Quantum Cryptography with Entangled Photons

Thomas Jennewein,[1] Christoph Simon,[1] Gregor Weihs,[1] Harald Weinfurter,[2] and Anton Zeilinger[1]

[1]*Institut für Experimentalphysik, Universität Wien, Boltzmanngasse 5, A-1090 Wien, Austria*
[2]*Sektion Physik, Universität München, Schellingstrasse 4/III, D-80799 München, Germany*
(Received 24 September 1999)

By realizing a quantum cryptography system based on polarization entangled photon pairs we establish highly secure keys, because a single photon source is approximated and the inherent randomness of quantum measurements is exploited. We implement a novel key distribution scheme using Wigner's inequality to test the security of the quantum channel, and, alternatively, realize a variant of the BB84 protocol. Our system has two completely independent users separated by 360 m, and generates raw keys at rates of 400–800 bits/s with bit error rates around 3%.

PACS numbers: 03.67.Dd, 42.79.Sz, 89.80.+h

The primary task of cryptography is to enable two parties (commonly called Alice and Bob) to mask confidential messages, such that the transmitted data are illegible to any unauthorized third party (called Eve). Usually this is done using shared secret keys. However, in principle it is always possible to intercept classical key distribution unnoticedly. The recent development of quantum key distribution [1] can cover this major loophole of classical cryptography. It allows Alice and Bob to establish two completely secure keys by transmitting single quanta (qubits) along a quantum channel. The underlying principle of quantum key distribution is that nature prohibits gaining information on the state of a quantum system without disturbing it. Therefore, in appropriately designed schemes, no tapping of the qubits is possible without showing up to Alice and Bob. These secure keys can be used in a one-time-pad protocol [2], which makes the entire communication absolutely secure.

Two well-known concepts for quantum key distribution are the BB84 scheme and the Ekert scheme. The BB84 scheme [1] uses single photons transmitted from Alice to Bob, which are prepared at random in four partly orthogonal polarization states: 0°, 45°, 90°, and 135°. If Eve tries to extract information about the polarization of the photons she will inevitably introduce errors, which Alice and Bob can detect by comparing a random subset of the generated keys.

The Ekert scheme [3] is based on entangled pairs and uses Bell's inequality [4] to establish security. Both Alice and Bob receive one particle out of an entangled pair. They perform measurements along at least three different directions on each side, where measurements along parallel axes are used for key generation and oblique angles are used for testing the inequality. In Ref. [3], Ekert pointed out that eavesdropping inevitably affects the entanglement between the two constituents of a pair and therefore reduces the degree of violation of Bell's inequality. While we are not aware of a general proof that the violation of a Bell inequality implies the security of the system, this has been shown [5] for the BB84 protocol adapted to entangled pairs and the Clauser-Horne-Shimony-Holt (CHSH) inequality [6].

In any real cryptography system, the raw key generated by Alice and Bob contains errors, which have to be corrected by classical error correction [7] over a public channel. Furthermore, it has been shown that whenever Alice and Bob share a sufficiently secure key, they can enhance its security by privacy amplification techniques [8], which allow them to distill a key of a desired security level.

A range of experiments have demonstrated the feasibility of quantum key distribution, including realizations using the polarization of photons [9] or the phase of photons in long interferometers [10]. These experiments have a common problem: the sources of the photons are attenuated laser pulses which have a nonvanishing probability to contain two or more photons, leaving such systems prone to the so-called beam splitter attack [11].

Using photon pairs as produced by parametric down-conversion allows us to approximate a conditional single photon source [12] with a high bit rate [13], and yet a very low probability for generating two pairs simultaneously. Moreover, when utilizing entangled photon pairs one immediately profits from the inherent randomness of quantum mechanical observations leading to purely random keys.

Various experiments with entangled photon pairs have already demonstrated that entanglement can be preserved over distances as large as 10 km [14], yet none of these experiments was a full quantum cryptography system. We present in this paper a complete implementation of quantum cryptography with two users, separated and independent of each other in terms of Einstein locality and exploiting the features of entangled photon pairs for generating highly secure keys.

In the following, we will describe the variants of the Ekert scheme and of the BB84 scheme, both of which we implemented in our experiment, based on polarization entangled photon pairs in the singlet state

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}[|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B], \qquad (1)$$

where photon A is sent to Alice and photon B is sent to Bob, and H and V denote the horizontal and vertical linear polarization, respectively. This state shows perfect

anticorrelation for polarization measurements along parallel but arbitrary axes. However, the actual outcome of an individual measurement on each photon is inherently random. These perfect anticorrelations can be used for generating the keys, yet the security of the quantum channel remains to be ascertained by implementing a suitable procedure.

Our first scheme utilizes Wigner's inequality [15] for establishing the security of the quantum channel, in analogy to the Ekert scheme which uses the CHSH inequality. Here Alice chooses between two polarization measurements along the axes χ and ψ, with the possible results $+1$ and -1, on photon A and Bob between measurements along ψ and ω on photon B. Polarization parallel to the analyzer axis corresponds to a $+1$ result, and polarization orthogonal to the analyzer axis corresponds to -1.

Assuming that the photons carry preassigned values determining the outcomes of the measurements χ, ψ, ω and also assuming perfect anticorrelations for measurements along parallel axes, it follows that the probabilities for obtaining $+1$ on both sides, p_{++}, must obey Wigner's inequality:

$$p_{++}(\chi, \psi) + p_{++}(\psi, \omega) - p_{++}(\chi, \omega) \geq 0. \quad (2)$$

The quantum mechanical prediction p_{++}^{qm} for these probabilities at arbitrary analyzer settings α (Alice) and β (Bob) measuring the Ψ^- state is

$$p_{++}^{qm}(\alpha, \beta) = \frac{1}{2} \sin^2(\alpha - \beta). \quad (3)$$

The analyzer settings $\chi = -30°$, $\psi = 0°$, and $\omega = 30°$ lead to a maximum violation of Wigner's inequality (2):

$$p_{++}^{qm}(-30°, 0°) + p_{++}^{qm}(0°, 30°) - p_{++}^{qm}(-30°, 30°) = \frac{1}{8} + \frac{1}{8} - \frac{3}{8} = -\frac{1}{8} \ngeq 0. \quad (4)$$

As Wigner's inequality is derived assuming perfect anticorrelations, which are only approximately realized in any practical situation, one should be cautious in applying it to test the security of a cryptography scheme. When the deviation from perfect anticorrelations is substantial, Wigner's inequality has to be replaced by an adapted version [16].

In order to implement quantum key distribution, Alice and Bob each vary their analyzers randomly between two settings, Alice: $-30°$, $0°$ and Bob: $0°$, $30°$ (Fig. 1a). Because Alice and Bob operate independently, four possible combinations of analyzer settings will occur, of which the three oblique settings allow a test of Wigner's inequality and the remaining combination of parallel settings (Alice $= 0°$ and Bob $= 0°$) allows the generation of keys via the perfect anticorrelations, where either Alice or Bob has to invert all bits of the key to obtain identical keys.

If the measured probabilities violate Wigner's inequality, then the security of the quantum channel is ascertained, and the generated keys can readily be used. This scheme is an improvement on the Ekert scheme which uses the CHSH inequality and requires three settings of Alice's and Bob's analyzers for testing the inequality and generating the keys. From the resulting nine combinations of settings, four are taken for testing the inequality, two are used for building the keys, and three are omitted completely. However, in our scheme each user needs only two analyzer settings and the detected photons are used more efficiently, thus allowing a significantly simplified experimental implementation of the quantum key distribution.

As a second quantum cryptography scheme we implemented a variant of the BB84 protocol with entangled photons, as proposed in Ref. [17]. In this case, Alice and Bob randomly vary their analysis directions between $0°$ and $45°$ (Fig. 1b). Alice and Bob observe perfect anticorrelations of their measurements whenever they happen to have parallel oriented polarizers, leading to bitwise complementary

keys. Alice and Bob obtain identical keys if one of them inverts all bits of the key. Polarization entangled photon pairs offer a means to approximate a single photon situation. Whenever Alice makes a measurement on photon A, photon B is projected into the orthogonal state which is then analyzed by Bob, or vice versa. After collecting the keys, Alice and Bob authenticate their keys by openly comparing a small subset of their keys and evaluating the bit error rate.

The experimental realization of our quantum key distribution system is sketched in Fig. 2. Type-II parametric down-conversion in β-barium borate (BBO) [18], pumped with an argon-ion laser working at a wavelength of 351 nm and a power of 350 mW, leads to the production of polarization entangled photon pairs at a wavelength of 702 nm. The photons are each coupled into 500 m long optical fibers and transmitted to Alice and Bob, respectively, who are separated by 360 m.

Alice and Bob both have Wollaston polarizing beam splitters as polarization analyzers. We will associate a detection of parallel polarization $(+1)$ with the key bit 1
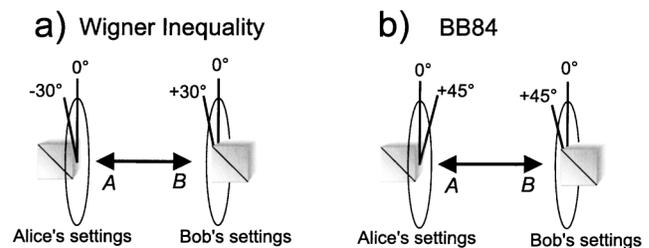
FIG. 1. Settings for Alice's and Bob's analyzers for realizing quantum key distribution based either on (a) Wigner's inequality or (b) the BB84 protocol. The angular coordinates are referenced to the propagation direction of the particle.
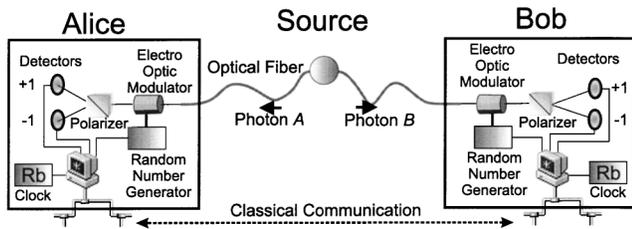
FIG. 2. The polarization entangled photons are transmitted via optical fibers to Alice and Bob, who are separated by 360 m, and both photons are analyzed, detected, and registered independently. After a measurement run the keys are established by Alice and Bob through classical communication over a standard computer network.

and orthogonal detection (-1) with the key bit 0. Electro-optic modulators in front of the analyzers rapidly switch (rise time <15 ns, minimum switching interval 100 ns) the axis of the analyzer between two desired orientations, controlled by quantum random signal generators [19]. These quantum random signal generators are based on the quantum mechanical process of splitting a beam of photons and have a correlation time of less than 100 ns.

The photons are detected in silicon avalanche photo diodes [20]. Time interval analyzers on local personal computers register all detection events as time stamps together with the setting of the analyzers and the detection result. A measurement run is initiated by a pulse from a separate laser diode sent from the source to Alice and Bob via a second optical fiber. Only after a measurement run is completed, Alice and Bob compare their lists of detections to extract the coincidences. In order to record the detection events very accurately, the time bases in Alice's and Bob's time interval analyzers are controlled by two rubidium oscillators. The stability of each time base is better than 1 ns for 1 min. The maximal duration of a measurement is limited by the amount of memory in the personal computers (typically 1 min).

Overall our system has a measured total coincidence rate of ~ 1700 s^{-1}, and a singles rate of $\sim 35\,000$ s^{-1}. From this, one can estimate the overall detection efficiency of each photon path to be 5% and the pair production rate to be 7×10^5 s^{-1}. Our system is very immune against a beam splitter attack because the ratio of two-pair events is only $\sim 3 \times 10^{-3}$, where a two-pair event is the emission of two pairs within the coincidence window of 4 ns. The coincidence window in our experiment is limited by the time resolution of our detectors and electronics, but in principle it could be reduced to the coherence time of the photons, which is usually of the order of picoseconds.

In realizing the quantum key distribution based on Wigner's inequality, Alice's analyzer switches randomly with equal frequency between $-30°$ and $0°$, and Bob's analyzer between $0°$ and $30°$. After a measurement, Alice and Bob extract the coincidences for the combinations of settings of $(-30°, 30°)$, $(-30°, 0°)$ and $(0°, 30°)$, and calculate each probability. For example, the probability

$p_{++}(0°, 30°)$ is calculated from the numbers of coincident events C_{++}, C_{+-}, C_{-+}, C_{-} measured for this combination of settings by

$$p_{++}(0°, 30°) = \frac{C_{++}}{C_{++} + C_{+-} + C_{-+} + C_{-}}. \quad (5)$$

We observed in our experiment that the left-hand side of inequality (2) evaluated to -0.112 ± 0.014. This violation of (2) is in good agreement with the prediction of quantum mechanics and ensures the security of the key distribution. Hence the coincident detections obtained at the parallel settings $(0°, 0°)$, which occur in a quarter of all events, can be used as keys. In the experiment Alice and Bob established 2162 bits raw keys at a rate of 420 bits/s [21], and observed a quantum bit error rate of 3.4%.

In our realization of the BB84 scheme, Alice's and Bob's analyzers both switch randomly between $0°$ and $45°$. After a measurement run, Alice and Bob extract the coincidences measured with parallel analyzers, $(0°, 0°)$ and $(45°, 45°)$, which occur in half of the cases, and generate the raw keys. Alice and Bob collected $\sim 80\,000$ bits of key at a rate of 850 bits/s, and observed a quantum bit error rate of 2.5%, which ensures the security of the quantum channel.

For correcting the remaining errors while maintaining the secrecy of the key, various classical error correction and privacy amplification schemes have been developed [7]. We implemented a simple error reduction scheme requiring only little communication between Alice and Bob. Alice and Bob arrange their keys in blocks of n bits and evaluate the bit parity of the blocks (a single bit indicating an odd or even number of ones in the block). The parities are compared in public, and the blocks with agreeing parities are kept after discarding one bit per block [22]. Since parity checks reveal only odd occurrences of bit errors, a fraction of errors remains. The optimal block length n is determined by a compromise between key losses and remaining bit errors. For a bit error rate p the probability for k wrong bits in a block of n bits is given by the binomial distribution $P_n(k) = \binom{n}{k} p^k (1 - p)^{n-k}$.

Neglecting terms for three or more errors and accounting for the loss of one bit per agreeing parity, this algorithm has an efficiency $\eta(n) = [1 - P_n(1)](n - 1)/n$, defined as the ratio between the key sizes after parity check and before. Finally, under the same approximation as above, the remaining bit error rate p' is $p' = [1 - P_n(0) - P_n(1)](2/n)$. Our key has a bit error rate $p = 2.5\%$, for which $\eta(n)$ is maximized at $n = 8$ with $\eta(8) = 0.7284$, resulting in $p' = 0.40\%$. Hence, from $\sim 80\,000$ bits of raw key with a quantum bit error rate of 2.5%, Alice and Bob use 10% of the key for checking the security and the remaining 90% of the key to distill 49 984 bits of error corrected key with a bit error rate of 0.4%. Finally, Alice transmits a 43 200 bit large image to Bob via the one-time-pad protocol, utilizing a bitwise XOR combination of message and key data (Fig. 3).
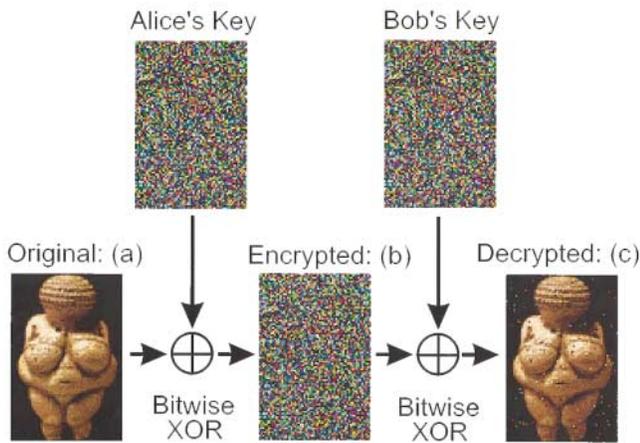
FIG. 3 (color). The 49984 bit large keys generated by the BB84 scheme are used to securely transmit an image [23] (a) of the "Venus von Willendorf" [24] effigy. Alice encrypts the image via bitwise XOR operation with her key and transmits the encrypted image (b) to Bob via the computer network. Bob decrypts the image with his key, resulting in (c) which shows only a few errors due to the remaining bit errors in the keys.

In this Letter we presented the first full implementation of entangled state quantum cryptography. All the equipment of the source and of Alice and Bob has proven to operate outside shielded lab environments with a very high reliability. While further practical and theoretical investigations are still necessary, we believe that this work demonstrates that entanglement based cryptography can be tomorrow's technology.

[1] C. H. Bennett and G. Brassard, in Proceedings of the International Conference on Computer Systems and Signal Processing, Bangalore, 1984, p. 175; C. H. Bennett, G. Brassard, and A. Ekert, Sci. Am. **267**, 26 (1992).

[2] In this classical cryptographic protocol the message is combined with a random key string of the same size as the message to form an encoded message which cannot be deciphered by any statistical methods. G. S. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).

[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[4] J. S. Bell, Physics (Long Island City, N.Y.) **1**, 195 (1965).

[5] C. Fuchs, N. Gisin, R. B. Griffiths, C. S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

[6] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[7] C. H. Bennett and G. Brassard, J. Cryptol. **5**, 3 (1992).

[8] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[9] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, J. Cryptol. **5**, 3 (1992); A. Muller, J. Breguet, and N. Gisin, Europhys. Lett. **23**, 383 (1993); J. D. Franson and B. C. Jacobs, Electron. Lett. **31**, 232 (1995); W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).

[10] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995); R. J. Hughes, G. G. Luther, G. L. Morgan, C. G. Peterson, and C. Simmons, Lect. Notes Comput. Sci. **1109**, 329 (1996); A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Appl. Phys. Lett. **70**, 793 (1997).

[11] N. Lütkenhaus, G. Brassard, T. Mor, and B. C. Sanders (to be published).

[12] One photon of the pair can be used as a trigger for finding the other photon of the pair, provided that the probability of producing two pairs at a single time can be neglected. P. Grangier, G. Roger, and A. Aspect, Europhys. Lett. **1**, 4 (1986); **1**, 173 (1986); J. G. Rarity, P. R. Tapster, and E. Jakeman, Opt. Commun. **62**, 201 (1987).

[13] Note also that in our case the beam splitter attack is less effective than for coherent pulses, because even when two pairs are produced simultaneously, Eve does not gain any information in those cases where Alice and Bob detect photons belonging to the same pair, because then the photon detected by Eve originates from a different pair and is completely uncorrelated to Alice's and Bob's photons.

[14] P. R. Tapster, J. G. Rarity, and P. C. M. Owens, Phys. Rev. Lett. **73**, 1923 (1994); W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **81**, 3563 (1998); G. Weihs, T. Jennewein, C. Simon, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **81**, 5039 (1998).

[15] E. P. Wigner, Am. J. Phys. **38**, 1005 (1970).

[16] M. Zukowski (private communication); L. C. Ryff, Am. J. Phys. **65**, 1197 (1997).

[17] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[18] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. H. Shih, Phys. Rev. Lett. **75**, 4337 (1995).

[19] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, Rev. Sci. Instrum. (to be published).

[20] S. Cova, M. Ghioni, A. Lacaita, C. Samori, and F. Zappa, Appl. Opt. **35**, 1956 (1996).

[21] Note that it would be simple to bias the frequencies of analyzer combinations to increase the production rate of the keys.

[22] Removal of one bit erases the information about the blocks contained in the (public) parities.

[23] Windows-BMP format containing 60×90 pixels, 8 bit color information per pixel: 43 200 bit of picture information. The file includes some header information and a color table, making the entire picture file 51 840 bit. We encrypted only the picture information, leaving the file header and the color table unchanged.

[24] The "Venus" von Willendorf was found in 1908 at Willendorf in Austria and presently resides in the Naturhistorisches Museum, Vienna. Carved from limestone and dated 24 000–22 000 BC, she represents an icon of prehistoric art.