New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

Information leakage via side channels in freespace BB84 quantum cryptography

New Journal of Physics
The open-access journal for physics

Information leakage via side channels in freespace BB84 quantum cryptography

Sebastian Nauerth[1,3], **Martin Fürst**[1],
Tobias Schmitt-Manderbach[1,2], **Henning Weier**[1]
and Harald Weinfurter[1,2]

[1] Department für Physik, Ludwig-Maximilians-Universität, 80799 München, Germany
[2] Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, D-85748 Garching, Germany
E-mail: Sebastian.Nauerth@physik.uni-muenchen.de

New Journal of Physics **11** (2009) 065001 (8pp)
Received 12 December 2008
Published 3 June 2009
Online at http://www.njp.org/
doi:10.1088/1367-2630/11/6/065001

Abstract. While the BB84 protocol is in principle secure, real implementations suffer from imperfections. Here, we analyse a free space BB84 transmitter, operating with polarization encoded attenuated pulses. We report on measurements of all degrees of freedom of the transmitted photons in order to estimate potential side channels of the state preparation at Alice.

Contents

[3] Author to whom any correspondence should be addressed.

1367-2630/09/065001+08$30.00

1. Introduction

Quantum key distribution (QKD) [1], especially in terms of key growing, can offer, in principle, a level of security [2] that cannot be reached with any classical method. When it comes to real implementations, however, security proofs for ideal protocols might have to be extended in order to also cover potential design flaws of a specific system. Otherwise, an adversary (usually called Eve) might be able to gather information about the transmitted key, for example by employing possible correlations between the different degrees of freedom of the photons that implement the qubits. Thereby, Eve would not cause quantum bit errors and hence would not be revealed. These so-called side channels are a major threat to the security of real QKD devices [3]–[5]. It is therefore essential to investigate QKD systems carefully with respect to their compliance with the theoretical assumptions and idealizations in the security proofs.

In this work, the system in question is our freespace BB84 [6] QKD system extended to decoy states [7]–[10]. For practical reasons the transmitter uses eight distinct laser diodes to prepare the quantum states according to the protocol. The photons prepared by this QKD transmitter then feature three degrees of freedom besides the polarization used for the protocol: while remaining undetected by the BB84 protocol, an adversary can measure the spatial, spectral and temporal properties of the photons. As the value of these degrees of freedom might differ for the various laser diodes, their measurement would allow us to determine, with a certain probability of success, the key bit of the sender. In order to determine a possible information leakage in the case of distinct measurements on single transmitted pulses by an eavesdropper, we therefore characterized the degrees of freedom in question of the transmitted pulses.

Even though this study analyses a particular system, the side channels described here can also be found in other implementations: whenever different sources or signal pathways are used to prepare the states in the transmitter, they might be distinguishable.

2. QKD setup

Our QKD setup, sketched in figure 1, implements the BB84 [6] protocol with polarization encoded qubits. In the transmitter, faint pulses ($\lambda = 850\,\text{nm}$) are prepared, avoiding the extra effort for true single photon pulses. Therefore decoy states and the accordingly modified privacy amplification [2] are used to secure the key distribution. These photonic states have to be encoded in four different polarizations and with two distinct intensities, each. For that purpose often Pockels cells and variable attenuators are used. We opted for a different solution to keep hardware and electronics simple and also to enable an increase of the repetition frequency more easily. The signal pulses (mean photon number per pulse μ_{signal}) with relative linear polarizations of 0°, 45°, 90° and 135° are generated by one laser diode each, mounted with its intrinsic polarization aligned, respectively. Thus there is no need for fast polarization rotations. The pulse intensities are calibrated digitally using a separate laser driver for each channel. Already at a repetition frequency of 10 MHz, it is very hard to switch between different pulse intensities electronically. This is why we decided to use a second set of four laser diodes for the decoy pulses, calibrated for a mean photon number of μ_{decoy}. When the system is used for QKD, random numbers control which laser diode is to be used for a certain pulse according to the chosen QKD protocol [8, 10].

Using eight laser diodes to encode the bit values obviously leads to side channels if the emitted pulses are not perfectly indistinguishable: first of all, their spatial position and

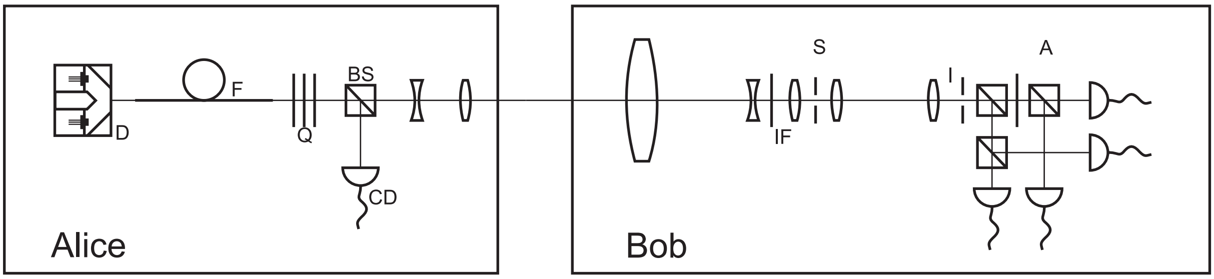

Figure 1. Simplified diagram of the Alice and Bob setup: D: cube housing the laser diodes, F: fibre mode filter, Q: quarter- and half-wave plates for polarization compensation of the fibre, BS: beamsplitter, CD: detector for calibration of mean photon number, IF: interference filter, S: spatial filter consisting of two lenses and a pinhole, I: iris, A: polarization analysing unit (bob module) as described in [12].

orientation differ and might be exploited by an adversary. Therefore, in the Alice module, a custom design of conical and pyramidal mirrors combines the light of the eight diodes into a short piece of single mode fibre acting as a spatial filter [11][4]. Next, a beamsplitter reflects parts of the light into a single photon detector (silicon avalanche photodiode (APD)) for calibration of the mean photon numbers. Finally, a telescope transmits the remaining photons to Bob. At Bob's site, incoming light is filtered very restrictively, both spectrally and spatially, and analyzed afterwards with respect to its polarization in a randomly chosen basis. This takes place in the actual Bob module (see [12]).

3. Information leakage through side channels

Eve might try to measure the spatial (X), spectral (Λ) or temporal (T) properties of the transmitted pulses. If there are correlations of these degrees of freedom with the actual bit value (B) encoded by Alice, Eve can use this side channel to gain knowledge about the key without introducing errors. A quantitative measure of the amount of information, directly accessible by a single, immediate measurement on one pulse, is the mutual information $I(X:B)$, $I(\Lambda:B)$ and $I(T:B)$, respectively. Most likely, more information on the bit value can be gathered from combined, e.g. temporal and spectral measurements, and even more sophisticated attacks. For example, Eve could measure one or more of the degrees of freedom and then, depending on her outcome, decide individually for every pulse whether to perform an intercept resend attack, to block the pulse or just to guess the bit value. This, however, is beyond the scope of this work.

The definition of the mutual information (see e.g. [13]) for a random variable A and the bit value (random variable $B = \{0, 1\}$) can be written as

$$I(A:B) = H(B) - H(B|A) \tag{1a}$$

$$= -\sum_{b\in B} p(b)\log_2 p(b) + \sum_{b\in B} p(a) \sum_{a\in A} p(b|a)\log_2 p(b|a) \tag{1b}$$

where $H(B)$ is the entropy of the random variable B and $H(A|B)$ is the conditional entropy between random variables A and B, and $p(b)$ is the probability of $b \in B$ and $p(b|a)$ is the

[4] The current design is an extension of the one used by our group in Tenerife/La Palma in 2006.

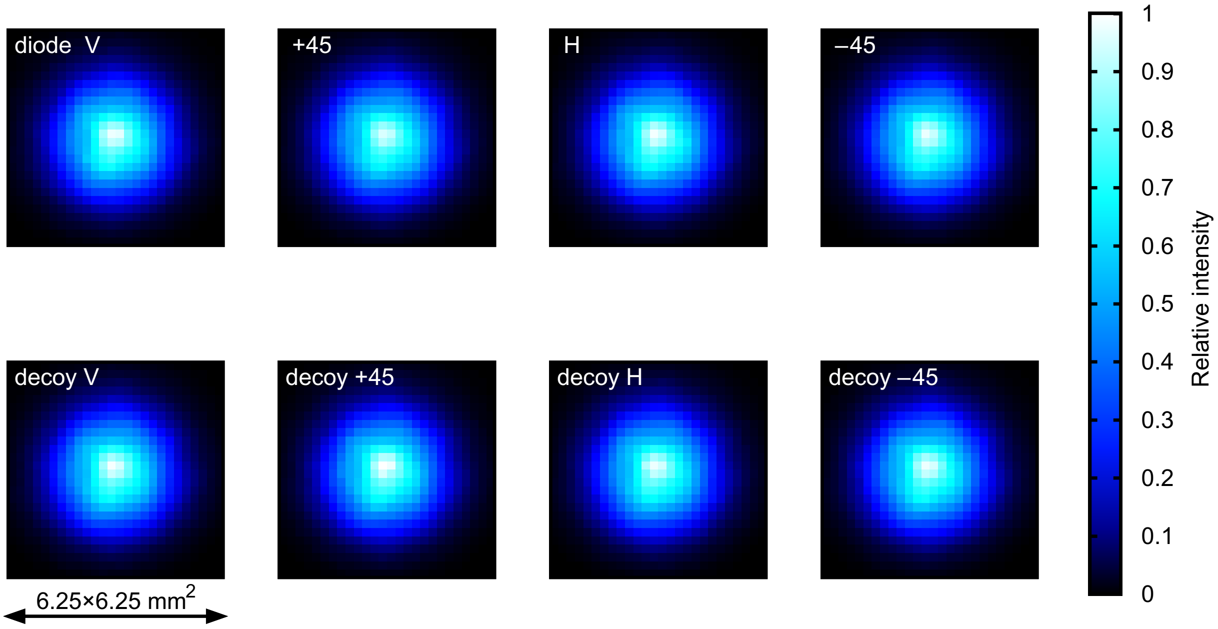

Figure 2. Spatial measurement of the beam of faint pulses coming from the Alice module. To obtain these beam profiles, the collimated beam was scanned with an APD at a distance of 40 cm from the fibre mode filter.

probability of b under the condition $a \in A$. The definition by discrete sums is chosen because the measurements of the transmitted pulses sample the continuous variables X, Λ and T in finite intervals, given by the pixel size and the step width of our measurement scans (see figures 2–4).

In the experiments, it is now the task to determine the values of $p(b|\alpha)$. The measurements investigating the physical properties of the eight diodes, however, provide us with the conditional probabilities $p(\alpha|d)$ where $d \in \{H, V, +, -, H_{\text{decoy}}, V_{\text{decoy}}, +_{\text{decoy}}, -_{\text{decoy}}\}$ denotes the laser diode, $\alpha \in \{x \in X, \lambda \in \Lambda, t \in T\}$. To obtain $p(b|\alpha)$ instead we have to perform further calculations.

As Eve will learn about the basis during sifting we have to treat two cases when averaging $p(\alpha|d)$ in order to get the conditional probabilities $p(\alpha|b)$ with the bit value $b \in B$. For this purpose we consider a decoy QKD protocol here that transmits both pulse classes equally frequently [8] with pulse intensities $\mu_{\text{signal}} = 0.3$ photons pulse^{-1} and $\mu_{\text{decoy}} = 0.35$ photons pulse^{-1}. We get

$$p_{\{HV\}}(\alpha|b=1) = \frac{1}{N}(n_{\text{signal}}\, p(\alpha|d = \text{‘}H\text{’}) + n_{\text{decoy}}\, p(\alpha|d = \text{‘}H_{\text{decoy}}\text{’})) \tag{2a}$$

$$p_{\{HV\}}(\alpha|b=0) = \frac{1}{N}(n_{\text{signal}}\, p(\alpha|d = \text{‘}V\text{’}) + n_{\text{decoy}}\, p(\alpha|d = \text{‘}V_{\text{decoy}}\text{’})) \tag{2b}$$

for the $\{H, V\}$ basis and

$$p_{\{+-\}}(\alpha|b=1) = \frac{1}{N}(n_{\text{signal}}\, p(\alpha|d = \text{‘}+\text{’}) + n_{\text{decoy}}\, p(\alpha|d = \text{‘}+_{\text{decoy}}\text{’})) \tag{2c}$$

$$p_{\{+-\}}(\alpha|b=0) = \frac{1}{N}(n_{\text{signal}}\, p(\alpha|d = \text{‘}-\text{’}) + n_{\text{decoy}}\, p(\alpha|d = \text{‘}-_{\text{decoy}}\text{’})) \tag{2d}$$

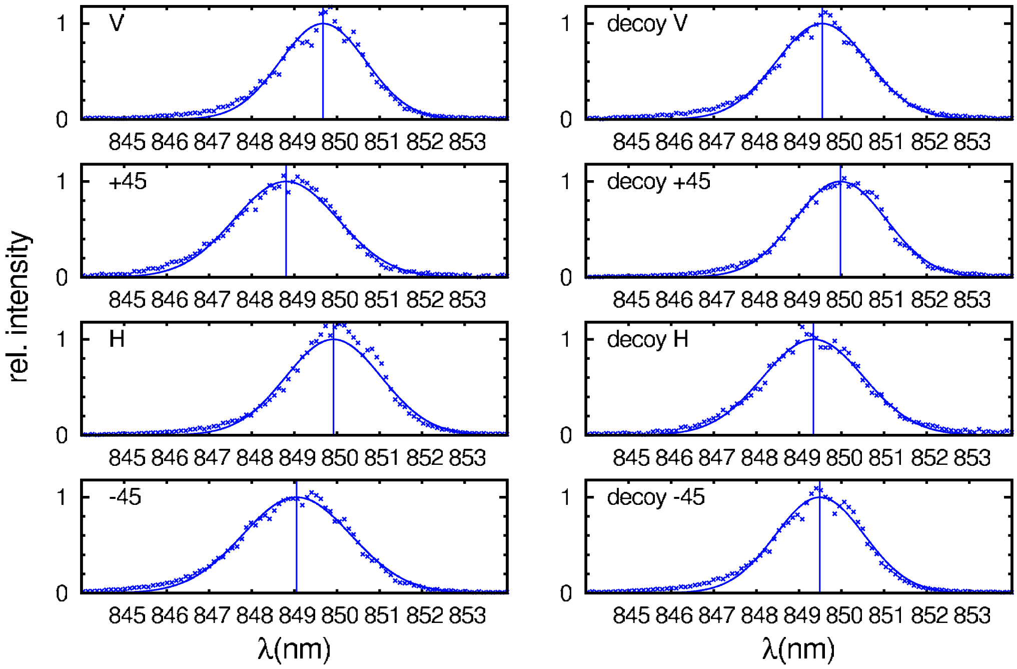

Figure 3. Single photon spectra of the eight transmitter diodes emitting short pulses. The vertical lines indicate the mean value.

for the {+45, −45} basis with the number of pulses that actually contain at least one photon

$$n_{\text{signal}} = 1 - \mathrm{e}^{-\mu_{\text{signal}}} \tag{2e}$$

$$n_{\text{decoy}} = 1 - \mathrm{e}^{-\mu_{\text{decoy}}} \tag{2f}$$

and the normalization

$$n = 2 - \mathrm{e}^{-\mu_{\text{signal}}} - \mathrm{e}^{-\mu_{\text{decoy}}}. \tag{2g}$$

From (2a) one can see that using a decoy protocol that transmits the pulse classes not equally frequently or that demands for height contrast in the pulse intensities may not be optimal with the hardware described here.

Note that if Alice evaluates the decoy security parameters, whether a pulse is of signal or decoy type is never published. Eve may, however, try to guess this information based on her measurements and thereby try to compromise the decoy protocol. This case is not considered here.

In order to get the values for $p(b|\alpha)$ in (1b), Bayes' theorem is used in the form

$$p(b|\alpha) = \frac{p(b)}{p(\alpha)} p(\alpha|b). \tag{3}$$

For example, we now get for the mutual information between the wavelength and the bit value $I_\beta(\Lambda : B)$ with $\beta \in \{\{H, V\}, \{+45, -45\}\}$ denoting the basis

$$I_\beta(\Lambda : B) = 1 + \sum_{\lambda\in\Lambda} \sum_b \frac{p_\beta(\lambda|b)}{2} \log_2\left(\frac{p_\beta(\lambda|b)}{2\, p_\beta(\lambda)}\right), \tag{4a}$$

where we already get $H(B) = 1$ as we expect the bit values to be equally distributed and totally random: $p(b) = 1/2$. Finally, as both bases are used equally frequently, the average

$$I(\Lambda : B) = \tfrac{1}{2}(I_{\{H,V\}}(\Lambda : B) + I_{\{+45,-45\}}(\Lambda : B)) \tag{4b}$$

is the actual mutual information accessible by a measurement as described. Here, we assume mutual independence of the different degrees of freedom X, Λ and T. Obviously, this has to be tested in the specific setups, too.

4. Measurements on the quality of state preparation in the transmitter

In order to obtain the conditional probabilities as required for (1*b*) we performed a series of measurements on the pulses transmitted by Alice. All these measurements have been carried out under authentic conditions, i.e. using the same electronic parameters and mean photon numbers used during QKD runs. This implies that all analyses have to be performed at light levels below the single photon level per pulse. We used passively quenched APDs, which have a quantum efficiency of 30% including an interference filter (FWHM 10 nm at a wavelength of 850 nm) mounted as entrance window. The time jitter of the APD diode together with the pulse shaping electronics was found to be 600 ps. For the measurements of these detector characteristics, downconverted photon pairs were used.

As described above, the usage of eight laser diodes in the Alice module, despite the many benefits, leads to obvious security concerns: the different light sources can be, in principle, distinguished spatially, by means of their wavelength or by a precise measurement of the pulse delay with respect to the 10 MHz beat. We therefore made huge efforts to anticipate these side channels right from the beginning. First, laser diodes with closely matching wavelengths were chosen and their special ordering in the Alice module minimizes the remaining distinguishability. The laser driver electronics features digitally programmable delay lines for each channel in order to overlap all emitters temporally and, finally, spatial information is erased in the single mode fibre. The following measurements are intended to quantify the remaining information accessible via measurements on the transmitted pulses. For the evaluation of the information leakage, we decided not to fit the acquired data to a model and not to use an integral form of (1*b*) because local aberrations of single diodes cannot be resembled in the fit and therefore would not contribute to the calculated mutual information. Evidently, Eve will especially search for such distinguishabilities to determine the diode that produced a certain pulse.

Spatial measurements. Because of the short length of about 6 cm of the single mode fibre, we had to check if there is still spatial information transmitted by the fibre cladding, i.e. whether the fibre has enough attenuation on all higher modes. For this purpose we scanned an intersection of the collimated beam at a distance of 40 cm after the fibre where the beam diameter was 3 mm (full width at half-maximum (FWHM)) (figure 2). The diameter of the sensitive surface of the APD used for this measurement is 500 μm. On this scale, we could not find any correlations between the bit value B and the detection place X above the noise level. The information leakage $I(X : B)$, calculated (in analogy to (4*a*)) from the data in figure 2, is of the order of 10^{-5} bits pulse^{-1}.

Spectral. In order to determine the spectral distinguishability of the pulses coming from eight different laser diodes, we acquired their emission spectra (figure 3) using a single photon spectrometer with a resolution of 0.4 nm. The width of these spectra

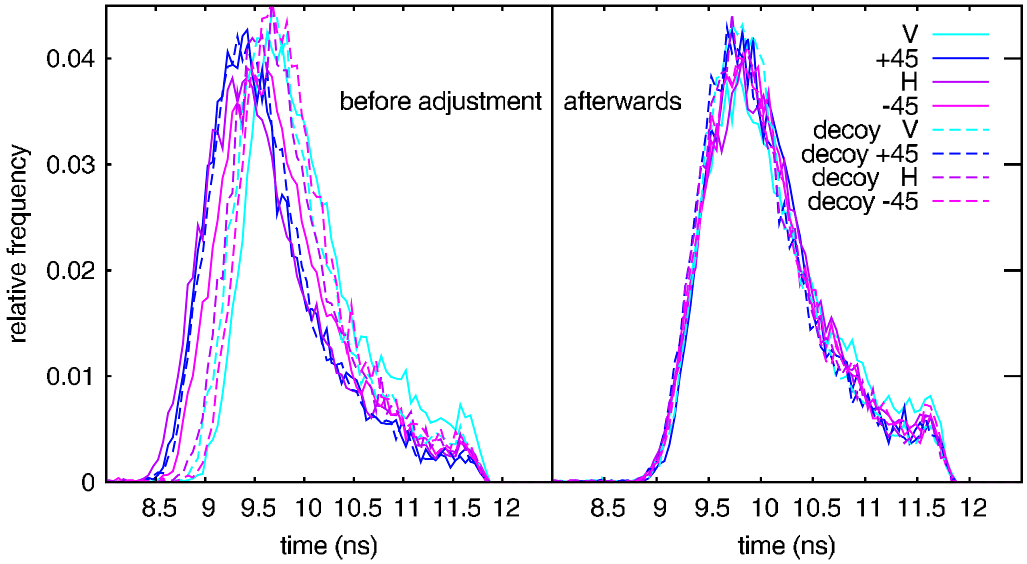

Figure 4. Time histograms of the transmitted pulses. Left: before adjustment, right: maximum temporal overlap due to digitally programmable delay lines in every channel.

is on average 2.6 nm and their mean is 849.49 nm with a standard deviation of 0.42 nm. The mutual information between the bit value B and the spectra Λ evaluates to $I_{\{H,V\}}(\Lambda : B) = 6.3 \times 10^{-3}$ bits pulse^{-1} and $I_{\{+45,-45\}}(\Lambda : B) = 6.8 \times 10^{-3}$ bits pulse^{-1} (average: $I(\Lambda : B) = 6.6 \times 10^{-3}$ bits pulse^{-1}) (4*a*).

Temporal. The temporal overlap between the pulses from different laser diodes can be maximized in our system by digitally programmable delay lines with a resolution of better than 50 ps. We measured a histogram of pulse delays T relative to the 10 MHz beat for each diode by focusing its pulses onto an APD (see figure 4). The electronic pulses were registered with an oscilloscope with an additional time jitter of about 40 ps. Given the time resolution of the detectors, we can infer the pulse length of all diodes to be well below 1 ns (FWHM). The statistical analysis led us to a mutual information between the bit value and the detection time of $I(T : B) = 2.8 \times 10^{-3}$ bits pulse^{-1} as an average over both bases ($I_{\{H,V\}}(T : B) = 2.6 \times 10^{-3}$ bits pulse^{-1}, $I_{\{+45,-45\}}(T : B) = 3.0 \times 10^{-3}$ bits pulse^{-1}).

5. Conclusions

Our experiments allow for an estimation of the amount of information a single measurement of one degree of freedom of a transmitted pulse can provide about the value of the sent keybit. Considering the above values for $I(X : B)$, $I(\Lambda : B)$ and $I(T : B)$ the according information leakage arising from the usage of eight separate laser diodes is small compared to the information leakage indicated by the QBER or the contribution of pulses with more than one photon. The analysis presented here gives a first indication of the possible information leakage, as Eve was allowed only to perform measurements on the side channels but not to manipulate the quantum channel depending on her measurement results. If Eve is allowed such conditional attacks, she can gather more information. This is, however, beyond the scope of this work but could be examined along the lines of [2]. In either case, the information leakage can be further reduced by narrower spectral filtering or shorter gate windows. Yet these countermeasures would require temperature-stabilized diodes and filters or novel faster timing circuits.

The design of the transmitter presented here, however, has already been demonstrated to be well suited for freespace QKD as it allows for simple electronics and small formfactor, while potential weaknesses of this approach involving distinct laser diodes can be kept under control.

Acknowledgments

This work was funded in the framework of SECOQC, QCCC and QPENS and by the German Bundesministerium der Verteidigung.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography *Rev. Mod. Phys.* **74** 145–95

[2] Gottesman D, Lo H-K, Lütkenhaus N and Preskill J 2004 Security of quantum key distribution with imperfect devices *Quantum Inf. Comput.* **5** 325

[3] Lamas-Linares A and Kurtsiefer C 2007 Breaking a quantum key distribution system through a timing side channel *Opt. Express* **15** 9388

[4] Makarov V, Anisimov A and Skaar J 2006 Effects of detector efficiency mismatch on security of quantum cryptosystems *Phys. Rev.* A **74** 022313

[5] Qi B, Fred Fung C-H, LO H-K and Ma X 2007 Time-shift attack in practical quantum cryptosystems *Quantum Inf. Comput.* **7** 073

[6] Bennett C H and Brassard G 1984 Quantum cryptography: public-key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing* (Bangalore, India) pp 175–9

[7] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[8] Wang X-B 2005 Beating the photon-number-splitting attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503

[9] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504

[10] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution *Phys. Rev.* A **72** 012326

[11] Schmitt-Manderbach T, Weier H, Fürst M, Ursin R, Tiefenbacher F, Scheidl T, Perdigues J, Sodnik Z, Kurtsiefer C, Rarity J G, Zeilinger A and Weinfurter H 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504

[12] Weier H, Schmitt-Manderbach T, Regner N, Kurtsiefer C and Harald W 2006 Free space quantum key distribution: towards a real life application *Fortschr. Phys.* **54** 840–5

[13] Cover T M and Thomas J A 1991 *Elements of Information Theory* (*Wiley Series in Telecommunications*) (New York: Wiley)