The Open University

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

William Ockmore

September 19, 2016

Abstract

Quantum key distribution (QKD) allows two parties to share an unconditionally secure key by means of a quantum channel, where eavesdropping can be detected in the signal itself. In this critical literature review, the two of the most prominent prepare and measure protocols are described, with focus on their sifting phase. The limitations of these protocols are analysed, centering on the Photon Number-Splitting (PNS) attack as an eavedropping method. A more recent protocol, SARG04, is detailed, and its benefits and limitations relative to these previous protocols are described at length, with particular focus on the comparison with BB84. Within this analysis, it is found that BB84 with decoy states has a higher secret key rate and secure distance, under realistic experimental parameter sets, than SARG04 with decoy states. This is the case even in the scenario of two photon pulses, for which SARG04 was developed. The only exception is the case of a channel with very low quantum bit error, and a multi-photon pulsed source, with the expectation that SARG04 is used when Eve (an eavesdropper) is present.

Contents

1 Introduction

Quantum key distribution (QKD) 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 unconditional security. Eve (the eavesdropper) has no restrictions other than the laws of physics. 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. 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. 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 outline possible improvements, either through practical engineering or new theory.

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, which involve sending individual quantum states (qubits) down a quantum channel, to be measured by a receiver at the other end.

2.1 BB84

BB84 was the first proposed QKD protocol (Bennett and Brassard, 1984; Brassard, 2005).

The protocol

In BB84, Alice uses a single photon source to transmit a set of polarization states to Bob. 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 her set 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 or 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 ($\times$) 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 (Bennett, 1992).

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

Ultimate proofs exist for both protocols; a well known one for BB84 by Shor and Preskill (2000); and similarly, for B92 there is Tamaki and Lütkenhaus (2004). Both 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).

If perfect single photon sources were easily 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, real world limitations have a large impact.

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.

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 he receives 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; 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.

B92

Against B92, PNS attack is even more straightforward. No quantum memory is required; Eve performs the same measurement as Bob, and blocks the message in the event of an inconclusive result (Kronberg and Molotkov, 2009). 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 whilst remaining 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; for coherent attacks she may process multiple qubits at a time, and measure them *coherently* (Gisin et al., 2002).

Individual attacks

Individual attacks impose a higher limitation on Eve, as she cannot wait for the sifting phase before she takes her measurements - she must measure sequentially. 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)

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.

Multi-photon pulses

The two previous sections dealt with the classification of attacks Eve might perform. 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 (Lucamarini et al., 2013; Huttner et al., 1995). Usually such weakly pulsed laser sources have low photon number μ per pulse; typically $\mu \ll 1$ (Scarani et al., 2009).

In this circumstance, Eve may perform the PNS attack described above; the effect on security can be large. 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? Quantum nondemolition measurements have increasingly been the subject of 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 (Scarani et al., 2009; 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, due to unavoidable Rayleigh scattering. Attenuation of the qubits 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, 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.

4 The SARG04 protocol

In this chapter, the SARG04 protocol, first described in Scarani et al. (2004) is explained in the context of previously discussed protocols. Its benefits and limitations are analysed, with reference to real world experiments and applications.

4.1 The protocol

SARG04 as a protocol is very similar to BB84; in fact, the steps followed by Alice and Bob are identical until the classical sifting phase. The same setup can be used in both cases, which makes comparison of the two protocols straightforward.

The same four states are used in SARG04 as in BB84; however rather than the state sent coding for the bit, the basis itself is used, as in B92. After the raw key has been transmitted, Alice declares for each qubit one of four pairs of non-orthogonal states $A_{\omega,\omega'}\left\{|\omega x\rangle, |\omega' z\rangle\right\}$ with $\omega, \omega' \in \{+, -\}$ and the convention that $|\pm x\rangle$ code for 0 and $|\pm z\rangle$ code for 1 (Scarani et al., 2004). Any two non-orthogonal bases σ_x and σ_z may be used; for example the $+$ and $\times$ polarisation bases used in the earlier description of BB84 and B92. Within each set $A_{\omega,\omega'}$ the overlap of the two states is $\chi = \frac{1}{\sqrt{2}}$.

The procedure for extracting the bit values is outlined in the following example. Suppose Alice sends $|-x\rangle$ and declares A_{-+}. If Bob has received this particular bit in the σ_x basis, he will measure $|-x\rangle$ with certainty. He cannot be certain that Alice did not send $|+z\rangle$ in this circumstance. However if he receives in the σ_z basis, he will measure $|-z\rangle$ with probability $\frac{1}{2}$. As this state is contradictory to the second member of the pair communicated by Alice, Bob knows that, in the absence of errors, Alice must have sent $|-x\rangle$.

4.2 Benefits of SARG04

As Alice does not communicate basis over the classical channel during the sifting phase, Eve does not have the ability to unambiguously determine the measurement basis for a qubit. For all two-photon pulses she now cannot be certain of achieving a valid result; for three photon pulses, she must implement an unambiguous state discrimination measurement $\mathcal{M}$, which succeeds with probability $\frac{1}{2}$ (Branciard et al., 2005). Hence in the case of two-photon pulses SARG04 is still provably secure, where BB84 is not (Fung et al., 2006).

To attack SARG04 Eve may implement a specific version of the PNS attack; discarding all one- and two-photon pulses, she performs $\mathcal{M}$, and with a conclusive result (occuring with probability $\frac{1}{2}$) she sends a new photon prepared in the good state to Bob. This attack is referred to as *intercept-resend with unambiguous discrimination attack* (IRUD) (Scarani et al., 2004). It needs neither the quantum memory or the lossless channel, as the new state can be prepared at some location close to Bob. There is a critical channel attenuation δ_c at which IRUD is always possible; for a conservative estimate of $\mu = 0.2$ as given in the original paper, $\delta_c = 25.6\text{dB} \approx 2\delta_c^{\text{BB84}}$. Hence under the circumstance of zero external QBER and incoherent attack, SARG04 gives twice the secure distance as

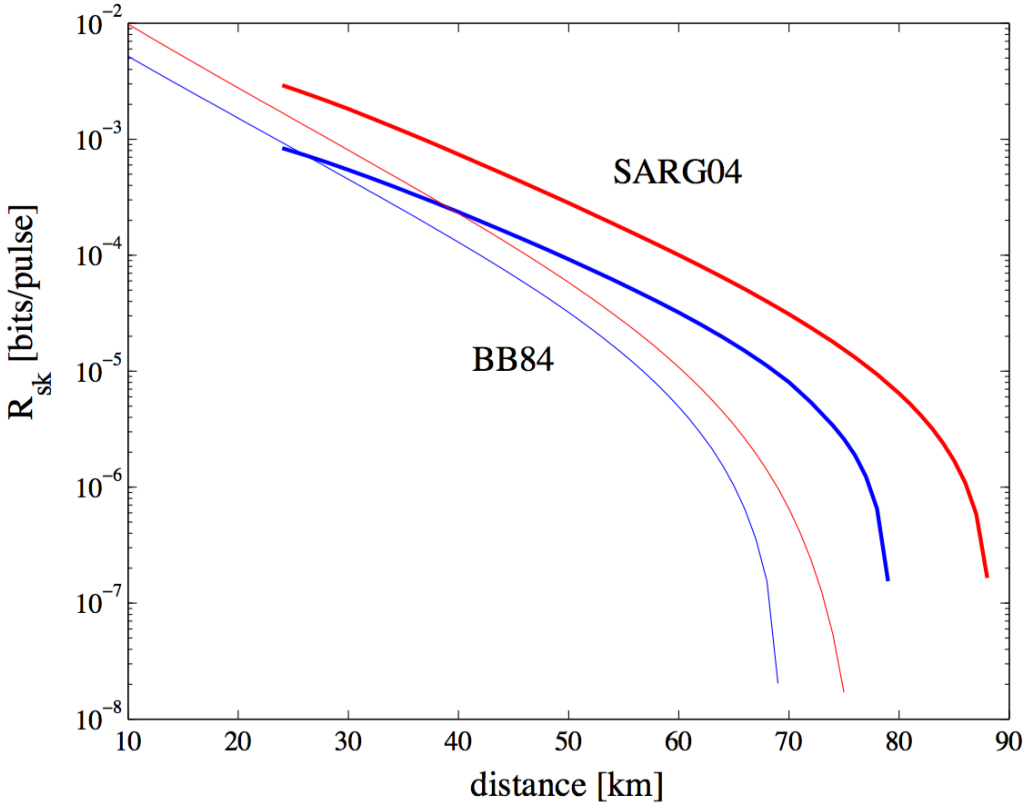

Figure 4.1: Optimal μ and upper bound for secret key rate per pulse R_{sk} with channel losses $\alpha = 0.25\text{dBkm}^{-1}$, detector quantum efficiency $\eta = 0.1$, dark count probability $p_d = 10^{-5}$, and channel visibility $V = 1, 0.95$. The thick lines are results for SARG04, thin lines BB84. (Branciard et al., 2005)

BB84. This was independently verified by Branciard et al. (2005). In their paper it was also shown that SARG04 has a higher secret key rate than BB84 under realistic source conditions and under the assumption of incoherent attack by Eve. Their results for a Poisonnian attenuated laser source are shown in Figure 4.1.

5 Limitations of SARG04

5.1 Single photon implementation

In a single photon implementation, the upper bound on the attainable secret key rate is given by Csiszar and Korner (1978) as

$$r \leq R_{sk} = \max_{A \to A'} \left\{ I(A' : B) - I(A' : E) \right\} \tag{5.1}$$

where A' represents any preprocessing performed by Alice, which gains a slight increase on the QBER bound where the secret key becomes zero. This leads to the corresponding bounds for single photon SARG04 and BB84 as given in Kraus et al. (2005); Branciard et al. (2005):

BB84	Lower	$Q \leq 12.4\%$
	Upper	$Q \geq 14.6\%$
SARG04	Lower	$Q \leq 10.95\%$
	Upper	$Q \geq 14.9\%$

This does not take into account channel noise and subsequent reduction in visibility. In the case of a channel with neligible dark count rate, the error rate on the sifted key is a function of the visibility. In the example of BB84, when when the good basis is chosen the probabilities of a right or wrong measurement are $p_{\text{right}} = \frac{1+V}{2}$ and $p_{\text{wrong}} = \frac{1-V}{2}$. This leads to

$$Q_{\text{BB84}} = \frac{p_{\text{wrong}}}{p_{\text{right}} + p_{\text{wrong}}} = \frac{1-V}{2} \tag{5.2}$$

As SARG04 codes by basis, whenever Bob accepts the good encoding basis (the one not used by Alice), he guesses right. This is independent of the visibility so $p_{\text{right}} = \frac{1}{2}$. If he chooses the wrong basis and accepts, then this is due to error, and occurs with $p_{\text{wrong}} = \frac{1-V}{2}$.

$$Q_{\text{SARG04}} = \frac{p_{\text{wrong}}}{p_{\text{right}} + p_{\text{wrong}}} = \frac{1-V}{2-V} \approx 1 - V \tag{5.3}$$

Hence for a fixed visibility, the QBER is almost twice that of BB84 (Branciard et al., 2005). Thus although the error bounds are comparable, they are more restrictive for an implementation of SARG04 and the protocol is more sensitive to error in the channel.

5.2 Key generation rate

The nature of SARG04's sifting phase means that Bob may only accept on average $\frac{1}{4}$ bits. This is in contrast to BB84, where choosing the correct measurement basis occurs 50% of the time, hence Bob accepts $\frac{1}{2}$. The raw key generation rate for a general protocol, under zero channel losses is

$$R = \nu_s P_b \tag{5.4}$$

where ν_s is the repetition rate and P_b is the probability that Bob accepts a bit. For a given source

$$R_{\text{SARG04}} = \frac{\nu_s}{4} = \frac{R_{\text{BB84}}}{2} \tag{5.5}$$

Under the same conditions, μ for SARG04 must then be twice that of BB84 for the same raw key rate (Fung et al., 2006; Scarani et al., 2004). In practical applications of the protocol this is a serious limitation; also, if Eve is not present then the use of SARG04 over BB84 is penalised with no associated benefit.

As documented in Jeong et al. (2014), this leads (along with SARG04's sensitivity to channel visibility) to BB84 generating more secret keys than SARG04 under real world conditions, where devices are imperfect and $V < 1$.

5.3 Decoy states

Decoy states were first proposed by Hwang (2003) with one- and two-photon signals, with the more popular and realistic intensity modulation implementation put forward soon after (Lo et al., 2005).

Description of the technique

The central idea behind decoy states is to randomly change some tunable parameter ξ in the protocol (most commonly the photon number/intensity μ); using some subset of possible values for the parameter to conduct the protocol itself, Alice and Bob then have a set of linear equations dependent on the channel properties.

After transmitting the set of qubits, Alice reveals the list of values $\xi \in \chi$, and after sorting the data Alice and Bob now have a linear system of $2|\chi|$ equations

$$R^\xi = \sum_{n\geq 0} R_n^\xi \quad \text{and} \quad Q^\xi = \sum_{n\geq 0} \frac{R_n^\xi}{R^\xi} \epsilon_n \tag{5.6}$$

If Alice and Bob know the characteristics of their setup, they can determine with high confidence the expected R and Q for a particular ξ; hence if Eve takes any action that will change either value substantially, the participants can detect her presence. This greatly limits her options (Lo et al., 2005; Scarani et al., 2009).

Optimum photon number

In order to illustrate the benefits gained with decoy states, consider the concept of optimum μ, a variable that only becomes relevant beyond the discussion of ideal single-photon sources (as clearly, the secret key rate K scales linearly with μ in the case of a single photon source (Gisin et al., 2002)). The probability for Alice's attenuated laser source to emit either one or two photons is given by

$$p_A(1) = \mu e^{-\mu} \quad \text{and} \quad p_A(2) = \mu^2 e^{-\frac{\mu}{2}} \tag{5.7}$$

Obviously the ideal situation for security is for $p_A(2) \approx 0$; however this entails small μ and by extension, small R. The optimum value for μ must maximise the achievable secret key rate.

Taking into account imperfect error correction, the definition for the secret key rate is given by

$$K = R\left[1 - \text{leak}_{EC}(Q) - I_E\right] \tag{5.8}$$

where $\text{leak}_{EC}(Q)$ is the information loss due to imperfect error correction (so the leaked information $\text{leak}_{EC}(Q) \geq h(Q)$, with $h(Q)$ the binary Shannon entropy); and I_E as usual is the maximal information available to Eve (Scarani et al., 2009).

Rather than follow the lengthy derivation, results for optimal μ for an attenuated laser in the case without, and with, decoy states are quoted below from Scarani et al. (2009).

In the implementation without decoy states, the highest achievable secret key rate is

$$\frac{K}{\nu_s t t_B \eta} \approx \frac{1}{2}\mu_{\text{opt}} F(Q) \qquad \text{(laser without decoy states)} \tag{5.9}$$

obtained for the optimal mean photon number

$$\mu_{\text{opt}} \approx t t_B \eta \frac{F(Q)}{1 - h(2Q)} \tag{5.10}$$

where t is the transmittivity of the quantum channel, t_B are the losses in Bob's device, η is the efficiency of the detector, and $F(Q) = 1 - h(2Q) - h(Q)$.

For the implementation with decoy states, the maximal value for K is

$$\frac{K}{\nu_s t t_B \eta} \approx \frac{1}{2}\mu_{\text{opt}}\left[1 - 2h(Q)\right] \qquad \text{(laser with decoy states)} \tag{5.11}$$

for optimal mean photon number

$$\mu_{\text{opt}} \approx \frac{1}{2}\left[1 - \frac{h(Q)}{1 - h(Q)}\right] \tag{5.12}$$

Consequently, without decoy states $\mu_{\text{opt}} \propto t$, and hence $K \propto t^2$: the larger the losses in the channel, the more attenuated the laser must be. For guarding against PNS attacks, it must be ensured that Eve cannot reproduce the detection rate at Bob's by using only photons from 2-photon pulses. With decoy states, the fraction of detections that come from 2-photon pulses can be determined; if this fraction is as low as is expected, a PNS attack can be ruled out. The major benefit gained is the recovery of $K \propto t$ scaling. This is the same as for ideal single-photon sources (Lo et al., 2005; Scarani et al., 2009).

Consequences for SARG04

A comparison simulation of the performance of SARG04 and BB84 using decoy states was published by Fung et al. (2006). With the addition of two way classical communications (allowing Alice and Bob to communicate with each other, rather than just one-way) it was shown that for all realistic parameter sets, SARG04 had a smaller key generation rate and shorter secure distance than BB84. In the case of small QBER, the optimum μ of SARG04 can be higher than BB84; this does not mean however that the key generation rate is necessarily greater, as mentioned earlier. These results are in the case of general attack by Eve.

It is interesting that the most robust and performant protocol is still BB84 (albeit with modifications such as the addition of decoy states). In recent papers by Lucamarini et al. (2015, 2013), the secret key rate was increased to almost 1Mbs^{-1} over 50km, with reduced sensitivity to finite-size effects; further legitimising real world applications of the protocol. Even taking into account the most optimised decoy-state versions of SARG04, they still compare poorly to BB84 (Yuan-Yuan et al., 2013).

However the caveat that must be properly understood in these comparisons is that decoy states are a method to gain knowledge on Eve's attack. If the attack is not taking place, then BB84 with its simpler sifting methodology will produce a higher secret key rate; however, if an attack is taking place, then in two photon implementations *with small QBER*, SARG04 will generate a key with higher probability. In simple terms, if BB84 can generate a key that is secure, it will do so faster; SARG04's application is for the times when this is not possible (Fung et al., 2006; Scarani et al., 2009).

6 Conclusion

In this report, SARG04 was introduced and compared to known prepare and measure protocols. It was found that although it brings a novel way to foil a PNS attack by changing the classical communication phase of BB84, once other factors of practical application - such as decoy states, key generation rate under imperfect conditions, and lossy channels - are brought into account, it compares unfavourably to the original protocol in realistic scenarios.

Extensive analysis was taken on the classical protocols, attack vectors, and the direct limitations of SARG04. Possible improvements to the methodology could include additional research into strong reference pulse based security and its implications for the protocol (Koashi, 2004); as well as comparison to new protocols that have not yet been fully explored, such as KMB09 (Khan et al., 2009).

The initial objectives given were considered before full understanding of the research area had been obtained. However in terms of scope, the review has stayed reasonably close to the original outline. A brief history of QKD was given, although its impact on society was not fully addressed. Limitations of historical protocols were investigated thoroughly; SARG04 was described and its benefits and limitations discussed at length. The real world improvements possible were highlighted in the decoy state method, although more was left to be said with regards to further study in the case of SARG04 itself.

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.

Branciard, C., Gisin, N., Kraus, B., and Scarani, V. (2005). Security of two quantum cryptography protocols using the same four qubit states. *Phys. Rev. A*, 72:032301.

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.

Hwang, W.-Y. (2003). Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901.

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.

Khan, M. M., Murphy, M., and Beige, A. (2009). High error-rate quantum key distribution for long-distance communication. *New Journal of Physics*, 11(6):063043.

Koashi, M. (2004). Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse. *Phys. Rev. Lett.*, 93:120501.

Kraus, B., Gisin, N., and Renner, R. (2005). Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.*, 95:080501.

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.

Lo, H.-K., Ma, X., and Chen, K. (2005). Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504.

Lucamarini, M., Dynes, J. F., FrÃűhlich, B., Yuan, Z., and Shields, A. J. (2015). Security bounds for efficient decoy-state quantum key distribution. *IEEE Journal of Selected Topics in Quantum Electronics*, 21(3):197–204.

Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., Yuan, Z. L., Penty, R. V., and Shields, A. J. (2013). Efficient decoy-state quantum key distribution with quantified security. *Opt. Express*, 21(21):24550–24565.

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

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.

Yuan-Yuan, Z., Xue-Jun, Z., Pei-Gen, T., and Ying-Jian, W. (2013). New protocols for non-orthogonal quantum key distribution. *Chinese Physics B*, 22(1):010305.

Glossary

Entanglement distillation protocol (EDP) A QKD protocol that makes use of non-local effects, rather than state orthogonality, to transmit a secret key.

Photon number The average number of photons in a pulse - typical values are $\mu \ll 1$.

Quantum non-demolition measurement A special type of measurement where the uncertainty of the measured observable does not increase. Typically in the context of QKD refers to counting photon number without disturbing polarisation (or phase) hence preserving the encoding.

Quantum bit error rate (QBER) The ratio of wrong bits against the total detected bits after the sifting phase, as measured by Bob.

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

Quantum key distribution (QKD) 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.

Raw key The sequence of bits received by Bob, prior to the sifting phase. The raw key rate is the rate at which Bob is able to receive the bits sent by Alice, and is given by $R = \nu_s P_b$, where ν_s is the repetition rate, and P_b is the probability that Bob accepts a bit..

Secret key rate The rate at which the secret fraction of the raw key can be generated.

Shannon entropy A measure of information contained in a message, as a function of characters (qubits or states) in a given stream. Given by the formula $H = -\sum_i p_i \log_b p_i$, where p_i is the probability of character i from character set of size b showing up in the output stream.

Strong reference pulse A pulse transmitted as a phase reference, at a much higher photon number than the weak signal pulse, with the aim of preventing Eve from blocking the entire signal without introducing error.

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