

Fast, efficient error reconciliation for quantum cryptography

W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson
University of California, Los Alamos National Laboratory, Los Alamos, New Mexico 87545
 (Received 19 March 2002; revised manuscript received 24 January 2003; published 15 May 2003)

We describe an error-reconciliation protocol, which we call Winnow, based on the exchange of parity and Hamming's "syndrome" for N -bit subunits of a large dataset. The Winnow protocol was developed in the context of quantum-key distribution and offers significant advantages and net higher efficiency compared to other widely used protocols within the quantum cryptography community. A detailed mathematical analysis of the Winnow protocol is presented in the context of practical implementations of quantum-key distribution; in particular, the information overhead required for secure implementation is one of the most important criteria in the evaluation of a particular error-reconciliation protocol. The increase in efficiency for the Winnow protocol is largely due to the reduction in authenticated public communication required for its implementation.

DOI: 10.1103/PhysRevA.67.052303

PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum cryptography [1] presents special problems in regard to error correction of noisy quantum communications. Under the constraint that the public channel can be authenticated, and the assumption that all public communications can be eavesdropped, classical information on the exchanged qubits must be revealed through a series of public discussions to test the quantum-key integrity and to remove the errors. Discrepancies within the qubits, observed as errors, must be treated as having been introduced by a hostile eavesdropper; the eavesdropper is generally referred to as Eve and labeled E in this work.

In a classical environment, *all* errors can *always* be removed with the condition that to remove all errors one may have to reveal all information. However, within the secrecy framework imposed by quantum-key distribution (QKD), revealed information, reduces privacy and the effective channel capacity. Because of this, great care must be taken to reveal a minimal amount of information to remove errors from quantum-key, while accounting for the leaked information to ensure key integrity after errors are removed.

Within this context of QKD, the two parties that exchange qubits over a quantum channel [Alice (A) and Bob (B) are the notation typically used within the quantum cryptography community] must have a fast and efficient method to mend the quantum-key; in addition, they must also reduce E 's knowledge gained during public discussions to a vanishingly small amount. These constraints require that any error-reconciliation protocol will also need supporting protocols to provide a complete framework for quantum cryptographic security. That is, a useable QKD system will comprise a quantum-key transmitter (A) and receiver (B), and a series of protocols to remove errors and account for and mitigate the information leakage attributable to E . The series of protocols includes [2,3], but is not necessarily limited to the following: error reconciliation [4,5], privacy amplification [6], and signature authentication [7].

In addition to these protocols, we acknowledge a protocol generally formulated in Ref. [4] that we refer to as privacy maintenance. We also note that the predecessor to CASCADE [5]—the best known and probably the most widely used

error-reconciliation protocol—is also generally formulated in Ref. [4] and is characterized by a binary search; here, we refer to the binary search, which is a major element of CASCADE, as BINARY. A fundamental difference between BINARY and CASCADE is that CASCADE neglects privacy maintenance: all data are retained until the necessary privacy amplification is performed on the error-free data. We observe that the reconciliation process is more efficient if privacy maintenance is implemented during reconciliation as will become obvious in the following discussion.

Finally, this work introduces an error-reconciliation protocol that uses a Hamming code [8,9] to remove errors. We refer to this protocol as Winnow. Which is characterized by the application of a parity test, a conditional Hamming hash, and privacy maintenance.

II. HAMMING ERROR DETECTION AND CORRECTION

The application of the Hamming hash function for error correction [8,9] is illustrated as follows.

First, after A and B exchange qubits on the quantum channel, A and B then divide their random bits into blocks of length $N_h = 2^m - 1$. (Due to the 1:1 correlation of these data, we henceforth refer to these blocks as a single data or bit block.) The m -bit ($m \geq 3$) syndromes S_a and S_b are then calculated, where S_a and S_b , respectively, depend only on A 's or B 's bits in a particular block.

Next, B transmits his syndrome to A and errors are only discovered if the syndrome difference S_d (*exclusive or* of S_a with S_b) is nonzero:

$$S_d = S_a \oplus S_b \neq \{0\}^m. \quad (1)$$

Finally, m bits are deleted from each bit block to eliminate the potential loss of privacy to E due to the (classical) communication of B 's syndromes: m bits of information are revealed on each block for which S_b is revealed reducing the channel capacity per symbol by m/N_h [10].

Specifically, data privacy is maintained by removal of m bits from each block at the $\{2^j\}$ positions, where $j \in \{0, \dots, m-1\}$. These bits are independent in the syndrome calculations as seen below in the matrix $h^{(m)}$,

$$h^{(3)} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}, \quad (2)$$

where for this particular matrix $m \equiv 3$. We refer to the operation of discarding bits in this manner [4] as *privacy maintenance*.

As a final comment on Eq. (2), note that the transpose of $h^{(3)} \equiv [h^{(3)}]^T$ are the binary equivalent numbers 1 to 7, and is generalized such that $[h^{(m)}]^T \equiv \{1, \dots, (2^m - 1)\}$, N_h binary numbers.

The matrix $h^{(m)}$ is a special form of the hash function [11] and is represented by

$$h_{i,j}^{(m)} = \left[\frac{j}{2^{i-1}} \right] \pmod{2}, \quad (3)$$

where $i \in \{1, \dots, m\}$ and $j \in \{1, \dots, N_h\}$; arithmetic is modulo 2.

The Hamming algorithm always corrects any single error within any N_h -bit block, but the effect of the Hamming algorithm, which is related to the *syndromes* and *privacy maintenance*, is less clear in the event that more than one error exists in a bit block. Such considerations are now discussed in detail in terms of the syndromes.

The syndromes S_a and S_b are formed by contraction of the N_h -bit blocks with the matrix $h^{(m)}$:

$$S_i = \left(\sum_{j=1}^{N_h} X_j h_{i,j}^{(m)} \right) \pmod{2} \in \{0, 1\}^m, \quad (4)$$

where subscript i represents syndrome bit i in the m -bit binary syndrome, X_j represents bit $j \in A$'s or B 's block, and $S = \{S_i\}$ is the binary syndrome value of either B 's or A 's block. Understanding the effect of the syndromes in locating and correcting errors is crucial to assessing the performance of the Hamming algorithm, and thus the Winnow protocol.

The syndrome difference [Eq. (1)] defines a binary number that gives the location of a single bit in A 's or B 's code word that when toggled from $0 \rightarrow 1$ or from $1 \rightarrow 0$ affects the syndrome difference S_d , such that when the syndrome difference is recalculated it gives the binary number $S'_d \equiv \{0\}^m$. The result is that the changing of the single bit indicated by the nonzero syndrome difference in the one code word either corrects an error, or introduces another, in that code word. This is no great mystery but rather reflects the fact that Hamming codes are n - k codes. In this case, $n = 2^m - 1$ relates the number of bits in each code word N_h , and $k = n - m$ relates the channel capacity (the channel capacity is $k/n \Leftrightarrow k/N_h$ per bit) given the code (a Hamming code in this discussion).

In an n - k Hamming code, there are $2^{(2^m - 1)}$ unique code words characterized by 2^m unique syndromes; further, there are 2^k code words with the same syndrome. Because this code can correct one error, it has a minimum Hamming dis-

tance of $d = 3$. This also means it can detect at least two errors. In fact the Hamming distance d for the Hamming code is $d \equiv 3$.

By definition, a code word with a single error will have $S_d \neq \{0\}^m$ (can obviously detect a single error if it can correct a single error). In addition, if a code word has exactly two errors then by definition $S_d \neq \{0\}^m$ (can detect at least two errors if it can correct a single error). Therefore, if a code word has exactly two errors, then after applying the Hamming algorithm, and after changing the bit value indicated by S_d , the code word will finish with exactly three errors. The proof is by contradiction; if a code word with two errors finished with one error (an error was corrected), then the new syndrome difference would be nonzero. Contradiction also proves that one error is corrected if there is exactly one error: If an error was introduced the syndrome difference would again be nonzero. Thus, in examining Hamming codes, we observe that a code word with one error will finish with zero error, but a code word with exactly two errors finishes with exactly three errors. In each case, the new syndrome difference changes such that $S'_d = \{0\}^m$.

By symmetry, if an N_h -bit code word contains exactly $N_h - 1$ errors (all the bits except one are in error), then after application of the Hamming algorithm all the bits in the code word will be in error. Further, a code word that contains $N_h - 2$ errors will finish with $N_h - 3$ errors, i.e., one of the errors is corrected.

The above arguments imply that a Hamming code only works well if the probability of two or more errors is low relative to the likelihood of a single, or no, errors. In either case, the Hamming code is inefficient as m bits are revealed in the syndrome (this fact is discussed in detail later).

The difficult question to answer in analyzing the performance of a Hamming code is how does the Hamming algorithm affect code words with more than two, but less than $2^{(m-1)}$, errors?

It is not obvious, but the number of code words with three errors and $S_d \equiv \{0\}^m$ is related to the number of ways two-error code words map to a code word with three errors (and $S_d = \{0\}^m$). In other words, there must be a way to arrange three errors in a code word and still maintain $S_d = \{0\}^m$. Lacking this would mean that the code could always detect more than two errors with a Hamming distance of $d = 3$.

To complete the Hamming efficiency analysis, how code words with three or more errors are affected after application of the Hamming algorithm must be analyzed. For three errors, it is now obvious that there must be at least $2^m - 1$ ways to start with three errors in an N_h -bit code word and still finish with three errors. In the case that there exist three errors in a code word, and $S_d \neq \{0\}^m$, then an error will be introduced into the N_h -bit code word because if the code word finished with two errors then $S_d \neq \{0\}^m$ —a contradiction.

As a special case (example), consider $m = 3$. There are $\binom{7}{3} = 35$ ways to arrange three errors in seven bits. Because there are exactly seven nonzero syndrome differences for $m = 3$ and exactly two errors, there must be *at least* seven ways to arrange three errors in seven bits and have S_d

$\equiv \{0\}^m$. In fact, for this special case this is the result. What this means is that, statistically, seven in 35 code words with three errors will finish with three errors, and 28 in 35 words with three errors will finish with four errors. Thus, code words that start with three errors will finish with 19/5 errors per seven-bit block, in the limit of an infinite number of seven-bit blocks with exactly three errors. By symmetry, it is obvious that given an infinite number of seven-bit blocks with exactly four errors, the final error rate per block would be 16/5—a lower final error rate.

Thus, what is needed is a way to calculate, for any number m of parity checks, in the Hamming algorithm, a way to calculate the number of ways to arrange the initial number of errors per block and finish with $S_d = \{0\}^m$ or with $S_d \neq \{0\}^m$. Equation (5) permits that calculation for any initial number of errors per block n_i , given any initial block size N_h :

$$\begin{aligned} N_{S_d \neq 0} + N_{S_d = 0} &= \binom{N_h}{n_i} - N_{S_d \neq 0} + N_h N_{S_d = 0} \\ &= (-1)^q N_h \binom{\frac{N_h - 1}{2}}{p} \\ &\Leftrightarrow \begin{bmatrix} N_{S_d \neq 0} \\ N_{S_d = 0} \end{bmatrix} = \begin{bmatrix} N_h & 1 \\ -1 & 1 \end{bmatrix}^{-1} \\ &\quad \times \begin{bmatrix} \binom{N_h}{n_i} \\ (-1)^q \binom{\frac{N_h - 1}{2}}{p} \end{bmatrix}, \end{aligned} \quad (5)$$

where $q = \lceil n_i/2 \rceil$, $p = \lfloor n_i/2 \rfloor$, n_i is the initial number of errors per Hamming block of $N_h = 2^m - 1$ bits per block; in this situation, $N_{S_d = 0}$ gives the number of syndrome differences with $S_d = \{0\}^m$ and $N_{S_d \neq 0}$ gives the number of syndrome differences with $S_d \neq \{0\}^m$. Equation (5) is generalized by dividing both sides by the total number of ways to arrange n_i errors in the N_h bits. In this situation, we find a more useful quantity

$$\Pi_{S_d = 0} = \frac{N_{S_d = 0}}{\binom{N_h}{n_i}}, \quad (6a)$$

and

$$\Pi_{S_d \neq 0} = \frac{N_{S_d \neq 0}}{\binom{N_h}{n_i}}. \quad (6b)$$

This result is required later.

These arguments are not obviously general for the case of $m > 3$, but they give insight into the general problem. The

difficulty with the special case of $m = 3$ and $n_i = 3$ is that the next case of $n_i = 4$ is symmetric and complementary with $n_i = 3$, as mentioned previously. Further, as was noted, there is no path to map three errors to two errors as $S_d \neq \{0\}^m$, when there are exactly two errors. However, Eq. (6) is the general technique to calculate the quantities specified, i.e., the number of ways to map n_i errors to $S_d = \{0\}^m$ or not, given $N_h = 2^m - 1$ bits in a block.

Given these facts, how the errors change for $m \geq 4$ and $4 \leq n_i < 2^{(m-1)}$ is the general result of interest.

Let $n_i^{(+)}$ be the number of ways to increase the number of errors from n_i to $n_i + 1$, in a bit block, and $n_i^{(-)}$ the number of ways to decrease the number of errors from n_i to $n_i - 1$; of course, the considerations relate to $m \geq 4$. The results are as follows:

$$\begin{aligned} n_i^{(+)} &= N_{S_d = 0}(N_h | n_i) + (n_i + 1) N_{S_d \neq 0}(N_h | n_i + 1) \\ n_i^{(-)} &= \binom{N_h}{n_i} - n_i^{(+)}, \end{aligned} \quad (7)$$

where $N_{S_d = 0}(N_h | n_i + 1)$ is the number of ways to arrange $n_i + 1$ errors in N_h bits and obtain $S_d = \{0\}^m$ (the reader will recall that earlier it was stated that the number of ways to get $S_d = \{0\}^m$ for $n_i + 1$ errors is directly related to the number of ways to map $n_i \mapsto n_i + 1$ errors); of course, $N_{S_d \neq 0}(N_h | n_i)$ is the number of ways to arrange n_i errors in N_h bits and get $S_d \neq \{0\}^m$. Thus, the generalized probability for the number of errors n_i to increase or decrease is

$$\Pi^{(+)} = \frac{n_i^{(+)}}{n_i^{(+)} + n_i^{(-)}} \quad (8a)$$

and

$$\Pi^{(-)} = 1 - \Pi^{(+)}. \quad (8b)$$

III. WINNOW PROTOCOL

As a general rule, the ideal error correcting protocol would correct all bit errors in each bit block, introduce no additional bit errors, and reveal a minimal amount of information on the key bits to an eavesdropper through public communication. The outlined Hamming protocol has a number of shortcomings regarding this ideal. First, the difference syndrome S_d does not distinguish between single- and multiple-bit errors. Therefore, additional errors may be introduced if instances of $S_d \neq \{0\}^m$ are treated as due to single errors. Second, up to m bits of information are exchanged for each data block reducing channel capacity per symbol with each exchange: information which can be compromised by eavesdropping.

One solution is to eliminate all bits within data blocks for which $S_d \neq \{0\}^m$. This certainly removes the possibility of introducing additional bit errors into the key, but, unfortunately, the efficiency of such a method is low as *every* block loses either m bits to privacy maintenance, or all bits because $S_d \neq \{0\}^m$. The efficiency of this approach is not optimal as

most of the discarded bits or blocks for which $S_d \neq \{0\}^m$ are probably not in error.

Another, more powerful solution is to introduce a preliminary parity comparison on a block of $N=2^m$ bits and to make a comparison of the syndromes S_a and S_b , conditional upon the result of the parity comparison.¹

If the block parities do not agree, an odd number of errors exists in the N -bit block. Moreover, if the bit errors are distributed randomly throughout the data, and if the number of errors is sufficiently small, then an odd number of errors in a block probably indicates a single error that can be corrected by the additional application of the Hamming algorithm. For example, in the situation that a block contains 1-bit error, if $S_d = \{0\}^m$ then the first bit is in error. (By symmetry it is clear that if there are exactly $N-1$ errors in the block the first bit would not be in error.) Thus, this approach always allows the correction of a single error in the N bits, i.e., if the bits are to be retained. However, in the protocol outlined here the one bit is regularly discarded for privacy maintenance (for the exchanged parity bit) and the Hamming algorithm is applied to the remaining N_h bits, as previously discussed, and then $\lceil \log_2(N_h) \rceil$ additional bits are discarded to complete the privacy maintenance giving a channel capacity of $(2^m - m - 1)/N$ per symbol on blocks that contain an initial parity error. This appears to be an additional loss of channel capacity, but because the syndromes are not exchanged and compared, when the block parities agree, the channel capacity actually increases over the basic Hamming algorithm; 1 bit is still discarded from the blocks that do not exhibit a parity error for privacy maintenance. We refer to this error-reconciliation protocol as Winnow.

The Winnow protocol reveals $\log_2(N)+1$ bits in two classical communications when the parities on the N bits do not agree: m bits for the syndrome and 1 bit for parity; conversely, the Winnow protocol reveals 1 bit of information in one classical communication when the parities agree.²

Therefore, the amount of key data discarded is

$$N_{dis}^{odd} = \log_2(N) + 1 = m + 1 \quad (9)$$

¹R. W. Hamming discusses the addition of a parity check on the $N_h = 2^m - 1$ bit block [9] (pp. 47–48; pp. 213–214). His conclusion is that A and B are more likely to introduce additional errors than correct errors by changing a bit if $S_d \neq \{0\}^m$ and the block-parities agree. In this situation, A and B could either remove the $m+1$ bits required to ensure privacy on the remaining bits (which may remove errors), or they could eliminate all of the bits in question, as $n_i \in \{2, 4, \dots, 2^m - 2\} > 1$. The expanded protocol described in this effort allows the detection of an even or odd number of errors and prevents a correction attempt on those data blocks with even numbers of errors. This is important since the Hamming algorithm will increase the number of errors in blocks that have $2 \leq n_i \leq N_h/2$.

²Exchanging the parity on $N=2^m$ bits instead of $N_h=2^m-1$ bits results in slightly higher channel capacity. That is, more information is revealed when the syndrome information is combined with the parity information on a N_h -bit block than is revealed when the parity and syndrome are revealed on N bits in the Winnow protocol.

bits for blocks with odd numbers of errors such that the fraction of the bits remaining after privacy maintenance is

$$\mu_{pm}^{odd} = 1 - \frac{N_{dis}^{odd}}{N}. \quad (10)$$

For $N \in \{8, 16, 32, 64, 128\}$, $\mu_{pm}^{odd} \in \{0.5, 0.69, 0.88, 0.89, 0.94\}$, respectively. Also,

$$\mu_{pm}^{even} = 1 - \frac{1}{N} \quad (11)$$

and $\mu_{pm}^{even} \in \{0.88, 0.94, 0.97, 0.98, 0.99\}$ for the same values of N . In either case, the appropriate overhead for the classical communications is also removed immediately from the data, so that the privacy of the bits is at least maintained if not improved.

All single-bit errors in an N block are guaranteed to be either eliminated or corrected after a single pass of the Winnow protocol (SPW). What remains to be considered is how blocks with multiple errors affect the overall efficiency of the Winnow protocol.

IV. WINNOWN EFFICIENCY

Define the change in number of errors in a given block and for a given initial number of errors as $\Delta n = n_f - n_i$, where n_i and $n_f \equiv n_f(n_i|N)$ are the initial and final numbers of bit errors in a block prior to and after a SPW, respectively. The average change in the number of errors, for a given number of initial errors, after a SPW (this step includes elimination of the parity bit but not the final m bits required for completion of the privacy maintenance step) can be expressed as

$$\overline{\Delta n} \equiv \langle \Delta n(n_i) \rangle = \sum_{\Delta n=-2}^1 \Delta n p(\Delta n|n_i), \quad (12a)$$

where

$$\sum_{\Delta n=-2}^1 p(\Delta n|n_i) = 1 \quad (12b)$$

and $p(\Delta n|n_i)$ is the probability that the number of errors will change by $\Delta n \in \{-2, -1, 0, 1\}$ given an initial condition of n_i errors in an N -bit data block. The $p(\Delta n|n_i)$ of interest can be written more instructively as

$$\begin{aligned} p(+1|n_i) &= \pi^{(n)} \Pi_{S_d \neq 0}(n_i) \Pi^{(+)}(n_i), \\ p(\pm 0|n_i) &= \pi^{(n)} \Pi_{S_d=0}(n_i) + \pi^{(y)} \Pi_{S_d \neq 0}(\delta n_i) \Pi^{(+)}(\delta n_i), \\ p(-1|n_i) &= \pi^{(n)} \Pi_{S_d \neq 0}(n_i) \Pi^{(-)}(n_i) + \pi^{(y)} \Pi_{S_d=0}(\delta n_i), \\ p(-2|n_i) &= \pi^{(y)} \Pi_{S_d \neq 0}(\delta n_i) \Pi^{(-)}(\delta n_i), \end{aligned} \quad (13)$$

where, n_i is as previously defined, $\delta n_i \equiv n_i - 1$, $\pi^{(y \vee n)}$ depends only on the initial number of errors n_i in the N -bit block and is the probability the bit discarded for privacy

TABLE I. \bar{n}_f for $N=8$ for various stages in the Winnow protocol (note that the Hamming algorithm is not applied to blocks that contain an even number of errors).

n_i	0	1	2	3	4	5	6	7	8
\bar{n}_f^p	0	0.88	1.75	2.63	3.5	4.38	5.25	6.13	7
\bar{n}_f^{ph}	0	0	1.75	3.5	3.5	3.5	5.25	7	7
\bar{n}_f	0	0	1.75	2.0	3.5	2.0	5.25	4	7

maintenance following the parity check was (y) , or (\vee) was not (n) in error; $\Pi_{S_d=0}(n_i^\vee \delta n_i)$ and $\Pi_{S_d \neq 0}(n_i^\vee \delta n_i)$ are the probabilities that $S_a = S_b$ or $S_a \neq S_b$ for n_i or δn_i errors in N_h bits and are concretely defined in Eq. (6), and $\Pi^{(\pm)}(n_i^\vee \delta n_i)$ is defined in Eq. (8).

Equation (12) can be expressed in terms of $\pi^{(y \vee n)}$, Π_{S_d} , and $\Pi^{(\pm)}$ as

$$\overline{\Delta n} \equiv \langle \Delta n^{(n)}(n_i) \rangle + \langle \Delta n^{(y)}(n_i) \rangle, = \overline{\Delta n}^{(n)} + \overline{\Delta n}^{(y)}, \quad (14)$$

where the arguments which depend on n_i have been suppressed, and

$$\begin{aligned} \overline{\Delta n}^{(n)} &= \pi^{(n)} \Pi_{S_d \neq 0}(n_i) [1 - 2\Pi^{(-)}(n_i)], \\ \overline{\Delta n}^{(y)} &= \pi^{(y)} \Pi_{S_d \neq 0}(\delta n_i) [1 - 2\Pi^{(-)}(\delta n_i)] - \pi^{(y)}. \end{aligned} \quad (15)$$

The final quantity needed to calculate the efficiency of the Winnow protocol is $\pi^{(y \vee n)}$:

$$\pi^{(y)} = \frac{n_i}{N}, \quad (16a)$$

where

$$\pi^{(y)} + \pi^{(n)} = 1. \quad (16b)$$

Table I and Table II provide a concrete example for the special case of $m=3$ of the effects of the Winnow protocol on blocks with exactly $n_i \in \{0, \dots, 8\}$ errors. Table I introduces a new quantity

$$\bar{n}_f \equiv \langle n_f \rangle = n_i + \overline{\Delta n}, \quad (17)$$

and in Table II a new parameter

$$p_f = \frac{\bar{n}_f}{N_f} \quad (18)$$

TABLE II. \bar{n}_f/N_f for $N=8$ for various stages in the Winnow protocol (note that the Hamming component of the Winnow protocol is not applied to blocks that contain an even number of errors).

p_i	0	0.13	0.25	0.38	0.5	0.63	0.75	0.88	1
p_f^p	0	0.13	0.25	0.38	0.5	0.63	0.75	0.88	1
p_f^{ph}	0	0	0.25	0.5	0.5	0.5	0.75	1	1
p_f	0	0	0.25	0.5	0.5	0.5	0.75	1	1

is defined.

The parameter p_f defines the probability for each bit in a given block to be in error. The number $N_f \in \{N-1, N-m-1\}$ and its value depends on the action required by the Winnow protocol for a given number of initial errors. For example, $N_f = N-1$ or $N-m-1$ for p_f and n_i even or odd, respectively.

These two tables illustrate the effect of the Winnow protocol on data that are divided into 8-bit blocks. The values marked with superscript p reflect the effect of discarding 1 bit following the parity comparison. The values marked with superscript ph refer to the data after the Hamming algorithm is also applied, but before the requisite $\log_2(N)=3$ bits of data are discarded for privacy maintenance. The final values denoted by subscript f reveal the effect of the Winnow protocol (including the effect of all discarded data required for privacy maintenance).

The parameter p_f clearly shows a reduction in errors for $n_i=1$ and an increase in errors for $n_i=3$. It also shows that discarding data to maintain privacy of the remaining key has no effect on the error probability.

The fraction of key remaining after a SPW is given by

$$\mu_N \equiv \frac{\langle N_f \rangle}{N} = \frac{\sum_{n_i=0}^N N_f P(n_i|N)}{N}, \quad (19)$$

and the probability for any key bit to be in error following a SPW is

$$p_N = \frac{\langle \bar{n}_f \rangle}{\langle N_f \rangle} = \frac{\sum_{n_i=0}^N \bar{n}_f(n_i) P(n_i|N)}{N \mu_N}, \quad (20)$$

where $P(n_i|N)$ is the probability for an N -bit block to contain n_i errors before a SPW.

Obviously, the efficiency with which the Winnow protocol removes errors depends upon the distribution of errors within the data. Without intimate knowledge of a specific QKD apparatus, a reasonable assumption is that the errors are random and normally distributed throughout the data. Given this assumption, $P(n_i|N)$ in Eq. (20) is given by the binomial distribution

$$P(n_i|N, p_0) = \binom{N}{n_i} p_0^{n_i} (1-p_0)^{N-n_i}, \quad (21)$$

where p_0 is the probability that any given bit is in (relative) error.

With this assumption, Eqs. (19) and (20) can be expressed as

$$\mu_N = \frac{N-1-m \sum_{n_i \text{ odd}} \binom{N}{n_i} p_0^{n_i} (1-p_0)^{N-n_i}}{N}, \quad (22)$$

where $m = \log_2(N)$ and

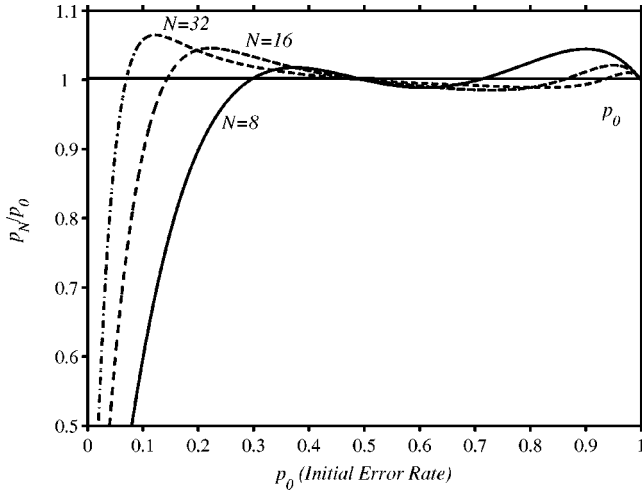


FIG. 1. The ratio p_N/p_0 for $N=8, 16,$ and 32 . These curves illustrate the change in the probability that a given bit is in error after a single application of the Winnow protocol for the indicated block size N . Note that $(p_8 < p_{16}) \forall (p_0 \leq 0.38)$; in addition, $(p_{16} < p_{32}) \forall (p_0 \leq 0.20)$. This indicates that applications of the Winnow protocol with smaller N are more efficient at removing errors than are applications with larger N within the region, where p_0 satisfies these conditions.

$$p_N = \frac{\sum_{n_i=0}^N \bar{n}_f(n_i) \binom{N}{n_i} p_0^{n_i} (1-p_0)^{N-n_i}}{N \mu_N}. \quad (23)$$

The efficiency with which the Winnow protocol reduces errors in the key is of great interest. Two related issues that concern the efficiency are (1) the number of iterations of the Winnow protocol necessary to achieve a sufficiently low probability of error in the remaining key data and (2) the amount of key data that is discarded through privacy maintenance.

The number of iterations is of concern because each iteration reveals information and consumes time with each communication between A and B . Moreover, each communication requires the use of some private key for signature authentication [7]. Most important, though, is that each iteration requires a significant amount of data to be discarded through privacy maintenance.

Smaller N require more data to be discarded than larger N as can be seen from Eq. (22). However, an effect that tends to mollify this undesirable condition is that smaller N are more efficient at removing errors for larger values of initial error probability. This effect is illustrated in Fig. 1, where we have plotted p_N/p_0 for several values of N . For all values of N and p_0 sufficiently small, $p_N/p_0 < 1$ and the protocol can remove errors from the key data. However, as p_0 increases from $p_0=0$, each of the curves passes through $p_N/p_0=1$ indicating that additional errors are being introduced into the key. Moreover, the value of p_0 for which $p_N/p_0=1$ is smaller for larger N and the curves do not intersect between $p_0=0$ and $p_N/p_0=1$.

As a primary requirement of a SPW on real data in an iterative application, a random shuffling of the data between

iterations is essential to randomly redistribute missed or introduced errors. Without this random shuffle, multiple errors remain clumped together and, in essence, are impossible to completely remove from the data. Under this constraint, it is obvious that the final error probability, and the amount of data remaining after a number of SPWs, depends on the way in which N is varied throughout the successive SPWs. An intuitive result that we have verified empirically is that less data are discarded for the same initial and final error probabilities if N is chosen well for the first iteration and is either held constant or increased for all subsequent iterations; there is no advantage in decreasing N in subsequent iterations if the Winnow protocol is applied as outlined here.

Define

$$p(p_0; \{j_N\}) \quad (24)$$

and

$$\mu(p_0; \{j_N\}) \quad (25)$$

as the final error rate and fraction of data remaining after a sequence $\{j_N\} = \{j_8, j_{16}, j_{32}, j_{64}, j_{128}\}$, where j_N iterations of the Winnow protocol are applied with a block size $N \in \{8, 16, 32, 64, 128\}$ beginning with $N=8$ and increasing monotonically in N by factors of 2.³

Because $(p_8 < p_0) \forall (p_0 \leq 0.3)$, it may appear that errors can be corrected in the data for this entire range of initial error probability. However, there is another criterion that must be met, which significantly reduces the maximum correctable error probability: There must remain a finite amount of error-free data after the potential information possessed by E is reduced through privacy amplification.

The maximum amount of potential information possessed by E can be determined by the initial error probability p_0 and depends on the QKD protocol and the type of attacks being employed. For example, if the BB84 protocol is used and E employs a complete intercept-resend attack on the quantum channel in the same bases used by B , she will introduce an error probability of $p_0=1/4$. She will also potentially know 1/2 of the data before error-reconciliation and up to 2/3 of the data that remains after error-reconciliation.

If E uses a more clever intercept-resend strategy of detecting and resending in the Breidbart basis (second paper in Ref. [4]), she would introduce the same number of errors ($p_0=1/4$) and could know up to a fraction of 0.59 of the data before error-reconciliation and 0.78 of the data remaining after error-reconciliation.

It should also be noted that certain states of light are more susceptible to attack than others. For example, consider weak coherent states that are commonly used in QKD systems. If E also employs a beam splitter attack [3,4,12] against one of these systems, an additional amount of data is compromised

³In this work N is constrained such that $8 \leq N \leq 128$ only for the sake of brevity. We have found that this constraint does not impose a serious limit on the ability of the Winnow protocol to correct errors. The ideas discussed below can be extended to include $N=4$ and $N > 128$ in a straightforward manner.

which is not greater than the mean number of photons in the state. However, this value can be made arbitrarily small, so it is neglected in the following calculations. Moreover, other states of light can be used in QKD schemes, which are not vulnerable to this type of attack [13].

Thus, the fraction of data remaining after error-reconciliation and privacy amplifications can be

$$\nu^{\text{BB84}} = \mu - (0.59)4 p_0, \quad (26)$$

for the BB84 protocol, where ν describes the remaining fraction of key.

From the above considerations, p and ν can be investigated as a function of p_0 . Of particular interest is the maximum p_0 for which some secure data remains, while achieving a sufficiently low final error probability to make the data useful. We have chosen, somewhat arbitrarily, $p \leq 10^{-6}$ as a reasonable target for the final error probability.

With this target and the remaining fraction of private data described by Eq. (26), we find the largest initial error probability for which some private data remains is

$$p_0 = 0.1322, \quad (27)$$

after multiple passes of the Winnow protocol and privacy amplification.

To achieve $p \leq 10^{-6}$ from this large initial error probability, the Winnow protocol must be applied in the sequence $\{j_N\} = \{3, 1, 0, 1, 3\}$. That is, three SPWs with $N=8$ must be followed by one SPW with $N=16$, etc. If this prescription is followed,

$$\nu^{\text{BB84}} = 0.0017 \quad (28)$$

of the original data remain and are secure following privacy amplification.

Some QKD schemes require a larger estimate of E 's knowledge. If Eq. (26) is replaced with [4]

$$\nu = \mu - 2\sqrt{2}p_0, \quad (29)$$

we find

$$p_0 = 0.1222, \quad (30)$$

for $\{j_N\} = \{3, 0, 1, 0, 4\}$. This leaves a fraction $\nu = 0.0017$ of the original data as secure data with a single-bit error probability $\leq 10^{-6}$.

Finally, if we estimate that E knows every bit of data by causing $p_0 = 1/4$, then

$$\nu = \mu - 4 p_0. \quad (31)$$

We then find that the largest reconcilable p_0 is

$$p_0 = 0.1037, \quad (32)$$

for $\{j_N\} = \{2, 1, 1, 0, 3\}$ and $\nu = 0.0020$.

The most efficient iteration sequence ($\{j_N\}$) for any QKD scheme can be determined by first applying the Winnow protocol with $N=8$ to estimate p_0 . Once the number of blocks

with odd and even (even includes zero) errors, M_e^{odd} and M_e^{even} , respectively, are known, the fraction

$$\frac{M_e^{\text{odd}}}{M_e^{\text{odd}} + M_e^{\text{even}}} = \frac{\sum_{n_i^{\text{odd}}} \binom{N}{n_i} p_0^{n_i} (1-p_0)^{N-n_i}}{N} \quad (33)$$

can be used to estimate p_0 . Knowledge of p_0 is sufficient to determine the $\{j_N\}$ which maximizes ν .

For small p_0 , the most efficient $\{j_N\}$ may start with $N > 8$. However, working systems that have been reported in the literature [4,14] have large enough error probabilities, so that the most key is left if $N=8$ for at least the first iteration.

A detailed analysis of the advantages of Winnow over other protocols is beyond the scope of this work. However, it is instructive to note the advantages over at least the best-known protocol CASCADE.

The most notable difference between Winnow or BINARY and CASCADE is that CASCADE does not employ privacy maintenance. The disadvantage of such a protocol is that super-redundant information must be exchanged with each successive iteration. This is to be compared with BINARY and Winnow which reduce the size of the dataset with each communication. With the reasonable requirement that a bit revealed through these communications requires at least a bit to be eliminated through some channel, either before or during privacy amplification, then the inefficiency of keeping all bits until all errors are removed becomes obvious: Retaining and repetitively exchanging information on the same bits are an additional expense to the protocol.

For the purpose of comparison, we have computed the maximum p_0 through BINARY (less privacy maintenance) that can successfully reconcile errors and preserve a small amount of secure data after privacy amplification and the removal of the super-redundant information. We find

$$p_0 = 0.114, \quad (34)$$

for $\{j_N\} = \{2, 1, 0, 2, 1\}$ and $\nu^{\text{BB84}} = 0.01$ when Eq. (26) describes the additional amount of key that must be discarded through privacy amplification. This is to be compared with $p_0 = 0.1322$ for the same considerations with the Winnow protocol. This application of BINARY is a reasonable approximation to CASCADE which may include a higher-order correction giving a slightly higher overall error reduction than BINARY without privacy maintenance.

This comparison (or any of the previous discussion) does not take into account bits used to authenticate messages sent between A and B . Both CASCADE and BINARY requires significantly more two-way communication than the Winnow protocol, and each packet of n bits sent may require $\lceil \log_2(n) \rceil$ for authentication [7]. We calculate that the most efficient application of CASCADE requires a minimum of $1 + \log_2(N)$ communications for any block size N that exhibits a parity error, while the Winnow protocol requires only two communications for any block size N that exhibits a parity error; the additional communications required imposes a tight limitation on practical efficiency. In addition, because CASCADE

does not maintain privacy, subsequent iterations require more bits to be exchanged in the initial parity phase with each iteration. The additional bit exchanges may require additional signature authentication bits.

We acknowledge that because CASCADE and BINARY always removes a single error and never introduces additional errors to multiple error blocks, both BINARY and CASCADE perform infinitesimally better than the Winnow protocol in an environment where signature authentication is not required and privacy maintenance is removed from the Winnow and BINARY protocols. However, the two communications of the Winnow protocol is a great advantage, where time is of the essence with regard to production of secure key bits over inefficient noisy quantum channels.

V. CONCLUSION

We have identified a fast, efficient, error-reconciliation protocol for quantum-key distribution which requires only two communications between the two parties attempting to

reconcile private, quantum-key material. We refer to this protocol as Winnow.

The Winnow protocol incorporates a preliminary parity comparison on blocks whose size is $N=2^m$, where $m \in \{3,4,5,6, \dots\}$. Subsequently, one bit is discarded from these blocks to maintain the privacy of the remaining bits. A Hamming hash function, which can be used to correct single errors, is applied to the remaining $N-1$ bits on the blocks whose parities did not agree. Finally, m bits are discarded from the blocks on which the Hamming algorithm was applied to maintain the privacy of those bits.

We find this protocol capable of correcting an initial error probability of up to 13.22% in privacy amplified BB84-like quantum-key distribution schemes.

ACKNOWLEDGMENTS

The authors extend their thanks and appreciation to R. J. Hughes, E. Twyffort, D. P. Simpson, and J. S. Reeve for many helpful discussions regarding this effort.

-
- [1] C.H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing, Bangalore, India, 1984* (IEEE, New York, 1984) pp. 175–179; A.K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991); C.H. Bennett and S.J. Wiesner, *ibid.* **69**, 2881 (1992); C.H. Bennett, *ibid.* **68**, 3121 (1992).
 - [2] C. Cachin and U.M. Maurer, *J. Cryptology* **10**, 97 (1997).
 - [3] N. Lütkenhaus, *Phys. Rev. A* **59**, 3301 (1999).
 - [4] C.H. Bennett *et al.*, *Lect. Notes Comput. Sci.* **473**, 253 (1990); *J. Cryptology* **5**, 3 (1992).
 - [5] G. Brassard and L. Salvail, *Lect. Notes Comput. Sci.* **765**, 410 (1994).
 - [6] C.H. Bennett *et al.*, *IEEE Trans. Inf. Theory* **41**, 1915 (1995).
 - [7] W. Diffie and M.E. Hellman, in *Proceedings of AFIPS National Computer Conference*, edited by S. Winkler (AFIPS Press, Montvale, NJ, 1976) pp. 109–112; R.L. Rivest, A. Shamir, and L.M. Adleman, *Commun. ACM* **21**, 120 (1978); C. Mitchell, F. Piper and P. Wild, *Contemporary Cryptography: The Science of Information Integrity*, edited by G.J. Simmons (IEEE Press, New York, 1992), pp. 325–378.
 - [8] R.W. Hamming, *Bell Syst. Tech. J.* **2**, 147 (1950).
 - [9] R.W. Hamming, *Coding and Information Theory* (Prentice-Hall, New Jersey, 1986), p. 293.
 - [10] C.E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948); **27**, 623 (1948).
 - [11] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography* (CRC Press, New York, 1997), p. 780.
 - [12] M. Dušek, O. Haderka, and M. Hendrych, *Opt. Commun.* **169**, 103 (1999).
 - [13] J. Kim *et al.*, *Nature (London)* **397**, 500 (1999); P. Michler *et al.*, *Science* **290**, 2282 (2000); B. Lounis and W.E. Moerner, *Nature (London)* **407**, 491 (2000).
 - [14] J.D. Franson and H. Ives, *Appl. Opt.* **33**, 2949 (1994); B. Jacobs and J.D. Franson, *Opt. Lett.* **21**, 1854 (1996); P.D. Townsend, *Nature (London)* **385**, 47 (1997); A. Muller, H. Zbinden, and N. Gisin, *Europhys. Lett.* **33**, 335 (1996); W.T. Buttler *et al.*, *Phys. Rev. Lett.* **84**, 5652 (2000); R.J. Hughes, G.L. Morgan, and C. Glen Peterson, *J. Mod. Opt.* **47**, 533 (2000); D.S. Bethune and W.P. Risk, *IEEE J. Quantum Electron.* **36**, 340 (2000); M. Bourennane *et al.*, *J. Mod. Opt.* **47**, 563 (2000); J.G. Rarity, P.R. Tapster, and P.M. Gorman, *ibid.* **48**, 1887 (2001).