The Open University

A Critical evaluation of Quantum Key Distribution, focusing on SARG04 as a benchmark

William Ockmore

September 6, 2016

Contents

1 Introduction

Quantum key distribution is the study of quantum mechanics as a mechanism to share an unconditionally secure key between two parties. Since the first protocol (BB84 or the four-state protocol) was proposed in the mid 1980s (Bennett and Brassard, 1984), the field has slowly grown; it now encompasses many different protocols, using a variety of quantum processes to enable ever more secure sharing of information. Still amongst the most widely used, BB84 is one of the most straightforward; using two sets of two non-orthogonal basis states, the key is encrypted in the state sent, and when the classical bit-sifting phase takes place Alice (the sender) communicates to Bob (the receiver) the basis used for a selection of the states sent. If the error is within the acceptable bounds, they can be sure that their key is secure, and communicate the basis used for the rest of the states. In this way, the unconditional security is achieved.

One major problem with BB84 is its reliance on a single photon source for true unconditional security. Consider the ideal for Eve (eavesdropper); no restrictions are made on her technology or capability other than the laws of physics. It is then clear that if the source used to send the key sends two or more quantum states per bit, Eve can execute a Photon Number Splitting (PNS) attack; for every pulse of two or more photons, she stores one state and lets the other state(s) continue on to Bob. Once Alice reads out the bases she used, Eve will therefore have the complete key without the knowledge of the other participants; the security is lost. This can be generalised to all prepare and measure protocols.

The area of study for this report focuses on the use of a recent protocol, SARG04, as a means to improve the robustness against PNS attacks as compared to the standard prepare and measure protocols. It compares its efficacy to BB84 and others, and discusses the impact of decoy states and other practical methods to increase security.

The objectives for the report are as follows: to give a brief history of QKD and its possible impact on current society; to discuss the limitations of historical protocols in the real world; to give a detailed analysis of the SARG04 protocol and its benefits over previous protocols; and finally to give a brief outline of real world improvements and limitations, either through practical engineering or new techniques.

The search methodology used in this report involved first doing a broad search of academic articles, using google scholar and similar tools, and then narrowing the scope through progressively more specific boolean search terms; then using papers already found to aid understanding of the research area, and to provide other papers to study in the form of references.

2 The BB84 and B92 prepare and measure protocols

In this chapter, we give a description of two QKD protocols; BB84 and B92. They both belong to the family of *prepare and measure* protocols, and as such rely on sending individual quantum states (qubits), rather than coding via entangled pairs or other means.

2.1 BB84

The BB84 protocol was the first proposed QKD protocol, introduced at an IEEE conference in India by Bennett and Brassard (1984), to little fanfare at the time (Brassard, 2005); it would grow to become the most well known and widely tested example of a QKD protocol. Today, it serves as the benchmark against which all others are measured.

The protocol

In BB84, Alice uses a single photon source to transmit a set of states to Bob, encoded in the polarization of the photons. Both Alice and Bob agree to align their polarizers in either the vertical/horizontal (+) basis, or the complementary basis of $\pm 45°$ ($\times$). Alice then transmits a set of photons down the quantum channel, randomly choosing one of the two bases for each photon, whilst Bob measures in his choice of basis for each photon received.

$$\begin{array}{ccc} |H\rangle & \text{codes for} & 0_+ \\ |V\rangle & \text{codes for} & 1_+ \\ |{+}45\rangle & \text{codes for} & 0_\times \\ |{-}45\rangle & \text{codes for} & 1_\times \end{array}$$

Both Alice and Bob now have a list of sent of received bits, each with a basis. The second phase of the protocol is the classical sifting step: over the unsecured classical channel, they first start by comparing which bases were used for each bit, and discarding the bits for which they used different bases. For a list of size N this step will on average reduce its size by half, to $N/2$. Having matched the measurement basis, this list is referred to as the *raw key* (Gisin et al., 2002).

Alice and Bob now reveal a random sample of their raw key to one another, to compare for errors. By comparing each bit publicly over the classical channel, they can estimate the error rate for the quantum channel. If no errors are found, the raw key is already the secret key. If there are errors, Alice and Bob must either correct for them or discard their key (Scarani et al., 2009). Both these actions can take place over the classical channel; hence this step is called the *classical post-processing*. At the end of this phase, depending on how much information Eve could possess, Alice and Bob either share a secret key, or they must discard the potentially compromised key.

2.2 B92

The B92 protocol, involving just 2 non-orthogonal states, is the most minimalist QKD protocol in terms of encoding. Described by Bennett (1992), the B92 coding allows the receiver to learn whenever they get the bit sent without further discussion from Alice.

The protocol

B92 can be carried out using the two bases used in BB84. Following on from the above description, Alice sends either $|H\rangle$ or $|{+}45\rangle$, and Bob chooses to measure the incoming

bit in either the (×) or the (+) basis. Both of these states code for 0 in BB84; if Bob measures the state that codes for 1 ($|-45\rangle$ or $|V\rangle$ respectively) he can be certain that Alice transmitted her bit in the opposite basis. Hence, B92 allows the participants to restrict their transmissions in the sifting phase to whether or not Bob made a conclusive measurement for each bit sent. After discarding all bits for which Bob cannot be certain, the raw key they are left with is on average $N/4$ bits long, for an initial transmission of N bits.

After a simple comparison of raw key length to the length of the initial string sent by Alice for the classical post processing step, the participants either possess a secret key, or have been alerted to the possibility of Eve's presence.

2.3 Discussion

The BB84 and B92 protocols are two of the most rigourously tested QKD protocols, with many published articles on their relative strengths and weaknesses. Ultimate proofs exist for both; a well known one for BB84 by Shor and Preskill (2000); and similarly, for B92 there is Tamaki and Lütkenhaus (2004). Both of these proofs rely on conversion to EDP entanglement protocols; shortly after the first entanglement-based QKD protocol was described by Ekert (1991), prepare-and-measure protocols were shown to have equivalent entanglement-based versions by Bennett et al. (1992). It must be noted, however, that the above proofs are valid only for perfect single photon sources.

Although sometimes easier to implement than the more popular BB84, it is more difficult to establish unconditional security of B92, as it is much more sensitive to losses and noise in the quantum channel. In the original paper, it is shown to be necessary to rely on a strong reference pulse to guard against losses and noise; again the security of this implementation has been proven (Tamaki et al., 2009).

In an idealised world, where perfect single photon sources were available, these protocols would provide complete security with no extensions required. However, this is not the case for practical applications of QKD; as discussed in the following chapter, BB84 and B92 are highly susceptible to Eve's methods when real world limitations are present on the protocols.

3 Limitations of QKD - Eavesdropping techniques

In most literature on QKD, Eve is assumed, for the completeness of security proofs, to have no restrictions on her eavesdropping, other than the fundamental limitations of quantum mechanics itself; namely, the no-cloning theorem and the effects of measurement on a free particle. Briefly described here are two of the most common eavesdropping techniques that are considered for BB84 and B92, followed by a more in-depth look at classification of eavesdropping strategies and discussion of the relevant literature.

3.1 Intecept-resend

Potentially the most straightforward eavesdropping technique is the intercept-resend strategy, which functions exactly the same for both BB84 and B92. Eve essentially takes the same actions as Bob; with her unrestricted capabilities, performs a quantum nondemolition measurement on the incoming photons from Alice, measuring in either the $\times$ or the $+$ basis. If she has measured in the basis used by Alice, the photon continues on to Bob, and Eve has obtained full information whilst introducing no errors to the signal. However, if she has measured in the wrong basis, her result will be uncorrelated with Alice's; meanwhile, she will have sent along a modified state, so even if Bob measures in the same basis as sent by Alice, half the time he will get the wrong result. (Scarani et al., 2009)

3.2 Photon Number Splitting attack - PNS

In real world applications of QKD, the photon source is never a true strong single photon emitter. Typically a weak coherent pulse laser source is used. (Moli-Sanchez et al., 2009) These sources emit pulses of coherent states, often containing 2 or more photons.

This presents a problem for the security of BB84 and B92, as described below.

3.2.1 BB84

The security weakness in coherent pulses comes from Eve's ability to nondestructively determine the number of photons in a pulse. The principle of the PNS attack is that Eve will block all single photon pulses, and for any pulse where multiple photons are detected, Eve will store in quantum memory a subset of the pulse, while allowing the rest to continue on to Bob (through an ideal quantum channel, to ensure his receipt of the photons). During the sifting phase, Alice and Bob's communications over the public channel can be used by Eve to construct a complete key from the stored states. The major benefit to Eve with this method is that it does not introduce an error in the states received by Bob; in fact, the only risk of detection comes from the losses due to single photon pulses being blocked (Kronberg and Molotkov, 2009).

As long as these losses do not reach a critical threshold (dependent on the length of the communication channel and the expected losses), Eve's actions remain undetected, and the security of the protocol is compromised.

3.2.2 B92

Against B92, the PNS attack is even more straightforward. No quantum memory is required; all that is sufficient is that Eve performs the same measurement as Bob, and blocks the message in the event of an inconclusive result (Kronberg and Molotkov, 2009). In this way, the losses are attributed to channel losses; as long as a critical threshold is not reached (as above), Eve will obtain full information of the key. Again, due to the lack of error in the received states, Eve will remain entirely unnoticed.

3.3 Classification of eavesdropping strategies and further discussion

Strategies for eavesdropping on QKD protocols can be generally split into two main groups; *individual* and *coherent*. Individual attacks involve Eve probing each qubit individually as she recieves them, whereas for coherent attacks she may process multiple qubits at a time, and measure them *coherently*; for instance, she can store them in quantum memory, and need not measure the qubits until some later point (Gisin et al., 2002). The two types have different consequences for generating a truly secure key.

3.3.1 Individual attacks

Individual attacks impose a higher limitation on Eve, as she cannot wait for the participants to enact the sifting phase before she takes her measurements - she must measure sequentially, as must Bob. Intercept-resend is classified as an individual attack.

In intercept-resend, after she has completed the process, Eve is left with full information of half the bits in the full key ($I_E = 0.5$). The measurement process introduces an error rate of 25% (QBER $= Q = 0.25$) into the key recieved by Bob. Using the assumptions given by Csiszar and Korner (1978), this means no secret key can be extracted. This is in fact true for *all* protocols under an individual-type attack (Scarani et al., 2009).

Even in the case where Eve does not eavesdrop on all photons in the key, and instead on just a fraction p, then clearly $Q = p/4$ and

$$I_E = p/2 = 2Q \tag{3.1}$$

More errors in the received qubits can then be assumed in worst case to be an increase in Eve's information, along with a corresponding decrease in Bob's information. When Eve's maximal information is compared with Bob's error (given by his Shannon information), an inequality is recovered which describes the relative advantage of Bob or Eve. The point at which this advantage shifts to Eve can be expressed as a specific error rate Q_0:

$$I(\alpha, \beta) = \max\{I(\alpha, \epsilon)\} \quad \Leftrightarrow \quad Q = Q_0 \approx 15\% \tag{3.2}$$

Hence a secure key can only be extracted if $Q \leq 15\%$. (Kumavor et al., 2005; Gisin et al., 2002; Huttner et al., 1995)

3.3.2 Coherent attacks

Gisin et al. (2002) succintly summarises the work of Shor and Preskill (2000) and others on the subject of coherent attacks; using two theorems, the upper bound is found for the QBER of a protocol expected to withstand coherent attack.

The first theorem originates from the field of classical cryptography (Csiszar and Korner, 1978); if Alice, Bob and Eve at some point perform measurements on their quantum systems they will obtain classical random variables α, β and ϵ, respectively, with

$P(\alpha, \beta, \epsilon)$ as the joint probability distribution. The the necessary and sufficient condition for Alice and Bob to extract a secret key is

$$I(\alpha, \beta) \geq I(\alpha, \epsilon) \qquad \text{or} \qquad I(\alpha, \beta) \geq I(\beta, \epsilon) \tag{3.3}$$

Where $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$ denotes the mutual information, and H is the Shannon entropy.

The second theorem expresses Heisenberg's uncertainty relation in terms of available information (Hall, 1995): it sets a bound on the sum of information about Alice's key available to Bob and Eve.

Let E and B be two observables in an N-dimensional Hilbert space. Let ϵ, β, $|\epsilon\rangle$ and $|\beta\rangle$ be the corresponding eigenvalues and eigenvectors, respectively, and let $c = \max_{\epsilon,\beta} \{|\langle \epsilon \,|\, \beta \rangle|\}$. Then

$$I(\alpha, \epsilon) + I(\alpha, \beta) \leq 2\log_2(Nc) \tag{3.4}$$

Where again, $I(\alpha, \epsilon) = H(\alpha) - H(\alpha|\epsilon)$ and $I(\alpha, \beta) = H(\alpha) - H(\alpha|\beta)$ are the entropy differences corresponding to the probability distribution of the eigenvalues α prior to and deduced from and measurement by Eve and Bob, respectively.

Theorem 1 means that to generate a secure key, Bob must have more information than Eve about the bits generated by Alice. Theorem 2 is a mathematical description of the fact that if Eve performs some measurement providing her with information, then because of the perturbation, Bob's information is necessarily limited.

Using symmetry arguments, and denoting the number of qubits received in the correct basis by Bob as n, theorem two implies

$$I(\alpha, \epsilon) + I(\alpha, \beta) \leq n \tag{3.5}$$

Which simply means that the sum of Eve and Bob's information per qubit is less than or equal to 1; they cannot collectively receive more information than Alice sends out. Combined with theorem one, this leads to the result that a secret key is obtainable whenever $I(\alpha, \beta) \geq n/2$. Finally using $I(\alpha, \beta) = n\,[1 - Q\log_2(Q) - (1-Q)\log_2(1-Q)]$, the bound for Q (the QBER) can be obtained:

$$Q\log_2(Q) + (1-Q)\log_2(1-Q) \leq 1/2 \qquad \Rightarrow \qquad Q \leq 11\% \tag{3.6}$$

This bound, when arrived at this way in particular, is only valid in the case where the key is much longer than number of qubits Eve attacks coherently - allowing the Shannon information used to represent averages over many measurements which return classical, random variables. However, the full proof given by Shor and Preskill (2000) can still be used even in the event of Eve coherently attacking an unlimited number of qubits. Precisely the same bound of 11% QBER is recovered.

3.3.3 Multi-photon pulses

The two previous sections dealt with the classification of attacks Eve might perform on a protocol that transmits a number of states, representing some string of symbols. In summary, if Eve can only be expected to perform individual attacks, then the threshold of QBER before a sifted key becomes insecure (assuming an infinite, or finite but large raw key) is 15%; if she has unlimited capacity to coherently measure the states sent over the quantum channel, then the upper bound is 11%. But what if Alice transmits to Bob not single quantum states, but instead pulses of multiple states? This is the reality for practical QKD (Huttner et al., 1995). Usually such weakly pulsed laser sources have low photon number μ per pulse; typically $\mu \approx 0.1$ (Scarani et al., 2009).

In this circumstance, Eve may perform the PNS attack described above; the effect on security can be quite large indeed. Remember that Eve is not restricted in the technology she uses; while all currently known transmission mediums incur some loss over distance, Eve could replace the channel between Alice and Bob by a perfect lossless channel, and with the extra power gained she is free to discard a certain proportion of pulses. Typical attenuation values for optical fibre are on the order of 10^{-2}dBkm^{-1}; most research findings indicate that under such conditions security can only be guaranteed over a medium distance; between 50 and 200km, depending on experimental parameters and assumptions (Fung et al., 2006; Moli-Sanchez et al., 2009; Jeong et al., 2014).

But how realistic is a quantum nondemolition measurement, or a lossless channel? In recent times, quantum nondemolition measurements have increasingly been the subject of new research (Brassard et al., 2000); ideal quantum nondemolition photon number measurements are beyond current technologies, although it may be reasonable to assume that they are possible (Nogues et al., 1999).

For Eve to count photon number for a pulse, she must measure it without disturbing the degree of freedom encoding the qubit. Eve must then store the qubit, in either a lossless looped channel, or by mapping the qubit to quantum memory. This may be unrealistic; as noted above, there is no perfect physical medium for transmission, even in theory, due to unavoidable Rayleigh scattering. Attenuation of the qubits Eve has stored reduces her information, and Alice and Bob may wait minutes before carrying out the sifting phase (Scarani et al., 2009); consequently, even if she chooses to use the quantum memory, it must have close to unlimited decoherence time. Two possibilities left for Eve are suggested by Gisin et al. (2002); either she must use high-fidelity, near lossless quantum teleportation of the qubits, or she can convert the photons to another wavelength, again without disturbing the qubit. In the forseeable future, neither option is realistic; however advances in quantum and optical technologies may make PNS attacks a serious threat.

References

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124.

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7 – 11.

Bennett, C. H., Brassard, G., and Mermin, N. D. (1992). Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559.

Brassard, G. (2005). Brief history of quantum cryptography: A personal perspective. *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information Theoretic Security*, pages 19–23.

Brassard, G., Lütkenhaus, N., Mor, T., and Sanders, B. C. (2000). Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85:1330–1333.

Csiszar, I. and Korner, J. (1978). Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348.

Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663.

Fung, C.-H. F., Tamaki, K., and Lo, H.-K. (2006). Performance of two quantum-key-distribution protocols. *Phys. Rev. A*, 73:012337.

Gisin, N., Ribordy, G., Tittel, W., and Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195.

Hall, M. J. W. (1995). Information exclusion principle for complementary observables. *Phys. Rev. Lett.*, 74:3307–3311.

Huttner, B., Imoto, N., Gisin, N., and Mor, T. (1995). Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869.

Jeong, Y.-C., Kim, Y.-S., and Kim, Y.-H. (2014). An experimental comparison of bb84 and sarg04 quantum key distribution protocols. *Laser Physics Letters*, 11(9):095201.

Kronberg, D. A. and Molotkov, S. N. (2009). Robustness of quantum cryptography: Sarg04 key-distribution protocol. *Laser Physics*, 19(4):884–893.

Kumavor, P. D., Beal, A. C., Yelin, S., Donkor, E., and Wang, B. C. (2005). Comparison of four multi-user quantum key distribution schemes over passive optical networks. *Journal of Lightwave Technology*, 23(1):268–276.

Moli-Sanchez, L., Rodriguez-Alonso, A., and Seco-Granados, G. (2009). Performance analysis of quantum cryptography protocols in optical earth-satellite and intersatellite links. *IEEE Journal on Selected Areas in Communications*, 27(9):1582–1590.

Nogues, G., Rauschenbeutel, A., Osnaghi, S., Brune, M., Raimond, J. M., and Haroche, S. (1999). Seeing a single photon without destroying it. *Nature*, 400(6741):239–242.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., and Peev, M. (2009). The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350.

Shor, P. W. and Preskill, J. (2000). Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444.

Tamaki, K. and Lütkenhaus, N. (2004). Unconditional security of the Bennett 1992 quantum key-distribution protocol over a lossy and noisy channel. *Phys. Rev. A*, 69:032316.

Tamaki, K., Lütkenhaus, N., Koashi, M., and Batuwantudawe, J. (2009). Unconditional security of the Bennett 1992 quantum-key-distribution scheme with a strong reference pulse. *Phys. Rev. A*, 80:032302.

Glossary

Quantum channel A transmission path that allows the sharing of quantum states. .

Quantum key distribution Quantum key distribution refers to the sharing of cryptographic keys using a quantum channel, to take advantage of coherence effects to guarantee security of the resulting key.

Ultimate security proof An ultimate proof guarantees security against entire classes of eavesdropping attacks, even if Eve has access to unlimited technology.