A Novel Error Correction Scheme in Quantum Key Distribution (QKD) Protocol

Siao Ping Lee, Chee Kyun Ng and Makhfudzah Mokhtar
Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia, Malaysia
Emails: xquire_v@hotmail.com; mpnck@upm.edu.my; fudzah@upm.edu.my

Abstract— Ideally, in any quantum key distribution (QKD) communication system, each sifted key is expected to be received without error. However, in practice, due to infeasibility of generating pure single photon and device impairment problem, some of the sifted key may experience errors. This results to the increment of quantum bit error rate (QBER) that requires error reconciliation for correcting error. The main concept in error reconciliation is very much related to the capability of correcting all errors while minimizing eavesdrop information. The quantum error correcting code such as Hamming code which used in Winnow protocol is found to be more attractive. However the Winnow protocol can only correct one error out of seven bits. In this paper, a modified Hamming encoder/decoder to improve Winnow protocol by correcting two errors out of seven bits which leads to reducing the QBER is presented. This design utilizes a pair of forward and reverse order syndromes for error pattern recognition. A new reconciliation protocol has been developed to enhance the error correcting capability in BB84 protocol. It is carried out in a simple structure which can correct up to double erroneous bits and detect four erroneous bits for each seven bits.

Index Terms— Cryptography, Hamming code, error correction, QKD, reconciliation protocol, BB84 protocol, Winnow Protocol.

I. INTRODUCTION

Algorithms of cryptography are mostly designed to comply with computational hardness assumption and not withstand imminent threat imposed by computationally efficient device. Permitting superposition of binary states, a quantum computer which executes operation on quantum bits (commonly known as qubits) is believed to be capable of speeding up tedious computations tremendously once the associated technologies are in place. Thus, it renders state-of-the-art asymmetric-key cryptography compromised and endangers computationally secure symmetric-key cryptography [1]. Therefore, a vintage technique of symmetric-key cryptography known as one-time pad (OTP) is heeded as the ultimate solution because it has been proven to be information theoretically impregnable against cryptanalysis, if a perfectly random secret key of infinite length is employed only once and never reused [1]-[4]. Owing to lack of practical implementation, it was not much attended until now.

As unguarded delivery of secret key may jeopardize the plausible scheme, quantum key distribution (QKD) which escorts key through quantum channel using quantum state encoding, i.e., photon polarization, is suggested to facilitate OTP in order to set up a secure communication for secret key sharing [5]. Having its security ascertained by Heisenberg uncertainty principle [6] and no-cloning theorem of quantum mechanics, QKD guarantees delivery of key in such a way that possible eavesdropping can be confidently detected during error rate estimation [7]. The renowned QKD protocol, which has been proven unconditionally secure against any eavesdropping and practically viable, was built upon inspiration from quantum realization of unforgeable bank notes [8] and promulgated by developers Charles Bennett and Gilles Brassard in 1984, typically known as Bennett-Brassard 1984 (BB84) protocol [9]. In fact, the joint venture between OTP and QKD is consistent with Kerckhoff’s principle which enunciates that key’s secrecy should be the one and only pivot leveraging security of a cryptosystem [10]. However, errors attributed to imperfections in the physical implementation are prevalent, with or without eavesdropping. Consequently, reconciliation is vital for secret key distillation, which serves as prerequisite for information-theoretically secure cryptography. Reconciliation is carried out in (noiseless) public yet authenticated classical channel to correct undesired errors such that discrepancies between sender’s and receiver's secret key can be fixed for successful encryption and decryption respectively. It can be accomplished by employing either simple classical error correcting code or advanced quantum error correcting code [1].

Winnow protocol decreases the disclosure of partial information to eavesdropper by taking advantage of both parity bit and Hamming code for single-bit error correction. Nevertheless, the need of several iterations is still indispensable because Winnow protocol tends to correct a block of sifted secret key that is interspersed with three or more
odd multiple bits of error inaccurately while abandoning detection of even multiple bits of error [11]. If convolutional code takes the place of Hamming code, the Winnow protocol can correct any odd number of erroneous bit(s) with the loss of operational simplicity [12]. Characterized to allow multiple-bit error correction, Bose-Chaudhuri-Hocquenghen (BCH) code suitably becomes a sound alternative for reconciliation. Nonetheless, its error correcting capability is rather limiting if closely examined [13]. After all, there is a very strong motivation to develop a reconciliation protocol that minimizes public communication between legitimate communicants with improved error correcting capability. Thus, this paper is aimed to enhance reliability of QKD by proposing an efficient and effective reconciliation protocol that rectifies errors in single pass with maximum of double-bit error correcting capability into BB84 protocol. This design utilizes a pair of forward and reverse order syndromes for error pattern recognition. The new reconciliation protocol has been developed and evaluated in terms of amount of disclosed bit and quantum bit error rate (QBER).

II. THE PROPOSED RECONCILIATION SYSTEM ARCHITECTURE

In the BB84 protocol as shown in Fig. 1, Alice sends a stream of random key through quantum channel to Bob after recording photon state of each key element. The key is firstly coded in bits then further encoded in conjugative quantum states, constituted by rectilinear and diagonal polarization of photon conventionally. Mapping of bit to respective polarization is indicated at the bottom of Fig. 1. Bob acknowledges his receipt of photons and measure them using a stream of random rectilinear and diagonal bases, independent from those of Alice. Whenever the photon state is a subset of basis of measurement, he gets correlated result. His choices of basis with corresponding measurement results, known as raw key, are recorded. After transference of the random key, Bob informs Alice about the stream of basis being used for measurement through (noiseless) public yet authenticated classical channel, which is accessible to passive eavesdropping solely.

![Fig. 1. Schematics of the BB84 protocol for ideal case.](image)

Alice notifies Bob which of his measurement is compatible with the photons delivered and should have the photon state detected correctly, enabling them to disregard those result that susceptible to disruptive measurement. After discarding anomalies in respective raw key, they deduce identical sifted keys in secret, which can be used for cryptographic purpose. Obviously, their secret key is not predetermined but is developed in conjunction of their random choices, with an aid of guided investigation [9].

Resultantly, Bob’s sifted key suffers from 25% [14] of QBER in respect to Alice’s sifted key. Thus, after the sifting process, reconciliation is necessitated to ascertain identicalness of the sifted keys pair. Grueling proofs of QKD’s security were presented to showcase corresponding noise resistant threshold [14],[15]. In the earliest attempts, BB84 protocol was proven secure against all attacks permissible by laws of quantum mechanics whenever the QBER is less than 7.4% [16] and up to 7.56% [17] in two independent research studies. Once reconciliation is initiated, error detection and correction make concerted effort to mitigate inconsistencies in the sifted keys pair using interactive or non-interactive protocol. An interactive reconciliation protocol requires repetitive exchange of parity bit between Alice and Bob via a two-way communication channel to detect and correct errors. On the contrary, a non-interactive reconciliation protocol applies concept of one-way source coding with side information to eliminate the interactivity between Alice and Bob when performing error correction [2], as shown in Fig. 2.

In a conceptual manner, Alice’s sifted key is first encoded into respective syndrome. The syndrome is then transmitted over a (noiseless) public yet authenticated classical channel to Bob and fed into a decoder together with his own sifted key to restore Alice’s sifted key with high probability. In this way, sifted key with flaw at receiving end is mended allegedly [12]. The non-interactive reconciliation protocol is a preferable technique since it can catalyze efficiency of error correction and minimize public communication concomitantly.

At the beginning of Winnow protocol, after shuffling the bits of sifted keys pair in the same way, Alice’s and Bob’s string of sifted key are also divided into blocks and then subjected to parity check correspondingly. One bit in each block is then discarded because of the parity check. After that, non-interactive reconciliation begins. First of all, syndrome is calculated and sent from Alice to Bob, for each of the blocks exhibiting odd result in preliminary test. It is noted that syndrome is primitively an indicator implying correctness of a received codeword during error detection, but here is where it fits into reconciliation.

![Fig. 2. Source coding with side information in reconciliation.](image)

At receiving end, syndrome measurement is carried out by Bob using received syndrome in tandem with his own sifted key’s syndrome to compute difference between their
syndromes, and determine associated correctable error pattern of his sifted key such that the most probable error can then be corrected by him independently. Normally, the assigned error correcting code is Hamming code, the first effective linear block code invented to be able to correct one bit of error in a valid codeword.

Confined by Hamming code’s limited error correcting capability, this method will have a block of sifted key deduced by Bob that is interspersed with three or more odd multiple bits of error incompletely corrected, i.e., only one of the erroneous bits is corrected, not corrected or worse yet, wrongly corrected, causing an extra erroneous bit. Furthermore, this method cannot detect even multiple bits of error, leaving them uncorrected. Hence, iterations that independent of each other are still a must during reconciliation. Remaining bits of sifted key in each block that equivalent to redundancy bits of a Hamming code’s codeword, are also discarded before commencement of new round of reconciliation. Some erroneous bits that fall among the removed bits are thus discarded without undergoing error correction [11],[18].

Hence, in our proposed reconciliation protocol, in order to detect any Hamming (7, 4, 3) codeword that is interjected with up to two bits of error, codewords with weight of two in every coset of the standard array are collectively gathered as extra correctable error patterns associated with respective syndrome. Resultantly, there is a mix of single-bit and double-bit error patterns associated with each non-zero syndrome. Without introducing additional parameter which may be favorable for possible eavesdropping, the syndrome measurement is done twice in slightly distinctive manner for an attempt to reconcile possible errors in the codeword such that two set of error patterns in respect to two set of syndromes are made available for matching analysis. Thus, a simple concept of logical reasoning is featured by analyzing the codeword in forward and reverse orders. It is utilizing an idea that the exact error pattern should remain the same regardless of the direction in which analysis is performed, i.e., whether from the most significant bit (MSB) toward the least significant bit (LSB) or vice versa as shown in Fig. 3. In QKD application, syndrome in forward order is the syndrome calculated when a block of sifted key is analyzed in forward order (MSB \(\rightarrow\) LSB) while syndrome in reverse order is the syndrome calculated when a block of sifted key is analyzed in reverse order (LSB \(\rightarrow\) MSB).

![Fig. 3. The order of analysis with respective syndrome.](image)

Indeed syndrome in forward order is the syndrome that has been used in Winnow protocol. The difference between a block syndrome of sifted key deduced by Alice and the one deduced by Bob in forward order as well as reverse order, are correspondingly computed by Bob to determine the associated error patterns in both orders as shown in Fig. 4. It can be seen that error patterns associated with non-zero syndrome in forward order are a collection of codewords with weight of one or two in every coset of the standard array during preparatory stage, while error patterns associated with non-zero syndrome in reverse order are those of forward order but experienced straight left right flipping. Such adjustment is made such that posterior matching analysis and error correction can be performed by Bob in reference to conventional forward order. Whenever syndrome measurement does not result in all-zero syndromes in forward order and that of in reverse order, maximum occurrence of two bits of error in a block of sifted key is detected. Otherwise, the differences are all-zero syndromes, intimating that the block of sifted key is errorless. Matching analysis is then carried out to determine the identical error pattern associated with difference between syndromes in respective order, ruling out irrelevant error patterns and pinpointing the exact one for successful error correction.

The algorithm of proposed reconciliation protocol that rectifies errors of BB84 protocol in single pass with maximum of double-bit error correcting capability is shown in Fig. 5. First of all, the position of bits in Alice’s and Bob’s string of sifted key is randomly permuted via folio interlacement such that possible sequent errors are dispersed at random. The shuffled strings of sifted key are partitioned by both parties into blocks that comprise seven bits out of the total bits each. Alice has syndrome of the first block of sifted key calculated in both forward and reverse orders using her portion of sifted key, and then sent to Bob via (noiseless) public yet authenticated classical channel. Meanwhile, Bob also has syndrome of the first block of sifted key calculated in both orders using his portion of sifted key. Syndrome measurement is carried out by Bob using received syndromes in tandem with his calculated syndromes to compute difference between their syndromes and determine associated error patterns in both orders.

The matching analysis is carried out by Bob to determine the identical error pattern associated with difference between syndromes in respective order. The conditional decision to be made by Bob will be if there is a match of identical error pattern after performing matching analysis, error correction is performed by adding his block of sifted key under test with pinpointed error pattern bitwise using binary XOR operation. Otherwise, there is not a match of identical error pattern after performing matching analysis. Error correction is skipped and his block of sifted key under test is discarded with a notification sent to Alice via the classical channel such that corresponding block of her sifted key is discarded too. Procedures are kept repeated for ensuing blocks of sifted key before the last block is analyzed. For all the blocks of sifted key that are successfully reconciled, the fourth bit in each block is reserved while the rest are discarded by both parties on account of privacy maintenance.
<table>
<thead>
<tr>
<th>Difference between syndromes</th>
<th>Error pattern</th>
<th>Difference between syndromes</th>
<th>Error pattern</th>
</tr>
</thead>
<tbody>
<tr>
<td>000</td>
<td>0000000</td>
<td>000</td>
<td>0000000</td>
</tr>
<tr>
<td>100</td>
<td>1000000</td>
<td>1100000</td>
<td>1000000</td>
</tr>
<tr>
<td>010</td>
<td>0100000</td>
<td>0010100</td>
<td>0101000</td>
</tr>
<tr>
<td>001</td>
<td>0100000</td>
<td>0101000</td>
<td>0001010</td>
</tr>
<tr>
<td>110</td>
<td>0010000</td>
<td>0001010</td>
<td>0010001</td>
</tr>
<tr>
<td>011</td>
<td>0100000</td>
<td>0100010</td>
<td>1000100</td>
</tr>
<tr>
<td>101</td>
<td>0010000</td>
<td>0100010</td>
<td>0101000</td>
</tr>
<tr>
<td>111</td>
<td>1000000</td>
<td>0100010</td>
<td>0001100</td>
</tr>
</tbody>
</table>

**Fig. 4.** The error patterns associated with difference between syndromes in respective orders.

---

**Forward order**

- Calculation of syndrome(s) of a block sifted key in forward and reverse order by Alice and Bob.
- Compute syndrome Alice and Bob in forward order by Bob.
- Obtain Error Pattern in forward order.
- Error Pattern Match?
- Yes
- End
- No

**Reverse order**

- Perform error correction with pinpointed error pattern.
- Discard the block of sifted key under test.
- Last block?
- Yes
- End
- No

**Fig. 5.** Flow of the proposed algorithm for reconciliation.
Fig. 6. Reconciliation and privacy maintenance utilizing the proposed algorithm.
The reconciliation and privacy maintenance utilizing the proposed protocol is shown through a self-explanatory example in Fig. 6. Remarkably, a 7-bit block of sifted key may be interspersed with three or four bits of error, but such a block will be discarded during reconciliation in accordance with fourth step of the proposed protocol.

III. PERFORMANCE EVALUATIONS

The proposed algorithm for reconciliation is simulated using MATLAB® software which supports matrix operations that are fundamental to error correction. The simulation is initiated by generating two strings of sifted key; one is errorless in reference while the other is interjected with sequent errors. Both strings underwent segmentation, random shuffling, syndrome computation, matching analysis, appropriate reconciliation, privacy maintenance and combination. The simulation is repeated using different initial QBER, i.e., QBER prior to reconciliation, and evaluated against final QBER, i.e., QBER right after reconciliation, which is the output of simulation.

Figure 7 shows the simulation result in comparison with Winnow protocol applying parity check and Hamming code. The line that corresponds to Winnow protocol is plotted by directly applying the data readily available in [18]. Length of sifted key of about 3000 bits and optimized block size are used in this simulation. The final QBER posts a rise in response to increment of initial QBER for both reconciliation protocols, but the percentages recorded for proposed algorithm are lower than those of Winnow protocol. The difference is noticeably clear for initial QBER ranging from 4% to 11%. It is due to the capability of the proposed algorithm in correcting up to two bits of error in an erroneous 7-bit block of sifted key, which is a feature not possessed by Winnow protocol. Furthermore, unlike the proposed algorithm, Winnow protocol is incapable of identifying and discarding the erroneous blocks of sifted key which constitutes toward number of remaining errors at the end of reconciliation in single pass. Hinging on the limited single-bit error correcting capability, several iterations are in need for complete reconciliation using Winnow protocol in general.

Figure 8 shows the simulation result in comparison with improved Winnow protocol applying parity check and convolutional code. The line that corresponds to Winnow protocol applying convolutional code is plotted by directly applying the data readily available in [12]. Length of sifted key of 100000 bits is used in their simulation in which the data presented are averaged values of 100 trials. The trend that corresponds to proposed algorithm outperforms that of Winnow protocol applying convolutional, although any odd number of erroneous bit(s) in a block of sifted key can be corrected via the improved Winnow protocol.

IV. CONCLUSIONS

The quantum error correcting code such as Hamming code which used in Winnow protocol is found to be more attractive. However, the Winnow protocol can only correct one error out of seven bits. In this paper, a new reconciliation protocol has been developed to enhance the error correcting capability in BB84 protocol. A single pass reconciliation protocol that capable corrects up to two bits of error in an erroneous 7-bit block of sifted key has been presented by applying simple Hamming (7, 4, 3) code. The syndrome measurement is done twice in slightly distinctive manner such that two set of error patterns in respect to two set of syndromes are made available for matching analysis. Thus, it is featured by analyzing the codeword in forward and reverse orders where the exact error pattern should remain the same regardless of the direction whether from the MSB toward the LSB or vice versa. With this new interpretation of Hamming code’s syndrome and an unprecedented matching analysis, occurrence of three or four bits of error in the erroneous block of sifted key can also be identified by the proposed reconciliation protocol.
REFERENCES


Chee Kyun Ng received his Bachelor of Engineering and Master of Science degrees majoring in Computer & Communication Systems from Universiti Putra Malaysia, Serdang, Selangor, Malaysia, in 1999 and 2002 respectively. He has also completed his PhD programme in 2007 majoring in Communications and Network Engineering at the same university. He is currently undertaking his research on information communication technology (ICT) towards ageing people. Since from his study programmes, he has published over 100 papers in journals and in conferences.

Makhdudzah Mokhtar received her B.Eng. degree from the Universiti Kebangsaan Malaysia in 2000. She started her career in education field at the Department of Computer and Communication Systems Engineering, Faculty of Engineering, Universiti Putra Malaysia as a tutor. In 2007, she completed her Ph.D. degree from University of Essex and served as a lecturer in the same institution. Since 2001, she has been involved in optical communication systems research and her research interests focus on channel coding, Optical Code Division Multiple Access and quantum key distribution. She is a member of the Institute of Electrical and Electronics Engineers (IEEE) and the Photonics Society under the IEEE.

© 2015 by the authors; licensee Asia-Pacific Advanced Network. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).

Siao Ping Lee received his Bachelor of Engineering and Master of Science degrees majoring in Computer & Communication Systems from Universiti Putra Malaysia, Serdang, Selangor, Malaysia, in 2009 and 2013 respectively. He was undertaking his research on optical communications specialized in error correction coding.