Simple security proof of twin-field type quantum key distribution protocol

Marcos Curty,[1] Koji Azuma,[2,3,*] and Hoi-Kwong Lo[4]

[1]*Escuela de Ingeniería de Telecomunicación, Dept. of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*
[2]*NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[3]*NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa 243-0198, Japan*
[4]*Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering and Department of Physics, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

(Dated: July 23, 2018)

Twin-field (TF) quantum key distribution (QKD) was proposed as a scheme that could beat the private capacity of a point-to-point optical QKD link by using single-photon interference in a middle repeater node. This remarkable result has recently triggered an intense research activity to prove its security. Here, we introduce a TF-type QKD protocol which is conceptually simpler than the original proposal. It relies on local phase randomization, instead of global phase randomization, which significantly simplifies its security analysis and is arguably less demanding experimentally. We demonstrate that the secure key rate of our protocol has a square-root improvement over the point-to-point private capacity, as conjectured by the original TF-QKD scheme.

PACS numbers: 03.67.Dd, 03.67.Hk 03.65.Bg, 03.67.Pp, 03.67.-a

There is a tremendous research interest towards developing a global quantum internet [1–6], as this could enable many useful applications of quantum technologies, including, for example, quantum key distribution (QKD) [7, 8], blind quantum computing [9, 10], distributed quantum metrology [11, 12] and distributed quantum computing [13]. Among these applications, QKD is certainty the most mature technology today. Experimentally, long-distance QKD has already been performed over 404 km [14] of telecom fibers with a standard measurement-device-independent QKD (MDI-QKD) protocol [15], as well as over 1000 km of free space through satellite to ground links [16, 17]. Nonetheless, optical loss in telecom fibers (typically about 0.2 dB/km) poses an important limit to the distance of secure QKD without trusted relay nodes [18]. Indeed, even with a GHz repetition rate, it would take about 100 years to send a single photon successfully over 1000 km of a telecom fiber [19]. In fact, fundamental limits for the key rate vs distance for secure QKD have been obtained recently [20, 21]. They essentially state that, in the absence of relays, the key rate scales as η, where η is the transmittance of the channel between Alice and Bob.

Remarkably, Lucamarini *et al.* [22] have recently proposed a novel MDI-QKD type protocol, called twin-field (TF) QKD, that uses single-photon interference and is conjectured to beat the fundamental bounds in [20, 21], similarly to the provably secure MDI-QKD schemes introduced in [23–25] based on two-photon interference. One experimental drawback of TF-QKD is however that single-photon interference requires subwavelength-order phase stability for optical channels, which is more demanding than achieving two-photon interference [26]. Nonetheless, if the conjecture on the security of TF-QKD is proven to be correct, the simplicity and conceptual importance of this protocol will definitively stimulate further investigations. Indeed, very recently, two independent works [27, 28] have analysed the security of slightly modified versions of the original TF-QKD scheme, and claim secure key rates that scale as $\sqrt{\eta}$ (under some suitable assumptions). While this is remarkable, the security proofs are rather complex; Ref. [27] exploits a quantum coin idea [29, 30], and both Refs. [27, 28] stick to the *global* phase randomization idea originally introduced in TF-QKD.

In this paper we present a conceptually simpler TF-QKD type protocol that inherits the use of single-photon interference from the original proposal [22], but uses *local* phase randomization instead of global phase randomization. In this regard, the protocol resembles the original MDI-QKD scheme [15]. At the same time, it is also regarded as using the X/Z-basis states, instead of the X/Y-basis states employed in its phase-encoding version [31]. The modification has two main consequences. First, it might simplify the path to an experimental implementation. And, second, combined with the decoy-state method [32–34], it allows the use of the number states as the complementary basis to prove the security [35], thus leading to a quite simple security proof. In so doing, we demonstrate that the secure key rate scales as $\sqrt{\eta}$.

The key idea originates from entanglement generation

protocols [36, 37] based on single-photon interference in quantum repeaters. In particular, suppose that Alice and Bob are separated over a distance L and there is a node C right in the middle between them. This node is connected to Alice (Bob) through an optical fiber with transmittance $\sqrt{\eta}$. If Alice and Bob implement the original MDI-QKD scheme in this scenario, it is clear that the key rate cannot scale better than η, as this protocol requires that two photon coincidence events with one photon from Alice and one from Bob interfere in the node C. In comparison, TF-QKD can provide a key rate scaling with $\sqrt{\eta}$ because it only requires singles, *i.e.*, one photon (either from Alice or from Bob) reaches the node C. Indeed, this scaling improvement is well-known in the field of quantum repeaters. For instance, the performance of the repeater schemes introduced in [36, 37] scales as $\sqrt{\eta}$ essentially because they use entanglement generation protocols based on single-photon interference in node C. Our starting point is then an ideal version of these entanglement generation protocols with an idealized photon source.

Protocol 1: It consists of the following six steps. (i) Alice (Bob) first prepares an optical pulse a (b) in an entangled state $|\phi_q\rangle_{Aa} = \sqrt{q}|0\rangle_A|0\rangle_a + \sqrt{1-q}|1\rangle_A|1\rangle_a$ ($|\phi_q\rangle_{Bb}$) with $0 \leq q \leq 1$, where $|0\rangle_{a(b)}$ is the vacuum state and $|1\rangle_{a(b)}$ is the single-photon state for optical pulse a (b), and system A (B) denotes a qubit in Alice's (Bob's) hands with computational basis $\{|0\rangle_{A(B)}, |1\rangle_{A(B)}\}$. (ii) Next, Alice and Bob send the optical pulses a and b through optical channels with transmittance $\sqrt{\eta}$, respectively, to the middle node C in a synchronized manner. (iii) The node C applies to the incoming pulses a 50:50 beamsplitter, followed by two threshold detectors. Let D_c (D_d) denote the detector located at the output port c (d) of the beamsplitter associated to constructive (destructive) interference. (iv) The node C announces the measurement outcome k_c (k_d) corresponding to detector D_c (D_d), where $k_c = 0$ and $k_c = 1$ ($k_d = 0$ and $k_d = 1$) indicates a no-click event and a click event, respectively. (v) With probability p_X Alice (Bob) performs the X-basis measurement on the qubit A (B), and with probability p_Z she (he) performs the Z-basis measurement. As a result, Alice (Bob) obtains the bit value b_A (b_B), where $(-1)^{b_A} = x$ ($(-1)^{b_B} = x$) for the eigenvalues $x = \pm 1$ of the Pauli operators $\hat{X}$ and $\hat{Z}$. (vi) Alice and Bob's raw keys are obtained from those b_A and b_B where node C reports a click in only one detector (*i.e.*, $k_c + k_d = 1$) and they measure their qubits in the X basis. Note that in this protocol no phase randomization is applied

We remark that step (iii) above actually corresponds to performing a "swap test" on the incoming signals. Such a swap test is commonly used in, for example, quantum digital signature schemes [38] and quantum fingerprinting protocols [39–41].

For simplicity and for the moment, let us neglect the effect of the dark counts in the detectors D_c and D_d and assume that their detection efficiency is perfect. Then, it is straightforward to show that the probability r with which node C observes only one click in say detector D_c (D_d) in step (iv) above is $r = r_1 + r_2$, where

$$r_1 = \sqrt{\eta}(1-q)q + (1-q)^2\sqrt{\eta}(1-\sqrt{\eta}), \tag{1}$$

$$r_2 = \frac{1}{2}(1-q)^2\eta. \tag{2}$$

That is, r_1 (r_2) corresponds to a detection event produced by a single-photon (two-photon) pulse.

Given only one detection click in say detector D_c (D_d), the joint state of Alice and Bob's qubit systems A and B is denoted by $\hat{\rho}^+_{AB}$ ($\hat{\rho}^-_{AB}$), where

$$\hat{\rho}^{\pm}_{AB} = \frac{r_1}{r}\left[\frac{q}{q+(1-q)(1-\sqrt{\eta})}|\Psi^{\pm}\rangle\langle\Psi^{\pm}|_{AB} + \frac{(1-q)(1-\sqrt{\eta})}{q+(1-q)(1-\sqrt{\eta})}|11\rangle\langle 11|_{AB}\right] + \frac{r_2}{r}|11\rangle\langle 11|_{AB}, \tag{3}$$

with $|\Psi^{\pm}\rangle_{AB} := (|01\rangle_{AB} \pm |10\rangle_{AB})/\sqrt{2}$.

According to Protocol 1, Alice and Bob obtain their raw key from those events where they measure their qubits A and B in the X basis. This means that the bit-error rate, e_X, is defined by the probability with which Alice's and Bob's measurement outcomes are different (*i.e.*, $b_A \neq b_B$) when $k_c = 1$ and $k_d = 0$, or they are equal ($b_A = b_B$) when $k_c = 0$ and $k_d = 1$. On the other hand, the phase-error rate, e_Z, is defined by the probability with which Alice's and Bob's measurement outcomes in the Z basis coincide ($b_A = b_B$) when $k_c + k_d = 1$. From Eq. (3) we obtain that e_X and e_Z satisfy

$$2e_X = e_Z = \frac{r_1}{r}\frac{(1-q)(1-\sqrt{\eta})}{q+(1-q)(1-\sqrt{\eta})} + \frac{r_2}{r}. \tag{4}$$

The asymptotic key rate formula R_X is then given by

$$R_X = 2r[1 - h(e_X) - h(e_Z)], \tag{5}$$

where $2r$ represents the total success probability and $h(x)$ is the binary entropy function, *i.e.*, $h(x) := -x\log_2 x - (1-x)\log_2(1-x)$. The parameter q is chosen such that R_X is maximized for each given distance.

Protocol 2: We can also consider a prepare-and-measure version of Protocol 1. For this, we note that, without loss of generality, the measurement in step (v) of Protocol 1 can be done soon after its step (i). This is because this measurement operation *commutes* with all the operations performed in the other steps. So, the ordering of the steps is not relevant to the physics. Hence, Protocol 1 is mathematically equivalent to a prepare-and-measure protocol where one omits step (v) and replaces step (i) with the following step: (i') Alice (Bob) prepares an optical pulse a (b) in the state $|X_0\rangle_{a(b)} := \sqrt{q}|0\rangle_{a(b)} + \sqrt{1-q}|1\rangle_{a(b)}$ for $b_A = 0$ ($b_B = 0$) or in the state $|X_1\rangle_{a(b)} := \sqrt{q}|0\rangle_{a(b)} - \sqrt{1-q}|1\rangle_{a(b)}$ for

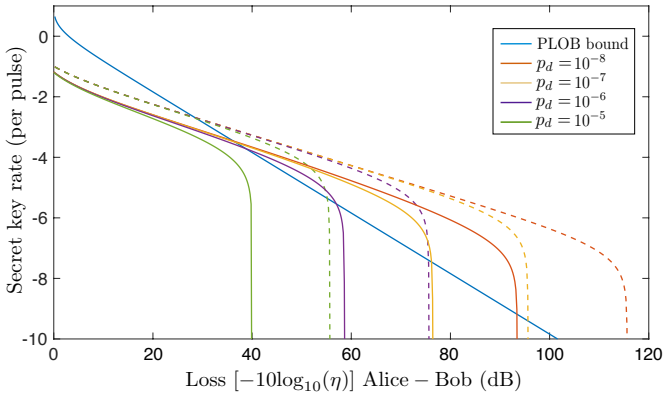

FIG. 1: Secret key rate (per pulse) in logarithmic scale as a function of the *overall* loss between Alice and Bob, which includes the finite detection efficiency of the threshold detectors in node C. For simulation purposes, we set a misalignment of 2% in each channel Alice-C and Bob-C. The dashed (solid) lines correspond to Protocol 1/Protocol 2 (Protocol 3) for different dark count rates, p_d, of the detectors in node C. The solid blue line illustrates the PLOB bound introduced in [21]. Our simulation results show clearly that, even in the presence of reasonably low values of dark counts of about 10^{-6} per pulse and misalignment, the Protocols could beat the PLOB bound.

$b_A = 1$ ($b_B = 1$) at random when she (he) chooses the X basis with probability p_X, while Alice (Bob) prepares the optical pulse a (b) in the state $|Z_0\rangle_{a(b)} := |0\rangle_{a(b)}$ for $b_A = 0$ ($b_B = 0$) with probability q or in the state $|Z_1\rangle_{a(b)} := |1\rangle_{a(b)}$ for $b_A = 1$ ($b_B = 1$) with probability $1-q$ when she (he) chooses the Z basis with probability p_Z. That is, Protocol 2 is composed of step (i'), as well as steps (ii)-(iv) and (vi) from Protocol 1.

In Fig. 1, we show the performance of these two protocols by maximizing R_X over q as a function of the overall loss between Alice and Bob. According to our computation calculation, the optimal value of $q = ||_a\langle 0||\phi_q\rangle_{Aa}||^2$ starts from about 0.88 at 0 dB, and then monotonically increases with the loss up to a value of about 0.94 at 20 dB, and afterward remains basically constant. The high value of q suggests that the states $|X_k\rangle$ ($k = 0, 1$) could be replaced by coherent states $|(-1)^k\alpha\rangle$ by choosing an appropriate amplitude $\alpha(\geq 0)$, as their good approximation. Also, since the states $|Z_k\rangle$ ($k = 0, 1$) are number states, Alice and Bob could estimate the phase-error rate e_Z by using phase-randomized coherent states in combination with the decoy-state method. These two observations lead to the following practical protocol.

Protocol 3: It is composed of the following modified first step (i") together with steps (ii)-(iv) and (vi) from Protocol 1: (i") Alice (Bob) first chooses the X basis with probability p_X and the Z basis with probability p_Z. If her (his) choice is the X basis, she (he) prepares an optical pulse a (b) in a coherent state $|\alpha\rangle_{a(b)}$ for $b_A = 0$ ($b_B = 0$) or $|-\alpha\rangle_{a(b)}$ for $b_A = 1$ ($b_B = 1$) at random. If her (his) choice is the Z basis, she (he) prepares an optical pulse a (b) in a phase-randomized coherent state $\hat{\rho}_{a,\beta_A}$ ($\hat{\rho}_{b,\beta_B}$) whose amplitude β_A (β_B) is chosen from a set $S = \{\beta_i\}_i$ of real nonnegative numbers $\beta_i \geq 0$ at random.

It is important to note that Protocol 3 requires that the node C shares a *phase reference* with Alice and Bob. However, since in QKD Alice and Bob may use ancillary strong pulses generated by lasers to establish such a pulse reference, we believe that establishing a phase reference is practical. In this scenario, we assume that all the X-basis (key generation) states of Alice and Bob are either of the same or opposite phase. That is, *no* phase randomization is needed for the key generation states. In contrast, all the Z-basis states (used for test for tampering) of Alice and Bob have random phases, which allows us to apply the decoy state technique to these states to infer the contributions from the vacuum, single-photon, and multi-photon components. Also, note that p_X can be chosen much higher than p_Z to have a high key generation rate.

Security proof of Protocol 3: For simplicity we shall consider the asymptotic scenario where Alice and Bob emit an infinite number of signals. Also, without loss of generality, we shall assume that the node C is under the full control of an eavesdropper, Eve. After a QKD run, Alice and Bob can estimate the probability distribution $p_{ZZ}(k_c, k_d|\beta_A, \beta_B)$ ($p_{XX}(k_c, k_d|b_A, b_B)$) over k_c and k_d given the choice of β_A and β_B (b_A and b_B) and the selection of the Z (X) basis. By noting that

$$p_{XX}(b_A, b_B|k_c, k_d) = \frac{1}{4}\frac{p_{XX}(k_c, k_d|b_A, b_B)}{p_{XX}(k_c, k_d)}, \quad (6)$$

where

$$p_{XX}(k_c, k_d) = \frac{1}{4}\sum_{b_A, b_B=0,1} p_{XX}(k_c, k_d|b_A, b_B), \quad (7)$$

we have that the bit-error rate, e_{X,k_ck_d}, for Eve's announcement of k_c and k_d is defined by

$$\begin{aligned} e_{X,10} &= \sum_{i,j|i\oplus j=1} p_{XX}(b_A = i, b_B = j|k_c = 1, k_d = 0), \\ e_{X,01} &= \sum_{j=0,1} p_{XX}(b_A = j, b_B = j|k_c = 0, k_d = 1). \end{aligned} \quad (8)$$

Next we consider the decoy-state method. In particular, since when Alice and Bob choose the Z basis in step (i") of Protocol 3 they prepare phase-randomized coherent states, Eve cannot distinguish this step from the following fictitious scenario: Alice (Bob) prepares an optical pulse a (b) in a number state $|n_A\rangle_a$ ($|n_B\rangle_b$) according to a Poissonian distribution $P_{\beta_A^2}(n_A)$ ($P_{\beta_B^2}(n_B)$), where $P_\lambda(n) = (e^{-\lambda}\lambda^n)/n!$. In this fictitious scenario, Eve's attack can only depend on the number states $|n_A\rangle$ and $|n_B\rangle$. This implies that Eve's announcement of k_c and

k_d follows a probability distribution $p_{ZZ}(k_c,k_d|n_A,n_B)$. Then, we have

$$p_{ZZ}(k_c,k_d|\beta_A,\beta_B) = \sum_{n_A,n_B=0}^{\infty} p_{ZZ}(k_c,k_d|n_A,n_B)P_{\beta_A^2}(n_A)P_{\beta_B^2}(n_B) \quad (9)$$

for any β_A and β_B. That is, once Alice and Bob know $p_{ZZ}(k_c,k_d|\beta_A,\beta_B)$ for any β_A and β_B, they can use the decoy-state method to estimate $p_{ZZ}(k_c,k_d|n_A,n_B)$ based on their knowledge of $P_{\beta_A^2}(n_A)$ and $P_{\beta_B^2}(n_B)$.

The next step is to relate the conditional probabilities $p_{ZZ}(k_c,k_d|n_A,n_B)$ with the phase-error rate to prove security [35]. For this, note that if Alice and Bob choose the X basis in step (i") of Protocol 3, Eve cannot distinguish this step from the following fictitious step: Alice (Bob) prepares an optical pulse a (b) and a qubit A (B) in an entangled state $|\psi_X\rangle_{Aa} = (|+\rangle_A|\alpha\rangle_a + |-\rangle_A|-\alpha\rangle_a)/\sqrt{2}$ ($|\psi_X\rangle_{Bb}$) with $|\pm\rangle_{A(B)} := (|0\rangle_{A(B)} \pm |1\rangle_{A(B)})/\sqrt{2}$. By running this fictitious step together with steps (ii)-(iv) in order, Alice and Bob obtain a state

$$|\chi_{k_ck_d}\rangle_{Aa'Bb'} := \frac{\hat{M}^{ab}_{k_ck_d}|\psi_X\rangle_{Aa}|\psi_X\rangle_{Bb}}{\sqrt{p_{XX}(k_c,k_d)}}, \quad (10)$$

with probability $p_{XX}(k_c,k_d)$, where $\hat{M}^{ab}_{k_ck_d}$ is the Kraus operator corresponding to the announcement of k_c and k_d. The phase-error rate, e_{Z,k_ck_d}, is then defined by

$$e_{Z,k_ck_d} = \sum_{j=0,1} \|_{AB}\langle jj||\chi_{k_ck_d}\rangle_{Aa'Bb'}\|^2. \quad (11)$$

Since ${}_A\langle i||\psi_X\rangle_{Aa} = |C_i\rangle_a$ with unnormalized cat states

$$|C_0\rangle_a = e^{-\frac{\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{2n}}{\sqrt{(2n)!}}|2n\rangle_a =: \sum_{n=0}^{\infty} c_n^{(0)}|n\rangle_a, \quad (12)$$

$$|C_1\rangle_a = e^{-\frac{\alpha^2}{2}} \sum_{n=0}^{\infty} \frac{\alpha^{2n+1}}{\sqrt{(2n+1)!}}|2n+1\rangle_a =: \sum_{n=0}^{\infty} c_n^{(1)}|n\rangle_a, \quad (13)$$

for nonnegative coefficients $c_n^{(i)} \geq 0$, from Eq. (10) and for any $i,j = 0,1$, we have

$$\begin{aligned} &p_{XX}(k_c,k_d)\|_{AB}\langle ij||\chi_{k_ck_d}\rangle_{Aa'Bb'}\|^2 \\ &= {}_a\langle C_i|_b\langle C_j|(\hat{M}^{ab}_{k_ck_d})^\dagger \hat{M}^{ab}_{k_ck_d}|C_i\rangle_a|C_j\rangle_b \\ &= \sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{(i)}_{m_A}c^{(j)}_{m_B}c^{(i)}_{n_A}c^{(j)}_{n_B} \\ &\times {}_a\langle m_A|_b\langle m_B|(\hat{M}^{ab}_{k_ck_d})^\dagger \hat{M}^{ab}_{k_ck_d}|n_A\rangle_a|n_B\rangle_b \\ &\leq \sum_{m_A,m_B,n_A,n_B=0}^{\infty} c^{(i)}_{m_A}c^{(j)}_{m_B}c^{(i)}_{n_A}c^{(j)}_{n_B} \\ &\times \|\hat{M}^{ab}_{k_ck_d}|m_A\rangle_a|m_B\rangle_b\|\|\hat{M}^{ab}_{k_ck_d}|n_A\rangle_a|n_B\rangle_b\| \\ &= \left[\sum_{n_A,n_B=0}^{\infty} c^{(i)}_{n_A}c^{(j)}_{n_B}\sqrt{p_{ZZ}(k_c,k_d|n_A,n_B)}\right]^2, \end{aligned} \quad (14)$$

where we have used the Cauchy-Schwarz inequality and $\|\hat{M}^{ab}_{k_ck_d}|m_A\rangle_a|m_B\rangle_b\|^2 = p_{ZZ}(k_c,k_d|m_A,m_B)$. By combining these results with Eq. (11), we conclude

$$\begin{aligned} &p_{XX}(k_c,k_d)e_{Z,k_ck_d} \leq p_{XX}(k_c,k_d)e^{\rm upp}_{Z,k_ck_d} \\ &:= \sum_{j=0,1}\left[\sum_{n_A,n_B=0}^{\infty} c^{(j)}_{n_A}c^{(j)}_{n_B}\sqrt{p_{ZZ}(k_c,k_d|n_A,n_B)}\right]^2. \end{aligned} \quad (15)$$

That is, we can estimate an upper bound, $e^{\rm upp}_{Z,k_ck_d}$, on the phase-error rate e_{Z,k_ck_d} from the observed data. This means that the asymptotic key rate formula, R_{X,k_ck_d}, can be lower bounded as

$$\begin{aligned} &R_{X,k_ck_d} = p_{XX}(k_c,k_d)\left[1 - h(e_{X,k_ck_d}) - h(e_{Z,k_ck_d})\right] \\ &\geq p_{XX}(k_c,k_d)[1 - h(e_{X,k_ck_d}) - h(\min\{1/2, e^{\rm upp}_{Z,k_ck_d}\})] \\ &=: R^{\rm low}_{X,k_ck_d}, \end{aligned} \quad (16)$$

which leads to the final key rate formula:

$$R_X = R_{X,10} + R_{X,01} \geq R^{\rm low}_{X,10} + R^{\rm low}_{X,01} =: R^{\rm low}_X. \quad (17)$$

The performance of Protocol 3 is illustrated in Fig. 1, where we maximize a further lower bound on $R^{\rm low}_X$ over α as a function of the overall loss between Alice and Bob. In particular, here we assume the asymptotic scenario where Alice and Bob use an infinite number of decoy settings and they can estimate the probabilities $p_{ZZ}(k_c,k_d|n_A,n_B)$, with $(n_A,n_B) = (0,0),(0,2),(2,0)$ and $(1,1)$, precisely, while the remaining probabilities are simply upper bounded as $p_{ZZ}(k_c,k_d|n_A,n_B) \leq 1$. Nonetheless, we remark that practical decoy state protocols with a finite number of types of decoy states and finite data size can be applied here. See e.g. [42, 49]. Clearly, the more probabilities $\{p_{ZZ}(k_c,k_d|n_A,n_B)\}_{n_A,n_B}$ Alice and Bob tightly estimate, the higher the resulting key rate is. Importantly, Fig. 1 demonstrates that $R^{\rm low}_X$ has $\sqrt{\eta}$ scaling.

The fact that the cases $(n_A,n_B) = (0,1)$ or $(1,0)$ do not contribute at all to the phase-error rate is remarkable. The reason for this behaviour is the following. The even (odd) cat state corresponding to $j = 0$ ($j = 1$) in Eq. (12) (Eq. (13)) includes only even (odd) photons. And Eq. (14) considers what happens when Alice's input and Bob's input are both (phase-randomized) even cat states or both (phase-randomized) odd cat states. Thus, the terms $(0,1)$ and $(1,0)$ never contribute. This means that by lowering bounding other contributions, such as $(n_A,n_B) = (0,0),(0,2),(2,0)$ and $(1,1)$, with decoy states, one can severely limit the amount of information Eve has on the sifted key. Moreover, note that the signals contain mainly only one photon or less originating from *either* Alice or Bob. The net transmittance of the signal is thus of order $\sqrt{\eta}$, which leads to a very high key rate for TF-type QKD at long distances. That is, it is mainly the interference between the single photon

component generated by either Alice or Bob that leads to security.

We also remark that by regarding $c_n^{(j)} = \sqrt{q_{n|j} q_j}$ with probability distributions $\{q_j\}_j$ and $\{q_{n|j}\}_n$, one can consider the terms $c_{n_A}^{(j)} c_{n_B}^{(j)} \sqrt{p_{ZZ}(k_c, k_d | n_A, n_B)}$ to be the square root of a joint probability. This implies that $p_{XX}(k_c, k_d)(e_{Z,k_c k_d} - e^{\rm upp}_{Z,k_c k_d})(\leq 0)$ is a convex function over probabilities that can be obtained by performing positive operator-valued measure (POVM) measurements on a quantum state for a round in a virtual scenario. This is enough [43] to prove the security of Protocol 3 against coherent attacks, thanks to Azuma's inequality [44].

Finally, we note that the structure of the security proof of Protocol 3 resembles that for the loss-tolerant QKD protocol [45]. Therefore, its extension to the finite-key scenario could be readily done by using similar techniques like those employed in [46–48], in combination with the decoy-state analysis employed in standard MDI-QKD [49].

In summary, we have introduced a novel TF-type QKD protocol, together with a simple proof of its security, which can beat the fundamental bounds on the private capacity of point-to-point QKD over a lossy optical channel presented in [20, 21]. Its secret key rate scales as $\sqrt{\eta}$ rather than η, being η the transmittance of the quantum channel. This protocol could also be regarded as a phase-encoding MDI-QKD scheme with single-photon interference. Indeed, it inherits the major advantage of standard MDI-QKD, *i.e.*, it is robust against any side channel in the measurement unit.

Acknowledgements.—We thank G. Kato and Y. Zhang for helpful discussions, M. Lucamarini and K. Tamaki for discussions related to the papers [22, 27], and X. Ma and P. Zeng for discussions related to the paper [28]. K.A. thanks support from CREST, JST JP-MJCR1671. M.C. acknowledges support from the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grants TEC2014-54898-R and TEC2017-88243-R, and the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 675662 (project QCALL). H.-K.L. thanks the US Office of Naval Research, NSERC, CFI, ORF, MITACS, Huawei Technologies Canada Co., Ltd, and the Royal Bank of Canada for financial support.

Author contributions. M.C. and K.A. contributed equally to this work; M.C. contributed more to the protocol design and K.A. to its security proof. H.-K.L. triggered the consideration of this research project. All authors contributed to the writing and generalization of the ideas.

Note added.—During the preparation of this paper, two other works considering similar protocols have been posted on preprint servers [50] or presented in a conference [51]. We thank N. Lütkenhaus' group for discussions regarding the results in [51]. While our formulation and discussion for security have some similarities with these results, there are also differences in the methodology and our initial idea was conceived independently of these two works.

* Electronic address: azuma.koji@lab.ntt.co.jp

[1] H. J. Kimble, Nature **453**, 1023 (2008).
[2] K. Azuma, A. Mizutani, and H.-K. Lo, Nat. Commun. **7**, 13523 (2016).
[3] S. Pirandola, arXiv:1601.00966 (2016).
[4] K. Azuma and G. Kato, Phys. Rev. A **96**, 032332 (2017).
[5] S. Bäuml and K. Azuma, Quantum Sci. and Technol. **2**, 024004 (2017).
[6] L. Rigovacca *et al.*, New. J. Phys. **20**, 013033 (2018).
[7] V. Scarani *et al.*, Rev. Mod. Phys. **81**, 1301 (2009).
[8] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).
[9] A. Broadbent, J. Fitzsimons and E. Kashefi, in *Proc. of the 50th Annual Symposium on Foundations of Computer Science (FOCS'09)*, (IEEE Computer Society, 2009), p. 517-526.
[10] D. Aharonov, M. Ben-Or and E. Eban, in *Proc. of Innovations in Computer Science*, Beijing, (Tsinghua University Press, 2010), p. 453.
[11] P. Kómór *et al.*, Nat. Phys. **10**, 582 (2014).
[12] D. Gottesman, T. Jennewein, and S. Croke, Phys. Rev. Lett. **109**, 070503 (2012).
[13] H. Buhrman and H. Röhrig H, in *B. Rovan, P. Vojtáš (eds) Mathematical Foundations of Computer Science 2003 (MFCS 2003)*, Lecture Notes in Computer Science, **2747**, p. 1-20, Springer, Berlin, Heidelberg.
[14] H.-L. Yin *et al.*, Phys. Rev. Lett. **117**, 190501 (2016).
[15] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[16] S.-K. Liao *et al.*, Nature **549**, 43 (2017).
[17] H. Takenaka *et al.*, Nat. Photon. **11**, 502 (2017).
[18] N. Sangouard, C. Simon, N. de Riedmatten, and N. Gisin, Rev. Mod. Phys. **83**, 33 (2011).
[19] N. Gisin, G. Ribordy, W. Tittel and H. Zbindon, Rev. Mod. Phys. **74**, 145 (2002).
[20] M. Takeoka, S. Guha, and M. M. Wilde, Nat. Commun. **5**, 5235 (2014).
[21] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[22] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 400 (2018).
[23] S. Abruzzo, H. Kampermann, and D. Bruß, Phys. Rev. A **89**, 012301 (2014).
[24] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, New J. Phys. **16**, 043005 (2014).
[25] K. Azuma, K. Tamaki, and W. J. Munro, Nat. Commun. **6**, 10171 (2015).
[26] B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, Phys. Rev. Lett. **98**, 240502 (2007).
[27] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, preprint arXiv:1805.05511.
[28] X. Ma, P. Zeng, and H. Zhou, preprint arXiv:1805.05538.
[29] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill,

Quant. Inf. Comput. **5**, 325 (2004).
[30] H.-K. Lo and J. Preskill, Quant. Inf. Comput. **8**, 431 (2007).
[31] K. Tamaki, H.-K. Lo, C.-H. F. Fung, and B. Qi, Phys. Rev. A **85**, 042307 (2012).
[32] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[33] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[34] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[35] M. Koashi, New J. Phys. **11**, 045018 (2009).
[36] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Nature **414**, 413 (2001).
[37] K. Azuma, H. Takeda, M. Koashi, and N. Imoto, Phys. Rev. A **85**, 062309 (2012).
[38] D. Gottesman and I. Chuang, preprint arXiv:quant-ph/0105032.
[39] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).
[40] F. Xu *et al.*, Nat. Commun. **6**, 87 (2015).
[41] J.-Y. Guan *et al.*, Phys. Rev. Lett. **116**, 240502 (2016).
[42] X. Ma, B. Qi, Y. Zhao and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[43] K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, Phys. Rev. A **80**, 032302 (2009).
[44] K. Azuma, Tohoku Math. J. **19**, 357 (1967).
[45] K. Tamaki, M. Curty, G. Kato, H.-K. Lo, and K. Azuma, Phys. Rev. A **90**, 052314 (2014).
[46] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New J. Phys. **17**, 093011 (2015).
[47] Y. Nagamatsu, A. Mizutani, R. Ikuta, T. Yamamoto, N. Imoto, and K. Tamaki, Phys. Rev. A **93**, 042325 (2016).
[48] A. Mizutani *et al.*, preprint arXiv:1803.09484.
[49] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nat. Commun. **5**, 3732 (2014).
[50] C. Cui *et al.*, preprint arXiv:1807.02334.
[51] J. Lin and N. Lütkenhaus, "A simple security analysis of twin-field quantum key distribution", 1st workshop on security proofs in QKD, Waterloo (Canada), July 5-6 (2018).