Four–photon interferometry for secure quantum key distribution

P. Hariharan[1] and Barry C. Sanders

School of Physics, University of Sydney,
Sydney, New South Wales 2006, Australia
Department of Physics, Macquarie University, Sydney, New South Wales 2109, Australia

barry.sanders@mq.edu.au
http://www.physics.mq.edu.au/ barry/

Abstract: We introduce a quantum key distribution scheme based on four–photon coincidence measurements. This scheme offers a much higher degree of security than current quantum key distribution methods and minimizes problems due to photon losses and dark counts.

OCIS codes: (270.5290) Photon statistics; (270.4180) Multiphoton processes

References and links

1. C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proc. of IEEE Inter. Conf. on Computers, Systems and Signal Processing, Bangalore, India* (Institute of Electrical and Electronics Engineers, New York, 1984), pp. 175–179.
2. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," J. Cryptol. **5**, 3–28 (1992).
3. W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, "Quantum cryptography using entangled photons in energy–time Bell states," Phys. Rev. Lett. **84**, 4737–.... (2000).
4. A. K. Ekert, J. G. Rarity, P. R. Tapster and G. M. Palma, "Practical quantum cryptography based on two–photon interferometry," Phys. Rev. Lett. **69**, 1293–1295 (1992).
5. J. D. Franson, "Bell inequality for position and time," Phys. Rev. Lett. **62**, 2205–2208 (1989).
6. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett. **85**, 1330–1333 (2000).
7. S. J. D. Phoenix, S. M. Barnett and A. Chefles, "Three-state quantum cryptography," J. Mod. Opt. **47**, 507–516 (2000).
8. H. Bechmann–Pasquinucci and A. Peres, "Quantum cryptography with 3–state systems," Phys. Rev. Lett. **85**, 3313–3316 (2000).
9. A. V. Burlakov, M. V. Chekhova, O. A. Karabutova, D. N. Klyshko, and S. P. Kulik, "Polarization state of a biphoton:Quantum ternary logic," Phys. Rev. A **60**, R4209–R4212 (1999).
10. Y. H. Shih and M. H. Rubin, "Four-Photon Interference Experiment for the Testing of the Greenberger-Horne-Zeilinger Theorem," Phys. Lett. A **204**, 16–22 (1995).
11. T. B. Pittman, "On the Use of Double Entanglement in Four-Photon Experiments," Phys. Lett. A **204**, 193–197 (1995).
12. D. Bouwmeester, J. -W. Pan, M. Daniell, H. Weinfurter and A. Zeilinger, "Observation of Three-Photon Greenberger-Horne-Zeilinger Entanglement," Phys. Rev. Lett. **82**, 1345–1349 (1999).
13. J. -W. Pan, M. Daniell, S. Gasparoni, G. Weihs and A. Zeilinger, "Experimental Demonstration of Four-Photon Entanglement and High-Fidelity Teleportation," Phys. Rev. Lett. **86**, 4435–4438 (2001).
14. Z. Zhao, J. -W. Pan, and M. S. Zhan, "Practical Scheme for Entanglement Concentration," Phys. Rev. A **64** 014301 (2001).
15. H. Weinfurter and M. Zukowski, "Four-Photon Entanglement From Down-Conversion," Phys. Rev. A **64**, 010102(R) (2001).
16. F. Verstraete, J. Dehaene, B. De Moor and H. Verschelde, "Four Qubits Can Be Entangled in Nine Different Ways," Phys. Rev. A **65**, 052112 (2002).
17. S. P. Tewari and P. Hariharan, "Generation of entangled 4-photon states by parametric down-conversion," J. Mod. Opt. **44**, 543–553 (1997).
18. P. Hariharan, J. Samuel and S. Sinha "Four-photon interference: a realizable experiment to demonstrate violation of EPR postulates for perfect correlations," J. Opt. B: Quantum Semiclass. **1**, 199–205 (1999).

Received August 15, 2002; Revised October 16, 2002

19. P. Hariharan and B. C. Sanders, “Cavity-enhanced parametric down-conversion as a source of correlated photons,” J. Mod. Opt. **47**, 1739–1744 (2000).
20. M. Oberparleiter and H. Weinfurter, “Cavity-enhanced generation of polarization-entangled photon pairs,” Opt. Commun. **183**, 133–137 (2000).
21. P. Hariharan, “Simple, high-efficiency, single-photon trap detectors,” J. Opt. B: Quantum Semiclass. **1**, 522–523 (1999).

For completely secure encryption, a key must be shared between a sender (Alice = A) and a receiver (Bob = B) that (1) is as long as the message, (2) is purely random and (3) is used only once. The major drawback of this technique of encryption (the one-time pad) is that, to establish the key for each message, the two users (A and B) need a perfectly secure channel to communicate with each other. This problem can be overcome with a quantum communication channel. For a quantum channel involving correlated photons, intrusion by an eavesdropper (Eve = E) becomes observable via the resultant disturbance of photon correlations. A and B sift their data and use a subset to determine if eavesdropping is possible by ensuring that compromises, such as losses, are less than a predetermined tolerance [1]; if so the key is deemed to be secure and subject to privacy amplification protocols, as necessary [2].

Nondegenerate parametric down–conversion (PDC) can be configured to produce polarization–entangled or polarization–correlated photon pairs that could be shared by A and B and used to construct a secure key. An alternative is for A to employ a single–photon source, perform polarization measurements and send the individual photons to B. The former, namely the use of photon pairs produced by PDC, is of interest here. However, proposed schemes for polarization–based quantum key distribution (QKD) suffer the practical problem that, over long distances, polarization is difficult to preserve. On the other hand, interferometric schemes can be robust over long distances [3]. One such scheme [4] employs PDC of a laser beam, with frequency ω_p, in a nonlinear crystal to produce pairs of photons that are correlated in energy and momentum. These two photons travel along separate optical fibres to identical Mach-Zehnder interferometers. One Mach-Zehnder interferometer is with A, and the other interferometer with B. Each of these interferometers contains a shorter path and a longer path, with a difference in transit time ΔT (≈ 1 ns) greater than the coherence time of the down–converted photons. [5] The outputs from the two interferometers go to two pairs of detectors.

In this two–photon, two–interferometer scheme, if the total phase shifts in the two interferometers are, respectively, $(\phi_A + \theta)$ and $(\phi_B + \theta)$, with $\theta = \omega_p \Delta T = 2m\pi$, where m is an integer, the coefficient of correlation of the four outputs is [4]

$$J(\phi_A, \phi_B) = \cos(\phi_A + \phi_B) \ . \tag{1}$$

To establish a key, A chooses, at random, values of $\phi_A \in \{0, \pi/2\}$, while B chooses, at random, values of $\phi_B \in \{0, -\pi/2\}$. After a sufficiently large number of photons have been recorded, A and B publicly reveal the settings of ϕ_A and ϕ_B that they have used, but not which detectors recorded a photon. They then discard all measurements such that $\phi_A + \phi_B \neq 0$, as well as those in which one or both of them failed to detect a photon. Finally, A and B publicly compare the results of the photo counts on a sufficiently large random subset of the measurements retained by them. If this test subset is correlated beyond the predetermined tolerance level, they can establish a secure cryptographic key. However, errors due to transmission losses, imperfect detector efficiency and dark counts can corrupt the key and conceal the activities of E [6].

Various proposals have been made to overcome these limitations due to eavesdropping, dark counts and photon losses, for example the extension to three mutually nonorthogonal states in each Hilbert space [7] or to three–state systems [8] such as for

#1452 - $15.00 US
Received August 15, 2002; Revised October 16, 2002

"biphotons" [9]. Here we consider an extension of the standard quantum key distribution scheme from the two–photon, two–interferometer scheme to a four–photon, four–interferometer scheme. In our proposal, A and B are each supplied with two photons and two interferometers. The Hilbert space is larger than two dimensions for each of A and B, and the protocol that A and B employ requires coincidence measurements.

Four-photon generation has been discussed [10], proposed [11], experimentally realized [12, 13] and studied theoretically [14, 15, 16], and the use of four-photon states in quantum information tasks such as quantum teleportation and entanglement swapping has been demonstrated [13]. However, all these four-photon schemes proceed by sequential photon pair production, typically by directing a laser beam through a nonlinear optical crystal to produce a pair of photons and retroreflecting the beam through the same crystal to obtain a second pair of photons. In contrast, our proposal uses the single-pass four-photon generation scheme of Tewari and Hariharan [17].

In this method, four highly correlated photons are generated from two pump photons by satisfying the required phase-matching conditions for such a process in a nonlinear crystal with two noncollinear pump beams (frequency ω_p). Down-conversion of individual photons to photon pairs is strictly inhibited since the phase matching condition for this process is not satisfied.

While the susceptibility for this two-photon down-conversion process is low, the gain depends on the second power of the pump amplitude, so that it should be possible to obtain an increase in the down-conversion efficiency by several orders of magnitude, even for a modest value of the average pump power, by using pulsed pump beams [18]. Typically, with a laser generating pulses with a duration of 1 μs, at a repetition rate of 10 pulses s^{-1}, it should be possible to obtain a peak power that is 10^5 greater than the average power and an improvement in down-conversion efficiency by a factor of this order.

In addition, since the number of down-converted photons produced is proportional to the square of the interaction time, an increase in down-conversion efficiency by almost two orders of magnitude may be obtained by placing the nonlinear crystal in a resonant cavity [19, 20]. With a crystal such as beta-barium borate (BBO), having a high nonlinear coefficient, it should be possible to obtain a usable down-converted flux of more than a thousand four-photon states s^{-1}.

As shown in Fig. 1, each of the four down–converted photons enters one of four identical Mach-Zehnder interferometers [18]. Each of these interferometers has a shorter path and a longer path with a difference in transit time ΔT greater than the coherence time of the down–converted photons, so that no interference effects due to single photons are observed in the individual interferometers.

A four–photon event is recorded when photons are detected in coincidence at four of the detectors. The probability of such a four–fold coincidence at the four detectors D$_1$, D$_2$, D$_3$ and D$_4$ is

$$P_{1234} = \frac{1+\cos\Phi}{2}, \tag{2}$$

with

$$\Phi = \phi_1 + \phi_2 + \phi_3 + \phi_4, \tag{3}$$

where $\phi_j = \omega_p \Delta T_j$ for $j = 1, \ldots 4$. The photocounts are perfectly correlated at the detectors D$_1$, D$_2$, D$_3$ and D$_4$ if the sum of the relative phases acquired by the individual photons in the four interferometers $\Phi = 2m\pi$, where m is an integer. Similarly, the photocounts at the four detectors D$'_1$, D$'_2$, D$'_3$ and D$'_4$ are perfectly correlated when $\Phi = (2m+1)\pi$.

Four-photon interference can be used to establish a shared secret key if two of the interferometers in such a system are with A, and the other two are with B. The four

#1452 - $15.00 US
Received August 15, 2002; Revised October 16, 2002

interferometers are initially adjusted so that $\Phi = 2m\pi$, and both A and B record coincidences at the outputs of the two interferometers assigned to each of them.

Both A and B then independently introduce, in one of their interferometers, additional phase shifts $\Delta\phi_A$ and $\Delta\phi_B$, chosen at random to have values of 0 or π, and record coincidences in the outputs from their pairs of interferometers. After a sufficiently large number of coincidences have been recorded, A and B discard all measurements in which either or both of them failed to detect coincidences and convert the results of their measurements into a binary key using a table similar to Table 1.

Table 1. Conversion of observations of coincidences to a binary key. The first column presents the two allowed (random) values of $\Delta\phi_A$, and the third row (second column) presents these two (random) values of $\Delta\phi_B$: the instances for which four-fold coincidences yield bits for the key are signified by the bit (0 or 1) chosen in those instances.

$\Delta\phi_A$	$\Delta\phi_B$			
	Coincidences at $D_1 \ldots D_4$		Coincidences at $D'_1 \ldots D'_4$	
	0	π	0	π
0	0			1
π		1	0	

Security of the key is ensured with this system, since the individual photons carry no information; it is the entanglement of the photons that makes it possible for A and B to generate identical copies of the key.

To determine whether a bit in the key is a 0 or a 1, E must obtain the corresponding values of the phase shifts $\Delta\phi_A$ and $\Delta\phi_B$; however, no information on these phase shifts is exchanged between A and B.

There is also no correlation between $\Delta\phi_A$ or $\Delta\phi_B$ and the probability of a coincidence in the outputs from the four interferometers, or from either pair of interferometers. In addition, the counts at the outputs from the individual interferometers do not depend on the phase shifts introduced in them. As a result, even if E has control of the source, she cannot obtain any information on the key from an intercept-resend attack.

With earlier systems using pairs of correlated photons, errors can arise from missed counts or spurious dark counts. In this system, missed counts due to transmission losses, or imperfect detection efficiency, only result in either A or B (or both) failing to detect a coincidence. As all such measurements are automatically rejected, missed counts do not corrupt the key; they can only decrease the number of bits recorded.

With trap detectors using a pair of avalanche photodiodes (APDs), it should be possible to obtain a detection efficiency > 0.97 [21]. Accordingly, the main source of missed counts would be transmission losses; after allowing for such losses, it should be possible to transmit a key at around a hundred bit s^{-1}. This key could be stored and used to encrypt data which could then be transmitted over an open channel at much higher rates.

Errors arising from dark counts are minimized with this system, as dark counts arising from individual detectors are ignored, and only a four–fold coincidence can produce a spurious bit. Cooled silicon APDs have a dark count rate $< 25\ \mathrm{s}^{-1}$, and since these dark counts occur at random, the probability of detecting a four-fold coincidence in a time window of 1.5 ns (the time resolution of a fast photodetector) is negligible.

The problem of accidental coincidences is also not serious. Since the output from each interferometer consists of a series of pulses with a duration of 1 μs, each containing

#1452 - $15.00 US Received August 15, 2002; Revised October 16, 2002

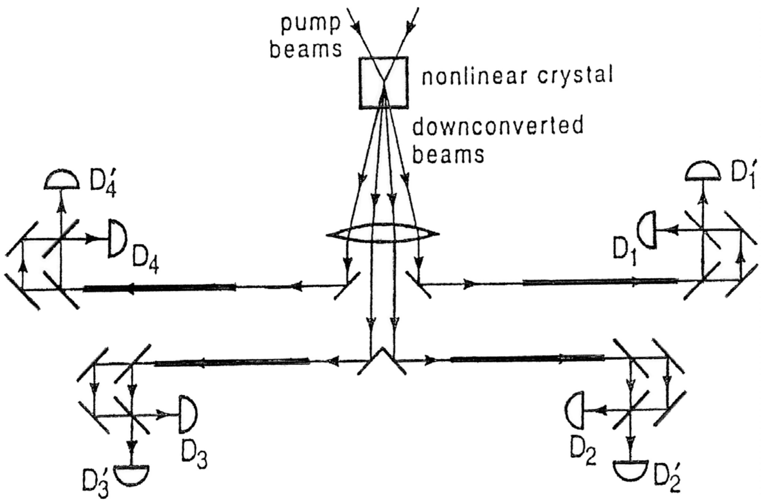

Fig. 1. Schematic of a system for distributing a cryptographic key using four–photon interferometry.

about 10 photons, the ratio of the probability of accidental coincidences at the four outputs, due to uncorrelated photons, to that for actual coincidences would be around 0.02 [18]. Because this figure is fairly low, it is not necessary for A and B to make a public comparison of the results of a fairly large subset of the measurements, which would then have to be discarded. The errors can be located and eliminated with much less waste by simply comparing the parity of randomly chosen subsets of the two versions of the key.

#1452 - $15.00 US Received August 15, 2002; Revised October 16, 2002