Enhancements to Prepare-and-Measure Based QKD Protocols

Peter Y.A. Ryan[1] and Bruce Christianson[2]

[1] University of Luxembourg
peter.ryan@uni.lu
[2] University of Hertfordshire
b.christianson@herts.ac.uk

Abstract. We propose some simple changes to a class of Quantum Key Distribution protocols. The first enhancement ensures early detection of any attempted Man-in-the-Middle attack and results in less leakage of key material to any eavesdropping attacker. We argue that this version is at least as secure as the original BB'84 scheme, but ensures a closer binding of the key establishment and authentication components of the protocol. Further proposed enhancements lead to a doubling of the key rate, but the security arguments become more delicate.

We also touch on the need to enhance the models used to analyze both the classical and quantum aspects of QKD protocols. This is prompted by the observation that existing analyses treat the quantum (key-establishment) and classical (authentication etc) phases separately and then combine them in a simple-minded fashion.

1 Introduction

The purpose of this paper is twofold: to present enhancements to existing prepare-and-measure Quantum Key Distribution (QKD) protocols, and to argue that we need to enrich our models for the analysis of QKD protocols, in particular to deal with this enhancement, but also for QKD protocols in general.

QKD exploits features of quantum mechanics, in particular Heisenberg's Uncertainly Principle and the No-Cloning Theorem, to ensure that any attempt by an eavesdropper to monitor the quantum channel will, with high probability be detected. Typically, QKD strives to provide unconditional secrecy, i.e. secrecy against an adversary with unbounded computational power. This contrasts with most classical crypto, where the security properties are typically based on hard computational problems and therefore assume an adversary with bounded computational power.

In this paper we focus on enhancing the BB'84 protocol due to Bennett and Brassard, [BB84]. The first enhancement proposed here is very simple but appears to be rather effective. After a quantum phase, protocols such as BB'84 involve a first classical step of agreeing for which photons the receiver used the "correct" measurement basis, followed by a step in which Anne and Bob agree a subset on which they

B. Christianson et al. (Eds.): Security Protocols 2013, LNCS 8263, pp. 123–133, 2013.

will compare their bits to detect any eavesdropping/noise on the quantum channel. In existing schemes, the agreement on the correct set and the eavesdropping detection subset is done by open negotiation, and so is known also to an attacker, indeed could potentially be manipulated by the attacker. Some form of end-to-end authentication and integrity property is required for the channel over which this negotiation takes place, and in practice this is provided by cryptographic means that require Anne and Bob to pre-share a secret authentication key. In our enhancement, Anne and Bob compute the subset for comparison separately and secretly, as a function of entropy derived from the previously established, secret authentication string. This results in less leakage of information to any eavesdropper and provides early, implicit authentication of the protocol.

The second enhancement is rather more audacious: we propose that the preparation/measurement bases, rather than being chosen purely randomly, are determined as pseudo-random functions of the prior, shared secret. Thus Anne and Bob are able to independently compute the basis sequence. Thus Bob can use the correct basis to measure all the photons emitted by Anne, rather than just guessing as for the conventional BB'84. This results in a doubling of the resulting bit rate, but now the security arguments become more delicate. A crucial observation that emerges from the analysis is that any measurements performed on a single photon by an eavesdropper, Yves, leak no information about the preparation basis. Consequently Yves cannot determine the seed of the pseudorandom function even with unlimited computational resources, as he cannot gain any information about the output from it. This, rather surprising observation is key to showing that this enhancement does not sacrifice security.

The third, even more radical, enhancement involves checking all the bits, not just a subset, without revealing anything about them. In certain circumstances, this makes the protocol more efficient.

We discuss the need for suitable models for the analysis of such protocols. Existing analyses typically use a physics (quantum mechanics based) model to argue that any eavesdropping on the quantum channel will be detectable during the classical phase, and any information leakage can be strictly bounded. The proofs are essentially reduction proofs: violation of these properties would imply the existence of a way to violate principles of quantum mechanics: Heisenberg Uncertainty and the no-cloning theorem for example. It is usually then argued that Man-In-The-Middle attacks can be thwarted by using unconditional authentication mechanisms on appropriate steps of the classical exchanges. Authentication is typically achieved using MACs based on universal hash functions such as the Carter-Wegman class. Most descriptions of QKD protocols in the literature are rather vague or inconsistent as to which of the classical exchanges should be authenticated.

Such a proof strategy is worrying: it treats the key-establishment and authentication phases separately and then composes them in a rather simple-minded fashion. We know from decades of experience analyzing classical protocols and primitives that great care needs to be taken in composing modules and arguments. We also know that it is essential that the key-establishment and authentication be inextricably bound together.

2 Background

BB'84, or variants of it, constitute the form of QKD that are most advanced in terms of implementation and commercialization. Similar constructs to those presented here apply to other QKD protocols, e.g. entanglement based protocols such as Ekert'91, [Eke91], but we'll stick to BB'84 based protocols for the purposes of this paper.

First we briefly outline the steps of conventional (prepare and measure) QKD protocols. We describe the idealized flow of the protocol, assuming a sufficiently low level of noise on the quantum channel and ignoring complications such as maintaining synchronization of the photon indices, multiple photon pulses etc. We then describe the changes to the eavesdropping detection and key sifting steps that constitute the enhancements proposed here.

As is standard, we assume that Anne and Bob share a secret bit string s prior to starting the protocol, and that this will be used to authenticate the key establishment. Note that, in order to achieve unconditional guarantees, none of the initial string should ever be re-used. If we use a stretch of the s string, say to authenticate a message using a MAC style mechanism, then this stretch of s must be discarded after use.

We assume that Anne possesses a device capable of emitting individual photons circularly polarized in one of four states: ($\uparrow$) 0° ($\nearrow$) 45° ($\rightarrow$) 90° ($\searrow$) 135°. Bob possesses a polarization measurement device that can be set to measure either in the horizontal ($\oplus$) or diagonal ($\otimes$) basis. We take the convention that in the $\oplus$ basis, a 0° photon encodes a 1 and a 90° photon encodes a 0, and in the $\otimes$ basis, 45° encodes a 1 and 135° a 0.

We will not go into the details of the "operational semantics" arising from the quantum mechanics, except to remark that when the circular polarization of a photon is measured with the "correct" basis the state will collapse to the correct eigenstate with 100% probability. If the "wrong" basis is used, the wave function will collapse into either of the eigenstates with 50% probability. Thus, for example, if a $\uparrow$ photon is measured in the $\oplus$ basis it will collapse to the $\uparrow$ state. If a $\nearrow$ photon is measured in the $\oplus$ basis it will collapse to a $\uparrow$ state with 50% probability and a $\rightarrow$ state with 50% probability, and similarly for the other combinations. More generally, if the angle between the photon state and an eigenstate is θ, then the probability that it will collapse to this eigenstate is given by $cos^2(\theta)$.

2.1 Phase 1 : The Quantum Channel

Anne emits a stream of photons over a suitable channel, e.g. optical fiber or free space. Each photon will be polarized in one of the four possible polarizations chosen randomly and independently. The source of this randomness is pure as opposed to pseudo-random. Anne keeps a record of the chosen polarization of each emitted photon. We will assume that mechanisms are in place to allow Anne and Bob to label each photon with a unique and consistent index, e.g. numbered consecutively. We'll refer to this indexing set as ϕ. Typically Anne emits a large number of photons, perhaps tens of thousands. Bob, at the other end of the quantum channel, measures each incoming photon in one of the two bases, chosen independently at random (again, really random). Bob keeps a record of the bases he used for each measurement and the outcome of the measurement (as a bit).

We now move to the classical phases of the protocol in which Anne and Bob exchange classical information over conventional, classical channels. These channels are not assumed to be secret, but are where necessary provided with integrity and endpoint authentication using information-theoretically secure MACs based on the prior shared secret string s.

2.2 Phase 2 : Key Sifting

Once the transmission and measurement of the photons is finished, Anne and Bob need to agree for which photons Bob used the "correct" measurement basis (the $\oplus$ basis in the case of $0°$ and $90°$ polarization, and the $\otimes$ in the case of $45°$ and $135°$ polarization). For these photons, in the absence of noise or eavesdropping on the quantum channel, the bit corresponding to the outcome of Bob's measurement should match Anne's bit. Where Bob used the "wrong" basis, the outcome of the measurement will be a random choice of 0 or 1. This agreement is established over open channels and so any attacker eavesdropping the classical channel will also learn this information.

To this end, for example, Bob reveals his choice of measurement basis for each photon (index). Anne responds by stating for which indices his choice was correct, but without revealing the polarization (i.e. the corresponding bit). At the end of this phase they have agreed the subset of the indices on which, aside from noise, they should have agreement between their bits. We'll refer to this set as ϕ_1. The complement set of ϕ_1 in ϕ is discarded.

2.3 Phase 3 : Detection of Eavesdropping

Now Anne and Bob need to agree a subset of ϕ_1 on which they will compare their bits to establish whether any eavesdropping occurred on the quantum channel. We will refer to this subset of ϕ_1 as ϕ_2. It is essential that ϕ_2 is chosen at random after the quantum phase is complete, but it is not, in the existing protocols, assumed that it is kept secret, rather it is established by open discussion and hence assumed known to the attacker.

Once they have agreed on ϕ_2, Anne and Bob compare bits for each index in ϕ_2. In the absence of eavesdropping and noise, they should agree on all these bits. In practice, due to noise on the quantum channel, there will be some level of disagreement, but as long as this is low enough to be compatible with the noisiness of the channel they conclude that there was either no eavesdropping or any possible eavesdropping is bounded to a sufficiently low level. If the level of disagreement exceeds an appropriate threshold, typically around 11%, they will conclude that a significant level of eavesdropping is likely and abort the protocol run. Note that they cannot distinguish between noise and eavesdropping. In line with the literature, we refer to this level of discrepancy as the Quantum Error Rate (QER).

2.4 Phase 4: Information Reconciliation

Assuming that they have not aborted after phase 3, Anne and Bob proceed to phase 4: where they start to construct the new session key. They now work with the complement of ϕ_2 in ϕ_1, which we will call ϕ_3. Thus ϕ_3 is the set of indices of photons for which Bob used the correct basis but for which they have revealed no information about the corresponding bits. For the bits indexed by ϕ_3, Anne and Bob should each have a string of bits which, aside from noise and eavesdropping, will match. The attacker should know at most a bounded amount about these bits. The problem is that there will inevitably be some disagreement between their bits strings due to the QER. They need to eliminate these mismatches while revealing as little as possible to an attacker eavesdropping on the classical channel about the actual bit strings. This is usually done using a "cascade" protocol [BS93]. This is quite standard and will be used unchanged in our first two enhancements, so we will not go into the details here. However our third enhancement will propose an alternative approach.

2.5 Phase 5: Secrecy Amplification

We assume that after completing phase 4 above, Anne and Bob share identical bit strings. An attacker should have at most a bounded amount of information about these strings, gleaned possibly from some "below the radar" level of eavesdropping on the quantum channel and by monitoring the classical channel, in particular from monitoring phase 4. Anne and Bob can use the QER they observed in phase 3 to bound the information that Yves might extract. This information now needs to be reduced to a negligible level by a process of "secrecy amplification". In essence the string is "distilled" down to a shorter string with purer entropy from the attacker's perspective. Again, the procedure here is perfectly standard and will be unchanged in our enhanced protocol so we omit details, [BBCM95].

2.6 Phase 6: Key Confirmation

Finally, to confirm that Anne and Bob indeed share the same distilled key and to authenticate the key, they can perform a final key confirmation step. They can for example each compute a keyed universal hash over the key, keyed using a fresh stretch of the initial shared string s, and exchange parts of the output. These values reveal no information about the session key to an eavesdropper, but if these values agree then Anne and Bob can be confident that they possess the same session key, and that the key has been shared with the correct counterparty.

They now have a confirmed secret key that can be used for secure communication in a One-Time-Pad (Vernam) encryption mode to provide unconditional secrecy, or in conjunction with a universal hash function to provide unconditional integrity. Alternatively, the key could be used for encryption under a suitable block cipher such as AES, but in this case the security properties are no longer unconditional.

Anne and Bob should set aside a suitable stretch of this freshly established key to use for authentication in the next run of the protocol.

Note that in existing descriptions of the protocol, these classical exchanges are over public channels and so the attacker knows the index sets ϕ_1, ϕ_2 and ϕ_3 and indeed the bits of the string indexed by ϕ_2. Descriptions vary as to which of these exchanges are authenticated and how, but these details are not relevant for our purpose here. The point for us is simply that at least some of the exchanges must be authenticated, and that in practice this requires a pre-established shared authentication secret.

3 The First Enhancement

The first proposed enhancement to the above style of protocol is very simple and modifies only phase 3: rather than have Anne and Bob agree the subset ϕ_2 in a public fashion, we provide a way for each of them to compute it in a secret fashion. Besides leaking less information, this approach also provides early, implicit authentication. For this they will use an agreed stretch of the shared initial shared secret string s, say the first 128 bits, call this s', to compute ϕ_2.

The details of this construction can be varied as necessary, but it should have the following properties:

- It must be a deterministic function of the secret string s'. Thus, given s', Anne and Bob should compute the same set of indices.
- It should be able to deal with an input of any given length (corresponding to the size of index set for which they establish that Bob used the correct measurement basis, i.e. the size of the ϕ_1 set).
- It should be able to accept a value p ($0 < p < 1$) as a parameter and extract a proportion p of the ϕ_1 indices.
- An attacker, who knows p but does not know s', should not have a strategy for guessing ϕ_2 that is significantly better than guessing at random with probability p, even if the attacker has been "lucky" in guessing a higher than average proportion of the bits of s'.

An example of a simple way to realize such a construction is for Anne and Bob to use the s' value as a key for AES in Counter mode to generate a pseudorandom string w. The reason for this is that block ciphers are designed to have the property that that streams produced by even slightly different keys will be uncorrelated. Note that we are not using difficulty of inversion: Yves has unlimited computational power but cannot, even indirectly, observe the cipher stream.

Suppose, for illustration, that Anne initially transmits 1024 photons to Bob. For approximately 512 of these they will establish that Bob used the correct measurement basis, i.e. the ϕ_1 set. Suppose that they want to select 25% of these to compare, i.e. approx 128 indices to form the ϕ_2 set on which they will compare bits to check their level of agreement. They each use s to produce a string w. They segment w into pairs of bits, and for each 00 pair they select the index in ϕ_1. The 01, 10, and 11 pairs are not selected. This will yield approximately 128 bits. Anne can now transmit the first 64 bits to Bob and Bob transmits the last 64 bits to Anne. They do not reveal publicly the positions to which these bit values correspond.

More generally, suppose Anne and Bob want to select approximately $1/m$ of the ϕ_1 bits on the set to form the ϕ_2 set, where m is an integer. The stream w can be segmented into pieces w_i of length at least $\log_2 m$, and interpreted as `select` for $w_i = 0$, `not select` for $0 < w_i < m$ and `ignore` for $w_i \geq m$.

The point of this construction is fourfold:

- An attacker, whom we assume does not know s (or hence s'), will not be able to compute ϕ_2, hence he does not know which photons Anne and Bob will use for their comparison.
- We have implicit authentication: an attacker cannot masquerade convincingly as either Anne or Bob. Even if he tries a MITM attack and say, measures all the photons emitted by Anne, he will not be able to provide Anne (or Bob) with a string of bits matching her (or his) bits without knowledge of ϕ_2.
- The process of key establishment and authentication are inextricably intertwined in the protocol.
- In contrast to the standard protocols, we leak only partial information about the bits in the ϕ_2 set. Consequently we have the possibility of using these in the final session key, as long as we use suitable privacy amplification. Thus the resulting bit rate will be higher than with previous QKD protocols. It is worth noting also that an attacker knows less about the bits of the ϕ_3 string: even if he has managed to surreptitiously measure some of the photons in this set, he will not know exactly where these sit in the final key string.

3.1 Discussion

As mentioned previously: the new approach leaks much less information to the attacker (about the ϕ_2 and hence the ϕ_3 set) and provides early implicit authentication. In fact, with our modification, we do not even have to explicitly authenticate the classical exchanges between Anne and Bob, hence we do not need to consume so much of the s string (for example via universal hash functions) in order to ensure integrity.

From the attacker's perspective, the protocol is unchanged aside from the fact that he does not now learn the ϕ_2 set. The security of this variant of BB'84 is thus reducible to that of the original BB'84.

The new approach also provides a counter to the Photon Number Splitting (PNS) attack [GBS00]: this can occur when photon pulses have more than one correlated photon and, in principle, the attacker could measure one (or more) of the photons in the pulse while leaving one untouched. This provides a way to eavesdrop on the quantum channel without triggering the detection mechanisms (the photon that Bob measures has not been interfered with by the attacker). Such attacks are worrying, as in practice it is very difficult to eliminate completely the occurrence of multiple photon pulses, and they break the abstractions on which previous correctness proof models were based. This has prompted proposed counter-measures, such as the SARG protocol [SARG04]. The SARG protocol is however significantly more complex that the one proposed here, in particular it involves Anne and Bob having to throw away 75% of the photons at the first step as opposed to 50% in the original BB'84. With the enhancement proposed here, even an adversary who succeeds in measuring some photons undetectably in this fashion cannot masquerade successfully during the eavesdropping/authentication step. Furthermore, even if he manages to extract some bits of the key stream in this fashion, Yves will not know exactly where they lie in the final key stream.

Another important point is that, from experience in the analysis of classical AKEs, we know that it is essential that the key establishment and authentication be explicitly bound together. The approach proposed here achieves this: the bits that they compare, and hence the bits retained to form the key ultimately, are derived from the pre-shared secret authentication string s, because the indices that are identified for the comparison step, the ϕ_2 set, are computed as a function of s.

In the event that bits from the ϕ_2 set are used in the final key, an issue to consider is the possibility of belated leakage of information about the s string. This is analogous to a "forward secrecy" property for a purely classical scheme. To avoid this threat Anne and Bob should ensure that the utilized parts of s are deleted as soon as they have served their purpose.

4 The Second Enhancement

Now we introduce the second innovation: rather than generating the basis sequence purely randomly, we propose that Anne and Bob also compute the basis sequence b_i as a pseudo-random function of the shared s string. Anne now generates a true random bit sequence z_i and prepares the ith photon according to the coding convention mentioned earlier. Bob, for his part, measures the i-th photon using the b_i basis. Thus, in the absence of noise or eavesdropping, Bob should recover the z_i sequence exactly as generated by Anne. They now perform a comparison of a randomly selected set of elements of the z sequence as before. They could of course combine this second enhancement with the first enhancement, and secretly compute the comparison subset pseudorandomly.

4.1 Discussion

An important, and rather surprising, observation that emerges from the analysis is that, in the absence of an PNS attack, any measurement that the attacker may perform on the photons during the quantum phase leaks no information about the basis sequence. A simple calculation using the "operation semantics" of the measurement operator shows that Yves will get a 0 with probability $\frac{1}{2}$ and a 1 with probability $\frac{1}{2}$, regardless of which generation basis was used by Anne, and which measurement basis Yves uses, including oblique ones. This calculation is based on the assumption that the z sequence and the basis choice have the same statistics as pure random.

The significance of this observation is that it thwarts the obvious strategy that Yves might attempt: measure lots of photons early in the quantum phase and try to improve his guesses at the bases further downstream. We also need to ensure that Yves cannot benefit from a better-than-average guess at the string s. As argued before, the use of a good block cipher such as AES in counter mode to provide the PRNG should ensure an adequate lack of correlation.

Suppose that we use a 128 bit string as the seed to generate the basis sequence. The property we require of the PRNG is that if the attacker gets even one bit wrong in his guess at the seed, then the `xor` of the resulting guessed sequence and the real basis sequence will be essentially random. Using a good block cypher such as AES in counter mode has exactly this property, by construction. Hence, unless the attacker gets really lucky and guesses the 128 bits exactly right, he faces the same challenge as the conventional protocol with a strictly random basis sequence. This, along with the observation that (in the absence of PNS style attacks) no observation he can make on the quantum channel can extract any information about the basis sequence, implies that the security of the enhanced scheme is essentially the same as that of BB'84.

The above argument is based on the assumption that the attacker has at most negligible information about the authentication string. This assumption is standard for BB'84 and QKD protocols in general. We need to take additional care though with such an assumption for our second enhancement: having non-zero information about the authentication key for one run may help the attacker launch a more effective attack in a subsequent run. In conventional BB'84, as the basis sequences are pure random, this is not an issue. In our case, there is the possibility that a lucky guess in one run might be amplified in subsequent runs. However, as long as the PRNG has the properties stated above, a better than average guess at the authentication string will not yield any advantage over a simple bitwise guessing at the basis sequence, and hence confers no advantage for a subsequent run of the protocol.

However the second enhancement is vulnerable to PNS attacks: for example, if Yves measures two photons (out of three) in the same basis and they are different, then he knows that the basis choice is wrong. With his infinite computational power, he can then eliminate approximately half of the potential values for s' for each such measurement.

On the other hand, vulnerability to PNS is an unsatisfactory feature of most QKD protocols - for example SARG itself is insecure if Yves can block all pulses with fewer than three photons (and half of the three-photon pulses) [SARG04].

One possible response is to stipulate that if Yves is to be equipped with a reliable photon counter then it is only fair for Anne to have one too. In this case Anne can eliminate PNS attacks simply by deleting pulses with more than one photon, and under this assumption protocols incorporating the second enhancement are invulnerable.

Of course, informal arguments such as the ones given above need to be made formal in the context of an appropriate model that encompasses both the quantum and classical aspects.

5 The Third Enhancement

The most radical of our proposals involves Anne and Bob effectively testing all of the bits in ϕ_1, and not merely a subset. To do this we use a trick from the Vintage Bit protocol of Christianson and Shafarenko [CS09]. The protocol sequence proceeds as usual (Section 2) until the end of Phase 2. At this point Anne has a bitstream z corresponding to the elements of ϕ_1 and Bob has a bitstream z' which is the same as z apart from the QER (including any eavesdropping.) Instead of Phases 3 and 4, Anne and Bob proceed as follows:

Anne and Bob have set aside a segment p of a previously agreed key stream. This is now used as One-Time Pad to conceal a Forward Error Correcting Code F and a collision-resistant hash h of the key stream z currently being agreed. Specifically:

$$A \to B : [F(z) \mid h(z)] \texttt{ xor } p$$

Bob now recovers $F(z)$, applies this to z', and checks that the result hashes to $h(z)$. If not, then Bob aborts the protocol, otherwise Anne and Bob proceed with Phase 5 as usual.

5.1 Discussion

Note that the property of the hash h being relied upon here is not non-invertibility (since Yves can never learn any bits of the hash value) but a particular form of collision resistance: Yves cannot manipulate the values for z or $h(z)$ plausibly without knowing p. Note also that no authentication or integrity is required for the open channel communication between Anne and Bob used to transmit the encoded $F(z)$ in this enhancement. Privacy amplification can be done deterministically by Anne and Bob, with no further communication. Of course, the hash could be replaced by the conventional use of an information-theoretically secure MAC at the end of the protocol; but equally, Step 6 could be replaced by an authenticated confirmation to Alice by Bob that the corrected value of z' has the correct hash[1].

[1] For example, $B \to A : p'$ where p' is another segment of a previously agreed key stream.

The requirement to use key bits from a previous run for p appears to be an additional burden, but this step replaces Phases 3 and 4 of the conventional protocol. Although the number of bits required for $F(z)$, and hence for p, is of the order of twice the maximum allowable QER for z, under the third enhancement no bits are lost from z by the need to reveal bits to detect eavesdropping, or to apply a cascade protocol.

The approach with the third enhancement has the advantage that any suitably aggressive FEC protocol can be used off the shelf, without concern for security issues, and Bob can count exactly how many of the bits in z needed to be corrected.

The third enhancement can be combined with the second enhancement, with similar caveats about PNS.

6 Conclusions

We have proposed some simple but effective enhancements to the BB'84 based QKD protocols. These enhancements explicitly ensure a closer binding between key-establishment and authentication than for previous protocols. They ensure very early detection of any MITM or masquerade attacks as well as the possibility of higher bit rates and an effective counter to PNS style attacks.

We have also argued that we need more powerful models, that encompass both the quantum and classical aspects of QKD protocols, in order to deal with richer threat models.

References

[BB84] Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, India, p. 175 (1984)

[BBCM95] Bennett, C.H., Brassard, G., Crepeau, C., Maurer, U.M.: Generalized privacy amplification. IEEE Trans. Inf. Theor. 41(6), 1915–1923 (1995)

[BS93] Brassard, G., Salvail, L.: Secret key reconciliation by public discussion. In: Helleseth, T. (ed.) EUROCRYPT 1993. LNCS, vol. 765, pp. 410–423. Springer, Heidelberg (1994)

[CS09] Christianson, B., Shafarenko, A.: Vintage bit cryptography. In: Christianson, B., Crispo, B., Malcolm, J.A., Roe, M. (eds.) Security Protocols. LNCS, vol. 5087, pp. 261–265. Springer, Heidelberg (2009)

[Eke91] Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. 67, 661–663 (1991)

[GBS00] Mor, T., Brassard, G., Lütkenhaus, N., Sanders, B.C.: Limitations on practical quantum cryptography. Physical Review Letters (2000)

[SARG04] Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. 92, 057901 (2004)