A survey on quantum cryptographic protocols and their security

Chi-Hang Fred Fung and Hoi-Kwong Lo
Center for Quantum Information and Quantum Control,
Edward S. Rogers Sr. Department of Electrical and Computer Engineering and Department of Physics
University of Toronto
10 King's College Road, Toronto, Ontario M5S 3G4, Canada
Email: {cffung,hklo}@comm.utoronto.ca

***Abstract*— Communications in secrecy are often required in many commercial and military applications. Unfortunately, many cryptographic schemes in use today such as public-key cryptography based on the RSA algorithm would be broken with either unanticipated advances in hardware and algorithm or the advent of quantum computers. Quantum cryptography, on the other hand, has been proven secure even against the most general attack allowed by the laws of physics and is a promising technology poised for widespread adoption in realistic cryptographic applications. Quantum cryptography allows two parties to expand on a secret key that they have previously shared. Various quantum cryptographic protocols have been proposed to perform this task. In this paper, we survey some popular quantum cryptographic protocols (including the famous Bennett-Brassard 1984 protocol) and discuss their security. Specifically, we consider their security in two cases: the ideal case where a perfect single-photon source is used and the practical case where a realistic laser source is used. We compare the protocols and find that the efficient six-state protocol outperforms the others both in the tolerable quantum bit error rate and in the key generation rate when a realistic laser source is used.**

I. Introduction

Communications in secrecy are often required in many commercial and military applications. However, since the security of many classical cryptographic schemes in use today such as public-key cryptography based on the RSA algorithm relies on the difficulty of solving certain mathematical problems, many of these schemes could be broken overnight with unanticipated advances in algorithms and hardware (such as quantum computers). For instance, quantum computers can efficiently factor large numbers, on which RSA is based, thus breaking the security of it. Quantum cryptography [1], on the other hand, has been proven secure even against the most general attack allowed by the laws of physics. More specifically, the security of quantum cryptography is based on the Heisenberg uncertainty principle of quantum mechanics. Thus, even when an eavesdropper is equipped with a powerful quantum computer, quantum cryptography is still able to provide perfect security between two legitimate users. Quantum cryptography, or more precisely quantum key distribution (QKD), allows two parties to expand on a secret key that they have previously shared. By transmitting quantum states through a quantum channel, they can grow a longer secret key. The secret key can then be used with some classical cryptographic scheme, such as the one-time pad which has been shown to be perfectly secure, to provide secret communications.

Various protocols have been proposed to perform quantum key distribution. The most well-known QKD protocol is the Bennett-Brassard 1984 (BB84) protocol [1], which has been proved unconditionally secure against any attacks allowed by quantum mechanics (e.g. [2], [3]). In this paper, we survey some popular quantum cryptographic protocols – the BB84 protocol, the six-state protocol [4], the Scarani-Acin-Ribordy-Gisin 2004 (SARG04) protocol [5], the symmetric three-state protocol [6], [7], and the asymmetric three-state protocol [8], [9]– and discuss their security. Specifically, we consider their security in two cases: the ideal case where a perfect single-photon source is used and the practical case where a realistic laser source is used. We compare the protocols and find that the efficient six-state protocol outperforms the others both in the tolerable quantum bit error rate and in the key generation rate when a realistic laser source is used.

II. QKD Protocols

QKD protocols generally consist of two main steps: the quantum state transmission step and the classical post processing step. In the quantum state transmission step, one party, Alice, randomly selects one state from a set of states and transmits it through a quantum channel to Bob. The set of allowable states is generally organized into a number of *bases* each containing two *basis states* representing bit "0" and bit "1". Alice selects a basis and a state within the basis and transmits it to Bob. Upon receiving the quantum state, Bob randomly chooses a basis and measures the incoming state using a measurement specific for that basis. He then records his measurement outcome. After all transmissions of quantum states have finished, they proceed to the classical post processing step.

In the classical post processing step, Alice and Bob generally perform four procedures: basis reconciliation, error testing, error correction, and privacy amplification. For each quantum state transmitted by Alice, the basis to which the state belongs may not be compatible with the measurement result obtained by Bob. When they are not compatible, Bob's measurement outcome is in general random and does not contain any information. Therefore, in the *basis reconciliation*

0840-7789/07/$25.00 ©2007 IEEE

phase, Alice announces her basis choices and based on this information, Bob decides which measurement outcomes are conclusive (i.e., a bit value can be assigned to an outcome) and announces this fact to Alice. They retain only the conclusive bits. The second phase of the post processing is *error testing*. Alice and Bob publicly compare a small random subset of the bits retained. Because of the presence of Eve or channel noise, some of the bits may be in error. Based on the number of errors in the subset, they compute the *quantum bit error rate* (QBER). Because of the random sampling theorem, the remaining untested bits, called the sifted key, exhibit the same value of QBER with high probability. Knowing the QBER allows Alice and Bob to apply the appropriate *error correction* and *privacy amplification* to the bits in order to, respectively, remove bit errors and eliminate Eve's information on the final key. If the QBER is too high, they may not be able produce any secret bit at all.

Note that all classical communications are authenticated, in order to ensure that all messages come from the other legitimate party. Authentication requires a small amount of secret key, which is sublinear in the length of the message sent. Asymptotically, QKD produces secret bits linear in the number of signals sent; thus, the amount of secret key required for authentication becomes insignificant. Nevertheless, since QKD requires some secret key to begin with for authentication purpose, QKD is a process for expanding a shorter secret key to a longer one. In the following, we describe some popular QKD protocols.

A. BB84 protocol

The BB84 protocol consists of two bases: $\{|0_z\rangle, |1_z\rangle\}$ and $\{|0_x\rangle, |1_x\rangle\}$. Note that the two basis states in each basis are orthogonal. The measurement for each basis by Bob is simply a projection onto the corresponding two basis states.

B. Six-state protocol

The six-state protocol consists of three bases; two are the same as in the BB84 protocol and the third one is $\{|0_y\rangle, |1_y\rangle\}$.

C. SARG04 protocol

The SARG04 protocol has the same four states as the BB84 protocol but organizes the states differently into four bases: $\{|0_z\rangle, |0_x\rangle\}$, $\{|0_x\rangle, |1_z\rangle\}$, $\{|1_z\rangle, |1_x\rangle\}$, and $\{|1_x\rangle, |0_z\rangle\}$. Note that the two basis states in each basis are not orthogonal. Because of that, the measurement for detecting the states in each basis may produce an inconclusive result. Specifically, the measurement for say the first basis produces one of three possible outcomes; the incoming state is either (i) $|0_z\rangle$, (ii) $|0_x\rangle$, or (iii) unknown (meaning the measurement result is inconclusive). The measurement consists of Bob randomly choosing with equal probability the projection onto $\{|0_z\rangle, |1_z\rangle\}$ or the projection onto $\{|0_x\rangle, |1_x\rangle\}$. The meaning of each of the four projection outcomes depends on the basis. For the first basis, when the projection outcome is $|1_z\rangle$ ($|1_x\rangle$), the decision by Bob is that the incoming state is $|0_x\rangle$ ($|0_z\rangle$); when the projection outcome is $|0_z\rangle$ or $|0_x\rangle$, Bob's decision is inconclusive.

D. Symmetric three-state protocol

This protocol consists of three states: $\{\cos(m\pi/3)|0_z\rangle + \sin(m\pi/3)|1_z\rangle : m = 0, 1, 2\}$. These states are symmetrically distributed in the upper half of the unit circle of the X-Z plane, hence the name. There are three bases, containing all possible pairs of states. The measurements by Bob are similar to those in the SARG04 protocol. He randomly selects one of three orthogonal projections, each containing one direction that is the same as one of the legitimate states sent by Alice. Based on the basis information announced later by Alice, Bob assigns meanings to the projection outcomes. Again three possible meanings are that the outcome is either bit "0", bit "1", or inconclusive.

E. Asymmetric three-state protocol

This protocol also contains three states: $\{|0_z\rangle, |0_x\rangle, |1_z\rangle\}$. There are two bases, one containing the two Z eigenstates and the other containing only the $|0_x\rangle$ state. This protocol is similar to the BB84 protocol except that the $|1_x\rangle$ state is never sent. Two QBER's are estimated in the protocol, one for the Z basis (denoted by e_b) and the other for the $|0_x\rangle$ state (denoted by α).

We note that all the above protocol except the asymmetric three-state protocol possess some rotational symmetry. In fact protocols with rotational symmetry have been generalized and analyzed in [10], [11]. In our earlier work [11], we have provided a unified security proof for a generalized rotationally symmetric protocol that includes the BB84, the SARG04, and the symmetric three-state protocols as specific cases.

III. Security

The security of QKD rests on the fact that non-orthogonal quantum states cannot be perfectly distinguished. Note that in all QKD protocols, the quantum states of any protocol do not form an orthogonal set, although two basis states may be orthogonal. Thus, Eve cannot find out which state has been sent by Alice without knowing the basis.

A. Ideal single-photon source

A quantum state may be encoded in the polarization state of a photon. Ideally, Alice uses a single-photon source to transmit quantum states to Bob. Each signal emitted by the source contains one photon and the quantum state is encoded in the photon. In this case, the unconditional security of BB84 has been proven (e.g. [2]), and the unconditional security proof of [2] can be extended to include other protocols as well. The key generation rate for the single-photon case is given by [2] (assuming the number of test bits goes to zero)

$$R = q(1 - H_2(e_b) - H_2(e_p)). \quad (1)$$

Here, e_b is the QBER estimated during a QKD experiment and e_p is the phase error rate inferred from e_b, $H_2(p) = -p\log_2(p) - (1-p)\log_2(1-p)$ is the binary entropy function, and q is the fraction retained after basis reconciliation ($1/2$ for BB84, $1/3$ for six-state, $1/2$ for asymmetric three-state, and variable for others). We remark that idea of efficient

Protocol	Relation	References
BB84	$e_p = e_b$	[2], [13]
Six-state	$e_p = e_b$	[14]
SARG04	$e_p = 3e_b/2$	[15], [16]
Sym. three-state	$e_p = 5e_b/4$	[7]
Asymmetric three-state	$e_p \leq \alpha + e_b(2 - 2\alpha - \alpha^2) + 2\sqrt{\alpha(1-\alpha)e_b(1-e_b-e_b\alpha)}$	[8]
Generalized rotationally symmetric	$e_p = e_b(1+\cos^2\theta)$, for $M > 2$ $e_p \leq \frac{1+\cos^2\theta}{\cos^2\theta} e_b$, for $M = 2$	[11]

TABLE I

RELATIONSHIPS BETWEEN BIT AND PHASE ERROR RATES.

BB84 [12] can be applied to both the BB84 protocol and the six-state protocol to allow the retained fraction q goes to one asymptotically in both cases. We refer to the resulting protocols as the *efficient BB84* protocol and the *efficient six-state* protocol. The phase error rate is related to the amount of information about the key leaked to Eve and is directly related to e_b with a protocol-dependent relationship. In (1), the second and third terms in the bracket represent the amount of key bits sacrificed for error correction and privacy amplification, respectively. In order to compute the key generation rate for a protocol, one needs to work out the relationship between the phase error rate e_p and the bit error rate e_b for that protocol. Once the relationship is available, (1) can be used to compute the key generation rate using the bit error rate experimentally estimated and the phase error rate inferred from it. The relationships between bit and phase error rates for the various protocols with single-photon signals have been studied in various papers and are tabulated in Table I.

The key generation rate in (1) may be increased by incorporating the mutual information between the bit and phase errors. Improvement due to the mutual information has been shown to be positive for the six-state protocol and the SARG04 protocol. Specifically, for the six-state and the SARG04 protocols, the key generation rates can be increased from (1) to, respectively,

$$R_{\text{six-state}} = \frac{1}{3}(1 - H_4(1 - 3e_b/2, e_b/2, e_b/2, e_b/2)) \quad (2)$$

$$R_{\text{SARG04}} = q(1 - H_4(1 - 2e_b, e_b/2, e_b/2, e_b)), \quad (3)$$

where $H_4(x_1, x_2, x_3, x_4) = \sum_{i=1}^{4} -x_i \log_2(x_i)$. Note that the value of q for the SARG04 protocol and the symmetric three-state protocol depends on the actual measurement results in a QKD experiment.

B. Realistic source

Although there have been some proposals for single photon sources and demonstrations in labs, single photon sources are still not commercially available. Often weak coherent sources are used to simulate single-photon sources. With a coherent source, the number of photons contained in each emitted signal follows the Poisson distribution. Thus, there is a certain probability that a multi-photon signal is emitted. This is not desirable, because multi-photon signals are in general insecure and do not in general contribute to key generation. Nevertheless, unconditional security for the coherent source case has been proved for the BB84 protocol in [3] and can easily be extended to include other protocols.

In the simplest scenario, Alice and Bob need to estimate two quantities in order to produce secret bits. They need to estimate the overall gain Q_{signal}, which is the probability of detection by Bob, and the overall QBER E_{signal}, which is the probability that Bob's result is incorrect given that Bob detects a signal. Once Alice and Bob have measured the overall gain and the overall QBER, the key generation rate may be obtained by using a result in GLLP [3] as follows (assuming the number of test bits goes to zero):

$$R = q\, Q_{\text{signal}} \big[- f(E_{\text{signal}}) H_2(E_{\text{signal}}) + \Omega(1 - H_2(e_p)) \big], \quad (4)$$

where $f(\cdot)$ is the error correction efficiency as a function of the QBER, $\Omega = Q_1/Q_{\text{signal}}$ is the fraction of single-photon states, Q_1 is the probability that Bob detects a signal and Alice has sent a one-photon signal, e_p is the phase error rate of the single-photon states, and q is the fraction retained after basis reconciliation. The first term in the bracket is related to error correction, while the second term is related to privacy amplification. Similar to the single-photon-source case, mutual information between the bit and phase errors can be incorporated by modifying the privacy-amplification term in order to increase the key generation rate for the six-state protocol and the SARG04 protocol. In this equation, Q_1 and e_p are not directly measured; e_p is directly related to the bit error rate of the single-photon states e_b with the relationships shown in Table I, and Q_1 and e_b may be bounded by assuming the worst-case situation [3] as follows. We may pessimistically assume that the overall gain Q_{signal} is contributed by multi-photon signals as much as possible, and all the errors come from single-photon detection events, leading to $Q_1 = Q_{\text{signal}} - p_{\text{multi}}$ and $e_b = E_{\text{signal}} Q_{\text{signal}}/Q_1$, where p_{multi} is the probability of Alice emitting multi-photon signals. We note that better estimation of e_b and Q_1 can be achieved by using decoy states (e.g. [17]–[19]) leading to higher key generation rates.

IV. COMPARISON

We compute the tolerable QBER for each of the various QKD protocols by finding the highest QBER for which the key generation rate is zero. For the BB84 protocol, the symmetric three-state protocol, and the asymmetric three-state protocol, we find the corresponding tolerable QBER by setting (1) to zero; for the six-state protocol and the SARG04 protocol, we use (2) and (3), respectively. The resulting tolerable QBER's are tabulated in Table II. Note that the tolerable QBER's for different protocols cannot be directly compared since the measurements for the different protocols are different. In order to facilitate the comparison, we model the quantum channel as a depolarizing channel parameterized by a single parameter, the depolarizing rate, and compute the tolerable depolarizing rate corresponding to the tolerable QBER for each protocol. The tolerable depolarizing rate and the relation between it and the QBER are also shown in Table II for each protocol. It can be seen that the six-state protocol can tolerate the highest

Protocol	Tolerable QBER(e_b)	Tolerable depolarizing rate(p)	Relation
BB84	0.1100	0.1650	$e_b = 2p/3$
Six-state	0.1261	0.1891	$e_b = 2p/3$
SARG04	0.09689	0.08046	$e_b = 4p/(3+4p)$
Sym. three-state	0.09812	0.1161	$e_b = 8p/(9+4p)$
Asymmetric three-state	0.04356 ($e_b = \alpha$)	0.06534	$e_b = 2p/3$

TABLE II

TOLERABLE QBER'S AND DEPLORIZING RATES.

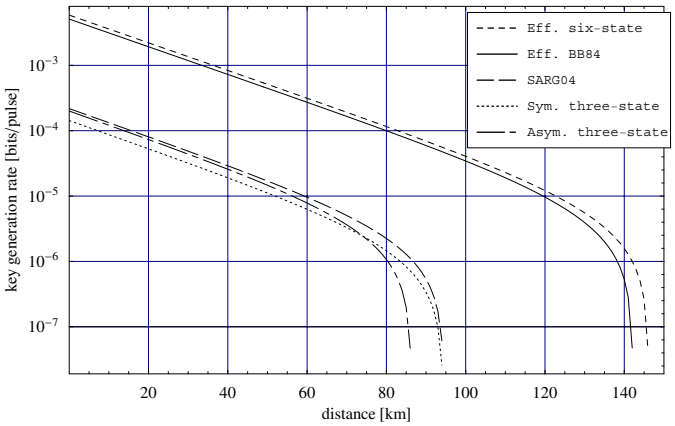

Fig. 1. Comparison between the various QKD protocols using the decoy-state method of [18], in a realistic situation where a coherent source and imperfect detectors are used. The simulation parameters used are from the Gobby-Yuan-Shields (GYS) experiment [20] and we have used $f(E_\mu) = 1.22$. The optimal mean photon numbers, μ, for all curves are used at all distances.

depolarizing rate and thus is the most error resistant among all the protocols shown in Table II. Note that the results for the BB84 and the six-state protocols shown in Table II also hold for the efficient BB84 and the efficient six-state protocols.

We compare the various protocols in a practical situation where a coherent source and imperfect detectors are used. The key generation rates for the protocols are plotted in Fig. 1[1]. We assume that infinite decoy states are used [18] for the purpose of comparison; thus the exact values of e_b and Q_1 (instead of the pessimistic estimation of them) generated by a QKD model are used to calculate the key generation rates. The simulation parameters for the QKD model are from the Gobby-Yuan-Shields (GYS) experiment [20]. It can be seen from Fig. 1 that the efficient BB84 protocol and the efficient six-state protocol outperform the SARG04 protocol, the symmetric three-state protocol, and the asymmetric three-state protocol. Focusing on the BB84 protocol and the six-state protocol, we note that both protocols have the same phase-and-bit-error-rate relation and that mutual information between the phase and bit errors is positive for the six-state protocol. Thus, the efficient six-state protocol always has a higher key generation rate than the efficient BB84 protocol, as both of them have the same retention probability in the basis reconciliation step ($q \approx 1$).

[1]For the SARG04 curve, only the single-photon part is included in the key generation rate for simplicity, even though the two-photon part has been shown in [15], [16] to be secure and may contribute to key bits.

V. CONCLUSIONS

We surveyed a few popular QKD protocols and compared their performances in both the ideal case where a single-photon source is used and the realistic case where a weak coherent source is used. We provided the relations between the bit and phase error rates, which are essential for the security proofs of the protocols. We computed the tolerable QBER's and depolarizing rates of the protocols when a perfect single-photon source is used, and found that the six-state protocol tolerates the highest QBER and depolarizing rate in this case. We also considered the realistic situation where a coherent source is used. The key generation rates of the protocols are plotted against distance and it can be seen that the efficient six-state protocol outperforms the others at any distance.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. of IEEE Int. Conference on Computers, Systems, and Signal Processing*. IEEE Press, New York, Dec. 1984, pp. 175–179.

[2] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, p. 441, 2000.

[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Information and Computation*, vol. 5, pp. 325–360, 2004.

[4] D. Bruβ, "Optimal eavesdropping in quantum cryptography with six states," *Phys. Rev. Lett.*, vol. 81, pp. 3018–3021, 1998.

[5] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," *Phys. Rev. Lett.*, vol. 92, p. 057901, 2004.

[6] S. Phoenix, S. Barnett, and A. Chefles, "Three-state quantum cryptography," *J. Mod. Opt.*, vol. 47, p. 507, 2000.

[7] J.-C. Boileau, K. Tamaki, J. Batuwantudawe, R. Laflamme, and J. M. Renes, "Unconditional security of three state quantum key distribution protocols," *Phys. Rev. Lett.*, vol. 94, p. 040503, 2005.

[8] C.-H. F. Fung and H.-K. Lo, "Security proof of a three-state quantum key distribution protocol without rotational symmetry," *Phys. Rev. A*, vol. 74, p. 042342, 2006.

[9] C. Branciard, N. Gisin, N. Lütkenhaus, and V. Scarani, "Zero-error attacks and detection statistics in the coherent one-way protocol for quantum cryptography," 2006. [Online]. Available: arXiv:quant-ph/0609090

[10] M. Koashi, "Security of quantum key distribution with discrete rotational symmetry," 2005. [Online]. Available: arXiv:quant-ph/0507154

[11] D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, "Discrete rotational symmetry and quantum key distribution protocols," 2006. [Online]. Available: arXiv:quant-ph/0604198

[12] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *J. of Cryptology*, vol. 18, pp. 133–165, 2005.

[13] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, pp. 2050–2056, Mar. 1999.

[14] H.-K. Lo, "Proof of unconditional security of six-state quantum key distribution scheme," *Quantum Inform. and Comp.*, vol. 1, p. 81, 2001.

[15] K. Tamaki and H.-K. Lo, "Unconditionally secure key distillation from multiphotons," *Phys. Rev. A*, vol. 73, p. 010302(R), 2006.

[16] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum-key-distribution protocols," *Phys. Rev. A*, vol. 73, p. 012337, 2006.

[17] W.-Y. Hwang, "Quantum key distribution with high loss: Toward global secure communication," *Phys. Rev. Lett.*, vol. 91, p. 057901, 2003.

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

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

[20] C. Gobby, Z. L. Yuan, and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," *Appl. Phys. Lett.*, vol. 84, p. 3762, 2004.