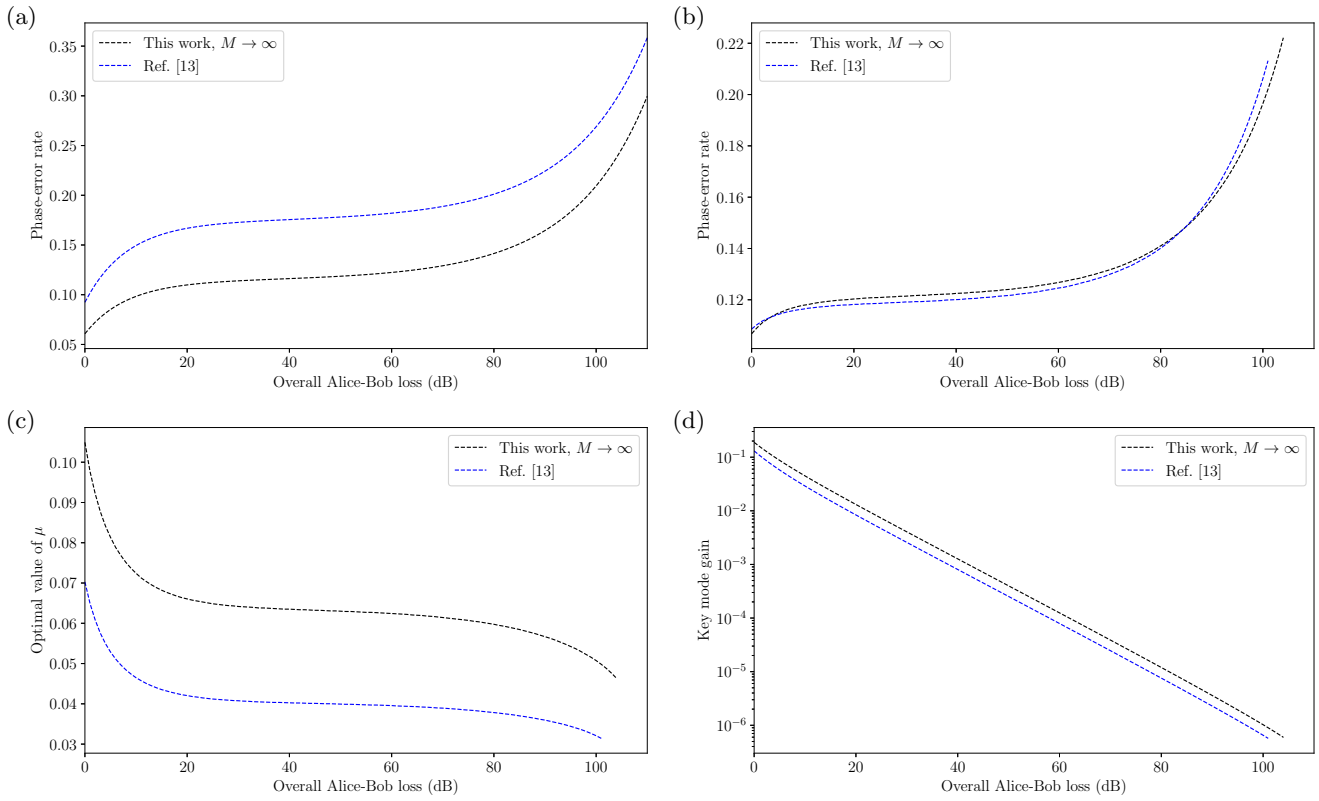

Figure 3. Comparison between the value of some terms in our analysis, for the ideal case $M \to \infty$, and the analysis in Ref. [13]. (a) Upper-bound on the phase-error rate, assuming a fixed value $\mu = 0.06$. (b) Upper-bound on the phase-error rate, for the value of μ that optimizes the key rate in each analysis. (c) Value of μ that optimizes the key rate in each analysis. (d) Key mode gain for the value of μ that optimizes the key rate in each analysis.

methodology introduced in this paper.

[1] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[2] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[3] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[4] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution, New J. Phys. **16**, 043005 (2014).

[5] S. Abruzzo, H. Kampermann, and D. Bruß, Measurement-device-independent quantum key distribution with quantum memories, Phys. Rev. A **89**, 012301 (2014).

[6] K. Azuma, K. Tamaki, and W. J. Munro, All-photonic intercity quantum key distribution, Nat. Commun. **6**, 10171 (2015).

[7] M. Minder, M. Pittaluga, G. Roberts, M. Lucamarini, J. Dynes, Z. Yuan, and A. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photonics **13**, 334 (2019).

[8] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field type quantum key distribution, Phys. Rev. Lett. **123**, 100506 (2019).

[9] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental twin-field quantum key distribution through sending or not sending, Phys. Rev. Lett. **123**, 100505 (2019).

[10] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system, Phys. Rev. X **9**, 021046 (2019).

[11] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, Z. Wang, L. You, M.-J. Li, H. Chen, Y.-A. Chen, Q. Zhang, C.-Z. Peng, X. Ma, T.-Y. Chen, and J.-W. Pan, Implementation of quantum

key distribution surpassing the linear rate-transmittance bound, Nature Photonics **14**, 422 (2020).
[12] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, X.-L. Hu, J.-Y. Guan, Z.-W. Yu, H. Xu, J. Lin, *et al.*, Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km, Phys. Rev. Lett. **124**, 070501 (2020).
[13] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, npj Quantum Inf. **5**, 1 (2019).
[14] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).
[15] X. Ma, P. Zeng, and H. Zhou, Phase-matching quantum key distribution, Phys. Rev. X **8**, 031043 (2018).
[16] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-field quantum key distribution without phase postselection, Phys. Rev. Appl. **11**, 034053 (2019).
[17] H.-K. Lo, X. Ma, and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[18] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, Discrete-phase-randomized coherent state source and its application in quantum key distribution, New J. Phys. **17**, 053014 (2015).
[19] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, and H.-K. Lo, Ultrafast quantum random number generation based on quantum phase fluctuations, Opt. Express **20**, 12366 (2012).
[20] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, J. Capmany, V. Pruneri, and M. Mitchell, Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode, Opt. Express **22**, 1645 (2014).
[21] W. Wang, K. Tamaki, and M. Curty, Measurement-device-independent quantum key distribution with leaky sources, arXiv:2001.08086 (2020).
[22] W. Wang, K. Tamaki, and M. Curty, Finite-key security analysis for quantum key distribution with leaky sources, New J. Phys. **20**, 083027 (2018).
[23] R. Wang, Z.-Q. Yin, F.-Y. Lu, S. Wang, W. Chen, C.-M. Zhang, W. Huang, B.-J. Xu, G.-C. Guo, and Z.-F. Han, Optimized protocol for twin-field quantum key distribution, Communications Physics **3**, 149 (2020).
[24] I. W. Primaatmaja, E. Lavie, K. T. Goh, C. Wang, and C. C. W. Lim, Versatile security analysis of measurement-device-independent quantum key distribution, Phys. Rev. A **99**, 062332 (2019).
[25] To compute the number of states, note that the set of test-mode states contains the set of key-mode states, so one only needs to count the former. Also, when Alice or Bob choose the vacuum intensity, they send the same vacuum state, independently of their choice of random phase.
[26] Y. Ye, Lecture notes in SDP rank reduction, `https://web.stanford.edu/~yyye/sdprank-slides09.pdf` (2009).
[27] J. Gondzio, Interior point methods 25 years later, Eur. J. Oper. Res. **218**, 587 (2012).
[28] M. Christandl, R. König, and R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett. **102**, 020504 (2009).
[29] M. Pereira, G. Kato, A. Mizutani, M. Curty, and K. Tamaki, Quantum key distribution with correlated sources, Sci. Adv. **6**, eaaz4487 (2020).
[30] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Numerical approach for unstructured quantum key distribution, Nat. Commun. **7**, 1 (2016).
[31] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1, `http://cvxr.com/cvx` (2014).
[32] M. Lucamarini, Recent progress on measurement-device-independent quantum key distribution, `http://2018.qcrypt.net/wp-content/uploads/2018/slides/Wednesday/01.Marco%20Lucamarini.pdf` (2018).
[33] G. Currás Lorenzo, A. Navarrete, K. Azuma, G. Kato, M. Curty, and M. Razavi, Tight finite-key security for twin-field quantum key distribution, arXiv:1910.11407 (2019).
[34] D. Bunandar, L. C. Govia, H. Krovi, and D. R. Englund, Numerical finite-key analysis of quantum key distribution, arXiv:1911.07860 (2019).
[35] I. George, J. Lin, and N. Lütkenhaus, Numerical calculations of finite key rate for general quantum key distribution protocols, arXiv:2004.11865 (2020).
[36] C.-M. Zhang, Y.-W. Xu, R. Wang, and Q. Wang, Twin-field quantum key distribution with discrete-phase-randomized sources, arXiv:2008.05277 (2020).