Mixed basis quantum key distribution with linear optics

MLADEN PAVIČIĆ,[1,2,5] OLIVER BENSON,[1,6] ANDREAS W. SCHELL,[3]
AND JANIK WOLTERS[4]

[1]*Department of Physics, Nanooptics, Math.-Nat. Fakultät, Humboldt-Universität zu Berlin, Germany*
[2]*Center of Excellence for Advanced Materials and Sensing Devices (CEMS), Photonics and Quantum Optics Unit, Ruđer Bošković Institute, Zagreb, Croatia*
[3]*Dep. of Electronic Science & Engineering, Kyoto Univ., Kyoto daigaku-katsura, Nishikyo-ku, Kyoto, Japan*
[4]*Department of Physics, University of Basel, Switzerland*
[5]*mpavicic@physik.hu-berlin.de*
[6]*oliver.benson@physik.hu-berlin.de*

Abstract: Two-qubit quantum codes have been suggested to obtain better efficiency and higher loss tolerance in quantum key distribution. Here, we propose a two-qubit quantum key distribution protocol based on a mixed basis consisting of two Bell states and two states from the computational basis. All states can be generated from a single entangled photon pair resource by using local operations on only one auxiliary photon. Compared to other schemes it is also possible to deterministically discriminate all states using linear optics. Additionally, our protocol can be implemented with today's technology. When discussing the security of our protocol we find a much improved resistance against certain attacks as compared to the standard BB84 protocol.

References and links

1. C. H. Bennett and G. Brassard, "Quantum cryptography, public key distribution and coin tossing," in "International Conference on Computers, Systems & Signal Processing, Bangalore, India, December 10-12, 1984," (IEEE, 1984), 175–179.
2. M. Stipčević and R. Ursin, "An on-demand optical quantum random number generator with in-future action and ultra-fast response," Sci. Rep. **5**, 10214 (2015).
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
4. H. Lo, "A simple proof of unconditional security of six-states quantum key distribution scheme," Quantum Inf. Comp. **1**, 81–94 (2001).
5. H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A **61**, 062308 (2000).
6. D. Bruß and C. Macchiavello, "Optimal eavesdropping in cryptography with three-dimensional quantum states," Phys. Rev. Lett. **88**, 127901 (2002).
7. M. Dušek, N. Lütkenhaus, and M. Hendrych, "Quantum cryptography," in *Progress in Optics*, **49** E. Wolf, ed. (Elsevier, 2006), chap. 5, 257–354.
8. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, "Hacking commercial quantum cryptography systems by tailored bright illumination," Nature Phot. **4**, 686–689 (2011).
9. K. Boström and T. Felbinger, "Deterministic secure direct communication using entanglement," Phys. Rev. Lett. **89**, 187902 (2002).
10. K. Boström and T. Felbinger, "On the security of the ping-pong protocol," Phys. Lett. A **372**, 3953–3956 (2008).
11. Q. Cai and B. Li, "Improving the capacity of the Boström-Felbinger protocol," Phys. Rev. A **69**, 054301 (2004).
12. A. Chamoli and C. M. Bhandari, "Secure direct communication based on ping-pong protocol," Quantum. Inf. Process. **8**, 347–356 (2009).
13. L. A. Ngah, O. Alibart, L. Labonté, V. D'Auria, and S. Tanzilli, "Ultra-fast heralded single photon source based on telecom technology," Laser Phot. Rev. **9**, L1–L5 (2015).
14. H. Chen, Z.-Y. Zhou, A. J. J. Zangana, Z.-Q. Yin, J. Wu, Y.-G. Han, S. Wang, H.-W. Li, D.-Y. He, S. K. Tawfeeq, B.-S. Shi, G.-C. Guo, W. Chen, and Z.-F. Han, "Experimental demonstration on the deterministic quantum key distribution based on entangled photons," Sci. Rep. **6**, 20962 (2016).
15. A. Wójcik, "Eavesdropping on the "Ping-Pong" quantum communication protocol," Phys. Rev. Lett. **90**, 157901 (2003).

16. M. Pavičić, "In quantum direct communication an undetectable eavesdropper can always tell Ψ from Φ Bell states in the message mode," Phys. Rev. A **87**, 042326 (2013).
17. B. A. Nguyen, "Quantum dialogue," Phys. Lett. A **328**, 6–10 (2004).
18. Y.-G. Yang, Y.-W. Teng, H.-P. Chai, and Q.-Y. Wen, "Revisiting the security of secure direct communication based on Ping-Pong protocol [quantum inf. process. 8, 347 (2009)]," Quantum Inf. Process. **10**, 317–323 (2011).
19. P. Zawadzki, "An improved control mode for the ping-pong protocol operation in imperfect quantum channels," Quantum Inf. Process **14**, 2589–2598 (2015).
20. J. Li, L. Li, H. Jin, and R. Li, "Security analysis of the "Ping-Pong" quantum communication protocol in the presence of collective-rotation noise," Phys. Lett. A **377**, 2729–2734 (2013).
21. Y.-G. Han, Z.-Q. Yin, H.-W. Li, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, "Security of modified Ping-Pong protocol in noisy and lossy channel," Sci. Rep. **4**, 4936 (2007).
22. M. Ostermeyer and N. Walenta, "On the implementation of a deterministic secure coding protocol using polarization entangled photons," Opt. Commun. **281**, 4540–4544 (2008).
23. Z.-X. Man, Z.-J. Zhang, and Y. Li, "Quantum dialogue revisited," Chin. Phys. Lett. **22**, 22–25 (2005).
24. Y.-H. Kim, S. P. Kulik, and Y. Shih, "Quantum teleportation of a polarization state with a complete Bell state measurement," Phys. Rev. Lett. **86**, 1370–1373 (2001).
25. L. Vaidman and N. Yoran, "Methods for reliable teleportation," Phys. Rev. A **59**, 116–125 (1999).
26. N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, "Bell measurements for teleportation," Phys. Rev. A **59**, 3295–3300 (1999).
27. D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, "Noise-free high-efficiency photon-number-resolving detectors," Phys. Rev. A **71**, 061803(R) (2005).
28. O.Thomas, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields, "Efficient photon number detection with silicon avalanche photodiodes," App. Phys. Lett. **97**, 031102 (2010).
29. D. Fukuda, G. Fujii, T. Numata, K. Amemiya, A. Yoshizawa, H. Tsuchida, H. Fujino, H. Ishii, T. Itatani, S. Inoue, and T. Zama, "Titanium-based transition-edge photon number resolving detector with 98% detection efficiency with index-matched small-gap fiber coupling," Opt. Express **19**, 870–875 (2011).
30. K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger, "Dense coding in experimental quantum communication," Phys. Rev. Lett. **76**, 4656–4659 (1996).
31. R. H. Hadfield, "Single-photon detectors for optical quantum information applications," Nature Phot. **3**, 696–705 (2009).
32. A. E. Lita, A. J. Miller, and S. W. Nam, "Counting near-infrared single-photons with 95% efficiency," Optics Express **16**, 3032–3040 (2008).
33. Z.-Y. J. Ou, *Multi-Photon Quantum Interference* (Springer, 2007).
34. M. Pavičić, "Spin correlated interferometry for polarized and unpolarized photons on a beam splitter," Phys. Rev. A **50**, 3486–3491 (1994).
35. M. Pavičić and J. Summhammer, "Interferometry with two pairs of spin correlated photons," Phys. Rev. Lett. **73**, 3191–3194 (1994).
36. M. Pavičić, *Quantum Computation and Quantum Communication: Theory and Experiments* (Springer, 2005).
37. R.-B. Jin, R. Shimizu, I. Morohashi, K. Wakui, M. Takeoka, S. Izumi, T. Sakamoto, M. Fujiwara, T. Yamashita, S. Miki, H. Terai, Z. Wang, and M. Sasaki, "Efficient generation of twin photons at telecom wavelengths with 2.5 GHz repetition-rate-tunable comb laser," Sci. Rep. **4**, 7468 (2014).
38. C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, "Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy," Phys. Rev. A **56**, 1163–1172 (1997).
39. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
40. T. Moroder, M. Curty, and N. Lütkenhaus, "One-way quantum key distribution: Simple upper bound on the secret key rate," Phys. Rev. A **74**, 052301 (2006).
41. J. H. Shapiro, "Performance analysis for Brandt's conclusive entangling probe," Quantum Inform. Process. **5**, 11–24 (2006).
42. J. H. Shapiro and F. N. C. Wong, "Attacking quantum key distribution with single-photon two-qubit quantum logic," Phys. Rev. A **73**, 012315 (2006).
43. R. García-Patróon, F. N. C. Wong, and J. H. Shapiro, "Optimal individual attack on BB84 quantum key distribution using single-photon two-qubit quantum logic," in "Quantum Information and Computation VIII", **7702** of *Proc. of SPIE - CCC code: 0277-786X/10/$18*, E. J. Donkor, A. Pirich, and H. E. Brandt, eds. (SPIE, 2010).
44. A. Niederberger, V. Scarani, and N. Gisin, "Photon-number-splitting versus cloning attacks in practical implementations of the Bennett-Brassard 1984 protocol for quantum cryptography," Phys. Rev. A **71**, 042316 (2005).
45. X.-B. Wang, "Quantum key distribution with two-qubit quantum codes," Phys. Rev. Lett. **92**, 077902 (2004).

---

1. Introduction

Quantum key distribution (QKD) promises secure information transfer based on the laws of quantum physics. The most prominent protocol is the famous BB84 protocol [1]. It is proven to

be *unconditionally* secure provided that Alice and Bob make use of a genuine random number generator [2] and that the quantum bit error rate (QBER) is below 11% [3]. The latter can be increased to 12.7% for the six-state protocol [4]. With a two-way classical communications QBER can be increased further and we shall come back to this point in Sec. 5. The secure QBER can also be increased by increasing the capacity of the protocol so as to send 3 or 4 messages (in contrast to 2 in BB84) via three or four states in a 3- or 4-dim space, achieving 22.7% or 25% respectively. [5, 6].

Beyond maximum tolerable QBER Eve (an eavesdropper) is undetectable when the losses are significant, however, she might be undetectable even below that limit because weak laser pulses, standardly used for implementing QKD with single photons, enable her a beam-splitting [7, 8.5.3, p. 440] and a photon-number splitting attack [7, 8.5.4, p. 441]. Also, recent commercial systems based on BB84 protocol were shown to be hackable by tailored bright illumination and that initiated "identifying and patching technological deficiencies" of BB84 implementation [8].

Therefore, time and again over the last decade a QKD with entangled photons has been considered and reconsidered mostly as modifications of the so-called *ping pong* (pp) protocol with two Bell states [9, 10], by means of all four Bell states, i.e. via the superdense coding (SDC) protocol [11], or even with three particle GHZ state [12]. It can be argued that "the potential of entanglement-based protocols need to be seriously explored, especially taking into account the rapid research progress [13] of entanglement light sources" [14]. On the other hand, correlated detections of photons from the same down-converted pairs provide us with higher loss tolerance.

Various kinds of attack on these deterministic protocols were designed [10, 15, 16] and to cope with them a number of modifications of the protocols were put forward [17–21]. Several implementations have been carried out [14, 22] and the security considered [10, 15, 17–21] although an unconditional one has not been reached.

One of the first proposed attacks on the pp protocol, given by Nguyen [17, 23], enables Eve to read all the messages in the message mode "absolutely unnoticeable." This kind of attack has been addressed in [14, 21] and the protocol shown to be secure via its control mode. Nguyen's pp modification, called *quantum dialog* (in which both, Alice and Bob, send entangled photons and messages) has been addressed in [23].

As we show in Sec. 4, Nguyen's attack can be easily extended to the aforementioned four-Bell-state pp protocol which was proposed to increase the capacity of the protocol—by a transfer of 2 bits via 4 messages—but which requires non-linear optics elements [24] (it cannot be carried out with linear optics ones [25, 26]).

In this paper we propose a high-capacity (four messages) entanglement-based pp-like protocol which is not only resistant to Nguyen's attack but also enables Alice and Bob to detect Eve during their data exchange without switching to a separate control mode and which can be implemented with linear optics elements because it is based on the mixed basis consisting of two Bell states and two states from the computational basis.

The paper is organized as follows. In Sec. 2 we introduce the basis our states are in and a description of our setup. In Sec. 3 we outline our protocol. In Sec. 4 we discuss the security of the protocol and in Sec. 5 we summarize the results we achieved.

2. Mixed basis and setup

Let us start with introducing the mixed basis used in our protocol. We define it as a basis consisting of the two Bell states

$$|\chi^{1,2}\rangle = |\Psi^{\mp}\rangle = \frac{1}{\sqrt{2}}(|H\rangle_1|V\rangle_2 \mp |V\rangle_1|H\rangle_2) \tag{1}$$

and the two computational basis states

$$|\chi^3\rangle = |H\rangle_1|H\rangle_2, \qquad |\chi^4\rangle = |V\rangle_1|V\rangle_2, \tag{2}$$

where $|H\rangle_i$ ($|V\rangle_i$) represents a horizontal (vertical) polarized photon in mode i.

A particular advantage of the mixed basis is that all four basis states can be deterministically discriminated using only a few linear optical elements. The discrimination setup consists of a non polarizing beam splitter (BS) and an additional polarizing beam splitter (PBS) in each of its two output ports—see Fig. 1.
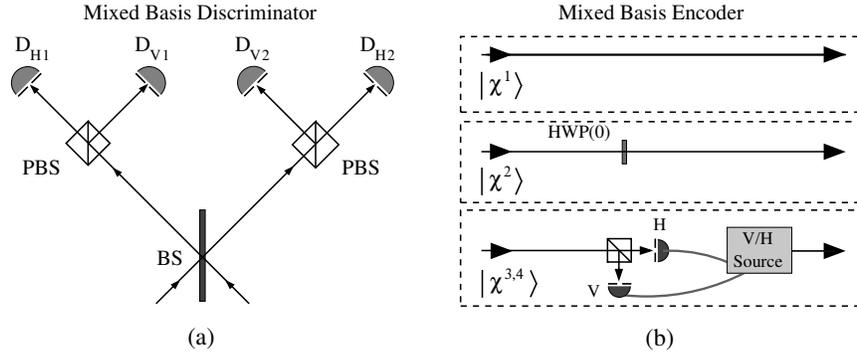
Fig. 1. (a) *Setup for the mixed basis state discrimination.* All four states of the mixed basis can be deterministically discriminated by using only a few linear optic elements like a beam splitter (BS), two polarizing beam splitters (PBS), and photon number resolving detectors (D). (b) *Setups for mixed basis encoding.* All four mixed basis states can be generated from Ψ^- by manipulating *one* of the two photons with one of the shown devices (see text). While for $\chi^{1,2}$ the state preparation is fully deterministic, it is heralded for $\chi^{3,4}$.

The outputs of the PBSs are monitored by four photon number resolving detectors [27–29]. They can also be approximated by purely linear elements such as additional concatenated beam splitters and single photon detectors [30–32].

In the case of $|\chi^3\rangle = |H\rangle_1|H\rangle_2$ and $|\chi^4\rangle = |V\rangle_1|V\rangle_2$ as input states of the discriminator, two indistinguishable parallel polarized photons are sent to the BS from different sides, as shown in Fig. 1(a). These photons will always exit the beam splitter at the same side, bunched together and showing the well known Hong-Ou-Mandel interference effect [33]. Both bunched photons keep the polarization direction they had before they entered the beam splitter [34–36]. On the other hand, $|\chi^2\rangle = |\Psi^+\rangle$ photons bunch together behind the BS, but have different polarization and split at a PBS behind the BS. In contrast, $|\chi^1\rangle = |\Psi^-\rangle$ photons split at the BS and are subsequently transformed into opposite polarization states by the PBSs. Thus, all four mixed basis states can be deterministically and unambiguously discriminated by means of photon number resolving detectors.

In the following, we demonstrate how to prepare the mixed basis states solely from the state $|\Psi^-\rangle$ generated by an entangled photon source [30, 37]. In order to do this we introduce also our QKD setup in Fig. 2, which consists of Alice's and Bob's part together with a quantum and classical communication channel. Bob has an entangled photon source, a quantum delay, and a mixed basis discriminator, as shown in Fig. 1(a). We assume that Bob's entangled photon source generates photon pairs in state $|\chi^1\rangle = |\Psi^-\rangle$. Bob sends one of the photons of the pair, the *travel* photon, to Alice and keeps the other, the *home* photon, delayed for later joint measurements with the travel photon returning from Alice.

Now, Alice can prepare any state of the mixed basis semi-deterministically by manipulating the travel photon she receives from Bob. For this she has a mixed basis encoder, which consists of an auxiliary on-demand single photon source and linear optical elements as shown in Fig. 1 (b). We will first consider the case when no additional HWP($\frac{\pi}{8}$) on Bob's or Alice's side, shown in Fig. 2, are put in.
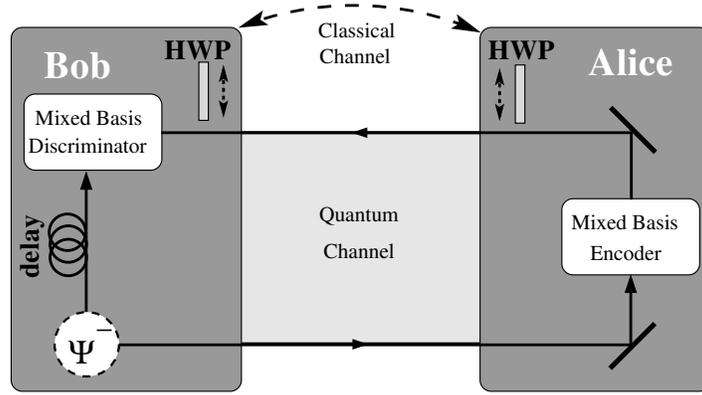
Fig. 2. *QKD setup.* Bob's part consists of an entangled photon pair source generating the state Ψ^-, a quantum delay, a mixed basis discriminator and a removable HWP($\frac{\pi}{8}$) aligned to $\pi/8$. Alice's part consists of a mixed basis encoder and a removable HWP($\frac{\pi}{8}$) also aligned to $\pi/8$. Alice and Bob exchange information on the bases and states over a classical channel.

To generate $|\chi^1\rangle = |\Psi^-\rangle$ nothing need be done—Fig. 1(b), top). To generate $|\chi^2\rangle = |\Psi^+\rangle$ Alice puts a half-wave plate [HWP($0°$)] into the photon path—Fig. 1(b), middle row. The HWP changes the sign of the vertical polarization and thereby transforms $|\Psi^-\rangle$ into $|\chi^2\rangle = |\Psi^+\rangle$. Thus, $|\chi^{1,2}\rangle$ can be generated deterministically.

To generate $|\chi^{3,4}\rangle$ Alice places a PBS with single photon detectors on its output ports and an auxiliary single photon source in her photon's path—Fig. 1(b), lower row. With this, the polarization of the photon is measured and thereby Bob's home photon is projected into $|V\rangle$ if Alice's measurement of the travel photon gives $|H\rangle$ and into $|H\rangle$ if Alice measured $|V\rangle$. Subsequently, Alice replaces the destructively measured photon with a photon of opposite polarization from an auxiliary single photon source. In doing so, it is possible to generate $|\chi^3\rangle = |H\rangle_1|H\rangle_2$ and $|\chi^4\rangle = |V\rangle_1|V\rangle_2$ in a heralded way. State generation of $|\chi^{3,4}\rangle$ is hence probabilistic in the sense that Alice obtains $|H\rangle$ or $|V\rangle$ after her PBS completely at random, but as soon as she does obtain them, the $|\chi^{3,4}\rangle$ states are determined because she knows what she sent and Bob will measure.

Let us now come back to the HWP($\frac{\pi}{8}$) shown in Fig. 2. We assume that Alice and Bob, independently of each other and randomly insert their HWPs aligned to $\pi/8$ (Hadamard gates) using a true quantum random number generator [2].

When both HWPs are inserted Bob will receive (in the absence of Eve) the same states as with no HWP inserted (since two consecutive Hadamards yield the identity). These two arrangements we call the *same bases*. The case when only Alice's or only Bob's HWPs are inserted we call *different bases*.

With a delay Bob informs Alice of his choice of bases and Alice him of hers, over a classical channel. The data obtained with different bases serve them as *control data* which they use to catch Eve. Alice, also with a delay, informs Bob of exact values of all control data. Since the capacity of the classical channels is practically unlimited compared to the quantum channel, the quantity of classical information exchanged should not be a problem. Handling of messages obtained with different bases and the corresponding control data we call the *control mode*.

3. Protocol

Now we describe how Alice and Bob using the setup from Fig. 2 proceed to securely exchange a one-time-key. Our suggested protocol is the following:

1. Bob decides randomly about his basis by placing or not placing his HWP. He prepares the

two photon state $|\chi^1\rangle$, stores the *home photon* in his quantum delay, and sends the *travel photon* to Alice through a quantum channel.

2. Alice decides randomly about her basis by placing or not placing her HWP. She decides to perform the coding operation for $|\chi^1\rangle$, $|\chi^2\rangle$ or $|\chi^{3,4}\rangle$ (with genuine quantum randomness) with probabilities $P(\chi^{1-4}) = 1/4$.

3. Bob measures the two qubit state by means of his mixed basis discriminator, and broadcasts on a public channel if he placed his HWP or not.

4. Alice checks if the transmitted message is valid. This is the case for all $|\chi^{1-4}\rangle$ messages if the bases were the same. If a message is valid, it is stored for later usage as one time key. The selection is called *sifting*. If the bases are different, the measurement data are stored for later usage as the control data. Alice announces the valid messages via a public channel with a delay. She also announces the values of all control data.

5. Bob repeatedly restarts with (a) and with a delay he processes the control data to check for Eve's presence. If yes, they abort the transmission. If not, they distill the key. Thereupon they carry out error correction and privacy amplification [3].

We would like to stress that even in the case of different bases Alice's and Bob's measurements are sensitive to detect the eavesdropper Eve. This is different from the BB84 protocol where part of the valid data has to be sacrificed. Also no active switching between a message and control mode has to be performed as in other pp-like protocols. This is an advantage since switching may open the possibility to advanced eavesdropping attacks, in particular when Eve can hide her presence in the message mode completely as shown below.

4. Security

As we mentioned in Sec. 1, Nguyen's attack [17, p. 7, par. containing Eq. (2)] is a powerful attack on pp-like protocols. We start with its brief presentation and only then we show that our protocol is resistant to it.

As shown in Fig. 3, Eve delays the photons Bob sent to Alice and instead, sends her own photons from her Ψ^- source to Alice to encode them. Eve intercepts the photons Alice encoded, measures them in her discriminator, encodes the read messages on the travel photons she kept delayed and sends them to Bob. Eve can read off all the states sent by Alice in the p-p protocol but cannot in the protocol of ours.

Our protocol is less susceptible to the above attack because:

1. When Alice prepares $|\chi^{3,4}\rangle$ states she collapses the states of both photons – her and Eve's. Eve can deterministically find out which states Alice's and her photons collapsed to, but can collapse Bob's photon states into ones of her own photons only with a probability of 50% (by means of her HWP);

2. When Alice and Bob put HWPs in their channel, then both Eve's reading and resending will be scrambled.

According to [6, 38, 39] we evaluate the condition for QKD to be secure in the presence of Eve: $I_{AB} > I_{AE}$, where I_{AB} (I_{AE}) is the mutual information between Alice and Bob (Eve). We calculate them as follows.

When Alice and Bob are in the same basis with no HWPs inserted and Alice sends $|\chi^1\rangle$ or $|\chi^2\rangle$ Eve can detect them and impose the same state on the Bob's photons. Eve is not necessarily always present in the line and we shall denote her presence by $X \in [0, 1]$; $X = 0$ means that Eve is not present at all and $X = 1$ that she is always present. Thus, Bob will always receive the correct $|\chi^1\rangle$ or $|\chi^2\rangle$, each with the probability 1/4, no matter whether Eve is present or not (when she is in the line she fatefully transmits what she reads), but Eve will read $|\chi^{1,2}\rangle$ only with the probability $X/4$, i.e., only when she is in the line. When Alice sends $|\chi^3\rangle$ or $|\chi^4\rangle$ Eve can detect them but cannot impose the same state on the Bob's photons with a probability higher than 50%. So, Bob's probability of receiving a correct state via Eve diminishes with her presence X
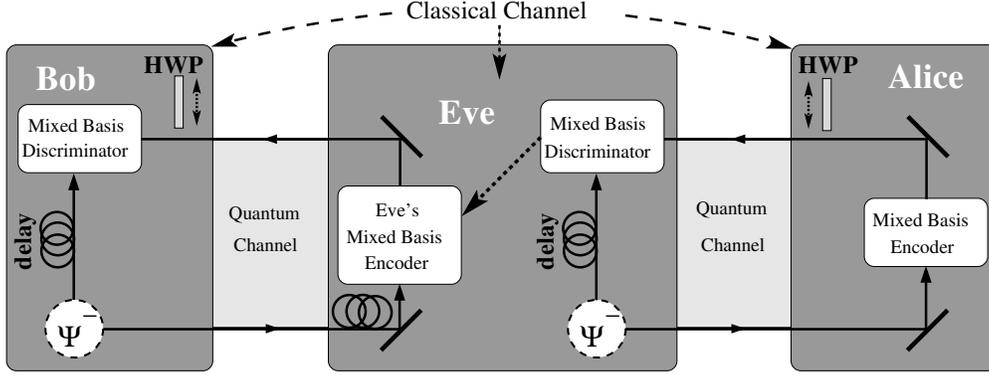
Fig. 3. *An efficient attack by Eve.* Eve delays Bob's photon and sends a photon from her own Ψ^- (χ^1) source. Alice prepares messages for Bob, but Eve deterministically reads them off but can only probabilistically prepare states of Bob's home photons. For instance, when detecting that Alice prepared $|\chi^3\rangle$ ($|HH\rangle$) she can replicate it only with a 50:50 probability, because Bob's home photon is entangled with the travel photon handled by Eve. Nguyen's attack [17, p. 7, par. containing Eq. (2)] on pp can be viewed as the one shown here only without HWPs and without the classical channel.

(probability falls as $(2 - X)/8$) and of receiving incorrect state increases with X. Eve's probability of receiving both correct and incorrect states increases with X.

We give an overview in Table 1 where we show the probabilities that what Alice ($j = 1, 2, 3, 4$) prepares will be received by Bob ($m = 1, 2, 3, 4$) weighted with Eve's ($k = 1, 2, 3, 4$) presence X, in the right-hand part entitled Bob as well as Eve's probabilities of gaining Alice's messages again weighted with her presence X, in the left-hand part entitled Eve.

Table 1. Bob: Probabilities that Bob (m) will measure what Alice (j) sends when HWPs are not inserted, weighted by Eve's (k) presence X; Eve: Probabilities that Eve will read messages that Alice sends and Bob receives weighted by her presence X; When Eve is not in the line we have $X = 0$ and when she is in the line all the time we have $X = 1$; Numbers 1,...,4 in the top two rows and the column on the left hand side denote $|\chi^1\rangle, \ldots, |\chi^4\rangle$.

		Eve						Bob					
j		1	2	3		4		1	2	3		4	
k		1	2	3	4	3	4	1	2	3	4	3	4
m	1	$\frac{X}{4}$						$\frac{1}{4}$					
	2		$\frac{X}{4}$						$\frac{1}{4}$				
	3			$\frac{X}{8}$		$\frac{X}{8}$				$\frac{2-X}{8}$		$\frac{X}{8}$	
	4				$\frac{X}{8}$		$\frac{X}{8}$				$\frac{X}{8}$		$\frac{2-X}{8}$

When Alice and Bob are in the same basis but with both HWPs inserted and Alice sends $|\chi^1\rangle$ or $|\chi^2\rangle$ her HWP($\frac{\pi}{8}$) can be regarded as an operator acting on the states as follows

$$\text{HWP}|\chi^{1,2}\rangle = \frac{1}{2}\left[|HH\rangle \mp |VV\rangle - (|HV\rangle \pm |VH\rangle)\right] = \frac{1}{\sqrt{2}}(|\chi^{3,4}\rangle - |\chi^{2,1}\rangle). \tag{3}$$

At Eve's BS Alice's $|\chi^1\rangle$ will be transformed into the following one:

$$\frac{1}{2\sqrt{2}}(|H\rangle_1|H\rangle_1 - |V\rangle_1|V\rangle_1 - |H\rangle_2|H\rangle_2 + |V\rangle_2|V\rangle_2) - \frac{1}{2}(|H\rangle_1|V\rangle_1 - |H\rangle_2|V\rangle_2)$$

$$= \frac{1}{2}(|\Phi^-\rangle_{11} - |\Phi^-\rangle_{22}) - \frac{1}{\sqrt{2}}|\chi_-^2\rangle, \qquad (4)$$

where the indices refer to the sides of BS. The states $|\chi^{2,3,4}\rangle$ transform similarly.

The probabilities of Eve reading a particular result for the states Alice sent will be

$$|\chi^{1,2}\rangle \longrightarrow |\chi^{2,1}\rangle:\ 50\%;\ |\chi^3\rangle:\ 25\%;\ |\chi^4\rangle:\ 25\%. \qquad (5)$$

Alice's HWP($\frac{\pi}{8}$) changes $|\chi^{3,4}\rangle$ in a similar way and we obtain for the probabilities of Eve's reading:

$$|\chi^{3,4}\rangle \longrightarrow |\chi^1\rangle:\ 25\%;\ |\chi^2\rangle:\ 25\%;\ |\chi^{3,4}\rangle:\ 50\%. \qquad (6)$$

In both cases Eve can resend $|\chi^{3,4}\rangle$ only randomly so that the probabilities for sending states in the latter case will be:

$$|\chi^1\rangle:\ 25\%;\ |\chi^2\rangle:\ 25\%;\ |\chi^3\rangle:\ 25\%;\ |\chi^4\rangle:\ 25\%, \qquad (7)$$

i.e., her $|\chi^3\rangle$ resending will be indistinguishable from her $|\chi^4\rangle$ resending. In Table 2 we give the probabilities for respective measurements with the HWPs inserted for $|\chi^1\rangle$ and $|\chi^3\rangle$ (denoted by 1 and 3 in the top row). For example, the 2nd probability $X/16$ is the probability that Bob will measure $|\chi^1\rangle$ when Alice prepared $|\chi^1\rangle >$ and Eve measured it as $|\chi^2\rangle$ and encoded it into a pair which Bob will measure as $|\chi^1\rangle$ due to his HWP; the last probability $X/64$ is the probability that Bob will measure $|\chi^4\rangle$ when Alice prepared $|\chi^3\rangle$ and Eve measured it as $|\chi^3\rangle$, but failed to encode it and encoded $|\chi^4\rangle$ instead. Double entries divided by a diagonal line refer to Eve's and Bob's reading, respectively. For example the entries in the first line, first column means Alice sent $|\chi^1\rangle$ and Bob will measure $|\chi^1\rangle$ with the probability $(X\text{-}1)/4$ (i.e., only when Eve is in line, not all the time). On the other hand Eve will never measure $|\chi^1\rangle$ in this case (0). A table with probabilities for $|\chi^2\rangle$ and $|\chi^4\rangle$ looks similar and is therefore omitted.

Table 2. Probabilities that Bob (m) will measure what Eve (k) sends him after her reading what Alice (j) prepared when HWPs are inserted. Alice's similar sendings of $|\chi^{2,4}\rangle$ are not shown here. Bob-columns and Eve-row contain marginal probabilities.

j	1					3				
k	1	2	3	4	Bob	1	2	3	4	Bob
m = 1	$\frac{1-X}{4}$ / 0	$\frac{X}{16}$	$\frac{X}{64}$	$\frac{X}{64}$	$\frac{8-5X}{32}$		$\frac{X}{32}$	$\frac{X}{64}$	$\frac{X}{64}$	$\frac{X}{16}$
2			$\frac{X}{64}$	$\frac{X}{64}$	$\frac{X}{32}$	$\frac{X}{32}$		$\frac{X}{64}$	$\frac{X}{64}$	$\frac{X}{16}$
3		$\frac{X}{32}$	$\frac{X}{32}$		$\frac{X}{16}$	$\frac{X}{64}$	$\frac{X}{64}$	$\frac{8-7X}{32}$ / $\frac{X}{32}$		$\frac{4-3X}{16}$
4		$\frac{X}{32}$		$\frac{X}{32}$	$\frac{X}{16}$	$\frac{X}{64}$	$\frac{X}{64}$		$\frac{X}{32}$	$\frac{X}{16}$
Eve	0	$\frac{X}{8}$	$\frac{X}{16}$	$\frac{X}{16}$	$\frac{1}{4}$ / $\frac{X}{4}$	$\frac{X}{16}$	$\frac{X}{16}$	$\frac{X}{16}$	$\frac{X}{16}$	$\frac{1}{4}$ / $\frac{X}{4}$

Let us now calculate the mutual information between Alice and Bob. We make use of its standard definition which is applicable to any communication protocol [40, Eq. (4)].

$$I_{AB} := H(A_B) + H(B) - H(A, B), \tag{8}$$

where the Shannon entropy and the Shannon joint entropy are defined as [40, Sec. II]

$$H(B) = -\sum_{i,n} p(a_i, b_n) \log_2 p(b_n),$$

$$H(A, B) = -\sum_{i,n} p(a_i, b_n) \log_2 p(a_i, b_n), \tag{9}$$

where $p(a_i, b_n)$ is the joint probability that $A = a_i$ and $B = b_n$, and $p(b_n)$ are marginal probabilities; base 2 of the logarithm gives the entropy and information in bits. $H(A_B)$ is the entropy calculated with respect to the messages received by Bob and therefore we have $H(A_B) = H(B) = 4\frac{1}{4} \log_2 \frac{1}{4} = 2$ bits. We define I_{AE} in an analogous way with $H(A_E) = H(E) = 2X - X \log_2 X$. We obtain the probabilities $p(a_i, b_n)$ from the probabilities p_{jkm} which are given in Tables 1 and 2 (i is j for Alice and n is k for Eve or m for Bob).

After a somewhat lengthy but straightforward calculation we obtain the mutual information after sifting with and without HWPs, the arithmetical means of which are given as the following functions of X:

$$I_{AB}(X) = \frac{1}{2} + \frac{X}{8} + \frac{1}{32}\Big(15X \log_2 X + 4(2 - X) \log_2(2 - x)$$
$$+ 2(4 - 3X) \log_2(4 - 3x) + (8 - 5X) \log_2(8 - 5x)\Big)$$
$$I_{AE}(X) = \frac{7X}{8} - X \log_2 X. \tag{10}$$

Their plots in Fig. 4 highlight the key result of our security analysis.
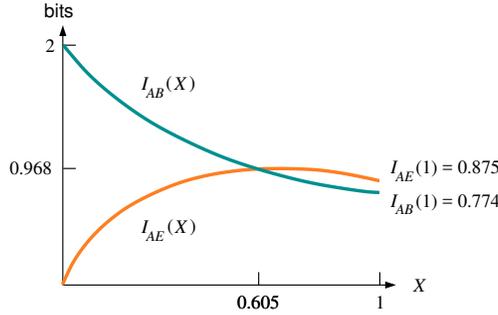
Fig. 4. Mutual information of Alice and Bob, $I_{AB}(X)$, vs. the one of Alice and Eve $I_{AE}(X)$ as functions of Eve's presence, X, in the line.

When Eve is in the line all the time we have $I_{AB}(1) = \frac{5}{8} + \frac{3}{32} \log_2 3 = 0.774$ and $I_{AE}(1) = \frac{7}{8} = 0.875$. Remarkably, the difference between $I_{AE}(X)$ and $I_{AB}(X)$ is even higher for some values of $0.605 < X < 1$, for which $I_{AE}(X) > I_{AB}(X)$.

Another method to estimate the security of our protocol is by means of the control mode. When only Bob's HWP is in place and Alice sends $|\chi^{3,4}\rangle$, according to Eq. (6), Eve will receive them as $|\chi^{3,4}\rangle$ and Bob should receive them as $|\chi^1\rangle$ or $|\chi^2\rangle$ with the probability of 25%, each, or as $|\chi^{3,4}\rangle$ with the probability of 50%. However, in half of the cases Eve will fail to resend the latter states, i.e., she will send them incorrectly as $|\chi^{4,3}\rangle$ instead, with the probability of 25% and

Bob will immediately detect Eve's presence due to Alice's classical information [see Eq. (7)] via Eve's bit-flips $|\chi^3\rangle \rightarrow |\chi^4\rangle$ ($|\chi^4\rangle \rightarrow |\chi^3\rangle$)) with the probability of 1/4, and therefore Eve's probability of escaping detection during each of these two sendings is $1 - 1/4 = 3/4$.

Within a complete set of 4 different messages $|\chi^{1-4}\rangle$ in the control mode Eve's probability of avoiding detection with either $|\chi^1\rangle$ or $|\chi^2\rangle$ is 1 and with $|\chi^3\rangle$ or $|\chi^4\rangle$ is 3/4. Alice's sendings come one after another and therefore the probabilities multiply and Eve will avoid detection within a single cycle with the probability of $1 \times 1 \times (3/4) \times (3/4) = (3/4)^2 \approx 0.56$. After a more detailed analysis we arrive at a result that with such repeated trials Eve's probability of snatching one character (8 bits) undetected is $(0.53/1.54)^8 \approx 0.0002$. We do not have to sacrifice data in order to detect Eve in this way.

5. Discussion

To summarize, we introduced a high capacity (2 bits) protocol that relies on a mixed state basis consisting of two Bell states and two states from the computational basis (a kind of blending ping-pong (pp) and BB84-like protocols) which can be realized experimentally right away since it relies only on off-the-shelf components. The protocol is supported by classical information exchanged between Alice and Bob over a classical channel as shown in Fig. 2. When both HWPs are inserted or none, photon states are in the same bases and the messages are being transferred.

When they are in different bases (only one of the HWPs is inserted) Alice and Bob will detect Eve's bit-flips with the probability of 99.98% during her snatching of her first byte of messages as shown in Sec. 4. So, the different bases do not only support the transfer of messages but function as a control mode as well, similarly to such a mode in the pp protocol and contrary to BB84-like protocols where different bases transmissions are simply discarded (and a portion of messages must be sacrificed for QBER verification).

Still, Eve can hide behind the exponential losses in the fibers and we carried out a security analysis in Sec. 4 to estimate at which level of Eve's presence Alice and Bob must abandon the transmission for the chosen attack. The attack we chose to consider is a modification of Nguyen's attack [17] shown in Fig. 3. When applied to the standard pp-like protocols it can be viewed as sending plain text messages protected by the control mode. For a modified two-state pp protocol with a vacuum state it can be proved secure [14, 21], but for the standard pp protocol or its extension to four states there is no critical presence of Eve in the protocol since we have constant and maximal Alice-Bob mutual information (I_{AB}) for any Eve's presence ($0 < X < 1$) and without it and without having a new kind of privacy amplification algorithms developed for absent critical presence (disturbance, QBER) we do not know when to abort the transmission in such a protocol. In contrast, our protocol is resistant against such Nguyen's attack because it also contains entanglement-based computational basis states.

On the other hand, it is also fundamentally different from the BB84 because Eve cannot send her photon particularly polarized without also affecting Bob's photon's polarization, i.e., she cannot deterministically resend photons in a particular state of polarization even when she knows whether HWPs are inserted of not.

A modified pp protocol with a vacuum state proposed in [14, 21] proved to be secure. In other pp-like protocols [7, 10, 15, 16, 41–44], whenever one can define a critical disturbance, Eve's attacks influence I_{AB} with respect to I_{AE} more than in our protocol. As shown in Fig. 4, for Eve's presence of up to 60% ($X < 0.605$) we have $I_{AB} > I_{AE}$ and the transfer is secure for the considered attack. This Eve's presence corresponds to the disturbance of 30% ($D = X/2$) which is much higher than 11% and 12.7% of D (QBER) for four- and six-state BB84 protocol and also higher than 22.7% and 25% for the 3- and 4-dim protocols mentioned in Sec. 1.

Recently, two-way classical communication channel was used to boost the critical QBER of four- and six-state BB84 protocols to 26% and 30%, respectively [45]. Similar two-way classical communication channel can be used to boost our critical QBER significantly over 30%. This is

the work in progress.

Taken together, the proposed protocol allows for much higher disturbance (QBER, Eve's presence), at which the mutual information between Alice and Eve reaches the mutual information between Alice and Bob, than other standard pp-like protocols. The price we have to pay for such an increased robustness of the protocol is a limited distance since the efficiency of Bob detecting both photons diminishes over four times the distance that a single photon would cover in a BB84 implementation. Hence, right now, the protocol is suitable for urban inter-institutional high-security networks.

Funding

Acknowledgment.