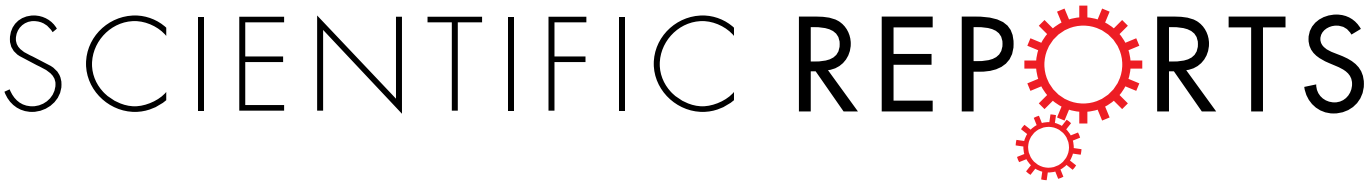

OPEN

Two-dimensional distributed-phase-reference protocol for quantum key distribution

Received: 10 June 2016
Accepted: 20 October 2016
Published: 22 December 2016

Davide Bacco*, Jesper Bjerge Christensen*, Mario A. Usuga Castaneda, Yunhong Ding, Søren Forchhammer, Karsten Rottwitt & Leif Katsuo Oxenløwe

Quantum key distribution (QKD) and quantum communication enable the secure exchange of information between remote parties. Currently, the distributed-phase-reference (DPR) protocols, which are based on weak coherent pulses, are among the most practical solutions for long-range QKD. During the last 10 years, long-distance fiber-based DPR systems have been successfully demonstrated, although fundamental obstacles such as intrinsic channel losses limit their performance. Here, we introduce the first two-dimensional DPR-QKD protocol in which information is encoded in the time and phase of weak coherent pulses. The ability of extracting two bits of information per detection event, enables a higher secret key rate in specific realistic network scenarios. Moreover, despite the use of more dimensions, the proposed protocol remains simple, practical, and fully integrable.

Sharing sensitive information has always been a great challenge within our society. In particular, QKD, first introduced by Bennett and Brassard, provides a unique procedure for exchanging a private key, based on the laws of quantum mechanics[1]. During the last decade, the effort from the scientific community has been focused on an enhancement of the quantum communication performances in terms of key rate, transmission distance and security aspects[2–9]. In later years this technology has matured enormously, but the lack of compact, efficient, inexpensive, and reliable systems, has restricted wide spreading of practical QKD systems.

The basic idea behind QKD systems, in the case of "prepare and measure" schemes, is based on quantum states prepared by Alice (the transmitter) and sent through a quantum channel towards Bob (the receiver). Depending on the quantum measurement, Bob can deduce which state was prepared by Alice. This way, after error reconciliation and privacy amplification methods established in a classical channel, the two users share an identical bit sequence.

Ideally, QKD systems are secure with no chance for an eavesdropper to extract information on the key. However, in real implementations of the systems, due to the losses and imperfections of devices, the secret key rate defines a bound on how much information can be assumed secure[10–12].

We here propose a new QKD protocol, which we refer to by the name: Differential phase time shifting (DPTS). In its essence, the protocol utilizes two degrees of freedom — time and phase — to encode information in a quaternary alphabet, i.e. {0, 1, 2, 3}[13]. The DPTS belongs to the family of distributed phase-reference (DPR) protocols, which rather than using the principle of random basis-choices between different mutually unbiased bases, encodes information in adjacent weak coherent pulses[6,10,14–18]. We study the performance of the DPTS protocol using infinite-key analysis in the case of collective attacks, and further show that the protocol holds great potential in intracity network scenarios.

Results

Principle of DPTS. As in most practical implementations of QKD, the DPTS protocol, which is sketched in Fig. 1, uses a source of weak coherent pulses to establish a key of random numbers between two authenticated parties, Alice and Bob. To initiate the key distribution process, Alice randomly encodes information in the train of pulses in two dimensions, time and phase. *The time encoding* is performed using an intensity modulator (IM) as in the coherent-one way (COW) protocol[15]. For every pair of pulses (we refer to such a pair as a *sub-block*), one pulse is transmitted with mean photon number $\mu < 1$ ($|\alpha\rangle$), and one is blocked completely ($|\text{vac}\rangle$). Hence, within each sub-block, information is carried by the time-of-arrival of a non-empty pulse[15,19]. *The phase encoding*

Technical University of Denmark, Department of Photonics Engineering, 2800 Kgs. Lyngby, Denmark. *These authors contributed equally to this work. Correspondence and requests for materials should be addressed to D.B. (email: dabac@fotonik.dtu.dk)

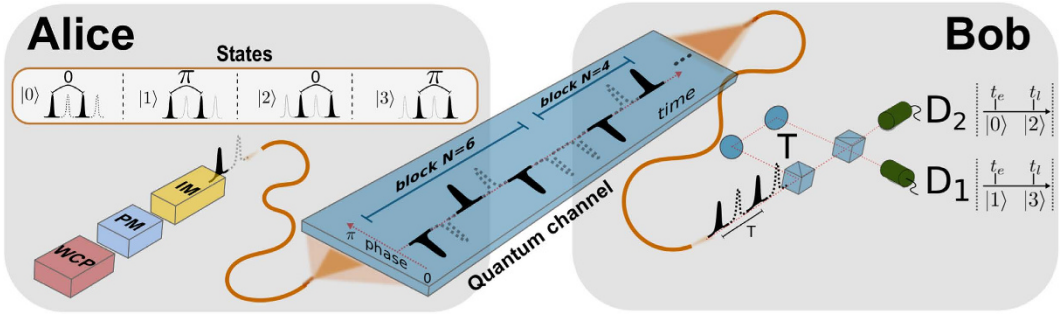

Figure 1. Basic scheme of the DPTS protocol exploiting phase and time domain. A train of weak coherent pulses (WCP) is emitted by a laser of repetition rate ν ($2/T$), and attenuated to the single photon level. A phase modulator (PM) encodes the first key bit in second-neighbor pulses with a period of T by choosing randomly either 0 or π. An intensity modulator (IM) is used to choose the position of the pulses to encode the second key bit. The number of pulses N, where the intensity modulator uses the same time instances, is defined as a *block*. In this way, Alice prepares a sequence of different states: $|0\rangle$, $|1\rangle$, $|2\rangle$, $|3\rangle$. Using a delay line interferometer with a delay of T between arms, Bob can simultaneously measure the phase and pulse position.

is performed using a phase modulator (PM), where a random phase between sub-blocks is either $\{0, \pi\}$. By combining the effect of the IM and the PM, Alice prepares states from the quaternary alphabet:

$$\begin{aligned} |0\rangle &= |\pm\alpha\rangle|\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle, \\ |1\rangle &= |\pm\alpha\rangle|\text{vac}\rangle|\mp\alpha\rangle|\text{vac}\rangle, \\ |2\rangle &= |\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle|\pm\alpha\rangle, \\ |3\rangle &= |\text{vac}\rangle|\pm\alpha\rangle|\text{vac}\rangle|\mp\alpha\rangle. \end{aligned} \quad (1)$$

Bob may distinguish unambiguously between these states by employing an unbalanced interferometer which interferes pulses in adjacent sub-blocks separated by $T = 2/\nu$, where ν is the laser repetition rate. Depending on the time of arrival (t_e or t_l in Fig. 1) and on which detector fired (D_1 or D_2), Bob can decide which of the four states was prepared. We would like to point out that, due to the used interferometer delay, no interference occurs in the case of a transition sequence, such as $|\pm\alpha\rangle\,|\text{vac}\rangle\,|\text{vac}\rangle\,|\pm\alpha\rangle$.

It is important to note that, analogous to the differential phase shift (DPS) protocol, each sub-block may participate in defining up to two states[14]. For instance, the sequence: $|\alpha\rangle\,|\text{vac}\rangle\,|-\alpha\rangle\,|\text{vac}\rangle\,|\alpha\rangle\,|\text{vac}\rangle\,|\text{vac}\rangle\,|\alpha\rangle\,|\text{vac}\rangle\,|-\alpha\rangle$ encodes the states: $|1\rangle\,|1\rangle - |3\rangle$. Here, the '$-$' indicates a change of the temporal sequence over the sub-block separation, in which case Bob is not able to interfere the non-empty pulses in his interferometer (for a detailed example, see Supplementary information).

To minimize the number of transition sequences, Alice and Bob may benefit from repeating the temporal encoding over long pulse intervals (i.e. only preparing $|0\rangle$ and $|1\rangle$, or $|2\rangle$ and $|3\rangle$). However, doing so permits a potential eavesdropper, Eve, to gain partial information on a given state by measuring the time-of-arrival of pulses in adjacent sub-blocks. This effectively means that the time-of-arrival information is more vulnerable to eavesdropping. To counteract this potential attack, Alice introduces the concept of *blocks*. Each block consists of N pulses (counting both empty and non-empty), within which the temporal sequence is repeated independently from the previous block (the sequences $|0\rangle\,|1\rangle\,|1\rangle$ and $|3\rangle\,|2\rangle$ are examples of blocks with $N = 8$ and $N = 6$). The value of N is for each block chosen randomly from a uniform distribution: $N \in \{4, 6, \ldots, N_{max}\}$. In contrast, if the value of N was fixed at e.g. $N = 6$, then Eve would know exactly for which sequences of pulses the temporal encoding was repeated. The modification of random block lengths, means that both Bob and Eve are essentially unaware of the positions of the block separations. Whereas this is of no importance to Bob (see section 'Protocol definition'), it is fundamental to Eve.

The security of DPTS relies on the same principle as other DPR protocols: the coherence between non-empty pulses[20,21]. In fact, the DPS aspect of the DPTS protocol makes it very robust against attacks such as the intercept-resend attack and the photon-number splitting attack[21,22]. Eve can not perform a measurement on any finite number of states without at some point breaking coherence between successive pulses. This is specifically true for the DPTS protocol as Eve is not able to predict the positions of the transition sequences. However, since coherence is distributed across sub-block separations whereas the temporal information lies within sub-blocks, a sophisticated Eve can address each sub-block separately trying to just learn the time-of-arrival information (i.e. is a state $|0\rangle$, $|1\rangle$ or is it $|2\rangle$, $|3\rangle$). Doing so, she only breaks coherence *within* sub-blocks, and thus Bob, who only checks coherence *across* sub-blocks, is not able to reveal her presence. To counter this attack, Alice introduces decoy sequences with probability $p_{decoy} \ll 1$, in which blocks consist of N non-empty pulses[20]. Interestingly, this decoy is just a DPS sequence in which the phase encoding is carried between every second pulse (as measured by Bob). Consequently, if Eve probes one or more sub-blocks containing two non-empty pulses, she inevitably disturbs the phase relation between these pulses[11]. As a result, there are cases where Eve introduces phase errors into the communication.

Protocol definition. We now describe in detail how Alice and Bob establish a common key using the DPTS protocol:

- Alice prepares states for transmission in the quantum channel using her phase- and intensity modulators. We assume that Alice chooses equally and randomly between the four different states {0, 1, 2, 3}. The temporal sequence is repeated within each block of random length, $N \in \{4, 6, \ldots, N_{max}\}$, whereas the phase difference between each sub-block is randomly chosen to either 0 or π.
- Once Bob has received a photon in one of the two detectors, he reveals over a public classical channel the sub-time (the number of the sub-block) instances of his recorded detection events.
- Alice reports back by telling which of the events corresponded to an overlap between adjacent blocks with opposite temporal sequence (a block separation was present in that instance). Bob must discard these events.
- For each of the remaining detection events, Alice and Bob establish two bits of information for their key: Alice easily figures out the detection time from her sent temporal sequence, and infers from her phase encoding which detector clicked at Bob's side.
- After estimating the quantum bit error rate (QBER), Alice and Bob perform standard error reconciliation and privacy amplification[23–25]. At the end of the process Alice and Bob share a secure identical key.

Secret key rate. To further describe the proposed protocol, let us consider the maximum extractable secret key rate R_{sk}[11]. For the DPTS protocol this quantity reads

$$R_{sk} = f R_B [I_{AB} - \min(I_{AE}, I_{BE})], \tag{2}$$

where $R_B = R + 4p_d(1-R)$ is the total detection rate with $R = [1 - \exp(-\mu t \eta_d)]/2$, μ is the mean photon number of non-empty pulses, t represents the quantum channel transmission coefficient, η_d is the (common) detector efficiency, and p_d is the dark count probability. The pre-factor $f = (1 - p_{decoy})(\langle N\rangle - 1)/\langle N\rangle$, where $\langle N\rangle = (N_{max} + 4)/2$ is the average block length, takes into account the fraction of Bob's detection events that is assigned to the key string. The unused fraction $1/\langle N\rangle$ is due to detections associated with adjacent sub-blocks of different temporal sequences. In these cases, the clicks are randomly distributed between the two detectors, and so the instances are discarded.

The mutual information between Alice and Bob, is expressed in terms of the Shannon entropy as $I_{AB} = H(A) - H(A|B)$[26]. Alice has a total of four different states to choose from, and by assuming that she prepares each state with equal probability, one finds $H(A) = -\sum_{i=1}^{4}(1/4)\ \log_4(1/4) = 1$. Note that we, for convenience, measure information using a base-4 logarithm rather than the common base 2 [in units of bits one acquires $H(A) = 2$]. Furthermore, the conditional entropy $H(A|B)$ is expressed as

$$H(A|B) = -(1 - e_r^{(1)})\ \log_4(1 - e_r^{(1)}) - \sum_{i=2}^{4} e_r^{(i)}\ \log_4(e_r^{(i)}), \tag{3}$$

where the four error probabilities satisfying $e_r^{(1)} = e_r^{(2)} + e_r^{(3)} + e_r^{(4)}$ are given as

$$\begin{aligned} e_r^{(1)} &= \frac{R\frac{1-V}{2} + 3p_d(1-R)}{R_B}, \\ e_r^{(2)} &= \frac{R\frac{1-V}{2} + p_d(1-R)}{R_B}, \\ e_r^{(3)} &= e_r^{(4)} = \frac{p_d(1-R)}{R_B}, \end{aligned} \tag{4}$$

where $V = (p_{D_1} - p_{D_2})/(p_{D_1} + p_{D_2})$ represents the visibility of the interferometer used by Bob and p_{D_1} (p_{D_2}) represents the probability of detection in detector D_1 (D_2). Note that, in the definition of the error probabilities, the visibility appears in only two of the four terms, since an interferometer error does not alter the time of arrival. Thus, since the time-of-arrival information remains correct, the DPTS protocol suffers less from interferometer imperfections in comparison with the DPS protocol which solely relies on relative phase measurements. On the other hand, the higher dimensionality of the DPTS protocol renders it more vulnerable to detector dark counts: each dark-count occurrence results in two random bits rather than one. This effectively makes the DPTS protocol less useful at longer communication distances where the dark count rate becomes comparable with the signal rate.

In order to evaluate the achievable secret key rate for Alice and Bob, we next introduce an upper bound on the information that a potential eavesdropper might obtain by performing the most basic attack; the beam-splitting attack. In the family of collective attacks, Eve is assumed to be able to interact with the same strategy on a predefined number of pulses. She can store the photons and try to extract the largest possible information after Alice and Bob has performed post-processing. A complete analysis would concentrate on I_{BE} since Eve is clueless about detection events resulting from imperfections at Bob's side (see equation (2)). However, as a first attempt to estimate her information, we restrict ourselves to the more simple analysis of I_{AE}.

Security analysis. This section presents an analysis of security based on the collective beam-splitting attack (BSA) and follows the method used in ref. 27 for the DPS and COW protocols. In the BSA, Eve replaces the quantum channel connecting Alice and Bob by a lossless line. Using a beam-splitter to simulate the losses of the

quantum channel, Eve acquires $1-t$ of the signal without disturbing the state sent by Alice. Thus, the BSA belongs to the family of zero-error attacks, and is therefore undetectable by Alice and Bob[28]. The states prepared by Alice consist of sequences $\otimes_k|\alpha_k\rangle$ with $\alpha_k \in \{+\alpha, \text{vac}, -\alpha\}$, so by performing the BSA, Eve receives states of the form $\otimes_k|\alpha_k^{(E)}\rangle$, where $\alpha_k^{(E)} \in \{+\alpha_E, \text{vac}, -\alpha_E\}$ with $\alpha_E = \alpha\sqrt{1-t}$.

At this point we assume that Eve stores the states in her quantum memory for measurement after Bob reveals his detection events. Indeed, for such a collective attack, the maximum information she may extract is given by the Holevo quantity (which must be maximized with respect to the strategies available to Eve, though here we only consider the BSA)[11,29]

$$\chi_{AE} = S(\rho_E) - \sum_j p_j S(\rho_{E|j}) \tag{5}$$

Here, $S(\rho) = -\text{Tr}\{\rho \log_4(\rho)\}$ is the von Neumann entropy, $\rho_E = \sum_j p_j \rho_{E|j}$ is a density operator with p_j being the probability of Alice preparing the four states $j \in \{0, 1, 2, 3\}$, and $\rho_{E|j}$ being Eve's state conditioned on preparation of state j.

As mentioned earlier, we consider only the balanced situation where Alice prepares each state with a probability $p_j = 1/4$. In the current protocol each value in the quaternary alphabet is encoded in four consecutive pulses. It follows that Eve's states conditioned on Alice's preparation are

$$\begin{aligned}
\rho_{E|0} &= \frac{1}{2}(P_{+\alpha_E,\text{vac},+\alpha_E,\text{vac}} + P_{-\alpha_E,\text{vac},-\alpha_E,\text{vac}}),\\
\rho_{E|1} &= \frac{1}{2}(P_{+\alpha_E,\text{vac},-\alpha_E,\text{vac}} + P_{-\alpha_E,\text{vac},+\alpha_E,\text{vac}}),\\
\rho_{E|2} &= \frac{1}{2}(P_{\text{vac},+\alpha_E,\text{vac},+\alpha_E} + P_{\text{vac},-\alpha_E,\text{vac},-\alpha_E}),\\
\rho_{E|3} &= \frac{1}{2}(P_{\text{vac},+\alpha_E,\text{vac},-\alpha_E} + P_{\text{vac},-\alpha_E,\text{vac},+\alpha_E}),
\end{aligned} \tag{6}$$

where P_x is the projection operator. To calculate the maximum accessible information for Eve, it is helpful to define $\gamma = e^{-|\alpha_E|^2}$. By this convention the overlaps between states can be written as $|\langle +\alpha_E, \text{vac}, +\alpha_E, \text{vac}| -\alpha_E, \text{vac}, -\alpha_E, \text{vac}\rangle| = \gamma^4$, and $|\langle j|k\rangle| = \gamma^2$ for $j \neq k$, where $j, k \in \{0, 1, 2, 3\}$. By writing ρ_E and $\rho_{E|j}$ in their respective eigenbasis, the von Neumann entropy takes the simple form $S = -\sum_n \lambda_n \log_4(\lambda_n)$, where λ_n are the eigenvalues. The resulting Holevo quantity is

$$\begin{aligned}
\chi_{AE}^{(0)} &= -\frac{(1+\gamma^2)^2 + (2\gamma)^2}{8} \log_4\left[\frac{(1+\gamma^2)^2 + (2\gamma)^2}{8}\right] - \frac{3(1-\gamma^2)^2}{8}\\
&\log_4 \times \left[\frac{(1-\gamma^2)^2}{8}\right] - \frac{1-\gamma^4}{2} \log_4\left(\frac{1-\gamma^4}{8}\right) + \left(\frac{1-\gamma^4}{2}\right) \log_4\left(\frac{1-\gamma^4}{2}\right)\\
&+ \left(1 - \frac{1-\gamma^4}{2}\right) \log_4\left(1 - \frac{1-\gamma^4}{2}\right).
\end{aligned} \tag{7}$$

and presents an upper bound on the information Eve can obtain by trying to distinguish between the four different states after Bob announces a detection event.

In the cases where Eve fails to get a conclusive measurement, she may instead try to establish partial information about the state Alice and Bob agreed upon. She can do this by trying to measure the temporal position (i.e. is a state $|0\rangle$, $|1\rangle$ or $|2\rangle$, $|3\rangle$) of the pulse in a sub-block adjacent to the sub-block corresponding to Bob's detection. In general for the considered block lengths, the probability of this measurement to be correct (if conclusive) exceeds 1/2 (for details, see Supplementary information), and thereby effectively provides Eve with information on the state. Since this additional attack by Eve is conditioned on her *not* getting a conclusive result in the primary measurement, the corrected Holevo quantity becomes

$$\chi_{AE} = \chi_{AE}^{(0)} + (1 - \chi_{AE}^{(0)})\,\chi_{AE}^{(1)}, \tag{8}$$

where $\chi_{AE}^{(1)}$ is derived and given in the Supplementary information. Note however, that Eve is essentially ignorant about the position of block separations. Therefore, making conclusions based on this secondary attack will result in errors for Eve, effectively reducing the gained information.

Numerical results. Combining the results of the previous sections (equations (2–8)) the secret key rate for DPTS reads $R_{sk}^{(DPTS)} = 2f\,R_B(1 - H(A|B) - \chi_{AE})$, where the factor of two stems from the conversion from a quaternary to binary alphabet. This expression enables us to plot a first upper bound on the secret key rate under the assumption of collective attacks. Specifically, Fig. 2 shows R_{sk} versus communication distance at the optimized values of the mean photon number μ. To assess the performance of the DPTS protocol, we have included plots for both COW and DPS. The secret key rate for COW and DPS are obtained by: $R_{sk}^{(COW)} = f_d(R + 2p_d(1-R))(1 - h(Q^{(COW)}) - \chi_{AE}^{(COW)})$ and $R_{sk}^{(DPS)} = (2R + 2p_d(1-2R))(1 - h(Q^{(DPS)}) - \chi_{AE}^{(DPS)})$, where R is defined below equation (2), $Q^{(COW)}$ and $Q^{(DPS)}$ are the quantum bit error rate for COW and DPS respectively, f_d represents the decoy state probability, $h(Q)$

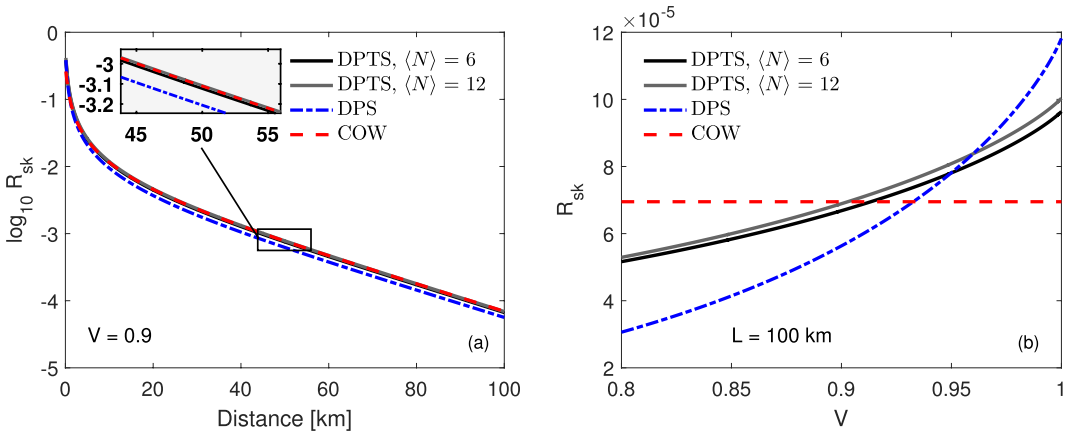

Figure 2. Secret key rate measured in bits per pulse. Performance versus (**a**) distance in the case of fixed visibility, $V = 0.9$, and (**b**) visibility at a channel length of $L = 100$ km. For each of the three protocols, an optimization was performed with respect to the mean photon number μ (see Supplementary Fig. S2). Parameters: $\eta_d = 0.1$, $p_d = 2 \times 10^{-8}$, $\alpha_{loss} = 0.2$ dB/km, and $p_{decoy} = 0.02$ for COW and DPTS.

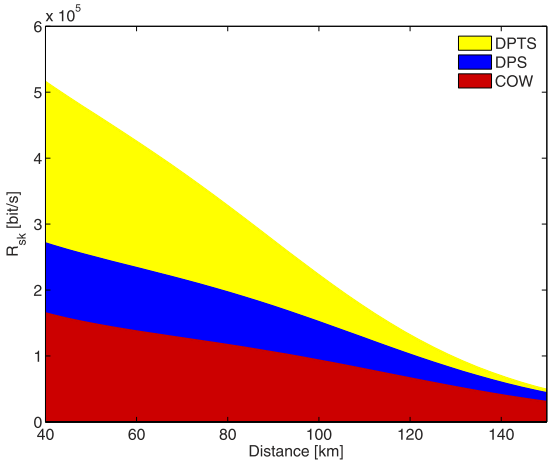

Figure 3. Secret key rate in real case scenario. Different secret key rates achievable in a medium-length link scenario, where the detector dead times play an important role. We use mean photon numbers for the different protocols of $\mu_{DPTS} = 0.23$, $\mu_{DPS} = 0.19$, and $\mu_{COW} = 0.52$, at repetition rate $\nu = 2$ GHz, and average block length of $\langle N \rangle = 6$. The detectors are specified by dark-count probability $p_d = 2 \times 10^{-8}$, a dead time of $t_d = 2\,\mu$s, and efficiency $\eta_d = 0.1$. We assume $V = 0.98$, and a decoy-sequence probability of $p_{decoy} = 0.02$ for COW and DPTS.

is the binary entropy and the Holevo bounds $\chi_{AE}^{(COW)}$ and $\chi_{AE}^{(DPS)}$ are defined in Branciard *et al.*[27]. These equations are derived under the same assumptions as made for the DPTS protocol to allow for a fair comparison. As a result, the COW protocol does not exhibit any visibility dependence (see Fig. 2(b)).

In comparison, the DPTS protocol has a similar performance as the other protocols under the realistic condition of non-ideal visibilities (as example we have used $V = 0.9$). Noteworthy, the DPTS protocol displays a less critical dependence on the visibility when compared to the DPS protocol.

In a more realistic situation, the comparison of the protocols must take into account the detector dead times. For example, considering the case of commercial InGaAs infrared single-photon detectors (the most used in fiber links and the most promising thanks to the non-cryogenic requirement), they generally exhibit a dead time in excess of 1 μs[30,31]. Thus, in any scenario where the detector dead time significantly influences the key generation rate, the ability to extract two bits of information per detection event grants the DPTS protocol an advantage. To illustrate this effect, Fig. 3 shows an example of the secret key rate in bits s^{-1}, after inclusion of the dead-time dependency.

Discussion

The main figure of merit in a QKD system is the achievable secret key rate. Therefore, to assess the performance of DPTS, Fig. 2 displays this quantity for DPTS in comparison with the standard COW and DPS protocols. The comparison shows very similar behavior of the three DPR protocols. Considering more specifically the case of DPTS, the final key rate is influenced by the length of the blocks N prepared by Alice. Even though a higher value of N allows an increased sifted key rate, it is necessary to consider a trade-off between the length of blocks and

the information leakage to Eve. In the case of long-distance links (in excess of 100 km), the behavior of the three protocols is maintained, but as the DPTS protocol is more severely influenced by dark count events, it is generally limited to shorter distances. On the other hand, as seen from Fig. 2(b), the DPTS protocol is less dependent on the interferometer visibility. This fact permits the proposed protocol to achieve a more stable secret key generation rate in comparison with the DPS protocol.

In implementing a QKD protocol, it is necessary to consider the limitations set by the optical and electronic devices[32–34]. An important example is the single-photon detector dead time t_d, which sets an upper limit on the key generation rate. This parameter is important in a short- or medium-length link scenario, where the average wait time between detection events is of the same order of magnitude as t_d (which is typically on the order of microseconds). In Fig. 3, it is shown that DPTS may achieve a significant increase in the secure key rate at distances where the detector dead time is a limiting factor. This potential arises due to the ability of the DPTS protocol to extract two bits of information per detection event.

The use of multiple degrees of freedom in transmission of information, intuitively increases the complexity of the scheme in comparison with protocols dealing with each individual degree of freedom. Despite DPTS not being an exception to this rule of thumb, the complexity overhead in comparison to DPS or COW is not crucial. On the other hand, DPTS does exhibit two significant practical advantages. Firstly, the COW protocol requires a monitoring line to check for the presence of an eavesdropper. However, such a monitoring line is unnecessary for DPTS, as an interferometer is directly used in the data line, and hence implements the necessary coherence check. Thus, the decrease in rate related to monitoring of the data line in COW, is not a limitation for DPTS. Secondly, the stability of the interferometer over time, is a considerable challenge in implementations of the DPS protocol in non-stable environments. The performance of the DPTS protocol is inherently more resilient against fluctuating interferometer visibilities, because the temporal bit remains unaffected by such inefficiencies. This entails, that DPTS might be better suited in cases where it is difficult to maintain the interferometer visibility above a certain required operation threshold.

Finally, DPTS can potentially play an important role in QKD networks spanning from metropolitan to intercity distances[35–39]. Interestingly, the required measurement apparatus is identical to the one used in DPS, and in fact, the receiver does not need to know *a priori* whether the signals arise from a DPS or a DPTS encoding. This compatibility suggests that a versatile network encompassing the use of both the DPS and DPTS protocols is feasible.

In conclusion, we have proposed a novel kind of distributed-phase-reference protocol for quantum key distribution. Utilizing both the time- and phase degrees of freedom, this protocol provides a significant step towards realization of fast, reliable, and practical quantum communication. Future directions include a finite-key analysis and a real-time field implementation.

References

1. Bennett, C. H. & Brassard, G. Quantum Cryptography: public key distribution and coin tossing. *In Proc. IEEE Int. Conf. on Computers, Systems & Signal Processing* 175–179 (1984).
2. Vallone, G. *et al.* Experimental Satellite Quantum Communications. *Phys. Rev. Lett.* **115,** 040502 (2015).
3. Korzh, B. *et al.* Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nat. Photon.* **9,** 163–168 (2015).
4. Bacco, D., Canale, M., Laurenti, N., Vallone, G. & Villoresi, P. Experimental quantum key distribution with finite-key analysis for noisy channels. *Nat. Commun.* **4,** 2363 (2013).
5. Ji, L. *et al.* Towards Quantum Communication in Free-Space Seawater. *arXiv 1602.05047* (2016).
6. Takesue, H., Sasaki, T., Tamaki, K. & Koashi, M. Experimental quantum key distribution without monitoring signal disturbance. *Nature Photon.* **9,** 827–831 (2015).
7. Wang, S. *et al.* Experimental demonstration of a quantum key distribution without signal disturbance monitoring. *Nature Photon.* **9,** 832–836 (2015).
8. Mirhosseini, M. *et al.* High-dimensional quantum cryptography with twisted light. *New J. Phys.* **17,** 033033 (2015).
9. Usuga, M. A. *et al.* Noise-Powered Probabilistic Concentration of Phase Information. *Nat. Phys.* **6,** 767–771 (2010).
10. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145–195 (2002).
11. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev. Mod. Phys.* **81,** 1301–1350 (2009).
12. Brassard, G., Lütkenhaus, N., Mor, T. & Sanders, B. C. Limitations on Practical Quantum Cryptography. *Phys. Rev. Lett.* **85,** 1330–1333 (2000).
13. Usenko, V. C. & Lev, B. I. Large-alphabet quantum key distribution with two-mode coherently correlated beams. *Phys. Lett. A* **348,** 17–23 (2005).
14. Inoue, K., Waks, E. & Yamamoto, Y. Differential-phase-shift quantum key distribution using coherent light. *Phys. Rev. A* **68,** 022317 (2003).
15. Stucki, D., Brunner, N., Gisin, N., Scarani, V. & Zbinden, H. Fast and simple one-way quantum key distribution. *Appl. Phys. Lett.* **87,** 194108 (2005).
16. Takesue, H. *et al.* Quantum key distribution over a 40-dB channel loss using superconducting single-photon detectors. *Nature Photon.* **1,** 343–348 (2007).
17. Wang, S. *et al.* 2-GHz clock quantum key distribution over 260 km of standard telecom fiber. *Opt. Lett.* **37,** 1008–1010 (2012).
18. Sasaki, T., Yamamoto, Y. & Koashi, M. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509,** 475–478 (2014).
19. Korzh, B. *et al.* Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre. *Nature Photon.* **9,** 163–168 (2014).
20. Gisin, N. *et al.* Towards practical and fast Quantum Cryptography. *arXiv:quant-ph/0411022* (2004).
21. Inoue, K. & Honjo, T. Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. *Phys. Rev. A* **71,** 042305 (2005).
22. Inoue, K. Differential Phase-Shift Quantum Key Distribution Systems. *IEEE J. Sel. Top. Quantum Electron.* **21,** 109–115 (2015).
23. Buttler, W. *et al.* Fast, efficient error reconciliation for quantum cryptography. *Phys. Rev. A* **67,** 052303 (2003).
24. Martinez-Mateo, J., Pacher, C., Peev, M., Ciurana, A. & Martin, V. Demystifying the information reconciliation protocol cascade. *Quantum Info. Comput.* **15,** 453–477 (2015).
25. Bennett, C. H., Brassard, G., Crepeau, C. & U. Maurer, G. P. A. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41,** 1915–1923 (1995).
26. Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information* (Cambridge University Press, 2000).

27. Branciard, C., Gisin, N. & Scarani, V. Upper bounds for the security of two distributed-phase reference protocols of quantum cryptography. *New J. Phys*. **10,** 013031 (2008).
28. Branciard, C., Gisin, N., Lutkenhaus, N. & Scarani, V. Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography. *Quantum Info. Comput*. **7,** 639–664 (2007).
29. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **461,** 207–235 (2005).
30. Hadfield, R. H. Single-photon detectors for optical quantum information applications. *Nature Photon*. **3,** 696–705 (2009).
31. Tosi, A., Calandri, N., Sanzaro, M. & Acerbi, F. Low-noise, low jitter, high detection efficiency InGaAs/InP Single-Photon Avalanche Diode. *IEEE J. Sel. Top. Quantum Electron*. **20,** 192–197 (2014).
32. Sibson, P. *et al.* Chip-based Quantum Key Distribution. *arXiv 1509.00768* 1–5 (2015).
33. Diamanti, E., Takesue, H., Langrock, C., Fejer, M. M. & Yamamoto, Y. 100 Km Differential Phase Shift Quantum Key Distribution Experiment With Low Jitter Up-Conversion Detectors. *Opt. Express* **14,** 13073–13082 (2006).
34. Takesue, H., Diamanti, E., Langrock, C., Fejer, M. M. & Yamamoto, Y. 10-GHz clock differential phase shift quantum key distribution experiment. *Opt. Express* **14,** 9522–9530 (2006).
35. Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19,** 10387–10409 (2011).
36. Fröhlich, B. *et al.* A quantum access network. *Nature* **501,** 69–72 (2013).
37. Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys*. **11,** 075001 (2009).
38. Stucki, D. *et al.* Long-term performance of the SwissQuantum quantum key distribution network in a field environment. *New J. Phys*. **13,** 123001 (2011).
39. Wang, S. *et al.* Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **22,** 21739–21756 (2014).

Acknowledgements

We would like to thank Dr. Giuseppe Vallone and Dr. Davide. G. Marangon of Department of Information Engineering (DEI), University of Padova for the useful discussions and for the insightful comments. Our work was supported by the DNRF Research Centre of Excellence, SPOC (Silicon Photonics for Optical Communications), ref. DNRF123 and the DFF Sapere Aude Adv. Grant NANO-SPECs

Author Contributions

D.B. conceived the work. D.B., J.B.C., M.A.U.C. and Y.D. obtained the conceptional main results. J.B.C. provided security proof. J.B.C., S.F. and D.B. formulated information theory analysis. K.R. and L.K.O. supervised the project. All authors discussed the results and contributed to the final manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Bacco, D. *et al.* Two-dimensional distributed-phase-reference protocol for quantum key distribution. *Sci. Rep.* **6**, 36756; doi: 10.1038/srep36756 (2016).

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.