Fast and simple one-way quantum key distribution

Stucki, Damien; Brunner, Nicolas; Gisin, Nicolas; Scarani, Valerio; Zbinden, Hugo

How to cite

STUCKI, Damien et al. Fast and simple one-way quantum key distribution. In: Applied physics letters, 2005, vol. 87, n° 19, p. 194108. doi: 10.1063/1.2126792

This publication URL: https://archive-ouverte.unige.ch/unige:36768
Publication DOI: 10.1063/1.2126792

Fast and simple one-way quantum key distribution

Damien Stucki, Nicolas Brunner, Nicolas Gisin, Valerio Scarani, and Hugo Zbinden
Group of Applied Physics, University of Geneva, 20, rue de l'Ecole-de-Médecine, CH-1211 Geneva 4, Switzerland

(Received 17 June 2005; accepted 15 September 2005; published online 2 November 2005)

We present and demonstrate a new protocol for practical quantum cryptography, tailored for an implementation with weak coherent pulses to obtain a high key generation rate. The key is obtained by a simple time-of-arrival measurement on the *dataline*; the presence of an eavesdropper is checked by an interferometer on an additional *monitoring line*. The setup is experimentally simple; moreover, it is tolerant to reduced interference visibility and to photon number splitting attacks, thus featuring a high efficiency in terms of distilled secret bit per qubit. © *2005 American Institute of Physics*. [DOI: 10.1063/1.2126792]

Quantum key distribution (QKD) is the only method to distribute a secret key between two distant authorized partners, Alice and Bob, whose security is based on the laws of physics.[1] QKD is the most mature field in quantum information; nevertheless, there is still some work ahead in order to build a practical system that is reliable and at a same time fast and provably secure. In this paper we present an important improvement in this direction. The quest for *rapidity* is the inspiring motivation of this system: the idea is to obtain the secret bits from the simplest possible measurement (here, the time of arrival of a pulse) without introducing lossy optical elements at Bob's. *Security* is obtained by occasionally checking quantum coherence: in QKD, a decrease of coherence is attributed to the presence of the eavesdropper Eve, who has attacked the line and obtained some information on the bit values, at the price of introducing errors. *Reliability* is achieved by using standard telecom components; in particular, the source is an attenuated laser, and bits are encoded in time bins, robust against polarization effects in fibers. In this paper, we first define the protocol and demonstrate its advantages: simplicity, and robustness against both reduced interference visibility and photon number splitting (PNS) attacks.[2] Then, we present a first proof-of-principle experiment.

To date, the most developed setups for practical QKD implement the Bennett-Brassard 1984 (BB84) protocol[3] using phase encoding between two time bins, as sketched in the top of Fig. 1 (see Ref. 1 for a detailed description). The four states belonging to two mutually orthogonal bases are the $|1\rangle|0\rangle+e^{i\alpha}|0\rangle|1\rangle$, where $\alpha=0,\pi$ (bits 0 and 1 in the X basis) or $\alpha=\pi/2,3\pi/2$ (bits 0 and 1 in the Y basis). Bob detects in the X (Y) basis by setting $\beta=0$ ($\beta=\pi/2$). Both bases correspond thus to an interferometric measurement. As a first step toward simplicity, we replace (say) the Y basis with the Z basis $\{|1\rangle|0\rangle, |0\rangle|1\rangle\}$. Measuring in this basis amounts simply to the measurement of a time of arrival, and is thus insensitive to optical errors.[4] Bits are encoded in the Z basis, which can be used most of the time, the X basis being used only occasionally to check coherence.[5]

In a practical QKD setup, the source is an attenuated laser: here, Alice's source consists of a cw laser followed by an intensity modulator (IM), which either prepares a pulse of mean photon number μ or blocks completely the beam (empty or "vacuum" pulses).[9] The kth logical bit is encoded in the two-pulse sequences consisting of a nonempty and an empty pulse:

$$|0_k\rangle = |\sqrt{\mu}\rangle_{2k-1}|0\rangle_{2k}, \tag{1}$$

$$|1_k\rangle = |0\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}. \tag{2}$$

Note that $|0_k\rangle$ and $|1_k\rangle$ are not orthogonal, due to their vacuum component; however, a time-of-arrival measurement, whenever conclusive, provides the optimal unambiguous determination of the bit value.[6] To check coherence, we produce a fraction $f \ll 1$ of *decoy sequences* $|\sqrt{\mu}\rangle_{2k-1}|\sqrt{\mu}\rangle_{2k}$; while for BB84, one should produce the two states $|\sqrt{\mu/2}\rangle_{2k-1}|\pm\sqrt{\mu/2}\rangle_{2k}$. Now, due to the coherence of the laser, there is a well-defined phase between any two nonempty pulses: within each decoy sequence, but also *across the bit-separation* in the case where bit number k is 1 and bit number $k+1$ is 0 (a "1–0 bit sequence"). Since we produce equally spaced pulses, the coherence of both decoy and 1–0 bit sequences can be checked with a single interferometer (see Fig. 1, bottom). And there is a further benefit: coherence being distributed both within and across the bit separations, Eve cannot count the number of photons in any finite number of pulses without introducing errors:[6] in our scheme the PNS attacks can be detected.[7] To detect PNS attacks in BB84, one needs to complicate the protocol by the technique of decoy states, which consists of varying μ.[8]

The pulses propagate to Bob on a quantum channel characterized by a transmission t, and are split at a nonequilibrated beamsplitter with transmission coefficient $t_B \lesssim 1$. The pulses that are transmitted (*dataline*) are used to establish the

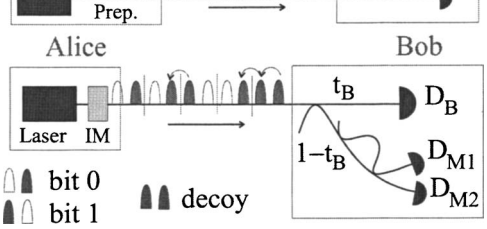

FIG. 1. A comparison of the currently implemented BB84 protocol with phase encoding (top) with the scheme proposed here (bottom). Arrows over pulses indicate coherence (the phase is set to 0 in our scheme).

raw key by measuring the arrival times of the photons. The counting rate is $R=1-e^{-\mu t t_B \eta}\approx \mu t t_B \eta$, where η is the quantum efficiency of the photon counter. The pulses that are reflected at Bob's beamsplitter go to the interferometer that is used to check quantum coherence (*monitoring line*). Indeed, when both pulses j and $j+1$ are nonempty, then only detector D_{M1} can fire at time $j+1$. Coherence can be quantified by Alice and Bob through the visibility of the interference,

$$V=\frac{p(D_{M1})-p(D_{M2})}{p(D_{M1})+p(D_{M2})}, \tag{3}$$

where $p(D_{Mj})$ is the probability that detector D_{Mj} fired at a time where only D_{M1} should have fired. These probabilities are small, the average detection rate on the monitoring line being $\frac{1}{2}\mu t(1-t_B)\eta$ per pulse. Still, if the bit rate is high, meaningful estimates can be done in a reasonable time.

Let's summarize the protocol.

(1) Alice sends a large number of times "bit 0" with probability $(1-f)/2$, "bit 1" with probability $(1-f)/2$ and the decoy sequence with probability f.
(2) At the end of the exchange, Bob reveals for which bits he obtained detections in the dataline and when detector D_{2M} has fired.
(3) Alice tells Bob which bits he has to remove from his raw key, since they are due to detections of decoy sequences (sifting).
(4) Analyzing the detections in D_{2M}, Alice estimates the break of coherence through the visibilities V_{1-0} and V_d associated, respectively, with $1-0$ bit sequences and to decoy sequences, and computes Eve's information.
(5) Finally, Alice and Bob run an error correction and a privacy amplification and end up with a secret key.

The performance of a QKD protocol is quantified by the achievable secret key rate R_{sk}. To compute this quantity, we need to introduce several parameters. The fraction of bits kept after sifting (sifted key rate) is $R_s(\mu)=[R+2p_d(1-R)]p_s$, with $R=\mu t t_B \eta$ the counting rate due to photons defined above, p_d the probability of a dark count, and $p_s=1-f$ here. The amount of errors in the sifted key is called the quantum bit error rate (QBER, Q). Moreover, this key is not secret: Eve knows a fraction I_{Eve} of it. Some classical postprocessing (error correction and privacy amplification) allows us to extract a key that is errorless and secret, while removing a fraction $h(Q)+I_{\mathrm{Eve}}$, where h is binary entropy. Then,

$$R_{\mathrm{sk}}=R_s(\mu)[1-h(Q)-I_{\mathrm{Eve}}]. \tag{4}$$

With this figure of merit, we can compare our scheme to BB84 implemented using the interferometric bases X and Y, as it is done today, with an asymmetric use of the bases such that $p_s=1-f$ ($\mathrm{BB84}_{XY}$). We require that all the visibilities are equal: $V_X=V_Y$ in $\mathrm{BB84}_{XY}$, $V_{1-0}=V_d$ in our scheme—otherwise, Alice and Bob abort the protocol. Under this assumption, the QBER of BB84 is $Q(\mu)=\{R[(1-V)/2]+(1-R)p_d\}p_s/R_s\equiv Q_{\mathrm{opt}}+Q_{\mathrm{det}}$; while in our scheme $Q(\mu)=Q_{\mathrm{det}}$, independent of V.

In order to estimate I_{Eve}, we restrict the class of Eve's attacks,[6] waiting for a full security analysis. Because of losses and the existence of multiphoton pulses, Eve can gain full information on a fraction of the bits without introducing any errors. This fraction is either $r=\mu(1-t)$ or $r=\mu/2t$, according to whether PNS attacks do not or do introduce errors.[2,6] Then Eve performs the intercept-resend attack on a fraction p_{IR} of the remaining pulses. In $\mathrm{BB84}_{XY}$, she introduces the error $(1-r)p_{\mathrm{IR}}\frac{1}{4}=(1-V)/2$ and gains the information $I=(1-r)p_{\mathrm{IR}}\frac{1}{2}=1-V$. On the present protocol, the IR will be performed in the time basis, so $I=(1-r)p_{\mathrm{IR}}$. However, since we use only one decoy sequence, if Eve detects a photon in two successive pulses she knows what sequence to prepare; the introduced error is then $1-V=I\xi$ with $\xi=2e^{-\mu t}/(1+e^{-\mu t})$ the probability that Eve detects something in one pulse and nothing in the other. Plugging $Q(\mu)$ and $I_{\mathrm{Eve}}=r+I$ into Eq. (4), we have R_{sk} as an explicit function of μ; Alice and Bob must choose μ in order to maximize it. The result of numerical optimization is shown in Fig. 2.[10] As expected, the present protocol is more robust than $\mathrm{BB84}_{XY}$ against the decrease of visibility.

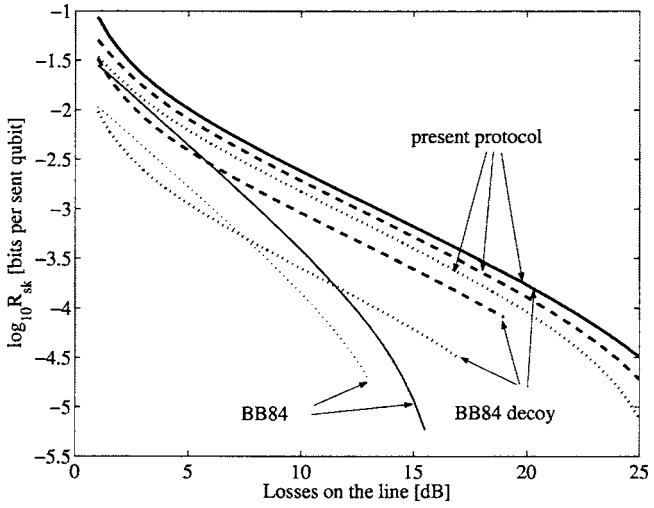

FIG. 2. An estimate of the secret key rates, Eq. (4), for the present protocol and for $\mathrm{BB84}_{XY}$ with and without decoy states, as a function of the losses on the line l ($t=10^{-l/10}$). Parameters: $\eta=10\%$, $p_d=10^{-5}$, $t_B=1$, and $f=0.1$. Visibility: $V=1$ (full lines, identical for the two first protocols), $V=0.9$ (dashed lines), and $V=0.8$ (dotted lines; $R_{\mathrm{sk}}=0$ for BB84 without decoy states).

We show that a reasonably low QBER and good visibility can be obtained using standard telecom components in an implementation with optical fibers. The experimental setup is sketched in Fig. 3. The light of a cw laser (wavelength 1550 nm) passes through an intensity modulator (IM), which prepares the chosen pulse sequence. For simplicity, we send always the same eight-pulse sequence as shown in the figure, namely the string $D010$, where D stands for a decoy sequence. The frequency of 434 MHz of clock C_1 defines the time τ between two successive pulses. The frequency of logical bits in a sequence is half this frequency. The clock C_2 at

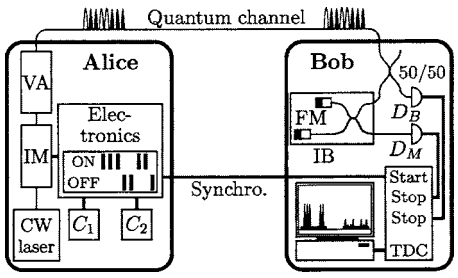

FIG. 3. Experimental setup.

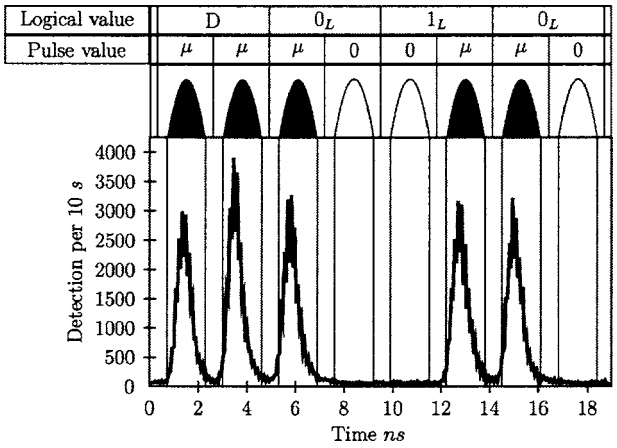

FIG. 4. Detection as a function of the difference of time between start and detection. Logical values and pulse values are depicted in more of the measurement. The difference of amplitude of the different peaks is due to the variation in efficiency in the detection gate.

600 kHz generates the delay between two successive sequences. After the modulator, the light is attenuated by the variable attenuator (VA) in order to obtain $\mu=0.5$ for 5 dB loss in the quantum channel.[10] The synchronization signal directly starts the time-to-digital converter (TDC) and triggers the detectors on Bob's side. The detectors D_B (dataline) and D_M (monitoring line) are opened with gates of 25 ns accepting the whole sequence, featuring quantum efficiency $\eta=10\%$ and a dark count probability $p_d=2.5\times10^{-5}$ per ns. Of course, due to the dead time of the detectors, only one event per sequence and detector can be detected. The stop signal from D_M arm is delayed, which allows us to record the events of both detectors by the same TDC. The Michelson interferometer of the monitoring line has the same pathlength difference τ (46 cm of optical fiber) corresponding to the clock frequency. It is enclosed in an insulated, temperature controlled box (IB). The phase can be changed by changing the temperature. The interferometer (hence our entire setup) is polarization insensitive due to Faraday mirrors (FM) and features a classical fringe visibility of 99%.

The raw detection rate is of 17.0 ± 0.1 kHz. The detection rate is limited by the detectors, due to the 10 μs dead time we have to introduce in order to limit afterpulses. With current detectors, the potential of an improved setup continuously sending pulses at the frequency of C_1, with optimized values for μ, f, and t_B, could only be exploited at long distances. Otherwise, one could use a detection system based on up-conversion and fast thin silicon detector.[11]

The QBER for the pulse sequences "10" and "01" is obtained by considering the time windows of 1.7 ns, as indicated in Fig. 4. The value is $Q=5.2\pm0.4\%$. The contribution of the detector noise and afterpulses (which are rather high for the long gates and high repetition rates we are using) is estimated to be 4%; we attribute the remaining 1% to unperfect intensity modulation, mainly due to too slow electronics and to the jitter of the detectors.

The visibility of the interfering pulses on detector D_M is measured by varying the phase (i.e., the temperature) of the interferometer. The raw visibility is $V_{\mathrm{raw}}\geqslant92\%$, if we consider 1.7 ns time windows. The net visibility, obtained deducing the dark counts and afterpulses, is $V\approx98\%$. We attribute the slight reduction of the visibility to a nonperfect overlap of the interfering pulses due to timing jitter and fluctuations in the intensity modulation. However, this reduced visibility has no significant consequence on the secret key rate (Fig. 2). This tolerance in visibility simplifies the adjustment of the interferometers. With our basic thermal stabilization the interferometer needed to be readjusted only about every 30 min. Indeed, for our pathlength difference, a temperature stability of 0.01 K guarantees $V\gtrsim80\%$. Note that, as the clock frequency of C_1 increases, the stabilization of the interferometer becomes easier.

We have introduced a scheme for QKD and presented the experimental results. The scheme features several advantages: The dataline is very simple, with low losses at Bob's side and small optical QBER. The scheme is tolerant against reduced interference visibility and is robust against PNS attacks (thus allowing the mean photon number to be large, typically $\mu\approx0.5$). Finally, it is polarization insensitive. The existence of such a scheme shows that the main limiting parameter for practical quantum cryptography are the imperfections of the detectors.

The authors acknowledge financial support from the Swiss NCCR "Quantum photonics" and the European Project SECOQC, and thank Avanex for the loan of an intensity modulator.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[3] C. H. Bennett and G. Brassard, in *Proceedings IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179.
[4] Our dataline is that of a classical communication channel, but with a photon counter. The same line is used in a different QKD protocol: T. Debuisschert and W. Boucher, Phys. Rev. A **70**, 042306 (2004).
[5] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 133 (2005); see also quant-ph/9803007.
[6] N. Gisin *et al.*, quant-ph/0411022.
[7] A similar argument applies to a different protocol: K. Inoue and T. Honjo, Phys. Rev. A **71**, 042305 (2005).
[8] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[9] Alternatively, the source could be a pulsed mode-locked laser followed by a pulse picker.
[10] If dark counts can be neglected ($Q_{\mathrm{det}}=0$), the optimization can be done analytically: for the present protocol, $\mu_{\mathrm{opt}}\simeq V/[2(2-V-t)]$; for BB84, $\mu_{\mathrm{opt}}=f(V)/[2(1-t)]$ with, and $\mu_{\mathrm{opt}}=tf(V)$ without decoy states, where $f(V)=\{V-h[(1-V)/2]\}$. For simplicity, in the optimization we have taken $t_B\approx1$ for both protocols, although this may be technically harder to achieve in BB84 because there are more optical components.
[11] R. Thew *et al.* (in preparation).