Method for decoupling error correction from privacy amplification

Hoi-Kwong Lo
Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, 10 King’s College Road, Toronto, Ontario, Canada, M5S 3G4
E-mail: hklo@comm.utoronto.ca

Abstract. In a standard quantum key distribution (QKD) scheme such as BB84, two procedures, error correction and privacy amplification, are applied to extract a final secure key from a raw key generated from quantum transmission. To simplify the study of protocols, it is commonly assumed that the two procedures can be decoupled from each other. While such a decoupling assumption may be valid for individual attacks, it is actually unproven in the context of ultimate or unconditional security, which is the Holy Grail of quantum cryptography. In particular, this means that the application of standard efficient two-way error-correction protocols like Cascade is not proven to be unconditionally secure. Here, I provide the first proof of such a decoupling principle in the context of unconditional security. The method requires Alice and Bob to share some initial secret string and use it to encrypt their communications in the error correction stage using one-time-pad encryption. Consequently, I prove the unconditional security of the interactive Cascade protocol proposed by Brassard and Salvail for error correction and modified by one-time-pad encryption of the error syndrome, followed by the random matrix protocol for privacy amplification. This is an efficient protocol in terms of both computational power and key generation rate. My proof uses the entanglement purification approach to security proofs of QKD. The proof applies to all adaptive symmetric methods for error correction, which cover all existing methods proposed for BB84. In terms of the net key generation rate, the new method is as efficient as the standard Shor–Preskill proof.
# Contents

1. **Introduction** .......................................................... 2  
   1.1. Background .................................................................. 2  
   1.2. First motivation: simplifying the construction of secure protocols for classical post-processing ........................................... 4  
   1.3. Second motivation: proving unconditional security of practical error correction protocols ........................................................................ 5  
   1.4. What is BB84? ............................................................ 6  
   1.5. Why BB84? ............................................................... 7  
   1.6. Organization of the paper ............................................. 7  

2. **Entanglement purification based QKD** .................................. 7  
   2.1. General strategy ......................................................... 7  
   2.2. Application of the general strategy ................................. 8  
   2.3. Entanglement purification based QKD .............................. 8  
   2.4. Symmetric stabilizer-based EPP ..................................... 10  
   2.5. Verification test ......................................................... 11  

3. **The Shor–Preskill proof** .................................................. 13  
   3.1. Reducing an EPP-based QKD protocol to a QECC-based protocol ...................................................................................... 13  
   3.2. Reducing a QECC-based QKD protocol to BB84 .................. 14  
   3.3. Summary of the Shor–Preskill protocol for secure BB84 ............ 15  
   3.4. Security of BB84 with two-way classical communications ........ 16  

4. **Constraint on local commutability** ...................................... 16  
   4.1. Adaptive symmetric error correction .................................. 17  
   4.2. Encrypted adaptive symmetric error correction .................. 17  
   4.3. Error correction in the EPP picture: using ancillary EPR pairs .... 17  

5. **Reduction to BB84** ........................................................ 19  
   5.1. Preliminaries ............................................................. 19  
   5.2. Second main theorem .................................................. 20  

6. **Concluding remarks** ....................................................... 23  

---

1. **Introduction**

1.1. **Background**

The human desire to communicate in secrecy has a long history. Perfectly secure communication and authentication can be performed if two parties, traditionally called Alice and Bob, initially share a long, common, random, secret string of bits. However, how to distribute such a long string in a secure way is a difficult problem that is commonly called the key distribution problem. Conventional key distribution schemes are often based on unproven computational assumptions such as the hardness of factoring. These assumptions may be broken by either a quantum computer [1] or unanticipated future advances in algorithms and hardware. Note that an eavesdropper can save intercepted messages today and wait for future technological advances...
to decode her saved messages. Since some secrets, including government secrets, trade secrets, personal biometric data, and personal health and financial records, are kept for decades, future technological advances are what we should worry about today.

Quantum key distribution (QKD)\[2, 3\] has been proposed as a solution to the key distribution problem. The Heisenberg uncertainty principle implies that it is fundamentally impossible for an eavesdropper to obtain a perfect description of an unknown quantum state. More generally, in quantum mechanics, there is a direct trade-off between information gain and disturbance. The more information an eavesdropper learns about an unknown quantum state, statistically, the more disturbance she will introduce to it. Therefore, Alice and Bob can use parts of their signals to test for tampering. If the error rate of the tested signals is too big (for example, greater than some prescribed number between 10 and 35%), they will throw away the whole transmission. No security is lost because only a random key, rather than sensitive information, has been transmitted. On the other hand, if the statistics of the tested signals are consistent with little eavesdropping, they will proceed with some classical post-processing of their quantum signals to distill out a final secure key. We will return to this classical post-processing issue later.

Unlike conventional key distribution schemes, QKD\[2, 3\] does not need to make assumptions about an eavesdropper’s computing power or technology. Rather, the security of QKD is supposed to be based on the fundamental laws of quantum mechanics. Here, security means basically that (i) the generated key is essentially random and (ii) if Eve has a non-negligible amount of information about the final key, she will almost surely be caught.

There are different classes of eavesdropping attack. A simple class of eavesdropping attack, so-called individual attacks, is for an eavesdropper, Eve, to prepare an independent probe to interact with each individual quantum signal that is sent from Alice to Bob. A measurement is then performed on each probe immediately or after hearing Alice and Bob’s public discussion in their classical post-processing step. In the most general class of eavesdropping attacks, the so-called joint attacks, Eve treats the whole sequence of quantum signals from Alice to Bob as a single entity. She prepares a probe and couples it with the entire sequence of quantum signals. Afterwards, she sends the sequence to Bob and keeps the probe for eavesdropping purposes. In my opinion, it would be too hard to try to quantify the limit of current or near-future technology. Indeed, a subtle quantum cloning attack has recently been experimentally realized\[4\]. Therefore, it is probably simplest to make the most conservative assumption that the eavesdropper can do anything that is consistent with quantum mechanics. A QKD scheme in a well-defined theoretical model that is secure against the most general eavesdropping attack consistent with quantum mechanics is called \textit{unconditionally} secure. Unconditional security is the Holy Grail of quantum cryptography. In particular, because of the lack of independence between various quantum signals in joint attacks, security proofs of QKD against joint attacks (which is the most general type of attack)—unconditional security—is an important but difficult problem in quantum information theory.

Mayers\[5\] and subsequently others\[6, 7\] attacked the problem directly and provided proofs of unconditional security of the BB84 scheme\[2\], which is a standard prepare and measure scheme published by Bennett and Brassard in 1984. In a prepare and measure scheme, Alice prepares a sequence of quantum states and sends them to Bob. Bob measures those quantum states individually. Another approach by myself and Chau\[8\] proved the unconditional security of a QKD protocol that uses reliable quantum computers. This new approach built on the idea of entanglement purification\[9, 10\] and also quantum privacy amplification by Deutsch \textit{et al} \[11\]. It has the advantage of being intuitive and conceptually simple, but unfortunately has
the drawback of requiring quantum computers for its implementation. These two classes of approaches have recently been unified by the work of Shor and Preskill [12], who proved the unconditional security of the BB84 scheme by using the entanglement purification approach and noting its deep connection with the original Mayers proof.

For a review of the Shor–Preskill proof, see, for example, [13], which proved the unconditional security of a QKD scheme based on squeezed states. Recently, Gottesman and myself [14] have generalized the Shor–Preskill proof to protocols involving two-way classical communications, and have shown that those two-way protocols can tolerate much higher quantum bit error rates than any protocols involving only one-way classical communications. For instance, BB84 can tolerate up to about 18.9% with two-way classical communications, whereas it is known that no one-way classical communications protocol for BB84 can be unconditionally secure at an error rate of about 14.6%. Reference [14] also shows that the six-state scheme [15, 16] can tolerate a bit error rate of up to about 26.8%. Since BB84 has been proven to be insecure above 25% by the intercept-resend strategy, the result of [14] demonstrates clearly the advantage of the six-state scheme over BB84 in tolerating a higher bit error rate. I remark that [14] is directly related to the idea of ‘advantage distillation’ [17] in classical information theory. It allows Alice and Bob to perform post-selection on their strings. By doing so, Alice and Bob can generate a secure string even when Eve is sharing a better channel with Alice than that between Alice and Bob. Furthermore, with only one-way classical communications, the unconditional security of the standard six-state QKD scheme [15] up to a quantum bit error rate of 12.7% has been proven in [18] by using the entanglement purification approach. Finally, efficient protocols for QKD, where each user employs the various bases with different probabilities, say $\varepsilon$ and $1 - \varepsilon$, have been proven to be secure in [19].

1.2. First motivation: simplifying the construction of secure protocols for classical post-processing

I shall now return to the classical post-processing stage of the data generated from QKD. A quantum transmission generates data—a raw key—that are generally noisy. Moreover, an eavesdropper may, in principle, control the quantum channel and, therefore, have a non-negligible amount of information on the raw key. The goal of Alice and Bob is to distill out a shorter but essentially completely secure final key from the raw key. To address the above two problems, to remove noises from the signal and to have the confidence of reducing the eavesdropper’s information to a negligible amount, at least two additional steps—error correction and privacy amplification—are needed. Error correction ensures that Alice and Bob will share a common string with a high probability and, roughly speaking, privacy amplification ensures that Eve most likely knows almost nothing about the key.

Analysis of protocols of QKD would be greatly simplified if one could divide up its procedure into different components and analyse each component independently. Suppose it is possible to decouple error correction from privacy amplification. The upshot would be the following. First, one can study error correction and pick the best that one can find. Then, one studies privacy amplification and picks the best that one can find. Finally, one puts the two together and the composite will remain good. This result is reminiscent of the decoupling of source coding from error correction in classical coding theory.

Indeed, I remark that decoupling between error correction and privacy amplification is a very useful simplifying assumption that has been made in many current implementations of
QKD. However, up until now, such a decoupling principle has been proven mainly for restricted attacks such as individual attacks. A brief list of papers that make use of, or are consistent with, this simplifying assumption can be found in [20]. Unfortunately, a general proof of the validity of the decoupling principle for the most general attacks, joint attacks, has been largely missing. This is a highly unsatisfactory situation because it means that a number of well-known protocols, including Cascade [21], have not been proven to provide unconditional security, the Holy Grail of quantum cryptography.

In this paper, I will provide the first proof of the decoupling principle between error correction and privacy amplification in the context of unconditional security. My proof applies to any adaptive symmetric error correction method. In an adaptive symmetric error correction method, Alice and Bob each hold a secret string, \( x \) and \( y \), respectively. At each step \( i = 1, 2, \ldots \), they pick another string, \( a_i \), and publicly announce the parity of \( a_i \cdot x \mod 2 \) and \( a_i \cdot y \mod 2 \). Their choice of the string, \( a_i \), can depend on the relative parities of the earlier strings, \( r_j = (a_j \cdot x) - (a_j = a_j \cdot (x - y)) \), all modulo two, for all \( j < i \), but not on the individual parities, \( a_j \cdot x \) and \( a_j \cdot y \). All existing proposed error correction protocols for QKD can be represented as adaptive symmetric error correction methods. (A more detailed definition of adaptive symmetric error correction methods can be found in section 4.1.) My proof requires a simple modification—that Alice and Bob share some initial secret string, say \( R = (R_1, R_2, \ldots, R_i, \ldots) \) and use it to encrypt the error correction syndrome. In other words, Alice broadcasts \((R_i + a_i \cdot x) \mod 2\) and Bob broadcasts \((R_i + a_i \cdot y) \mod 2\). Note that I allow Alice and Bob to use the same bit \( R_i \) to encrypt both Alice and Bob’s parities—\( a_i \cdot x \mod 2 \) and \( a_i \cdot y \mod 2 \) and yet maintain unconditional security. But we will see that this is indeed the case.

1.3. Second motivation: proving unconditional security of practical error correction protocols

A key motivation of this work is to provide a rigorous proof of unconditional security of practical interactive protocols for error correction in QKD. Let me explain in more detail. In QKD, one often has to perform error correction at a rather high bit error rate of say a few per cent, which is much higher than the typical value of say \( 10^{-5} \) in conventional communications. Moreover, one would like to implement a QKD scheme efficiently. That is to say with a minimal amount of computational power.

The standard theory of error-correcting codes is based on the idea of ‘forward error correction’ [22]. Given say \( k \) bits of classical information, an encoder, Alice, encodes it into an \( n > k \)-bit long string, called a codeword, and sends it through a noisy communication channel. A simple example is a 3-bit repetition code which maps 0 → 000 and 1 → 111. The signal becomes corrupted by noises in the channel. In our example, one of the three bits might flip by mapping 111 to say 101. A decoder, Bob, attempts to correct the error. In our example, assuming that at most one bit has been flipped, Bob performs a majority vote to recover 101 as 1. Note that in standard error-correcting codes, only communication from Alice to Bob is allowed, not from Bob to Alice. For this reason, they are based on forward error correction and are useful for both storage and communication of information. Forward error correction is commonly employed in conventional communications and works efficiently at low error rates of, say, around \( 10^{-5} \). Unfortunately, QKD usually has a high bit error rate of around a few per cent and statistical fluctuations become a major problem for a block code of small size. For this reason, if forward error correction is employed in QKD, a very large block size of order \( 10^5 \) would probably be
needed to achieve a useful (probabilistic) bound on Eve’s information. This translates to a large amount of computing power.

There is a simple solution to the above problem. By allowing two-way communications between Alice and Bob in the decoding step, the required computing power for error detection/correction can be substantially reduced in a high error rate classical communication channel. Standard protocols in high error rate classical communication channels often involve some simple resend strategies. Whenever a decoder detects an error, he will ask the sender to resend the message. Similarly, in the literature of QKD, several such interactive protocols such as ‘BBS’ [23] and ‘Cascade’ [21] and their improved variants (see for example [24]) have been proposed for error correction. The Cascade protocol, invented by Brassard and Salvail, for instance, has the advantage of being computationally highly efficient. It works very well at an error rate of a few per cent.

Another advantage of a two-way communications protocol like Cascade is that it is one of the best protocols for minimizing the number of publicly exchanged bits between Alice and Bob. Note that Eve can listen in freely to all information that is publicly exchanged between Alice and Bob. Therefore, Alice and Bob must take this information leakage to Eve into account. In the original Cascade paper [21], the amount of information leaked is bound by considering individual attacks only. In this restricted case, the information leakage is found to be quite close to Shannon’s limit and is closely related to the number of bits exchanged between Alice and Bob. Therefore, Cascade gives a high key generation rate (see [21] and [24] for details). It is a priori a hard problem to work out the amount of information leakage for the most general type of attacks. (Intuitively, one might expect that the total number of bits exchanged between Alice and Bob, which is twice the number of bits broadcast by Alice (because Bob broadcasts the same number of bits in a symmetric protocol), would give an upper bound to the information leakage to Eve. For individual attacks where Eve measures her system immediately after eavesdropping, the above expectation is correct except for a factor of 2 [25]. That is to say, each bit disclosed in public discussion will shorten the final key by at most two bits. For independent individual attacks where Eve measures her system immediately after eavesdropping, the above expectation is exactly correct [25]. That is to say, each bit disclosed in public discussion will shorten the final key by at most one bit. For a general attack, whether the above expectation is correct is still open.)

Owing to the above two advantages, i.e. requiring limited computational power and giving high key generation rate, Cascade is well suited for implementations. Unfortunately, up until now, proofs of security of the Cascade scheme are restricted to individual attacks only. In other words, a proof of unconditional security of a QKD scheme based on Cascade (and followed by, for example, a standard Shor–Preskill [12] or Mayers [5] privacy amplification procedure) has been missing. A key contribution of this paper is to provide such a proof. The proof of security here applies to not only Cascade, but also any adaptive symmetric protocol for error correction.

Finally, I note that the proposed method can be employed as a sub-routine in concatenated entanglement purification procedures, including those involving two-way classical communications, as studied by [14] and those involving degenerate codes [18].

1.4. What is BB84?

The best-known QKD scheme is BB84 [2], in which the sender, Alice, prepares and sends to the receiver, Bob, a sequence of single photons randomly in one of the four polarizations,
horizontal, vertical, 45° and 135°. Bob then performs a measurement randomly along one of the two polarization bases—rectilinear and diagonal. BB84 is an example of standard prepare-and-measure protocols, which can be executed without quantum computers.

1.5. Why BB84?

I emphasize that standard protocols like BB84 have been well studied and are near practical. Therefore, they have served as useful benchmarks in the investigations of unconditional security of QKD [5]–[7, 12, 14]. Note that a security proof of a more practical set-up (weak coherent states, lossy channels and inefficient detectors, etc) has been presented by Inamori *et al* [26] by generalizing Mayers’ proof\(^1\). Perhaps it is natural to expect that security of BB84 can be extended to more realistic set-ups. In any case, BB84 is the best-known QKD protocol and has been the standard benchmark in many security analyses of QKD. With this understanding in mind, this paper will focus on standard protocols such as BB84 only and leave the important but complex issues of imperfections (weak coherent states, lossy channels and inefficient detectors, etc) for future investigations.

1.6. Organization of the paper

The organization of this paper is as follows. In section 2, the entanglement purification approach to QKD will be reviewed in detail. Section 3 is a review of the Shor–Preskill proof. In section 4, I will discuss the constraint in local commutability and introduce adaptive symmetric protocols for error correction. The connection between an encrypted version of the adaptive symmetric error correction method and a generalized breeding protocol in entanglement purification will be noted. Section 5 contains the main result—proof of the unconditional security of BB84 that includes an encrypted version of an adaptive symmetric method for error correction combined with an arbitrary privacy amplification protocol (that is based on phase error correction).

2. Entanglement purification based QKD

2.1. General strategy

In section 2.3, I will discuss QKD protocols that are based on the idea of ‘entanglement purification’. I remark that general theories of entanglement purification, which are a generalization of quantum error correction, have been developed in the last few years. A key advantage of the entanglement purification approach to security proofs of QKD is the following: one can apply general theories of entanglement purification developed in the last few years to study security of the standard BB84, thus allowing a transparent and conceptually simple understanding of unconditional security of a standard protocol in a systematic language. By turning on the relationship between entanglement purification and QKD, QKD is likely to become one of the first real-life (i.e., experimentally accessible) arenas for the application of abstract concepts in entanglement purification.

\(^1\) Inamori *et al*’s [26] proof is a very nice and important theoretical result. Yet it still contains some notable assumptions. For instance, for any given quantum signal, the detection efficiency is assumed to be independent of the measurement basis by Bob. In future investigations, it is important to re-examine those assumptions in theory and practice.
The overall strategy of the entanglement purification approach, adopted in the present paper, can be summarized as follows: first, one constructs an entanglement purification based QKD scheme and proves its unconditional security using ideas from entanglement purification. Second, one shows that the unconditional security of such an entanglement purification based protocol implies the unconditional security of a standard protocol such as BB84.

2.2. Application of the general strategy

In the entanglement purification approach to QKD, one sees clearly that there is originally a non-trivial constraint between the two processes (error correction and privacy amplification): namely, the corresponding measurement operators employed by Alice and Bob must be locally commuting. Such a local commutability constraint means that the two processes a priori are not totally decoupled from each other. However, I will make the key observation that this local commutability constraint can be automatically satisfied if one introduces perfect ancillary EPR pairs shared by Alice and Bob and allows them to collect their measurement outcomes into those ancillary EPR pairs. So, such an entanglement based QKD protocol can be shown to be unconditionally secure.

Now, following the general strategy outlined above, I will show that the unconditional security of this entanglement purification based protocol implies the unconditional security of the standard BB84 where Alice and Bob encrypt their communication in the error correction stage by using one-time-pad encryption.

2.3. Entanglement purification based QKD

Entanglement purification is useful for correcting errors in a quantum communicating channel. Suppose Alice and Bob share $N$ imperfect EPR pairs. By applying local quantum operations and classical communications, they can purify them into a smaller number, say $m$ pairs, of essentially perfect EPR pairs. Such a purification process is called entanglement purification [9, 10]. Entanglement purification is a generalization of quantum error correction. A restricted class of entanglement purification protocols, the ones that can involve only one-way classical communications from Alice to Bob, is mathematically equivalent to quantum error correcting codes, which are useful for the storage of quantum information.

Consider the following entanglement purification based QKD scheme. Alice prepares a sequence of say $2N$ EPR pairs and sends half of each pair to Bob. Owing to channel noises and eavesdropping attacks, those pairs will be corrupted. Alice and Bob randomly sample say $n$ of their pairs and measure each pair randomly along either the rectilinear or diagonal basis to estimate the error rates in the two bases. For simplicity, one may take $n = N$, but a more general choice of $n$ is also possible. See [19] for details. Those $n$ pairs will be called check bits in subsequent paragraphs. If the error rates are too high, they abort. Otherwise, they now apply an entanglement purification protocol (EPP) $C$, which attempts to distill from the $N$ remaining impure pairs a smaller number, say $m$, of almost perfectly entangled EPR pairs. They then measure those pairs to generate a secure key by, for example, measurements along a single basis, the Z-axis.

First of all, suppose Alice and Bob share $m$ nearly perfect EPR pairs and generate a key by measuring them. The following theorem shows that Eve cannot have much information on the key.
Theorem 1 [8]. If a density matrix $\rho$ has high fidelity $F$ to a state of $m$ perfect EPR pairs, and Alice and Bob produce their key by measuring individual qubits of $\rho$, then with high probability, Alice and Bob have identical $k$-bit strings with a uniform distribution, and Eve has essentially no information about those strings. In fact, if one considers a set of $\rho_k$ with fidelities $F_k$ for various values of $k$ such that $F_k \to 1$ exponentially with $k$, then Eve’s information also approaches 0 exponentially with $k$.

Proof. The proof consists of two lemmas in the supplementary material to [8]. Lemma A says that high fidelity implies low entropy and lemma B says that the entropy is a bound to the eavesdropper’s mutual information with Alice and Bob.

More specifically, lemma A says the following: if $\langle k \text{ singlets} | \rho | k \text{ singlets} \rangle > 1 - \delta$ where $\delta \ll 1$, then the von Neumann entropy $S(\rho) < -(1 - \delta) \log_2 (1 - \delta) - \delta \log_2 \left( \frac{\delta}{(2^k - 1)} \right)$. Proof of lemma A: if $\langle k \text{ singlets} | \rho | k \text{ singlets} \rangle > 1 - \delta$, then the largest eigenvalue of the density matrix $\rho$ must be larger than $1 - \delta$. The entropy of $\rho$ is, therefore, bound above by that of $\rho_0 = \text{diag}(1 - \delta, \frac{\delta}{(2^k - 1)}, \frac{\delta}{(2^k - 1)}, \ldots, \frac{\delta}{(2^k - 1)})$, which has an entropy $-(1 - \delta) \log_2 (1 - \delta) - \delta \log_2 \left( \frac{\delta}{(2^k - 1)} \right)$.

Lemma B says the following: given any pure state $\phi_{A'B'}$ of a system consisting of two subsystems, $A'$ and $B'$, and any generalized measurements $X$ and $Y$ on $A'$ and $B'$ respectively, the entropy of each subsystem $S(\rho_{A'})$ (where $\rho_{A'}$ is the reduced density matrix, $\text{Tr}_{B'} |\phi_{A'B'}\rangle \langle \phi_{A'B'}|$) is an upper bound to the amount of mutual information between $X'$ and $Y'$. Lemma B is a corollary of Holevo’s theorem [27].

Now, Suppose Alice and Bob share a bipartite state $\rho_{AB}$ of fidelity $1 - \delta$ to $k$ EPR pairs. By applying lemma A, one shows that the entropy of $\rho_{AB}$ is bounded by $S(\rho) < -(1 - \delta) \log_2 (1 - \delta) - \delta \log_2 \left( \frac{\delta}{(2^k - 1)} \right)$.

Let us now introduce Eve to the picture and consider the system consisting of the subsystem, $A'$, of Eve and the subsystem, $B'$, of combined Alice–Bob. (i.e., $B' = AB$). Let us consider the most favorable situation for Eve where she has perfect control over the environment. In this case, the overall (Alice–Bob–Eve) system wavefunction can be described by a pure state, $\phi_{A'B'}$, where Eve controls $A'$ and the combined Alice–Bob controls $B'$. By lemma B, Eve’s mutual information with Alice–Bob’s system is bounded by $(1 - \delta) \log_2 (1 - \delta) - \delta \log_2 \left( \frac{\delta}{(2^k - 1)} \right)$.

Definition: [Bell basis]. Given a pair of qubits, a convenient basis to use is the Bell basis, which has Bell states as its basis vectors. The Bell states are of the form:

\[
\Psi^\pm = \frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle \pm |\downarrow\uparrow\rangle)
\]

and

\[
\Phi^\pm = \frac{1}{\sqrt{2}}(|\uparrow\uparrow\rangle \pm |\downarrow\downarrow\rangle).
\]

It is convenient to label them by two bits such that:

\[
\Phi^+ = 00, \quad \Psi^+ = 01, \quad \Phi^- = 10, \quad \Psi^- = 11.
\]

As discussed in [19], if we demand that Eve’s information is bounded by some small number independent of $k$, then the number of test particles only scales logarithmically with $k$.
Definition: \([N\)-Bell basis and BDSW notation\]. Suppose Alice and Bob share \(N\) pairs of qubits. A convenient basis to use is the \(N\)-Bell basis. That is to say, each basis vector is the tensor product state of \(N\) Bell basis vectors. Following equation (3), it is convenient to label an \(N\)-basis vector by \(2N\) bits. This is the notation employed by Bennett, DiVincenzo, Smolin and Wootters (BDSW) \([9]\).

Definition: \([Pauli\ operator\].\ A Pauli operator, \(P\), is defined as a tensor product of single-qubit operators of the form I (the identity), \(X\), \(Y\) and \(Z\) where \(X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\), \(Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}\) and \(Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\).

Definition: \((stabilizer [28] and [29, p 18]).\ An\ Abelian\ group whose generators are (up to phases \(\pm 1\) and \(\pm i\)) Pauli operators is called a stabilizer group\(^3\).

Remark. In the general theory of quantum error correction, the four single-qubit Pauli operators represent four possible types of errors: I represents the identity, \(X\) represents a bit flip error, \(Z\) represents a phase flip and \(Y\) represents a combined bit and phase error. A general error can be decomposed into a combination of these four types of errors. For \(m\)-qubits, a general error can be decomposed into a linear combination of \(2^{2m}\) possible types of errors.

Definition: \([symmetric\ stabilizer-based\ EPP\].\ An\ EPP\ is called symmetric, stabilizer-based if it involves Alice and Bob measuring the same set of abstract operators, \(M_i\), that are the generators of some stabilizer group.

2.4. Symmetric stabilizer-based EPP

Let us consider entanglement purification in more detail. The following paragraphs follow very closely the discussion in \([13]\) (see \([12, 13]\) for further details). Suppose that Alice and Bob start with \(n\) pairs of \(\Phi = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\). That is to say, ideally, they should share \(\Phi^n\). However, owing to noises, they only share a corrupted version of \(\Phi^n\). They would like to perform entanglement purification to distill out a smaller number, say \(k\), of almost perfect EPR pairs from the \(n\) highly imperfect pairs.

In the Shor–Preskill proof, one focuses on entanglement purification protocols that are directly related to stabilizer codes. Alice and Bob pick in advance a \([n, k, d]\) stabilizer code \([29]\), which encodes \(k\) logical qubits into \(n\) physical qubits and has a minimal distance, \(d\). The codespace is a simultaneous eigenspace of a set of \(n - k\) commuting operators, \(M_i\), \((i = 1, 2, \ldots, n - k)\). It has a dimension \(2^k\). Let also \(\tilde{X}_a\) and \(\tilde{Z}_a\) (where \(a = 1, 2, \ldots, k\) labels the specific logical qubit that the encoded operation acts on) be a set of encoded \(X\) and \(Z\) operators acting on the codespace\(^4\).

\(^3\) Here, I use the canonical representation of a stabilizer group.

\(^4\) So far the discussion is applicable to any stabilizer code and there is no direct connection between the operators, \(\tilde{X}_a, \tilde{Z}_a\), and the measurements in BB84 yet. In any case, each \(\tilde{X}_a\) is an abstract mathematical operation that is not physically performed by Alice or Bob. (Alice and Bob need to measure \(\tilde{Z}_a\) to generate the final key.) However, as will be discussed in section 3.2, Shor and Preskill’s proof specializes in the case where the encoded \(Z\) operator, \(\tilde{Z}_a\), is of the form of a tensor product of some \(Z\) operators on the individual qubits. In this case, Alice and Bob can obtain the value of \(\tilde{Z}_a\) by measuring the individual qubits along the \(Z\)-axis directly and computing some parity function of their measurement outcomes.

New Journal of Physics 5 (2003) 36.1–36.24 (http://www.njp.org/)
Note that the Bell state $\Phi$ is a simultaneous eigenstate with eigenvalue +1 of the two commuting operators $X_A \otimes X_B$ and $Z_A \otimes Z_B$, where $X_A$ and $Z_A$ act on Alice’s qubit and $X_B$ and $Z_B$ act on Bob’s qubit. The uncorupted $n$-Bell state $\Phi^N$ is a simultaneous eigenstate of the following set of commuting operators:

$$M_i \otimes M_{i'}, \quad i = 1, 2, \ldots, n-k$$
$$\bar{X}_a \otimes \bar{X}_{a'}, \quad a = 1, 2, \ldots, k$$
$$\bar{Z}_a \otimes \bar{Z}_{a'}, \quad a = 1, 2, \ldots, k.$$ (4)

For simplicity, in what follows I will assume that all the eigenvalues of the above operators are +1 for the state $\Phi^N$. (If some of the eigenvalues are $-1$, a similar argument still applies after a simple relabelling of eigenvalues and a change in the identity of the encoded state, which remains maximally entangled and, therefore, useful for secure key generation.) Suppose Alice and Bob both measure $M_i$ ($i = 1, 2, \ldots, n-k$) in their laboratories. If the state is the uncorrupted $\Phi^N$, Alice and Bob’s measurement outcomes are identical. Moreover, since the operators $M_i, \bar{X}_a$ and $\bar{Z}_b$ all commute with each other, the measurement of $M_i$ in no way affects the measurement outcomes of $\bar{X}_a$ and $\bar{Z}_b$. Notice that the eigenvalue of each of the operators, $\bar{X}_a \otimes \bar{X}_{a'}$ and $\bar{Z}_a \otimes \bar{Z}_{a'}$, is +1 for the state $\Phi^N$. One concludes that the measurement of $M_i$ by Alice and Bob simply gives rise to an encoded state $\Phi^k$ in the subspace with some specified eigenvalues of $M_i = \pm 1$.

If the initial state shared by Alice and Bob is noisy, Alice’s measurement outcome of $M_{i,A}$ will generally no longer match Bob’s measurement outcome of $M_{i,B}$. Let Alice and Bob broadcast those measurement outcomes. Then, the relative measurement outcome, $M_{i,A} \cdot M_{i,B}$, is called the error syndrome because it will tell them what types of errors have occurred. Alice and Bob can then attempt to correct the errors by applying some so-called recovery operator on their system.

Alice and Bob now share $k$ encoded EPR pairs with improved fidelity. By measuring $\bar{Z}_a$, $a = 1, 2, \ldots, k$, Alice and Bob obtain a string of $k$ entries, each of which is either +1 or −1. It is, however, convenient to call the +1 eigenstate of $\bar{Z}_a$, $|0\rangle$, and −1 eigenstate, $|1\rangle$, and convert the outcome of a $\bar{Z}_a$ measurement to ‘0’ or ‘1’, according to the label of the eigenstate in the output. By doing so, Alice and Bob share a $k$-bit string that is made up of 0s and 1s.

**Remark on notation.** There is a more mathematical way of saying the same thing. The original notation $\{+1, -1\}$ is just one way of labelling the two objects in a set consisting of two objects. An alternative notation is simply to use 0 and 1. This is done by identifying +1 (−1 respectively) in the first notation with 0 (1 respectively) in the second notation. By using the alternative notation, the final secret key shared by Alice and Bob can be described by a $k$-bit string. This alternative notation has the advantage of being directly compatible with the notation of the mathematics of a finite field of two elements, as is commonly used in classical coding theory.

### 2.5. Verification test

To foil eavesdropping attacks, Alice and Bob generally need to test for tampering. For simplicity, this can be done by random sampling. Instead of sharing $n$ EPR pairs, Alice and Bob should initially share $M$ EPR pairs. They can pick a random sample of $m$ pairs to compute the bit error rate in the $X$ basis and another random sample of $m$ pairs to compute the bit error rate in the $Z$ axis. Only when both bit error rates are sufficiently small will Alice and Bob use the remaining $n = M - 2m$ pairs to generate a secure $k$-bit key using a $[[n, k, d]]$ stabilizer code.
Definition: [correlated Pauli strategies]. An eavesdropper, Eve, is said to be employing a correlated Pauli strategy if she applies a Pauli operator, $\mathcal{P}_i$, to the quantum signals with some probability $p_i$.

While Eve may use any eavesdropping strategy, the following theorem states essentially that, to consider security, one only needs to consider correlated Pauli strategies.

**Theorem 2 (adapted from [8]).** Suppose Alice creates $M$ EPR pairs and sends half of each to Bob. Alice and Bob then test the error rates, $p_X$ and $p_Z$, along the $X$ and $Z$ bases for randomly chosen disjoint subsets, $D_1$ and $D_2$, each of $m \ll M$ objects respectively. If the error rate is too high, they abort. Otherwise, they perform an EPP $\mathcal{C}$ on the remaining $n = M - 2m$ pairs to try to distill out $k$ EPR pairs of high fidelity. Suppose the EPP $\mathcal{C}$ can correct up to $n(p_X + \varepsilon)$ phase errors and up to $n(p_Z + \varepsilon)$ bit-flip errors. Define a Hilbert subspace $\mathcal{H}_{\text{good}}$ of the $n$ EPR pairs to be the subspace spanned by $n$-Bell states with good error patterns (i.e., with up to $n(p_X + \varepsilon)$ phase errors and up to $n(p_Z + \varepsilon)$ bit-flip errors). Let us denote the projection operator into $\mathcal{H}_{\text{good}}$ by $\Pi$. Then, we have the following:

Given any eavesdropping strategy, $S_1$, by Eve, there exists a correlated Pauli strategy, $S_2$, by Eve that will yield exactly the same values to the following two important quantities:

(i) $P(\text{verification test is passed by the test sample } |D_1, D_2)$ and

(ii) $\text{tr}(\Pi \rho)$,

for all choices of $D_1$, and $D_2$.

**Sketch of proof.** The ‘commuting observables’ idea in [8] is employed. An eavesdropping strategy is defined by the choice of an ancilla and the unitary transformation between the combined system of the ancilla and the $M$ EPR pairs. Given any eavesdropping strategy $S_1$ by Eve, let us consider a fixed but arbitrary choice of sampling subsets, $D_1$ and $D_2$. Let $O_{D_1, D_2}$ be the observable that determines whether the verification test is passed. Recall that $\Pi$ is defined as the projection operator into the good (i.e., correctable) Hilbert subspace. Consider also $W$, the observable that gives the $2M$-bit string representing the state $w$ in the BDSW notation. Since all the observables, $O_{D_1, D_2}$, $\Pi$, and $W$ are simultaneously diagonalizable in the $M$-Bell basis, they all commute with each other. Therefore, it is mathematically consistent to assign probabilities to the simultaneous eigenvalues of those observables, thus giving rise to the two quantities $P(\text{verification test is passed by the test sample } |D_1, D_2)$ and $\text{tr}(\Pi \rho)$ for all possible choices of $D_1$, and $D_2$.

Now, imagine applying a hypothetical measurement $W$ to Alice and Bob’s state before the measurements of $O_{D_1, D_2}$ and $\Pi$. Given that $W$ commutes with $O_{D_1, D_2}$ and $\Pi$, a prior measurement of $W$ in no way affects the outcomes of measurements of $O_{D_1, D_2}$ and $\Pi$. In other words, if Eve pre-measures the state in the $N$-Bell basis (i.e., measures $W$), neither the probability of passing the verification test, nor the probability of being in the good Hilbert subspace will be affected by such a prior measurement. However, with such a prior measurement, Eve has reduced her eavesdropping strategy $S_1$ to a correlated Pauli strategy, $S_2$.

**Remark.** This commuting observables idea applies to all symmetric stabilizer-based EPPs including ones that involve two-way classical communications.

Theorem 2 is telling us that one can treat the two important quantities—(i) the probability of passing a verification test and (ii) the probability of being in the good Hilbert subspace, $\text{tr}(\Pi \rho)$—as classical. In essence, one can apply classical sampling theory to a quantum problem.

Furthermore, $\text{tr}(\Pi \rho)$ provides a bound to the fidelity of the corrected EPR pairs:
Theorem 3 [12, 13]. Consider a stabilizer-based EPP \( \mathcal{C} \) which distills \( k \) EPR pairs from \( n \) impure pairs. Suppose \( \mathcal{C} \) works perfectly in a Hilbert subspace \( \mathcal{H}_{\text{good}} \), which is spanned by Bell states with good error patterns (i.e., correctable by \( \mathcal{C} \)). Denote the projection operator onto \( \mathcal{H}_{\text{good}} \) by \( \Pi \). If we apply the EPP \( \mathcal{C} \) to an initial state \( \rho \), then the fidelity of the recovered state as \( k \) EPR pairs is bound below by

\[
F \equiv \langle \tilde{\Phi}^{(k)} | \rho_{\text{rec}} | \tilde{\Phi}^{(k)} \rangle \geq \text{tr}(\Pi \rho). \tag{5}
\]

Here, \( \rho_{\text{rec}} \) is the recovered state after error correction, \( \tilde{\Phi}^{(k)} \) is the \( k \)-EPR pair state.

Proof. This theorem follows from standard stabilizer quantum error correcting code (QECC) theory. An explicit proof of essentially the same result can be found in [13].

3. The Shor–Preskill proof

Because of theorem 3, EPP based QKD schemes are particularly convenient to analyse. Unfortunately, they are difficult to implement because they generally require Alice and Bob to possess quantum computers. A key insight of Shor and Preskill is to remove the requirement of quantum computers by showing that, in fact, the unconditional security of a special class of EPP based QKD schemes implies the unconditional security of BB84. This section follows closely the discussion in [13].

More concretely, Shor and Preskill considered a special class of quantum error-correcting codes, called Calderbank–Shor–Steane (CSS) [31, 32] codes (see below for properties of CSS codes) and proved the following theorem:

Theorem 4 [12]. Given an EPP-based QKD scheme that is based on a CSS code and a verification procedure that involves only two bases, its unconditional security implies the unconditional security of a BB84 scheme.

Remark. Similarly, when the verification procedure involves three bases, an analogous theorem shows that the unconditional security of an EPP-based QKD scheme that is based on a CSS code implies the unconditional security of the six-state scheme.

Here, I will recapitulate the proof of theorem 4 in [12]. It can be done in two steps: first, reduce an EPP-based QKD protocol to a quantum-error-correcting-code-based (QECC-based) QKD protocol. Second, reduce the QECC-based QKD protocol to BB84.

3.1. Reducing an EPP-based QKD protocol to a QECC-based protocol

Here, I show how to turn an EPP-based QKD protocol to one based on a quantum error-correcting code. The key point is that Alice can perform all her measurements on her halves of the EPR pairs before sending the other halves to Bob. The argument [12] is closely related to those in [8]. Commutability will play a key role in the following discussion.

More concretely, first of all, Alice can measure all her check bits before transmitting the other halves to Bob. This corresponds to Alice preparing the check bits in the four random polarizations as in BB84. Second, since her measurement operators \( M_{i,A} \) commute with those of Bob, she has the liberty of measuring \( M_{i,A} \) before, rather than after, the transmission of quantum signals to Bob. Let the specific outcomes be \( M_{i,A} = m_i \). Third, Alice also can measure \( \tilde{Z}_{a,A} \) before or after the transmission. Let the specific outcomes be \( \tilde{Z}_{a,A} = K_a \). It is convenient
to convert the string \( K = (K_1, K_2, \ldots, K_k) \), which is made up of +1s and −1s into a binary string of 0s and 1s by simply relabelling +1s as 0s and −1s as 1s. Let us also call the relabelled string simply \( K = (K_1, K_2, \ldots, K_k) \), which is the secret key generated by QKD. Note that if Alice measures those values before the quantum transmission, the resulting protocol will be mathematically equivalent to her choosing a random \( k \)-bit key \( K \), encoding it in a \([n, k, d]\) quantum error-correcting code in the eigenspace of \( M_{i,A} = m_i \) and then transmitting it to Bob.

### 3.2. Reducing a QECC-based QKD protocol to BB84

To reduce the protocol further, one specializes to a class of quantum codes—CSS codes discovered by Shor and Calderbank [31] and also by Steane [32]. A CSS code is a stabilizer-based quantum code with generators that are either (i) tensor products of the identities and \( Z \) only or (ii) tensor products of the identities and \( X \) only. It has the advantage that the phase and bit-flip error correction procedures are totally decoupled from each other.

Let us define a CSS code. Consider a binary linear classical code \( C_1 \) and its subcode \( C_2 \), as in standard classical coding theory [22]. Let \( H_1 \) be the parity check matrix of \( C_1 \). From standard classical coding theory, the parity check matrix of \( C_2 \) which is a subcode of \( C_1 \) can be written in the form \( \left( \begin{array}{c} H_1 \\ P \end{array} \right) \) for some submatrix, \( P \). Also, let \( H_2 \) be the generator matrix of \( C_2 \) (and, thus, the parity check matrix of \( C_2^\perp \), the dual code of \( C_2 \)). Let \( k_1 \) be the dimension of \( C_1 \) and \( k_2 \) the dimension of \( C_2 \). Let \((H_1)_{ij} ((H_2)_{ij} \text{ respectively})\) denote the \((i, j)\)th entry of the matrix \( H_1 \) (\( H_2 \) respectively). A defining feature of a CSS code is the following: its stabilizer generators, \( M_i \), in equation (4) can be divided into two classes, \( M_{Z,i} \) and \( M_{X,i} \) where:

\[
M_{Z,i} = \bigotimes_{j=1}^{n} (Z_j)^{(H_1)_{ij}} \tag{6}
\]

and

\[
M_{X,i} = \bigotimes_{j=1}^{n} (X_j)^{(H_2)_{ij}}. \tag{7}
\]

In other words, \( M_{Z,i} \) are products of \( Z \) only and \( M_{X,i} \) are products of \( X \) only. Since \( H_1 \) has \( n-k_1 \) rows and \( H_2 \) has \( k_2 \) rows, the total number of stabilizer generators listed in equations (6) and (7) is \( n-k_1+k_2 \). This implies the number of encoded qubits, \( k \), is given by \( k = n - (n-k_1+k_2) = k_1-k_2 \).

Note that the bit-flip error correction and phase-flip error correction procedures are decoupled. Indeed, from the measurements of the \( Z \) generators in equation (6), one finds the bit-flip error syndrome and corrects bit-flip errors. Independently, from the measurements of the \( X \) generators in equation (7) one finds the phase-flip error syndrome and corrects the phase-flip errors.

Given some arbitrary but fixed simultaneous eigenvalues for the stabilizer generators, \( M_{Z,i} \) and \( M_{X,i} \), say

\[
M_{Z,i} = (-1)^{\alpha_u}, \quad M_{X,i} = (-1)^{\beta_u}, \tag{8}
\]

the basis elements of the codespace can be represented by

\[
|\phi_{u}\rangle_{z,x} = \frac{1}{|C_2|^{1/2}} \sum_{v \in C_2} (-1)^{u \cdot v} |u + v + z\rangle, \tag{9}
\]

where \( u \in C_1 \) and \( x, z \) are \( n \)-bit strings such that

\[
H_1 z = \alpha, \quad H_2 x = \beta. \tag{10}
\]
Note that, if $u_1 - u_2 \in C_2$, then $|\phi_{u_1}\rangle = |\phi_{u_2}\rangle$, up to an overall phase. Therefore, the codeword (i.e., basis elements) of a CSS code are in one-to-one correspondence with the cosets of $C_2$ in $C_1$.

Now, consider the whole QKD process. Alice picks random $u \in C_1$, and transmits $|\phi_u\rangle_{z,x}$ to Bob. Bob acknowledges receipt of the quantum signals. Alice broadcasts the bit-flip error syndrome, $\alpha$, and the phase-flip error syndrome, $\beta$. Bob compares Alice’s broadcast syndrome with the outcomes of his own stabilizer measurements and determines the relative error syndrome, which tells him the actual error of the transmission. He can perform both bit-flip and phase error correction. Assuming that the error correction procedure is successful, he will recover the original state, $|\phi_u\rangle_{z,x}$, transmitted by Alice. Now, Bob measures the encoded $Z$ operators to recover the key. For CSS code, this can be simply done by Bob measuring all the $Z$ operators of the physical qubits. He obtains the string $u + v + z$. Bob works out the most likely string $z$ that will give $H_1 z = \alpha$. Bob subtracts $z$ from $u + v + z$ to get $u + v$. Bob applies $P$ to the string and obtains $P(u + v) = Pu + Pv = Pu$ as the final key. Note that $Pu$ only depends on the coset $C_2$ of the element $u \in C_1$.

Note that Bob obtains the key value by measuring the operator $Z$ on each qubit. While the bit-flip error syndrome, $\alpha$, is important for obtaining the value of the key, the phase-flip error correction syndrome, $\beta$, in no way affects the value of the key. That is to say, Bob does not really need the value of $\beta$ for key extraction. Therefore, Shor and Preskill reached the following surprising conclusion: Alice does not need to send the value of $\beta$ at all! Now, suppose Alice does not send $\beta$ to Bob, the effect will be equivalent to averaging the state $|\phi_u\rangle_{z,x}$ for all values of $x$. For any fixed but arbitrary $u$, Alice is sending

$$
\sum_{v_1, v_2} \frac{1}{|C_2|} \sum_{x} (\text{Tr})_{v_1, v_2}^{|u + v_1 + z\rangle, \langle u + v_2 + z|} = \frac{1}{|C_2|} \sum_{u \in C_2} (u + v + z)\langle u + v + z|,
$$

which is equivalent to a mixture of the state $|u + v + z\rangle$. Let us denote $u + v$ by $w$. Note that $w$ is simply a codeword in $C_1$.

### 3.3. Summary of the Shor–Preskill protocol for secure BB84

In summary, one can describe the Shor–Preskill protocol for an unconditionally secure BB84 scheme as follows. Alice sends a random string $w + z$ using photons to Bob. Owing to channel noises, Bob receives a corrupted string $w + z + e$. Alice then gives the bit-flip syndrome $\alpha$ to Bob, which allows him to obtain the likely error $z$ (using the equation $H_1 z = \alpha$). Bob subtracts $z$ from his string to obtain $w + e$. Using the error correcting capability of $C_1$, Bob corrects the error from $w + e$ to recover $w$. Finally, Bob computes $Pw = P(u + v) = Pu + Pv = Pu$ as the final key shared between him and Alice. (Recall that $\begin{pmatrix} H_1 \\ P \end{pmatrix}$ is the parity check matrix of $C_2$.)

Using CSS codes and theorem 4, BB84 is proven to be secure up to an error rate of 11% by Shor and Preskill.
3.4. Security of BB84 with two-way classical communications

By using two-way classical communications, BB84 can be made secure at a much higher error rate of about 18.9%. This is due to the following theorem by Gottesman and myself [14], which generalizes theorem 4.

**Theorem 5 [14]**. Suppose a two-way EPP satisfies the following conditions:

1. **Symmetric.** It can be described as a series of measurements $M_i$, with both Alice and Bob measuring the same $M_i$.
2. **CSS-like.** Each of its generators $M_i$ can be written as either (a) a product of $X$ only or (b) a product of $Z$ only.
3. **Locally commuting.** Each pair of $M_i$ and $M_j$ commute locally on Alice’s (or Bob’s) side.
4. **Conditional on $Z$ only.** All conditional operations depend on the result of measuring $Z$ operators only.

**Claim.** The above protocol can be converted to a standard ‘prepare-and-measure’ QKD scheme with security equal to the EPP-based QKD scheme.

**Remark.** Here, the notation has been slightly abused. By a product of $Z$ only, I actually mean a product of the identities and $Z$ only. Similarly for $X$.

**Remark.** If the verification stage involves two bases, then the ‘prepare-and-measure’ QKD scheme is BB84. If it involves three bases, then the ‘prepare-and-measure’ QKD scheme is the six-state scheme.

We will refer the readers to [14] for the details of the proof of theorem 5.

4. Constraint on local commutability

Theorem 5 is a strong result in QKD. Nonetheless, the constraint (3) in theorem 5 seriously restricts its applicability. In the EPP picture, the constraint demands that all the local measurement operators that Alice and Bob employ must commute locally with each other. Therefore, one is not at liberty to choose the bit-flip and phase error correction measurement operators independently.

I remark that the local commutability constraint is a big obstacle in the application of theorem 5 to prove the security of interactive Cascade scheme for error correction proposed by Brassard and Salvail [21]. Recall the Cascade protocol involves a binary search subroutine, ‘BINARY’, by Alice and Bob, which allows them to identify the location of an error. The binary search subroutine, BINARY, involves the computation of the parity of a set and subsequently dividing it into two sets and computing the parity of each subset, etc, until the location of the error is found. Note that at the end of BINARY, the size of a subset is reduced to a single object, which means Alice (and also Bob) has to announce the eigenvalue $Z_i$ of a single qubit at location $i$ (i.e., the $i$th qubit). Now, any quantum error correcting procedure that corrects the phase error of the announced bit must also contain a measurement operator $M_i$ for the $i$th qubit. This means that $M$ anti-commutes rather than commutes with $Z_i$. In conclusion,

5 Note that it has been shown that BB84 with only one-way classical communications is necessarily insecure at an error rate of about 15% [33, 34]. Therefore, the result in [14] shows clearly that BB84 with two-way classical communications is definitely better than BB84 with only one-way classical communications.
with the Cascade protocol, it would be impossible to correct all the phase errors. Therefore, the application of theorem 5 to the Cascade protocol looks problematic. However, as will be shown in section 5.2 below, a modified version of the Cascade Protocol can, in fact, be used to obtain an unconditionally secure BB84 protocol. This is one of the main contributions of the present paper.

4.1. Adaptive symmetric error correction

The Cascade protocol belongs to a rather general class of protocols for error correction, the adaptive symmetric method for error correction, which is defined as follow:

Definition: [adaptive symmetric method for error correction]. Suppose Alice has an n-bit string x and Bob has an n-bit string y, which is a corrupted version of x. In an adaptive symmetric method for error correction, Alice picks an n-bit string a_1 and broadcasts a_1 and the parity p_{x,1} = a_1 \cdot x. In this paper, unless otherwise stated, all parities are computed modulo two. Bob broadcasts the parity p_{y,1} = a_1 \cdot y. Alice and Bob compute the relative parity r_1 = p_{x,1} - p_{y,1} = a_1 \cdot (x - y). Now, Alice picks an n-bit string a_2. The choice of a_2 may depend on the value of relative parity, r_1, between Alice and Bob, but not on the individual parities, p_{x,1} and p_{y,1}. Alice then broadcasts a_2 and the parity p_{x,2} = a_2 \cdot x. Bob broadcasts p_{y,2} = a_2 \cdot y. Alice and Bob compute the relative parity r_2 = p_{x,2} - p_{y,2} = a_2 \cdot (x - y). Now, Alice picks an n-bit string a_3. Her choice of a_3 can depend on the value of the relative parities, r_1 and r_2, but not on the individual parities, p_{x,1}, p_{x,2}, p_{y,1}, and p_{y,2}. In total, s < n rounds of the above process are performed. In general, for i = 1, 2, \ldots, s, Alice picks an n-bit string a_i. Her choice of a_i can depend on a_j for j < i and the relative parities, r_j = p_{x,j} - p_{y,j}, for j < i, but not on the individual parities, p_{x,j} and p_{y,j}, for j < i. Alice broadcasts a_i. Alice (Bob respectively) then broadcasts the parity p_{x,i} = a_i \cdot x (p_{y,i} = a_i \cdot y respectively). They compute the relative parity r_i = p_{x,i} - p_{y,i}. This process continues until Alice and Bob have computed all the s relative parities, r_i, for i = 1, 2, \ldots, s. Finally, using the values of the relative parities, r_i = p_{x,i} - p_{y,i} for 1 \leq i \leq s, Bob corrects errors in y by applying a recovery operator \mathcal{R}(y, r_1, r_2, \ldots, r_s) = z. Ideally, z = x and Alice and Bob will now share the same string x.

4.2. Encrypted adaptive symmetric error correction

Note that in an adaptive symmetric method for error correction such as Cascade, only the relative error syndrome between Alice and Bob is of interest. Therefore, given an adaptive symmetric method for error correction, one can construct an encrypted version of an adaptive symmetric method for error correction in which only the relative error syndrome between Alice and Bob, but not the individual error syndromes of Alice and Bob, is publicly broadcast. More concretely, in an encrypted version of an adaptive symmetric method for error correction, Alice and Bob initially share an s-bit of a common secret string, R = (R_1, R_2, \ldots, R_s). Alice broadcasts (R_i + a_i \cdot x) \mod 2, rather than a_i \cdot x \mod 2. Bob broadcasts (R_i + a_i \cdot y) \mod 2, rather than a_i \cdot y \mod 2.

4.3. Error correction in the EPP picture: using ancillary EPR pairs

Let us map the aforementioned encrypted version of an adaptive symmetric method for error correction into the EPP picture. In a corresponding EPP-based QKD protocol, Alice and
Bob are only interested in the measurement outcome of symmetric measurement operators, \( M_i = M_i^A \otimes M_i^B \), rather than the individual outcomes for the operators \( M_i^A \) and \( M_i^B \). Note that \( M_i = M_i^A \otimes M_i^B \) is a global operator involving both Alice and Bob’s systems. Now, a simple method to bring two distant quantum systems (Alice’s and Bob’s) together and allow a global operator to be measured is teleportation. To achieve teleportation, some ancillary EPR pairs must be shared by Alice and Bob. This motivates the basic insight of the current paper—to use ancillary EPR pairs to compute the relative error syndrome.

Instead of teleportation, a more efficient way of measuring the global error syndrome will be employed. Here is a main theorem of the current paper.

**Theorem 6** Suppose Alice and Bob share a number of impure EPR pairs and they would like to compute \( s \) symmetric global operators each of the form \( M_i = M_i^A \otimes M_i^B \). The choice of \( M_i \) can be adaptive (i.e., depends on the measured values of the previous \( M_j \) for \( j < i \)). As before, by symmetric, we mean that \( M_i^A \) is the same as \( M_i^B \) except that they act on Alice’s and Bob’s Hilbert spaces respectively and \( M_i^A \) is a Pauli operator. Suppose further that they would like to know only the eigenvalues of \( M_i \), but otherwise leave the state unchanged. The claim is that they can do so with \( s \) ancillary EPR pairs.

**Remark.** It should be emphasized that in theorem 6 above, only global measurements are performed. Local measurements of \( M_i^A \) and \( M_i^B \) are not performed at all.

**Sketch of proof.** The notation is such that an EPR pair is an eigenstate of \( ZZ \) and \( XX \), with eigenvalue +1 for both. Let us call the two qubits of the \( j \)th EPR pair shared by Alice and Bob, \( A'_j \) and \( B'_j \) respectively. For each operator, \( M_i \), Alice measures \( M_i^A \otimes Z_{A'_i} \) and broadcasts her outcome and Bob measures \( M_i^B \otimes Z_{B'_i} \) and broadcasts his outcome. The relative outcome, the product of \( M_i^A \otimes Z_{A'_i} \otimes M_i^B \otimes Z_{B'_i} \) gives the eigenvalue of the operator \( M_i \) (because the state of the ancillary EPR pair gives an eigenvalue +1 for the operator \( Z_{A'_i} \otimes Z_{B'_i} \)). More importantly, by an explicit calculation analogous to the argument in teleportation, one can show that no disturbance to the state is made except for the determination of the eigenvalue of \( M_i = M_i^A \otimes M_i^B \).

The above theorem employs a generalization of the so-called breeding method for EPP studied in [10] (see also [9]). In [9], the breeding method was only mentioned in passing because it had been superseded by the standard hashing method, which can be performed without ancillary EPR pairs. Let me call a general EPP that involves ancillary EPR pairs a generalized breeding protocol/method. In contrast to prior art, here I notice that the generalized breeding protocol appears to be not reducible to a non-breeding protocol. In fact, it appears to be more powerful because it allows the decoupling of error correction from privacy amplification. In summary, the decoupling of error correction from privacy amplification is achieved at the price of introducing ancillary EPR pairs shared by Alice and Bob.

I remark that the calculation of \( M_i^A \otimes Z_{A'_i} \) (and similarly \( M_i^B \otimes Z_{B'_i} \)) in theorem 6 can, indeed, be done by local quantum gates. The actual quantum circuit diagram is very similar to the ones discussed in, for example, [9] and [10]. Since the actual construction is outside the main theme of this paper, the details will be skipped here.

**Remark.** Later in this paper, in theorem 7, a mapping from an EPP-based QKD protocol to a prepare-and-measure protocol will be described. In such a mapping, a generalized breeding protocol, as described in theorem 6, is a subroutine in an EPP-based QKD protocol and is mapped to the aforementioned encrypted version of an adaptive symmetric method for error correction.
5. Reduction to BB84

5.1. Preliminaries

First of all, some definitions:

**Definition:** [privacy amplification based on symmetric phase error correction]. In a symmetric phase error correction method, Alice and Bob initially share say \( n \) EPR pairs. They are then given a \( t \times n \) parity check matrix, \( H_2 \), for some code, say \( C_2^\perp \). Let \( Q \) denote the \( (n-t) \times n \) parity check matrix for \( C_2 \). Both Alice and Bob then compute \( t \) operators, \( M_{X,i} \), where

\[
M_{X,i} = \bigotimes_{j=1}^{n} (X_j)^{(H_2)_{ij}}. \tag{12}
\]

In other words, \( M_{X,i} \) are products of individual qubit operators of the form \( I \) and \( X \) only. They broadcast the measured values of \( M_{X,i} \) and \( M_{X,i}^b \). The relative values of \( M_{X,i}^b \) with respect to \( M_{X,i} \) (for \( i = 1, 2, \ldots, t \) ) give the phase error syndrome. Alice and Bob then correct phase errors using the code \( C_2^\perp \). Now Alice and Bob share \( n \) EPR pairs of improved fidelity.

A symmetric phase error correction procedure can be used for privacy amplification. This is done by adding the following steps at the very end. Alice and Bob measure \( Z \) on all qubits to obtain strings \( w_a \) and \( w_b \) respectively. Note that \( w_a = w_b = w \), assuming that, prior to the phase error correction, a bit-flip error correction procedure has been successful in removing bit-flip errors. \( w \) is a string made of \( +1 \)s and \( -1 \)s. One can rewrite \( w \) as a binary string of \( 0 \)s and \( 1 \)s by relabelling \( +1 \)s as \( 0 \)s and \( -1 \)s as \( 1 \)s. (Such a relabelling is a group isomorphism of the modulo 2 addition group in two different representations.) Alice and Bob then perform privacy amplification by computing an \( (n-t) \)-bit string \( Q(w) \) by matrix multiplication. \( Q(w) \) is now their final key.

**Remark.** The above privacy amplification based on the symmetric phase error correction method is very similar to the privacy amplification procedure in the Shor–Preskill proof. A key difference is that in the above privacy amplification procedure, I allow some arbitrary phase error correction method on the \( n \) EPR pairs. In contrast, in the Shor–Preskill proof, the phase error correction procedure is much more restrictive: it is built into the proof by requiring that (i) \( C_2 \) is a subcode of some good code \( C_1 \) and that (ii) the code \( C_1 \) be used for error correction. Because of these differences, whereas in the Shor–Preskill proof the value of the final key is restricted to a coset of \( C_2 \) in \( C_1 \), here, the final key is a general coset of \( C_2^\perp \) in \( \{0, 1\}^n \). Also, whereas in the Shor–Preskill proof the parity check matrix of \( C_2 \) is \( \left( \begin{array}{c} H_1 \\ P \end{array} \right) \), where \( P \) is the privacy amplification matrix in the Shor–Preskill proof, here, the parity check matrix of \( C_2 \) is simply \( Q \), the current privacy amplification matrix.

**Definition:** [directly reducible EPP-based QKD protocol]. Suppose Alice and Bob share \( N \) impure EPR pairs and also \( s \) perfect ancillary EPR pairs. An EPP-based QKD protocol is called directly reducible if it consists of the following steps:

1. Alice and Bob share \( N \) imperfect EPR pairs. They pick a random sample of \( m \) pairs and measure them along the \( X \)-axis to compute the bit error rate along the \( X \)-axis. Similarly, they pick a random sample of \( m \) pairs from the remaining \( N-m \) pairs and measure them along the \( Z \)-axis to compute the bit error rate along the \( Z \)-axis. They abort if either error rate is too large. (Here, I am considering the reduction to BB84. An analogous step for the

New Journal of Physics 5 (2003) 36.1–36.24 (http://www.njp.org/)
six-state scheme will involve Alice and Bob measuring random samples along three rather
than two bases.)

(2) Consider the remaining \( n = N - 2m \) imperfect EPR pairs. Alice and Bob measure an
adaptive set of \( s \) global operators, \( M_{Z,i} = M^{A}_{Z,i} \otimes M^{B}_{Z,i} \) where \( M^{A}_{Z,i} \) is the same as \( M^{B}_{Z,i} \),
except for the fact that \( M^{A}_{Z,i} \) acts on Alice’s subsystem of \( n \) halves of EPR pairs only and
\( M^{B}_{Z,i} \) acts on Bob’s subsystem of the other halves. As shown in theorem 6, this is done by
a generalized breeding method which sacrifices the \( s \) perfect ancillary EPR pairs. Alice
collects the parity of \( M^{A}_{Z,i} \) into her half of an ancillary EPR pair and measures it. She
then broadcasts the result of her measurement. Similarly, Bob collects the parity of \( M^{B}_{Z,i} \)
to his corresponding half of an ancillary EPR pair and measures it. He then broadcasts
the result of his measurement. The relative parity of their measurements gives the value of
\( M^{A}_{Z,i} \otimes M^{B}_{Z,i} \). Those values are the bit-flip error syndrome. Bob applies a recovery operator
on his \( n \) halves of EPR pairs to correct bit-flip errors.

(3) Alice and Bob then perform a symmetric phase error correction method on their \( n \) EPR
pairs. They agree on a \( t \times n \) parity check matrix, \( H_2 \), for some code, say \( C_{⊥}^{2} \). Let \( Q \) denote
the \( (n - t) \times n \) parity check matrix for \( C_{2} \). Both Alice and Bob then compute \( t \) operators,
\( M_{X,i} \), where

\[
M_{X,i} = \bigotimes_{j=1}^{n} (X_j)^{(H_3)_{ij}}. \tag{13}
\]

In other words, \( M_{X,i} \) are products of individual qubit operators of the form \( I \) and \( X \) only.
They broadcast the measured values of \( M^{A}_{X,i} \) and \( M^{B}_{X,i} \). Here, the superscripts \( A \) and \( B \)
label the parity whose measurement we are considering. The relative value of \( M^{A}_{X,i} \) with
respect to \( M^{B}_{X,i} \) (for \( i = 1, 2, \ldots, t \)) gives the phase error syndrome. Alice and Bob then
correct phase errors using the code \( C_{⊥}^{2} \). Now, Alice and Bob share \( n \) EPR pairs of improved
fidelity.

(4) Alice and Bob measure \( Z \) on all qubits to obtain strings \( w_{a} \) and \( w_{b} \) respectively. Note that
\( w_{a} = w_{b} = w \), assuming that the bit-flip error correction procedure in step 1 above has
been successful in removing bit-flip errors. Note that \( w \) is made up of +1s and −1s. Alice
and Bob convert \( w \) into a string (which, for convenience, is also called \( w \)) that is made up of
0s and 1s by simply relabelling +1s as 0s and −1s as 1s. Afterwards, they perform privacy
amplification by computing an \( (n - t) \)-bit string \( Q(w) \) by matrix multiplication, which is
their final key.

Remark. Since in the EPP picture, steps 2 and 3 above can clearly correct bit-flip and phase
errors, the above EPP-based QKD protocol is unconditionally secure. It is immaterial whether
the measured operators \( M_{Z,i} \) and \( M_{X,j} \) commute or not. This is quite different from the Shor–
Preskill proof where the measured operators \( M^{A}_{Z,i} \) and \( M^{A}_{X,j} \) are assumed to commute.

5.2. Second main theorem

Here is the second main theorem of the current paper.

Theorem 7 A directly reducible EPP-based QKD protocol, as defined above, can be converted
to a standard ‘prepare-and-measure’ QKD scheme such as BB84 with security equal to the
EPP-based QKD scheme. The net key generation rate is \( n - t - s \)-bit. In the reduced
protocol, Alice and Bob must initially share an \( s \)-bit random uniformly distributed secret string,
$R = (R_1, R_2, \ldots, R_s)$ and use $R$ to encode the parities exchanged in an adaptive symmetric method for error correction that is reduced from step 2. In other words, Alice broadcasts $S_i^A = (R_i + a_i \cdot x) \mod 2$ and Bob broadcasts the value of $S_i^B = (R_i + a_i \cdot y) \mod 2$, where $x$ and $y$ respectively are Alice and Bob’s raw keys and $a_i$ is the string induced from $M_{Z,i}$. More specifically, if $M_{Z,i} = \bigotimes_{j=1}^n (Z_j)^{(H_1)_{ij}}$, then the $j$th component of $a_i$ is $(H_1)_{ij}$.

**Remark.** Note that the same key $R_i$ is used to encode both Alice and Bob’s parities, $a_i \cdot x$ and $a_i \cdot y$. This is because the relative error syndrome is allowed to be disclosed to Eve.

**Remark.** In more detail, the procedure for error correction/privacy amplification of the reduced protocol goes as follows:

1. Alice and Bob initially share a string of an $s$-bit randomly and uniformly distributed secret, $R = (R_1, R_2, \ldots, R_s)$.
2. Alice sends Bob a sequence of say $4n(1 + \delta)$ quantum signals as in BB84.
3. Bob measures the quantum signals randomly in the two conjugate bases and acknowledges to Alice receipt of quantum signals.
4. Alice and Bob broadcast their bases and throw away the polarization data that are transmitted and received in different bases, keeping only the $2n$ quantum signals that are transmitted and received in the same bases. They abort if there are less than $2n$ such kept signals.
5. Alice and Bob test for tampering by, for example, computing the error rate of a randomly chosen test sample of say $n$ such signals. If the error rate is too large, they abort.
6. Alice now converts her polarization data into an $n$-bit string, $x$, which is her raw key. Similarly, Bob converts his polarization data into an $n$-bit string, $y$, which is his raw key.
7. Alice and Bob apply an *encrypted* version of an adaptive symmetric method for error correction to their raw keys. They do so by adaptively choosing $s$ strings, $a_1, a_2, \ldots, a_s$. If $M_{Z,i} = \bigotimes_{j=1}^n (Z_j)^{(H_1)_{ij}}$, then the $j$th component of $a_i$ is $(H_1)_{ij}$. For $i = 1, 2, \ldots, s$, Alice broadcasts the encrypted parity, $S_i^A = (R_i + a_i \cdot x) \mod 2$ and Bob broadcasts the encrypted $S_i^B = (R_i + a_i \cdot y) \mod 2$. (Note that the same bit $R_i$ is used to encode both Alice and Bob’s parities, $a_i \cdot x$ and $a_i \cdot y$.) For each $i$, the choice of $a_i$ may depend on the previous relative parities, $R_i = S_i^A + S_j^B \mod 2 = a_j \cdot (x - y) \mod 2$, for $j < i$.
8. Bob applies a recovery operator $R(y, R_1, R_2, \ldots, R_s, a_1, a_2, \ldots, a_s) = z$. Ideally, $z = x$.
9. Alice and Bob each apply the same pre-agreed privacy amplification matrix $Q$ to his/her string, $x$, to obtain $Q(x)$ by matrix multiplication. $Q(x)$ is their final key.

**Sketch of proof.** Combine the proofs of theorems 5 and 6. In other words, the proof of theorem 6 can be used to relax the constraint of local commutability in the Gottesman–Lo proof, thus giving theorem 7. In more detail, following BDSW [9], one uses the $n$-Bell basis and labels each of the $n$-Bell basis vectors by $2n$ bits. In other words, the $2n$-bit string represents the state of the $n$ pairs of qubits shared between Alice and Bob. Consider (a subroutine of) an EPP starting from $n$ pairs of qubits shared between Alice and Bob and resulting in $k$ pairs of qubits shared between Alice and Bob. Such an EPP induces a *classical* deterministic mapping of a $2n$-bit string to a $2k$-bit string, which represents the state of the remaining $k$ pairs of qubits after the EPP.

First, consider bit-flip error correction. If a generalized breeding protocol is applied, the induced classical deterministic mapping is the *identity* map from a $2n$-bit string to a $2n$-bit string. Yet Bob can learn the bit-flip error syndrome from Alice to correct all bit-flip errors with high...
probability. From [14], it is not too hard to see that the EPP can be reduced to BB84 with an encrypted version of an adaptive symmetric error correction.

Next, consider phase error correction. Here comes the key point. Note that, in an adaptive symmetric bit-flip correction method, $n$ (imperfect) EPR pairs are always left behind and the induced classical map is always the identity map. Therefore, for phase error correction, the same phase error correction circuit, independent of the actual bit-flip error correction procedure, can be applied by Alice and Bob. This is the underlying reason why error correction can be decoupled from privacy amplification. Now, as noted in [12, 14], the phase error correction procedure in an EPP-based QKD scheme can be reduced to a parity extraction procedure in BB84. I argue that the final key is given by $Q(w)$ in such a parity extraction procedure. □

**Corollary.** A modified version of the Shor–Preskill protocol where Alice and Bob share a $s$-bit secret string with $s > nH(p)$ where $p$ is the bit error rate and use it to encode the error correction syndrome, $\alpha$, can be proven to be unconditionally secure.

**Remark.** In the modified Shor–Preskill protocol in the above corollary, the initial ancillary secret shared by Alice and Bob is at least of length $nH(p)$, where $n$ is the length of the raw key. The final key length is at most $n(1 - H(p))$, due to the need for privacy amplification. Therefore, the net key generation rate of the modified Shor–Preskill protocol in the above corollary is bound by $n(1 - H(p) - H(p)) = n(1 - 2H(p))$. Asymptotically, the bound is exactly the same as that in the original Shor–Preskill proof and the net key generation rate of the modified Shor–Preskill protocol in the above corollary is positive up to a bit error rate of about 11%. This shows clearly that the protocols investigated in the current paper can give competitive key generation rates.

**Corollary.** As an application of theorem 7, the following protocol for error correction/privacy amplification of QKD is unconditionally secure. Step 1: the Cascade scheme for error correction, modified by the one-time-pad encryption of its error syndrome, followed by step 2: a random hashing procedure [5, 12].

**Remark.** Reference [24] found that the number of exchanged bits in BBBSS, Cascade and a modified version of Cascade (introduced in [24]) are all less than $n/2$ at an error rate of 0.075. This implies that, asymptotically, the net key generation rate, $R_{\text{key}}$ for those protocols $R_{\text{key}} > n(1 - 0.5) - H(0.075) > 0$ at an error rate of 7.5% for BB84. This shows clearly that there is a parameter region where the Cascade scheme (modified by one-time-pad encryption of the error syndrome introduced in the current paper) can be made unconditionally secure. While Cascade and its variants are known to be secure against individual attacks, this is the first time that a modified version of the Cascade protocol has been proven to be unconditionally secure. Since the resulting protocol is computationally efficient and can tolerate a rather high error rate of at least 7.5%, this new result is of practical interest.

For schemes involving concatenation, there is the following theorem

**Corollary 8** Suppose an EPP, $\mathcal{C}$, is a concatenation of two subroutines, $S_1$ and $S_2$, where the first subroutine, $S_1$, satisfies all the conditions in theorem 5 (i.e., symmetric, CSS-like, locally commuting and conditional on $Z$ only) and the second subroutine, $S_2$ satisfies theorem 7. Then, the protocol $\mathcal{C}$ can be converted to a prepare-and-measure QKD protocol with the same security, provided that Alice and Bob initially share an $s$-bit secret string and use it for one-time-pad encryption of the error syndrome in subroutine $S_2$.

The upshot of the above corollary is that the decoupling result remains valid even when concatenated codes are employed [14].
6. Concluding remarks

In summary, I have considered a rather general class of entanglement purification schemes, more specifically, adaptive symmetric schemes and their reduction to BB84. It was shown that in those schemes the procedure for error correction can be decoupled from the procedure for privacy amplification. The decoupling is achieved by requiring Alice and Bob to share an initial string and use it for the one-time-pad encryption of the error syndrome. This is no change in the net key generation rate, for at least the case of the Shor–Preskill proof, because the loss of this initial string will be exactly compensated by the generation of a longer key. As a corollary, I prove the unconditional security of the Cascade scheme, modified by one-time-pad encryption of error syndrome, followed by a random hashing privacy amplification procedure at a bit error rate as high as 7.5%. This is an efficient scheme in terms of both key generation rate and computational power. Note that, in prior art, Cascade and its variants have only been proven to be secure against individual attacks. This is the first time that a variant of Cascade has been proven to be unconditionally secure.

Acknowledgments

I particularly thank Norbert Lütkenhaus for helpful discussions and for bringing to my attention the question of the security proof of the Cascade scheme. Enlightening discussions with Tsz-Mei Ko on forward error correction and two-way schemes for error detection/correction are gratefully acknowledged. I am also grateful for helpful conversations with colleagues including William Buttler, Daniel Gottesman, Philippe Grangier, Debbie Leung, John Preskill and Peter Shor.

References

[1] Shor P W 1997 Algorithms for quantum computation: discrete logarithms and factoring Proc. 35th Annual Symp. on Foundations of Computer Science (USA, Nov. 1994) (Piscataway, NJ: IEEE) Shor P W 1997 SIAM J. Comput. 26 1484–509
[2] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (Piscataway, NJ: IEEE) pp 175–9
[3] Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661–3
[4] Lamas-Linares A, Simon C, Howell J C and Bouwmeester D 2002 Science 296 712–14 (published online March 28, 2002; 10.1126/science.1068972)
[5] Mayers D 2001 Unconditional security in quantum cryptography J. Assoc. Comp. Mach. 48 351–406 A preliminary version in Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels Advances in Cryptology —Proc. Crypto’96 (New York: Springer) pp 343
[6] Biham E, Boyer M, Boykin P O, Mor T and Roychowdhury V 2000 A proof of security of quantum key distribution Proc. 32nd Annual ACM Symp. on Theory of Computing (New York: ACM) p 715
[7] Ben-Or M 2002 presentation at Introductory Workshop in Quantum Computation http://zeta.msri.org/calendar/talks/TalkInfo/1416/show_talk
[8] Lo H-K and Chau H F 1999 Unconditional security of quantum key distribution over arbitrarily long distances Science 283 2050–6 (Preprint quant-ph/9803006)
[9] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Phys. Rev. A 54 3824
[10] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 Phys. Rev. Lett. 76 722
[11] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 Phys. Rev. Lett. 77 2818
   Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1998 Phys. Rev. Lett. 80 2022 (erratum)
[12] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution scheme Phys. Rev. Lett. 85 441–4
[13] Gottesman D and Preskill J 2000 Secure quantum key distribution using squeezed states Preprint quant-ph/0008046
[14] Gottesman D and Lo H-K 2001 Proof of security of quantum key distribution with two-way classical communications IEEE Trans. Inf. Theory 49 457 (Preprint quant-ph/0105121)
[15] Bruss D 1998 Optimal eavesdropping in quantum cryptography with six states Phys. Rev. Lett. 81 3018–21
[16] Gisin N and Wolf S 1999 Quantum cryptography on noisy channels: quantum versus classical key-agreement protocols Phys. Rev. Lett. 83 4200–3
[17] Maurer U M 1993 IEEE Trans. Inf. Theory 39 733–42
   Maurer U M and Wolf S 1999 IEEE Trans. Inf. Theory 45 499–514
[18] Lo H-K 2001 Proof of unconditional security of six-state quantum key distribution scheme Quantum Inf. Comput. 1 81–94
[19] Lo H-K, Chau H F and Ardehali M 2001 Efficient quantum key distribution scheme and proof of its unconditional security available at http://xxx.lanl.gov/abs/quant-ph/0011056
[20] Slutsky B, Rao R, Sun P C, Tancevski L and Fainman Y 1998 Appl. Opt. 37 2869–78
   Gilbert G and Hamrick M 2001 Preprint quant-ph/0106043
   Slutsky B, Rao R, Sun P C and Fainman Y 1998 Phys. Rev. A 57 2383–98
   Bennett C H, Brassard G, Crépeau C and Maurer U 1995 IEEE Trans. Inf. Theory 41 1915–23
[21] Brassard G and Salvail L 1993 Secret key reconciliation by public discussion Advances in Cryptology: Eurocrypt’93 Proc. pp 410–23
[22] MacWilliams F J and Sloane N J A 1977 The Theory of Error-Correcting Code (Amsterdam: North-Holland)
[23] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography J. Cryptol. 5 3–28
[24] Sugimoto T and Yamazaki K 2000 IEICE Trans. Fundam. Electron. Commun. Comput. Sci. A 83 1987–91
[25] Cachin C and Maurer U M 1997 J. Cryptol. 10 97–110
[26] Inamori H, Lütkenhaus N and Mayers D 2001 Unconditional security of practical quantum key distribution Preprint quant-ph/0107017
[27] Holevo A S 1973 Probl. Inf. Transm. (USSR) 9 117
[28] Gottesman D 1998 The Heisenberg representation of quantum computers Preprint quant-ph/9807006
[29] Gottesman D 1997 Stabilizer codes and quantum error correction PhD Thesis Caltech (Preprint quant-ph/9705052)
[30] Bennett C H, Brassard G, Crépeau C and Maurer U M 1995 Generalized privacy amplification IEEE Trans. Inf. Theory 41 1915–23
[31] Calderbank A R and Shor P 1996 Good quantum error correcting codes exist Phys. Rev. A 54 1098–105
[32] Steane A M 1996 Multiple particle interference and error correction Proc. R. Soc. A 452 2551–77
[33] Fuchs C, Gisin N, Griffiths R B, Niu C S and Peres A 1997 Optimal eavesdropping in quantum cryptography. I Phys. Rev. A 56 1163
[34] Cirac I and Gisin N 1997 Coherent eavesdropping strategies for the 4-state quantum cryptography protocol Phys. Lett. A 229 1