Security Aspects of Practical Quantum Cryptography

Gilles Brassard[1,⋆], Norbert Lütkenhaus[2,⋆⋆], Tal Mor[3,4,⋆⋆⋆], and Barry C. Sanders[5]

[1] Département IRO, Université de Montréal, C.P. 6128, succ. centre–ville
Montréal (Québec), Canada H3C 3J7
brassard@iro.umontreal.ca
[2] Helsinki Institute of Physics, P.O.Box 9, 00014 Helsingin yliopisto, Finland
lutkenha@rock.helsinki.fi
[3] Electrical Engineering, College of Judea and Samaria, Ariel, Israel
talmo@cs.technion.ac.il
[4] Electrical Engineering, University of California at Los Angeles
Los Angeles, CA 90095–1594, USA
talmo@ee.ucla.edu
[5] Department of Physics, Macquarie University, Sydney
New South Wales 2109, Australia
barry.sanders@mq.edu.au

Abstract. The use of quantum bits (qubits) in cryptography holds the promise of secure cryptographic quantum key distribution schemes. Unfortunately, the implemented schemes are often operated in a regime which excludes unconditional security. We provide a thorough investigation of security issues for practical quantum key distribution, taking into account channel losses, a realistic detection process, and modifications of the "qubits" sent from the sender to the receiver. We first show that even quantum key distribution with perfect qubits might not be achievable over long distances when fixed channel losses and fixed dark count errors are taken into account. Then we show that existing experimental schemes (based on weak pulses) currently do not offer unconditional security for the reported distances and signal strength. Finally we show that parametric downconversion offers enhanced performance compared to its weak coherent pulse counterpart.

1 Introduction

Quantum information theory suggests the possibility of accomplishing tasks that are beyond the capability of classical computer science, such as information-theoretically secure cryptographic key distribution [3,5]. The lack of security

⋆ Supported in part by Canada's NSERC and Québec's FCAR.
⋆⋆ Supported by grant 43336 by the Academy of Finland.
⋆⋆⋆ Supported in part by grant #961360 from the Jet Propulsion Laboratory, and grant #530–1415–01 from the DARPA Ultra program.

B. Preneel (Ed.): EUROCRYPT 2000, LNCS 1807, pp. 289–299, 2000.

proofs for standard (secret- and public-) key distribution schemes, and the insecurity of the most widely used classical schemes (such as RSA [27]) against potential attacks by quantum computers [29], emphasizes the need for provably information-theoretically secure key distribution.

Whereas the security of idealized quantum key distribution (QKD) schemes has been reported against very sophisticated collective [8,7] and joint [22,23,6] attacks, we show here that already very simple attacks severely disturb the security of existing experimental schemes, for the chosen transmission length and signal strength. For a different parameter region a positive security proof against individual attacks has been given recently [19,20] making use of ideas presented here.

In the four-state scheme introduced in 1984 by Bennett and Brassard [3], usually referred to as BB84, the sender (Alice) and the receiver (Bob) use two conjugate bases (say, the rectilinear basis, +, and the diagonal basis, $\times$) for the polarization of single photons. In basis + they use the two orthogonal basis states $|0_+\rangle$ and $|1_+\rangle$ to represent "0" and "1" respectively. In basis $\times$ they use the two orthogonal basis states $|0_\times\rangle = (|0_+\rangle + |1_+\rangle)/\sqrt{2}$ and $|1_\times\rangle = (|0_+\rangle - |1_+\rangle)/\sqrt{2}$ to represent "0" and "1". The basis is revealed later on via an authenticated classical channel that offers no protection against eavesdropping. The signals where Bob used the same basis as Alice form the *sifted key* on which Bob can decode the bit value. In absence of disturbance by an eavesdropper (Eve) and errors of various kinds, the sifted key should be identical between Alice and Bob. The remaining signals are ignored in the protocol and in this security analysis. Finally, Alice and Bob test a few bits to estimate the error rate, and if it is less than some threshold, they use error correction and privacy amplification [2,4] to obtain a secure final key [6,23].

In order to be practical and secure, a quantum key distribution scheme must be based on existing—or nearly existing—technology, but its security must be guaranteed against an eavesdropper with unlimited computing power whose technology is limited only by the rules of quantum mechanics. The experiments that have been performed so far are usually based on weak coherent pulses (WCP) as signal states with a low probability of containing more than one photon [2,13,30,11,25]. Initial security analysis of such weak-pulse schemes were done [2,15], and evidence of some potentially severe security problems (which do not exist for the idealized schemes) have been shown [15,32].

Using a conservative definition of security, we investigate such limitations much further to show insecurity of various existing setups, and to provide several explicit limits on experimental QKD. First, we show that secure QKD to arbitrary distance can be totally impossible for given losses and detector dark counts, even with the assumption of a perfect source. Second we show that QKD can be totally insecure even with perfect detection, if considering losses and multi-photon states. In a combination we compute a maximal distance beyond which (for any given source and detection units) secure QKD schemes cannot be implemented. Finally we prove the advantage of a better source which makes use of parametric downconversion (PDC).

2 Losses and Dark Counts

The effect of losses is that single-photon signals will arrive only with a probability F at Bob's site where they will lead to a detection in Bob's detectors with a probability η_{B} (detection efficiency). This leads to an expected probability of detected signals given by $p_{\mathrm{exp}}^{\mathrm{signal}} = F\eta_{\mathrm{B}}$. For optical fibres, as used for most current experiments, the transmission efficiency F is connected to the absorption coefficient β of the fibre, the length ℓ of the fibre and a distance-independent constant loss in optical components c, via the relation

$$F = 10^{-\frac{\beta\ell + c}{10}} \tag{1}$$

which, for given β and c, gives a one-to-one relation between distance and transmission efficiency. Quantum key distribution can also be achieved through free space [2,11], in which case the problem of lossy fibres is replaced by the problem of beam broadening. Each of Bob's detectors is also characterized by a dark count probability d_{B} per time slot in the absence of the real signal, so that for a typical detection apparatus with two detectors the total dark count probability is given by $p_{\mathrm{exp}}^{\mathrm{dark}} \approx 2d_{\mathrm{B}}$. The dark counts are due to thermal fluctuations in the detector, stray counts, etc. Throughout the paper we assume conservatively that Eve has control on channel losses and on η_{B}, that all errors are controlled by Eve (including dark counts), and that Bob's detection apparatus cannot resolve the photon number of arriving signals. Without these assumptions, one gets a relaxed security condition, which, however, is difficult to analyse and to justify.

The total expected probability of detection events is given by

$$\begin{aligned} p_{\mathrm{exp}} &= p_{\mathrm{exp}}^{\mathrm{signal}} + p_{\mathrm{exp}}^{\mathrm{dark}} - p_{\mathrm{exp}}^{\mathrm{signal}} p_{\mathrm{exp}}^{\mathrm{dark}} \\ &\leq p_{\mathrm{exp}}^{\mathrm{signal}} + p_{\mathrm{exp}}^{\mathrm{dark}} \quad . \end{aligned} \tag{2}$$

There are two differently contributing error mechanisms. The signal contributes an error with some probability due to misalignment or polarization diffusion. On the other hand, a dark count contributes with probability approximately $1/2$ to the error rate. As the transmission efficiency F becomes smaller and smaller when the distance ℓ is increased, the errors due to dark counts become dominant. Therefore, considering the relevant limit where we can neglect the coincidence probability between a signal photon and a dark count, or between dark counts in both detectors, we have for the error rate e (per sent signal) the approximate lower bound

$$e \succeq \tfrac{1}{2}\, p_{\mathrm{exp}}^{\mathrm{dark}} \quad , \tag{3}$$

where "$x \succeq y$" means that x is approximately greater than or equal to y, when second-order terms are neglected. The contribution to the error rate per sifted key bit is then given by $p_e = e/p_{\mathrm{exp}}$.

If the error rate per sifted key bit p_e exceeds $1/4$, there is no way to create a secure key. With such an allowed error rate, a simple intercept/resend attack (in which Eve measures in one of the two bases and resends according to her

identification of the state) causes Bob and Eve to share (approximately) half of Alice's bits and to know nothing about the other half; hence, Bob does not possess information which is unavailable to Eve, and no secret key can be distilled. Using $p_e = e/p_{\rm exp}$ and $p_e < \frac{1}{4}$, we obtain a necessary condition for secure QKD

$$e < \tfrac{1}{4}\, p_{\rm exp} \ , \tag{4}$$

and using (2, 3), we finally obtain $p_{\rm exp}^{\rm signal} \succeq p_{\rm exp}^{\rm dark}$.

For ideal single-photon states we therefore obtain (with $p_{\rm exp}^{\rm signal} = F\eta_{\rm B}$ and $p_{\rm exp}^{\rm dark} \approx 2d_{\rm B}$) the bound $F\eta_{\rm B} \succeq 2d_{\rm B}$. We see that even for ideal single-photon sources (SP), the existence of a dark count rate leads to a minimum transmission efficiency

$$F > F_{\rm SP} \approx 2d_{\rm B}/\eta_{\rm B} \tag{5}$$

below which QKD cannot be securely implemented. Even for perfect detection efficiency ($\eta_{\rm B} = 1$) we get a bound $F > F_{\rm SP} \approx 2d_{\rm B}$. These bounds correspond, according to (1), to a maximal covered distance, which mainly depends on β.

3 Losses and Imperfect Sources

In a quantum optical implementation, single-photon states would be ideally suited for quantum key distribution. However, such states have not yet been practically implemented for QKD, although proposals exist and experiments have been performed to generate them for other purposes. The signals produced in the experiments usually contain zero, one, two, etc., photons in the same polarization (with probabilities p_0, p_1, p_2, etc., respectively). The multi-photon part of the signals, $p_{\rm multi} = \sum_{i\geq 2} p_i$, leads to a severe security gap, as has been anticipated earlier [2,15,32]. Let us present the *photon number splitting* (PNS) attack, which is a modification of an attack suggested in [15] (the attack of [15] was disputed in [32] so the modification is necessary): Eve deterministically splits one photon off each multi-photon signal. To do so, she projects the state onto subspaces characterized by n, which is the total photon number, which can be measured via a quantum nondemolition (QND) measurement. The projection into these subspaces does not modify the polarization of the photons. Then she performs a polarization-preserving splitting operation, for example by an interaction described by a Jaynes-Cummings Hamiltonian [26,16] or an active arrangement of beamsplitters combined with further QND measurements. She keeps one photon and sends the other $(n-1)$ photons to Bob. When receiving the data regarding the basis, Eve measures her photon and obtains full information. Each signal containing more than one photon in this way will yield its complete information to an eavesdropper.

The situation becomes worse in the presence of loss, in which case the eavesdropper can replace the lossy channel by a perfect quantum channel and forward to Bob only chosen signals. This suppression is controlled such that Bob will find precisely the number of non empty signals as expected given the characterization

of the lossy channel. If there is a strong contribution by multi-photon signals, then Eve can use only those signals and suppress the single-photon signals completely, to obtain full information on the transmitted bits. For an error-free setup, this argument leads to the necessary condition for security,

$$p_{\text{exp}} > p_{\text{multi}} \ , \tag{6}$$

where now the signal contribution is given by

$$p_{\text{exp}}^{\text{signal}} = \sum_i p_i[1-(1-F)^i] \ . \tag{7}$$

If this condition is violated, Eve gets full information without inducing any errors nor causing a change in the expected detection rate. For given probabilities p_i and transmission rate F, a bound on the distance is obtained, even for perfect detection. The limitation on practical QKD as shown in (6) was reported independently in [10,18] after having been anticipated in [15].

Whereas this work concentrates mainly on insecurity results, we make here also an important observation, which is useful for positive security proofs. For a general source (emitting into the four BB84 polarization modes) analysing all possible attacks in a large Hilbert space (the Fock space) is a very difficult task. However, if Alice can dephase the states to create a mixture of "number states" (in the chosen BB84 polarization state) the transmitted signals are replaced by mixed states. Then, these states do not change at all when Eve performs a QND measurement on the total photon number as part of a PNS attack! Therefore Eve can be assumed to perform the QND part of the PNS attack without loss of generality. In that case, it is much easier to check that the PNS attack is actually optimal since we start with an eavesdropper who knows the total photon number of each signal. Fortunately, in realistic scenarios the dephasing happens automatically since the eavesdropper has no reference phase to the signal. Therefore, the signal states appear to be phase-averaged ("dephased") signals from her perspective. In some experiments, a phase reference exists initially [25], but could be destroyed by Alice adding random optical phase shifts to her weak signals. Following this observation, a complete positive security proof against all individual particle attacks has been subsequently given [19,20]. More sophisticated collective and joint attacks can also potentially be restricted to the PNS attacks.

4 Putting It All Together

Let us return to the necessary condition for security. We can combine the idea of the two criteria (4, 6) above to a single, stronger one, given by

$$e < \tfrac{1}{4}\,(p_{\text{exp}} - p_{\text{multi}}) \ . \tag{8}$$

This criterion stems from the scenario that Eve splits all multi-photon signals while she eavesdrops on some of the single-photon signals—precisely on a proportion $(p_{\text{exp}} - p_{\text{multi}})/p_1$ of them—via the intercept/resend attack presented

before, and suppresses all other single photon signals. We can think of the key as consisting of two parts: an error-free part stemming from multi-photon signals, and a part with errors coming from single-photon signals. The error rate in the second part has therefore to obey the same inequality as used in criterion (4).

We now explore the consequences of the necessary condition for security for two practical signal sources. These are the weak coherent pulses and the signals generated by parametric downconversion.

5 Weak Coherent Pulse Implementations

In QKD experiments, the signal states are, typically, weak coherent pulses (WCP) containing, on average, much less than one photon. The information is contained in polarization mode of the WCP.

Coherent states

$$|\alpha\rangle = e^{-\alpha^2/2} \sum_n \alpha^n/\sqrt{n!}\,|n\rangle \tag{9}$$

with amplitude α (chosen to be real) give a photon number distribution (per pulse [9])

$$p_n = e^{-\alpha^2} \left(\alpha^2\right)^n /n! \ . \tag{10}$$

Since we analyse PNS attacks only, it doesn't matter if the realistic "coherent state" is a mixture of number states. Thus,

$$p_{\text{exp}}^{\text{signal}} = \sum_{n=1}^{\infty} e^{-F\eta_{\text{B}}\alpha^2} \left(F\eta_{\text{B}}\alpha^2\right)^n /n! \tag{11}$$

and

$$p_{\text{multi}} = \sum_{n=2}^{\infty} e^{-\alpha^2} \left(\alpha^2\right)^n /n! \ . \tag{12}$$

With $p_{\text{exp}} \leq p_{\text{exp}}^{\text{signal}} + 2d_{\text{B}}$ and the error rate $e \succeq d_{\text{B}}$ in (8) we find for $\alpha^2 \ll 1$ (by expanding to 4th order in α and neglecting the term proportional to $F^2\eta_{\text{B}}^2\alpha^4$) the result

$$F \succeq \frac{2d_{\text{B}}}{\eta_{\text{B}}\ \alpha^2} + \frac{\alpha^2}{2\ \eta_{\text{B}}} \ . \tag{13}$$

The optimal choice $\alpha^2 = 2\sqrt{d_{\text{B}}}$ leads to the bound

$$F > F_{\text{WCP}} \approx 2\sqrt{d_{\text{B}}}/\eta_{\text{B}} \ . \tag{14}$$

To illustrate this example we insert numbers $\eta_{\text{B}} = 0.11$ and $d_{\text{B}} = 5 \times 10^{-6}$ taken from the experiment performed at $1.3\mu m$ by Marand and Townsend [21]. Then

the criterion gives $F \succeq 0.041$. With a constant loss of 5 dB and a fibre loss at 0.38 dB/km, this is equivalent, according to (1), to a maximum distance of 24 km at an average (much lower than standard) photon number of 4.5×10^{-3}. As we used approximations to reach (14), the achievable distance could differ slightly from this value either way.

With $\alpha^2 = 0.1$, as in the literature, secure transmission to any distance is impossible, according to our conditions. In that case, even if we assume η_{B} to be out of control of the eavesdropper, we find that secure transmission to a distance of more than 21 km is impossible. Frequently we find even higher average photon numbers in the literature, although Townsend has demonstrated the feasibility of QKD with intensities as low as $\alpha^2 = 3 \times 10^{-5}$ at a wavelength of $0.8\mu m$ [30].

6 Parametric Downconversion Implementations

The WCP scheme seems to be prone to difficulties due to the high probability of signals carrying no photons (the vacuum contribution). This can be overcome in part by the use of a parametric downconversion (PDC) scheme, which serves to approximate single-photon states. Parametric downconversion has been used before for QKD [12,28]. We use a different formulation, which enables us to analyse the advantages and limits of the PDC method relative to the WCP approach.

To a good approximation, PDC produces pairs of photons. Although each pair creation occurs at a random time, the two photons in the pair are created simultaneously, and they are correlated in energy, direction of propagation and polarization. Thus, detection of one photon provides information about the existence and properties of the partner photon without any destructive probing of the partner photon itself [14]. More technically, we create the state in an output mode described by photon creation operator $a^\dagger$ conditioned on the detection of a photon in another mode described by $b^\dagger$. If we neglect dispersion, then the output of the PDC process is described [31] on the two modes with creation operators $a^\dagger$ and $b^\dagger$ using the operator

$$T_{a\,b}(\chi) = e^{\mathrm{i}\chi(a^\dagger b^\dagger - ab)} \ , \tag{15}$$

with $\chi \ll 1$, as

$$\begin{aligned} |\Psi_{a\,b}\rangle &= T_{a\,b}(\chi)|0,0\rangle \\ &\approx \left(1 - \tfrac{1}{2}\,\chi^2 + \tfrac{5}{24}\,\chi^4\right)|0,0\rangle + \left(\chi - \tfrac{5}{6}\,\chi^3\right)|1,1\rangle \\ &\quad + \left(\chi^2 - \tfrac{7}{6}\,\chi^4\right)|2,2\rangle + \chi^3|3,3\rangle + \chi^4|4,4\rangle \ . \end{aligned} \tag{16}$$

This state is a superposition of two–mode number states where $|m,m\rangle$ corresponds to a *flux* of m photons in each mode. Whereas the earlier discussion on the WCP concerns distinct pulses, and the number state corresponds to a specific number of photons in the pulse (i.e. localized in time), the continuous output of the PDC is better represented in terms of photon flux states [9]. On the other

hand, we can interpret these number states for PDC as localized number states, to compare with the WCP case, by assuming the presence of choppers in each of the modes. A chopper periodically blocks the mode, thus converting a continuous output into a periodic sequence of pulses. By placing synchronized choppers in each mode, the continuous output becomes a sequence of pulses and the photon flux state can be regarded as a photon number state (per pulse).

If we had an ideal detector resolving photon numbers (that is, a perfect counter) then we could create a perfect single-photon state by using the state in mode a conditioned on the detection of precisely one photon in the pulse in mode b. However, realistic detectors useful for this task have a single-photon detection efficiency far from unity and can resolve the photon number only at high cost, if at all. Therefore, we assume a detection model which is described by a finite detection efficiency η_{A} and gives only two possible outcomes: either it is not triggered or it is triggered, thereby showing that at least one photon was present. The detector may experience a dark count rate at d_{A} per time slot. The two POVM elements describing this kind of detector can be approximated for our purpose by

$$E_0 = (1 - d_{\mathrm{A}})|0\rangle\langle 0| + \sum_{n=1}^{\infty}(1 - \eta_{\mathrm{A}})^n |n\rangle\langle n| \tag{17}$$

and

$$E_{\mathrm{click}} = d_{\mathrm{A}}|0\rangle\langle 0| + \sum_{n=1}^{\infty}(1 - (1 - \eta_{\mathrm{A}})^n)|n\rangle\langle n| \ . \tag{18}$$

The reduced density matrix for the output signal in mode b conditioned on a click of the detector monitoring mode a is then given by

$$\begin{aligned}\rho &= \frac{1}{N}\mathrm{Tr}_b\left[|\Psi_{a\,b}\rangle\langle\Psi_{a\,b}|E_{\mathrm{click}}\right] \\ &\approx \frac{1}{N}\Big[d_{\mathrm{A}}\Big(1 - \chi^2 + \tfrac{2}{3}\,\chi^4\Big)|0\rangle\langle 0| \\ &\quad + \eta_{\mathrm{A}}\chi^2\Big(1 - \tfrac{5}{3}\,\chi^2\Big)|1\rangle\langle 1| + \eta_{\mathrm{A}}(2 - \eta_{\mathrm{A}})\chi^4|2\rangle\langle 2|\Big]\end{aligned} \tag{19}$$

with the normalization constant N. To create the four signal states we rotate the polarization of the signal, for example using a beam-splitter and a phase shifter. Note that a mixture of Fock states is created by the detection process, so that the PNS attack is optimal for Eve.

After some calculation following the corresponding calculation in the WCP case, the necessary condition for security (8) takes for the signal state (19) the form

$$F \geq \frac{2d_{\mathrm{A}}\ d_{\mathrm{B}}}{\eta_{\mathrm{A}}\ \eta_{\mathrm{B}}\ \chi^2} + \frac{2d_{\mathrm{B}}}{\eta_{\mathrm{B}}} + \frac{2 - \eta_{\mathrm{A}}}{\eta_{\mathrm{B}}}\chi^2 \tag{20}$$

since we assume $d_{\mathrm{B}} \ll 1$ and $\chi^2 \ll 1$ and neglect terms going as χ^4, $d_{\mathrm{B}}d_{\mathrm{A}}$, and $\chi^2 d_{\mathrm{B}}$. The first error term is due to coincidence of dark counts, the second error

term is due to coincidence of a photon loss and a dark count at Bob's site; the third term is the effect of multi photon signal (signals that leak full information to the eavesdropper). As in the WCP case, the optimal choice of

$$\chi^2 = \sqrt{\frac{2d_{\rm A}d_{\rm B}}{\eta_{\rm A}(2-\eta_{\rm A})}} \tag{21}$$

leads to the necessary condition for security

$$F > F_{\rm PDC} \approx 2\sqrt{\frac{2d_{\rm A}\ d_{\rm B}\ (2-\eta_{\rm A})}{\eta_{\rm A}\ \eta_{\rm B}^2}} + \frac{2d_{\rm B}}{\eta_{\rm B}}\ . \tag{22}$$

If we now assume that Alice and Bob use the same detectors as in the WCP case with the numbers provided by [21], we obtain $F_{\rm PDC} \succeq 8.4 \times 10^{-4}$ corresponding via (1) to a distance of 68 km.

Since we can use downconversion setups which give photon pairs with different wavelength, we can use sources so that one photon has the right wavelength for transmission over long distances, e.g. 1.3 μm, while the other photon has a frequency which makes it easier to use efficient detectors [12]. In the limit of Alice using perfect detectors (but not perfect counters), $\eta_{\rm A} = 1$ and $d_{\rm A} = 0$, we obtain

$$F_{\rm PDC} \approx 2d_{\rm B}/\eta_{\rm B}\ , \tag{23}$$

as for single-photon sources, yielding a maximal distance of 93 km. This optimal distance might also be achievable using new single-photon sources of the type suggested in [17].

7 Conclusions

We have shown a necessary condition for secure QKD which uses current experimental implementations. We find that secure QKD might be achieved with the present experiments using WCP if one would use appropriate parameters for the expected photon number, which are considerably lower than those used today. With current parameters, it seems that all current WCP experiments cannot be proven secure. The distance that can be covered by QKD is mainly limited by the fibre loss, but, with $\alpha^2 > 0.1$, WCP schemes might be totally insecure even to zero distance (in several of the existing experiments), due to imperfect detection. The distance can be increased by the use of parametric downconversion as a signal source, but even in this case the fundamental limitation of the range persists, and a radical reduction of β or of the dark counts is required in order to increase the distance to thousands of kilometers.

The proposed "4+2" scheme [15], in which a strong reference pulse (as in [1]) from Alice is used in a modified detection process by Bob, might not suffer from the sensitivities discussed here, but the security analysis would have to follow

different lines. The use of quantum repeaters [24] (based on quantum error-correction or entanglement purification) or of a string of teleportation stations in the far future can yield secure transmission to any distance, and the security is not altered even if the repeaters or stations are controlled by Eve.

Acknowledgements

We thank C. H. Bennett, N. Gisin, J. H. Kimble, E. Polzik and H. Yuen, for important comments. We are also grateful to one anonymous referee for her generously detailed report.

References

1. C. H. Bennett, "Quantum cryptography using any two nonorthogonal states", *Physical Review Letters*, Vol. 68, no. 21, 25 May 1992, pp. 3121 – 3124.
2. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin, "Experimental quantum cryptography", *Journal of Cryptology*, Vol. 5, no. 1, 1992, pp. 3 – 28.
3. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1994, pp. 175 – 179.
4. C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", *IEEE Transactions on Information Theory*, Vol. IT–41, no. 6, November 1995, pp. 1915 – 1923.
5. C. H. Bennett, G. Brassard and A. K. Ekert, "Quantum cryptography", *Scientific American*, Vol. 267, no. 4, October 1992, pp. 50 – 57.
6. E. Biham, M. Boyer, P. O. Boykin, T. Mor and V. Roychowdhury, "A proof of security of quantum key distribution", in *Proceedings of 32nd ACM Symposium on Theory of Computing*, May 2000, to appear.
7. E. Biham, M. Boyer, G. Brassard, J. van-de-Graaf and T. Mor, "Security of quantum key distribution against all collective attacks", Los Alamos archives `quant-ph/9801022`, January 1998.
8. E. Biham and T. Mor, "Bounds on information and the security of quantum cryptography", *Physical Review Letters*, Vol. 79, no. 20, 17 November 1997, pp. 4034 – 4037.
9. K. J. Blow, R. Loudon, S. J. D. Phoenix and T. J. Sheperd, "Continuum fields in quantum optics", *Physical Review A*, Vol. 42, no. 7, October 1990, pp. 4102 – 4114.
10. G. Brassard, T. Mor and B. C. Sanders, "Quantum cryptography via parametric downconversion", in *Quantum Communication, Computing, and Measurement 2*, P. Kumar, G. Mauro D'Ariano and O. Hirota (editors), Kluwer Academic/Plenum Publishers, New York, 2000, pp. 381 – 386.
11. W. T. Buttler, R. J. Hughes, P. G. Kwiat, G. G. Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson and C. M. Simmons, "Free-space quantum-key distribution", *Physical Review A*, Vol. 57, no. 4, April 1998, pp. 2379 – 2382.
12. A. K. Ekert, J. G. Rarity, P. R. Tapster and G. M. Palma, "Practical quantum cryptography based on two-photon interferometry", *Physical Review Letters*, Vol. 69, no. 9, 31 August 1992, pp. 1293 – 1295.
13. J. D. Franson and H. Ilves, "Quantum cryptography using polarization feedback", *Journal of Modern Optics*, Vol. 41, no. 12, December 1994, pp. 2391 – 2396.

14. P. Hariharan and B. C. Sanders, "Quantum phenomena in optical interferometry", *Progress in Optics*, Vol. XXXVI, 1996, pp. 49 – 128.
15. B. Huttner, N. Imoto, N. Gisin and T. Mor, "Quantum cryptography with coherent states", *Physical Review A*, Vol. 51, no. 3, March 1995, pp. 1863 – 1869.
16. E. T. Jaynes and F. W. Cummings, "Comparison of quantum and semiclassical radiation theories with application to the beam maser", *Proceedings of the IEEE*, Vol. 51, 1963, pp. 89 – 109.
17. J. Kim, O. Benson, H. Kan and Y. Yamamoto, "A single-photon turnstile device", *Nature*, Vol. 397, no. 6719, 1999, pp. 500 – 503.
18. N. Lütkenhaus, "Dim coherent states as signal states in the BB84 protocol: Is it secure?", in *Quantum Communication, Computing, and Measurement 2*, P. Kumar, G. Mauro D'Ariano and O. Hirota (editors), Kluwer Academic/Plenum Publishers, New York, 2000, pp. 387 – 392.
19. N. Lütkenhaus, "Security of quantum cryptography with realistic sources", *Acta Physica Slovaca*, Vol. 49, 1999, pp. 549 – 556.
20. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution", Los Alamos archives `quant-ph/9910093`, October 1999.
21. C. Marand and P. D. Townsend, "Quantum key distribution over distances as long as 30 km", *Optics Letters*, Vol. 20, 15 August 1995, pp. 1695 – 1697.
22. D. Mayers, "Quantum key distribution and string oblivious transfer in noisy channels", in *Advances in Cryptology: Proceedings of Crypto'96*, Lecture Notes in Computer Science, Vol. 1109, Springer-Verlag, August 1996, pp. 343 – 357.
23. D. Mayers, "Unconditional security in quantum cryptography", Los Alamos archives `quant-ph/9802025`, February 1998.
24. T. Mor, "Quantum memory in quantum cryptography", Ph.D. Thesis, Technion, Haifa, 1997; Los Alamos archives `quant-ph/9906073`.
25. A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden and N. Gisin, "Plug and Play systems for quantum cryptography", *Applied Physics Letters*, Vol. 70, 1997, pp. 793 – 795.
26. K. Mølmer, private communication.
27. R. L. Rivest, A. Shamir and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM*, Vol. 21, no. 2, 1978, pp. 120 – 126.
28. A. V. Sergienko, M. Atatüre, Z. Walton, G. Jaeger, B. E. A. Saleh and M. C. Teich, "Quantum cryptography using femtosecond-pulsed parametric down-conversion", *Physical Review A*, Vol. 60, no. 4, October 1999, pp. R2622 – R2625.
29. P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", *SIAM Journal on Computing*, Vol. 26, no. 5, 1997, pp. 1484 – 1509.
30. P. D. Townsend, "Experimental investigation of the performance limits for first telecommunications-window quantum cryptography systems", *IEEE Photonics Technology Letters*, Vol. 10, 1998, pp. 1048 – 1050.
31. D. F. Walls and G. J. Milburn, *Quantum Optics*, Springer-Verlag, Heidelberg, 1994.
32. H. P. Yuen, "Quantum amplifiers, quantum duplicators and quantum cryptography", *Quantum and Semiclassical Optics*, Vol. 8, 1996, pp. 939 – 949.