IMPROVED RECONCILIATION EFFICIENCY WITH CHANNEL CODING FOR QUANTUM KEY DISTRIBUTION

PATCHARAPONG TREEVIRIYANUPAB

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN INFORMATION ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2012

KMITL–2012–EN–M–230–182

IMPROVED RECONCILIATION EFFICIENCY WITH CHANNEL CODING FOR QUANTUM KEY DISTRIBUTION

PATCHARAPONG TREEVIRIYANUPAB

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
MASTER OF ENGINEERING IN INFORMATION ENGINEERING
FACULTY OF ENGINEERING
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2012

KMITL-2012-EN-M-230-182

หัวข้อวิทยานิพนธ์	การปรับปรุงประสิทธิภาพการไกล่เกลี่ยความผิดพลาดด้วยรหัสช่องสัญญาณสำหรับระบบกระจายกุญแจรหัสลับเชิงควอนตัม
นักศึกษา	นายพัชรพงษ์ ตรีวิริยานุภาพ
รหัสนักศึกษา	52611310
ปริญญา	วิศวกรรมศาสตรมหาบัณฑิต
สาขาวิชา	วิศวกรรมสารสนเทศ
พ.ศ.	2555
อาจารย์ที่ปรึกษาวิทยานิพนธ์	รศ. อรลาภ แสงอรุณ
อาจารย์ที่ปรึกษาวิทยานิพนธ์ร่วม	ดร. เกียรติศักดิ์ ศรีพิมานวัฒน์

บทคัดย่อ

การไกล่เกลี่ยความผิดพลาดเป็นหนึ่งในขั้นตอนสำคัญของการกระจายกุญแจรหัสลับเชิงควอนตัมมีจุดประสงค์เพื่อการยืนยันความถูกต้องของข้อมูลกุญแจระหว่างผู้ส่งกับผู้รับตัวจริงให้มีค่าที่ตรงกัน สำหรับการนำไปใช้งานในระบบวิทยาการรหัสลับอย่างมีประสิทธิภาพ โดยทั่วไปวิธีการไกล่เกลี่ยความผิดพลาดจะอาศัยพื้นฐานการค้นหาแบบไบนารี่ ดังตัวอย่างของโพรโทคอลบีบีบีเอสเอส และโพรโทคอลคาสคาด เป็นต้น อย่างไรก็ตาม โพรโทคอลเหล่านี้ จำเป็นต้องอาศัยการติดต่อสื่อสารระหว่างผู้ส่งและผู้รับอย่างเป็นจำนวนมาก ส่งผลต่อการประมวลผลที่ล่าช้า อันเป็นข้อจำกัดสำคัญของอัตราการกำเนิดกุญแจรหัสลับสำหรับระบบฯ ที่ต้องการความเร็วสูง จึงเป็นเหตุสำคัญนำมาสู่วัตถุประสงค์ของงานวิจัยนี้ เพื่อการออกแบบและพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดประสิทธิภาพสูงด้วยรหัสช่องสัญญาณหรือรหัสแก้ไขความผิดพลาดประยุกต์ทำงานร่วมกับการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียง ซึ่งแบ่งวิธีการที่นำเสนอเป็นสามวิธี วิธีการแรกคือ การไกล่เกลี่ยความผิดพลาดด้วยรหัสคอนโวลูชันจากตัวอย่างอัตราการเข้ารหัสที่ 1/2 ซึ่งผลการทดสอบให้ความสามารถในการแก้ไขความผิดพลาดข้อมูลกุญแจรหัสลับที่สูงกว่าโพรโทคอลวินนาวที่มีพื้นฐานมาจากรหัสแฮมมิ่ง วิธีการที่สองคือ การพัฒนารหัสบีซีเอชบนพื้นฐานการเข้ารหัสซลีเพียน-วูลฟ์ โดยการคัดเลือกชุดอัตราการเข้ารหัสบีซีเอชที่เหมาะสมกับอัตราความผิดพลาดกุญแจรหัสลับเชิงควอนตัมบนเงื่อนไขของการเข้ารหัสแหล่งกำเนิดข้อมูลข่าวสารข้างเคียง อีกทั้งยังได้ปรับปรุงส่วนภาคถอดรหัสด้วยกระบวนการแจ้งตอบกลับภาคส่งบนพื้นฐานการถอดรหัสข้อมูลซินโดรมในกรณีที่เกิดความล้มเหลวในการแก้ไขความผิดพลาดขึ้น และวิธีการสุดท้ายคือ การพัฒนาวิธีการไกล่เกลี่ยความผิดพลาดด้วยรหัสแอลดีพีซีแบบไม่สม่ำเสมอที่สามารถปรับค่าอัตราการเข้ารหัสให้สอดคล้องกับเงื่อนไขความผิดพลาดกุญแจรหัสลับเชิงควอนตัมที่เกิดขึ้น ซึ่งอาศัยคุณสมบัติของการถอดรหัสข้อมูลซินโดรมในการยืนยันความถูกต้องของชุดข้อมูลกุญแจรหัสลับเมื่อการถอดรหัสให้ค่าซินโดรมระหว่างภาคส่งและภาครับที่ตรงกัน โดยจากการวิเคราะห์และเปรียบเทียบผลการทดสอบพบว่า การไกล่เกลี่ยความผิดพลาดด้วยเทคนิคของรหัสช่องสัญญาณเหล่านี้ ให้ผลของค่าประสิทธิภาพการไกล่เกลี่ยความผิดพลาด รวมถึงการลดทรัพยากรการติดต่อสื่อสารในระหว่างกระบวนการได้ดีกว่าโพรโทคอลที่นิยมใช้งานจากการสำรวจ ได้แก่ โพรโทคอลคาสคาด และวินนาว นำไปสู่เป้าหมายของการเป็นวิธีการทางเลือกหนึ่งในการเพิ่มขีดกำจัดด้านอัตราการกำเนิดกุญแจรหัสลับ สนับสนุนการประยุกต์ใช้งานจริงบนระบบการกระจายกุญแจรหัสลับเชิงควอนตัมประสิทธิภาพสูง

Thesis Title	Improved Reconciliation Efficiency with Channel Coding for Quantum Key Distribution
Student	Mr. Patcharapong Treeviriyanupab
Student ID.	52611310
Degree	Master of Engineering
Program	Information Engineering
Year	2012
Thesis Advisor	Assoc. Prof. Ornlarp Saengaroon
Co-Thesis Advisor	Dr. Keattisak Sripimanwat

ABSTRACT

Reconciliation is the one of classical parts in a Quantum Key Distribution (QKD) protocol and aims at correcting transmission error after the distribution of quantum keys. Generally, the several quantum key reconciliation protocols have been done using the interactive error correction based on a binary searching, such as the first *BBBSS* and the well-known *Cascade*. However, the speed of these protocols are fundamentally limited by the network latency in their high interactivity. In this thesis, the novel quantum key reconciliation methods are proposed by the mean of channel coding schemes. Specifically, convolutional BCH and LDPC codes are adopted as the technique of source coding with side information. To overcome the research problem, this study examines three main proposed methods covering possible cases of error rates in QKD system. The first method is that ½-rate convolutional code with side information. It deploys the fixed rate code and achieved a good error-correcting performance than that the Hamming syndrome in *Winnow*. Secondly, in order to achieve a good efficiency, the optimal set of BCH code rates are optimized with the Slepian-Wolf bound. This technique also uses a feedback syndrome decoding to detect and to discard the uncorrectable blocks of key whenever the failure of BCH decoder is declared. Finally, the interactive reconciliation with rate-compatible irregular LDPC codes is also proposed to improve the reconciliation efficiency with minimal interactive communications. The advantage of this syndrome decoding confirms as that the successful method. Eventually, gain of these proposed schemes impacts significantly on the achievable secret key generation rate responding to the high efficiency for QKD applications.

Acknowledgments

The research leading to this thesis was carried out under the supervision of Assoct. Prof. Ornlarb Sangaroon from Department of Information Engineering, Faculty of Engineering, at King Mongkut's Institute of Technology Ladkrabang, and Dr. Keattisak Sripimanwat, the group leader of Optical and Quantum Communications (OQC) Laboratory, National Electronics and Computer Technology Center (NECTEC), Thailand. I would like to thank them for their encouragement and support. They always opened the doors for me to discuss both scientific and non-scientific problems. I am highly appreciated to them.

I would also like to thank Paramin Sangwongngam and all the members of Optical and Quantum Communications (OQC) Laboratory, for their contribution to the knowledge of quantum cryptography, and other relates. This would not have been possible without their support and helpful discussions. I am also glad to work with them.

I am also very grateful to Dr. Pisit Vanichchanunt from Department of Electrical and Computer Engineering, at King Mongkut's University of Technology North Bangkok, Assoc. Prof. Ryutaroh Matsumoto from Department of Communications and Integrated Systems, at Tokyo Institute of Technology, Dr. Christoph Pacher, Dr. Momtchil Peev, Dr. Andreas Poppe, and Oliver Maurhart from the group of Optical Quantum Technology, at Austrian Institute of Technology (AIT), for their helpful comments, suggestions, and invaluable discussions in this work.

I gratefully acknowledge the scientific location, computer resources, and technical expertise provided by Optical and Quantum Communications (OQC) Laboratory, National Electronics and Computer Technology Center (NECTEC), Thailand Science Park.

Finally and most importantly, I would like to thank my family for their love and unconditional support.

This research is as a part of collaboration between Department of Information Engineering, Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, and Optical and Quantum Communications (OQC) Laboratory, National Electronics and Computer Technology Center (NECTEC) under the project P0040152 funded by National Electronics and Computer Technology Center (NECTEC), National Science and Technology Development Agency (NSTDA)

Patcharapong Treeviriyanupab

Contents

List of Figures

List of Tables

Abbreviations

AWGN	Additive White Gaussian Noise
BCH	Bose, Chaudhuri, and Hocquenghem codes
BEC	Binary Erasure Channel
BER	Bit Error Rate
BM	Branch Metric
BSC	Binary Symmetric Channel
DMC	Discrete Memoryless Channel
ECC	Error-Correcting Code
FSM	Finite State Machine
GF	Galois Field
ITS	Information-Theoretic Security
LCM	Least Common Multiple
LDPC	Low-Density Parity-Check codes
LTI	Linear Time-Invariant
PM	Path Metric
QBER	Quantum Bit Error Rate
QKD	Quantum Key Distribution
SP	Survivor Path

Variables

c_j	Check node
C	Channel capacity
C_{BEC}	Capacity of binary erasure channel
C_{BSC}	Capacity of binary symmetric channel
d	Disclosed bits
d_v, d_c	Degree of the variable and check nodes
e	Crossover probability, Quantum bit error rate
$e(x)$	Error polynomial
$g(x)$	Generator polynomial
f	Reconciliation efficiency
$g(D)$	Code generator of convolutional code
G	Generator matrix
$G(D)$	Polynomial generator matrix
$h(x)$	Parity-check polynomial
H	Parity-check matrix
$h_{bin}(p)$	Binary random variable with probability distribution p
$H(X)$	Shannon entropy
$H(X,Y)$	Joint entroy
$H(X \mid Y)$	Conditional entropy
I	Identity matrix
$leak_{recon}$	Information leakage of reconciliation scheme
$I(X;Y)$	Mutual information
k	Input symbols, Input length
K	Secret key
m	Memory of convolutional encoder
M	Shared information during reconciliation, Check nodes
$M(i)$	Set of check nodes
n	Output symbols, Block length
n_{err}	Number of errors in block length n
N	Variable nodes
$N(j)$	Set of variable nodes
$Par^{i}_{x,J}$	Parity of subsets of X
$P_x(x)$	Probability distribution

p	Parity informations, Probability distribution
P	Matrix for generating the parity bits
$P_{XY}(x,y)$	Joint probability distribution
$P_{X\|Y}(x\|y)$	Conditional probability distribution
$p(y^n \mid x^n)$	n-Dimensional conditional distribution
$q_{i\to j}$	Message sent by the variable node to the check node
$\bar{r}$	Received codeword vector
$r_{j\to i}$	Message sent by the check node to the variable node
r_{real}	Actual secure key rate
r_{th}	Theoretical secure key rate
$r(x)$	Received codeword polynomial
R_S	Slepian-Wolf compression rate
R_C	Channel coding rate
$\bar{s}$	Syndrome vector
S_{diff}	Syndrome matching informations
S_X	Syndrome information bits of X
t	Error capability
$\bar{u}$	Message vector
$u(x)$	Message polynomial
$\bar{v}$	Codeword vector
$v(x)$	Codeword polynomial
x_i	Variable node$_i$
X	Main information, *Alice*'s information, *Alice*'s sifted key
Y	Side information, *Bob*'s information, *Bob*'s sifted key
Z	Evaesdropper's knowledge
α	Primitive element
ε	Crossover probability over a binary symmetric channel
$\lambda(x)$, $\rho(x)$	Degree distribution polynomial for the variable and check nodes
$\Phi(x)$	Minimal polynomial of primitive element α
Λ	Coefficient of the error-locator polynomial
$\Lambda(x)$	Error-locator polynomial
Ψ	Common key string after reconciliation
$\mathcal{C}$	Linear block code
$\mathcal{H}$	Two-universal family of hash functions
$\mathcal{X}$	Alphabet of random variable X
$\mathcal{Y}$	Alphabet of random variable Y

Chapter 1
Introduction

The well-known technique to achieve the secrecy of communication is *"cryptography"*. It is an art of transforming information into a concealing form that anyone can not know the meaning except the legitimate recipient. The process for transforming information is called *"encryption"* which an initial message (*plaintext*) is encrypted by the sender before transmitting an encrypted message (*ciphertext*) to receiver. Then, the receiver uses the *"decryption"* process to re-transform the ciphertext into the plaintext. Its main objective is to ensure the confidentiality of a transmission between the legitimate parties which has been using for, such as military, online marketing and banking, health information exchange, and other services of private communication.

In the cryptographic system, sender and receiver need to share a relatively small amount of common secret information known as *"key"* to encrypt and decrypt the information. A key is an essential parameter replying on the security of a cryptographic system. The Kerckhoffs's[1] principle says that *"a cryptosystem should be secure even if everything about the system, except the key, is public knowledge."* **[*Kerckhoffs, 1883*]**. It is implied that the adversary can get all details of the cipher but only the key must be kept secret. Correspondingly in the classical key distribution, an eavesdropper can monitor and do everything in the communication channel. Therefore, it is only secure against a computationally bound of eavesdropper which is possible to execute a certain key distribution protocol in order to break the cryptographic systems, but it would take a limitation of overwhelming time on any computer. However, the development of computing devices such as *quantum computer* could be sufficient in the computation resources and time. It would render on the classical communications which could make the existing cryptographic systems insecure.

In 1984, C. H. Bennett and G. Brassard firstly proposed the *quantum key distribution* (QKD) protocol based on both classical cryptography with quantum

---

1 Auguste Kerckhoffs (19 January 1835 – 1903), a Dutch linguist and cryptographer who was professor of languages in the late 19th century at the School of Higher Commercial Studies (École des Hautes Études Commerciales), Paris. In 1883, he published the journal titled "La Cryptographie Militaire" (military cryptography) **[*Kerckhoffs, 1883*]** that deal with the famous six principles of practical cipher design for military. The most well-known of this work is the second of his six principles, also known as the *Kerckhoffs's principle*.

physics known as *BB84* [***Bennett_1, 1984***]. It is one of the quantum information processing technologies which employs properties of quantum mechanics to guarantee secure secret key exchanging between two parties for cryptographic purposes. The QKD protocol achieves the security through laws of quantum physics called "*Heisenberg's uncertainty principle*" [***Heisenberg, 1927***] where is the unconditionally secure, unlike a secure with computationally bound in the classical cryptography. Since the passive monitoring by eavesdropper is a disturbance of QKD system that can be detected from the error rate in quantum communication channel. This system must abort by the legitimate parties whenever the observed error rate is higher than that the common threshold. Consequently, the output of this case is a key of length zero which can not be used to cryptographic processes [***ETSI-QKD, 2010***].

Generally, the QKD protocol consists of four steps. In the first one that occurred on the quantum channel, *quantum states* such as the polarization or phase of single photons (BB84) are transmitted and received between two legitimate parties (*Alice* and *Bob*). This process gives a *raw key* corresponding to the list of bit values that *Alice* and *Bob* have sent and measured over the quantum channel, respectively. Secondly, *Alice* and *Bob* use the key sifting procedure over the classical channel to obtain correlated classical bits of the same length called "*sifted key*". Then, a part of their information is revealed to each other in order to estimate the error rate in the quantum channel, known as *quantum bit error rate* (*QBER*). This quantity is surprising feature on QKD. It can determine the joint probability distribution among *Alice* and *Bob* as well as eavesdropper (*Eve*) which cannot be known within the classical key agreement. The third step is key reconciliation. It is the technique needed to ensure that *Alice* and *Bob*'s sifted keys are equal. Finally, privacy amplification [***Bennett_3, 1988***] is to transform this partially secured *Eve*'s information into a highly secret key by public discussion. Basically, the last two steps (reconciliation and privacy amplification) are the same as a scenario of theoretically secret-key agreement by public discussion from correlated randomness discussed in [***Maurer, 1993***], known as *secret-key distillation*. This scenario can explain the QKD system without basics of knowledge in the quantum theory when the classical noisy channel is replaced by the quantum noisy channel.

Since the first publication of QKD prototype in 1992 [***Bennett_2, 1992***], the QKD protocol is already developed and possible place into a competitive industry with commercial QKD products [***ID Quantique, 2012***]. Unfortunately, even if no eavesdropper exists, some quantum bit error may occur from many other reasons as

these in the classical communication systems. For example, it is due to the imperfect system configuration and noise. Therefore, the key reconciliation process was invented to solve these problems where the two parties use a classical interactive communication to shares their correlated bits for agreeing on the common key string. However, the performance of a QKD protocol is reached with respect to the obtained secret key rate. It depends especially on both the efficiency in the detection facilitates of quantum state at the optical hardware level, and also the efficiency of purely classical information process called *QKD-post processing*, such as the secret-key distillation.

1.1 Background

Since the quantum key reconciliation occurs on a classical communication system, it is generally modeled as the context of secret-key agreement between two legitimate parties. In QKD system, the several key reconciliation protocols have been proposed such as the first *BBBSS* [***Bennett_2, 1992***] and the well-known *Cascade* [***Brassard, 1994***]. They are a binary interactive error correction which imply that two legitimate parties exchange parities of subsets of their keys over the public classical authenticated channel. These parities help both parties to locate and to correct the position of errors in their sifted keys by using a binary searching. In *Cascade*, it is certainly the most widely used reconciliation protocol in practical QKD system which the efficiency of reconciliation was improved from *BBBSS* by keeping the track of all investigated block to minimize the number of disclosed informations during reconciliation step. Moreover, relevant works on the optimization for *BBBSS* and *Cascade* are also discussed in [***Van Dijk, 1997***] [***Sugimoto, 2000***] [***Yamazaki, 2000***]. However, these protocols require amount of interactive communications between *Alice* and *Bob* for the binary search process, that perform a high latency over these communications, is then not suitable for high-speed QKD applications.

Apart from above protocols, the others have been also proposed in the literature. For instance, the existing *Winnow* [***Buttler, 2003***] uses the syndrome from a Hamming code as the property of forward error correcting to correct the error in a block with a different parity between *Alice* and *Bob*. Although *Winnow* requires less interactive communication during the reconciliation step that is significantly faster than that of *BBBSS* and *Cascade* protocols, but unfortunately the performance of error detection and correction is also limited with the Hamming code that is still far from the theoretical limit (Shannon's limit). In [***Makkaveev, 2005***], the practical

reconciliation scheme by mean of BCH codes is proposed. These codes can be used to correct the several error bits in a block of key. However, this scheme shows only the BCH parameters for using in the different cases of error rate while does not provide the optimal code rates to achieve the best efficiency of reconciliation scheme.

Furthermore, the other applications of the modern coding theory [*Richardson_1, 2008*] were also addressed in the quantum key reconciliation problem such as the using of LDPC codes in [*Pearson, 2004*] [*Elkouss_1, 2009*] [*Elkouss_2, 2010*]. These proposed schemes can reduce the cost of communication resources, and to improve the efficiency in the key reconciliation step. Nevertheless, LDPC codes employ the message-passing decoding algorithm which are defined by a huge sparse parity-check matrix, so it requires more memory to operate during the reconciliation process. In addition, LDPC codes are usually found efficient for large block length, where is the size of sifted key in case of quantum key reconciliation [*Elkouss_1, 2009*], [*Elkouss_2, 2010*]. Therefore, it can not discard any block of key in the reconciliation process whenever the LDPC decoding fails.

1.2 Motivation

Since the first practical demonstration of QKD over a short distance of approximately 32 centimeters performed by [*Bennett_2, 1992*], the R&D activities on QKD have been conducted ample progress in superior long term security of secret key exchanging. It is now becoming an invaluable component to secure communication infrastructure into a competitive industry with commercial products [*ID Quantique, 2012*], but its applicability is hindered by its low key generation rates. However, the development of QKD post-processing are capable of improving higher-speed secret key generating, if the secret-key distillation, or more precisely, key reconciliation can be handled.

Basically, the channel coding schemes (Error-Correcting Code) can be investigated and applied into the alternative quantum key reconciliation methods. Because, it can be seen as a scenario of classical secret-key agreement problem. In this research, the reconciliation improvement by using error-correcting code schemes is focused on three main subjects; (1) the error-correcting performance, (2) the number of disclosed bits during the reconciliation step, and (3) the reconciliation efficiency for the various possible cases of error rates in QKD system.

The purpose of this work is to present the alternative quantum key reconciliation methods for discrete-variable QKD protocol by adapting the applications of error-correcting code. Specifically, this work addressed on the following research objectives:

- Study on the principles of quantum key distribution, in particular key reconciliation step together with the concept of information theory.
- Research and develop on the alternative quantum key reconciliation methods by adapting error-correcting code schemes.
- Evaluate the efficiency of the proposed quantum key reconciliation methods based on error-correcting code schemes comparable to the existing interactive reconciliation protocols such as *Cascade* and *Winnow*.

In order to overcome these research objectives, the applications of error-correcting codes play a significant role in the improvement of reconciliation efficiency on the view of classical information theory. Specifically, convolutional, BCH, and LDPC codes are adopted as the technique of source coding with side information (*Slepian-Wolf coding*) in order to achieve a good error-correcting performance, to increase the reconciliation efficiency significantly for different cases of error rates, and to minimize the leaked information during the reconciliation. This opens to the promising reconciliation schemes with the lower cost of interactive communication as the target. The expected gain of its ability would significantly impact on the achievable secure secret key generation rate that could be practically implemented in higher-speed QKD system.

In this work, the methodologies for reconciliation improvement are examined by the follows of three main proposed schemes. The first scheme is that the *½-rate convolutional code with side information*. This method uses the fixed ½-rate code based on source coding with side information to achieve a good error-correcting performance. Secondly, the proposed reconciliation is that the *BCH-based Slepian-Wolf coding* with the optimal set of binary BCH code rates to the Slepian-Wolf bound. In this scheme, the BCH decoder is modified by adding one-bit feedback based on syndrome decoding to detect uncorrectable errors whenever the decoding process fails. Finally, the *rate-compatible irregular LDPC codes* are also proposed in the system of Slepian-Wolf coding. The rate-compatible LDPC codes are optimized for the binary symmetric channel (BSC) which the cross-over probability distribution obviously corresponds directly to the various error rates in QKD system. This proposed scheme is expected as a successful reconciliation by interactive feedbacks of syndrome decoding.

1.3 Outline of the Thesis

After a brief introduction on the background and motivation, the remaining chapters of this thesis are organized as follows:

Chapter 2 briefly reviews the principles of quantum key distribution, including the general steps in QKD protocol. In particular, the main focus on the quantum key reconciliation step is explained together with the definitions of two typical binary reconciliation schemes such as *one-way reconciliation* and *reconciliation based on channel coding*, and also with the examples of reconciliation protocols from literature. Finally, the proof of secure secret key capacity are finally discussed in terms of simple entropic quantities.

Chapter 3 first reviews the basics of classical information theory, which concentrates on the notations of source coding, channel coding, and properties of relevant quantities such as entropy and mutual information. Then, the underlying principles of coding theory and some applications of error-correcting codes are briefly introduced in order to improve the efficiency of the key reconciliation. Finally, the definition of Slepian-Wolf coding is introduced with the main focus on its construction for solving the quantum key reconciliation problem, and the equivalence between Slepian-Wolf coding and channel coding is also revealed to be applied the error-correcting code schemes based on the Slepian-Wolf system.

Chapter 4 presents the proposed reconciliation schemes based on applications of error-correcting codes. Specifically, the using of convolutional, BCH, and LDPC codes are adapted in the technique of source coding with side information. This work is conducted based on three main proposed schemes; (1) *½-rate convolutional code with side information*, (2) *BCH-based Slepian-Wolf Coding*, and (3) interactive reconciliation with *rate-compatible irregular LDPC codes*.

Chapter 5 gives the performance evaluation of the proposed schemes through the description of simulation results. These are compared with the currently implemented binary reconciliation protocols in terms of error-correcting capability, reconciliation efficiencies, and number of disclosed informations. Moreover, simulated efficiencies of the main proposed schemes are also compared together with the existing reconciliation protocols.

Finally, the conclusion and discussion are provided in Chapter 6 in order to summarize the results of this work, and then to point out for the future work.

Chapter 2
Principle of Quantum Key Distribution and Reconciliation

This chapter aims at giving the technique needed to distribute the secret keys through the properties of quantum mechanics, called *quantum key distribution* (QKD). It is one of the quantum information processing technologies based on classical cryptography and quantum physics. In this chapter, the principles of QKD is first briefly reviewed including its general steps in Section 2.1. Next, the main focus on the quantum key reconciliation is explained in Section 2.2, together with the definitions of two typical binary reconciliation schemes such as *one-way reconciliation* and *reconciliation based on channel coding*, and also the examples of reconciliation protocols in literature are reviewed in Section 2.3. Then, the proof of secure secret key capacity are discussed in terms of simple entropic quantities in Section 2.4.

2.1 Quantum Key Distribution

The most important function of QKD protocol is used to share a common random bit string, called a *secret key*. It guarantees the distribution of secret keys between two legitimate parties (*Alice* and *Bob*) secretly form an adversary who trying to wiretap the quantum communication channel, conventionally called Eavesdropper (*Eve*). The first QKD protocol is commonly known as the *BB84* ***[Bennett_1, 1984]*** which can be used to illustrate the main principle of quantum key distribution. It consists two types of communication channel as depicted in Fig. 2.1. In a quantum channel, the quantum states are transmitted and received between *Alice* and *Bob* that *Eve* is suspected of wiretapping on the line. Then, a public classical authenticated channel is used for secure key agreement by their public discussion that *Eve* could monitor all the contents in this channel. In BB84, a classical bit are encoded into qubit which is an unit of quantum information by using the polarization of single photon[2]. The encoding is with respect to one of two different orthogonal bases, called the *rectilinear* (0°, 90°) and the *diagonal* basis (+45°, -45°) corresponding to two reference qubits $|0\rangle$ and $|1\rangle$. For example, the classical bit "0" can be encoded with either $|0\rangle$

2 BB84 is that the QKD protocol based on single photon. Meanwhile, the another QKD protocol based entangled photon pair was invented independently by Artur Ekert in 1991, called E91.

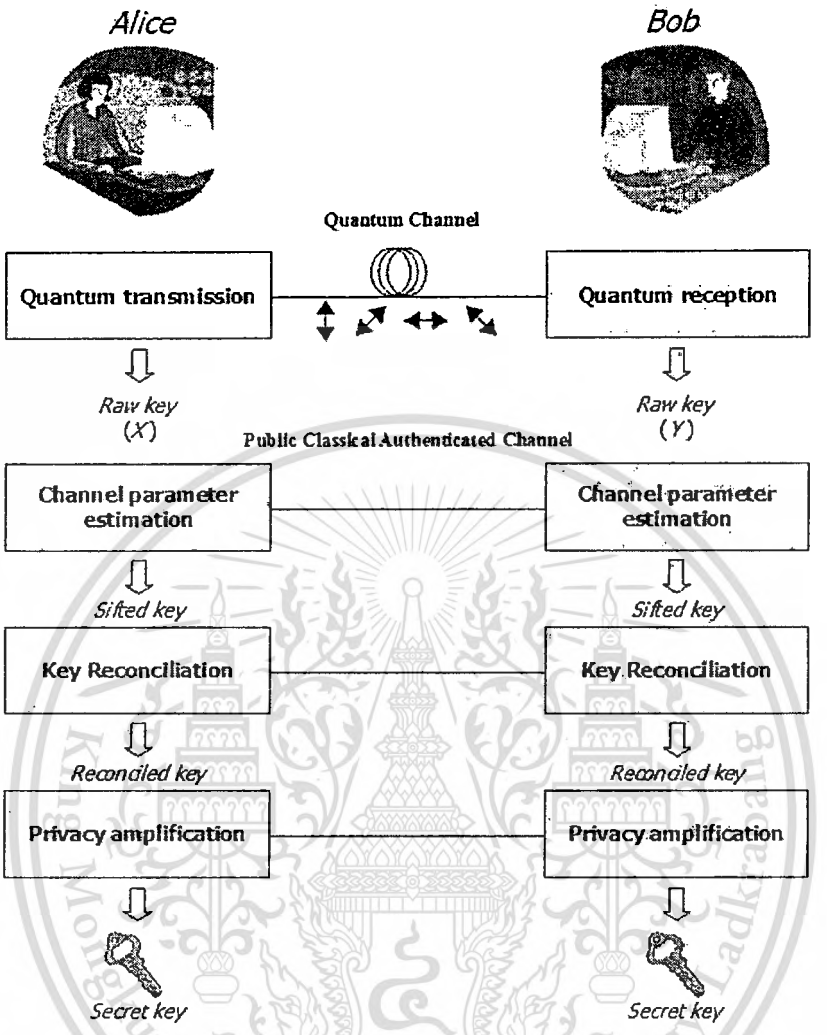


Fig. 2.1 Overview of Quantum Key Distribution

or $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and bit "1" can be encoded with either $|1\rangle$ or $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Generally, the QKD protocol consists of following four steps:

2.1.1 Quantum Transmission and Reception: This step only occurs on the quantum channel which are described by the concept of quantum information theory. First, *Alice* chooses N random bits X_1 , ... , X_N, and encodes each of these bits into qubits form. These encodings are respected with the chosen at random either the rectilinear or the diagonal basis. Then, she sends quantum states carrying these chosen qubits such as polarization or phase of single photon to *Bob* over the quantum channel. When the quantum states arrive to *Bob*'s side,

Table 2.1 Example of quantum transmission and reception by BB84

	Time (t_N)	t_1	t_2	t_3	t_4	t_5	t_6
Alice	Raw keys	0	1	1	0	0	1
	Encoding	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
	quantum states (polarization)	→ (0°)	↗ (45°)	↑ (90°)	↘ (-45°)	↘ (-45°)	↑ (90°)
Bob	measurement	$\|0\rangle/\|1\rangle$	$\|+\rangle/\|-\rangle$	$\|+\rangle/\|-\rangle$	$\|0\rangle/\|1\rangle$	$\|+\rangle/\|-\rangle$	$\|0\rangle/\|1\rangle$
	results	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
	Raw keys	0	1	0	1	0	0

Table 2.2 Key sifting of the key elements from Table. 2.1

	Time (t_N)	t_1	t_2	t_3	t_4	t_5	t_6
Alice	Sifted keys	0	1	-	-	0	-
	Encoding	$\|0\rangle$	$\|-\rangle$	$\|1\rangle$	$\|+\rangle$	$\|+\rangle$	$\|+\rangle$
	quantum states (polarization)	→ (0°)	↗ (45°)	↑ (90°)	↘ (-45°)	↘ (-45°)	↑ (90°)
Bob	measurement	$\|0\rangle/\|1\rangle$	$\|+\rangle/\|-\rangle$	$\|+\rangle/\|-\rangle$	$\|0\rangle/\|1\rangle$	$\|+\rangle/\|-\rangle$	$\|0\rangle/\|1\rangle$
	results	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|1\rangle$	$\|+\rangle$	$\|0\rangle$
	Raw keys	0	1	0	1	0	0
	Compatibility	✓	✓	✗	✗	✓	✗
	Sifted keys	0	1	-	-	0	-

the quantum measurement are performed by *Bob* in order to decode what *Alice* sent. He measures received each of quantum states by a randomly chosen one of two different orthogonal bases. Hence, in this case, *Bob* can obtain classical bits Y_i corresponding to his measurement. After this step, *Alice* and *Bob* have the classical bits $X = (X_1, \ldots, X_N)$ and $Y = (Y_1, \ldots, Y_N)$ respectively, called *raw key*. An example of quantum transmission and reception by BB84 is shown in Table. 2.1.

It is noted that the remaining steps of the QKD protocol are purely classical information processing that occurred on the classical channel, called *QKD post-processing*.

2.1.2 Channel Parameter Estimation: After sending a long stream of key elements in quantum transmission and reception step, *Alice* and *Bob* use the *key sifting* procedure to share the encoding and decoding rules over the classical channel. Its objective is to discard all bits of their raw key where the encoding and the measurement bases (rectilinear and diagonal basis) are not compatible, which is shown in Table 2.2. The result of the sifting is the pair of correlated classical bits with the same length which is held by *Alice* and *Bob* called *sifted key*. Then, they reveal a part of their information to each other in order to estimate the *error rate* in the quantum channel called *"quantum bit error rate (QBER)"*. This quantity is used to determine the joint probability distribution among *Alice* and *Bob* as well as *Eve*, which it might be implied the presence of eavesdropping on the quantum channel. In particular, it can not be known within the classical key agreement. However, if the QBER is too large, *Alice* and *Bob* must abort this system.

2.1.3 Key Reconciliation: The purpose of key reconciliation step is to solve the effect of transmission error over a quantum channel. For example, it is due to the imperfect system configuration and noise. In a general one-way reconciliation scheme, *Alice* first sends a partial correlated information of her sifted keys to *Bob*. Then, *Bob* can guess the value of *Alice* by using the received information and his sifted keys. This step ensures that both *Alice* and *Bob's* sifted keys are equal, called *reconciled key*.

2.1.4 Privacy Amplification: This is the last step of general QKD protocol. It uses to wipes out *Eve's* information for producing a highly secret key by public discussion. Basically, *Alice* and *Bob* shorten their bits by multiplying a binary matrix of universal hashing **[*Bennett_3*, *1988*]**. After this step, they have the identical bits called *secret key* which almost statistically independent of *Eve*'s information, including the leaked information from quantum and classical channels.

It is noted that the last two steps (key reconciliation and privacy amplification) are basically the same as a scenario of theoretically secret-key agreement by public discussion from correlated randomness discussed

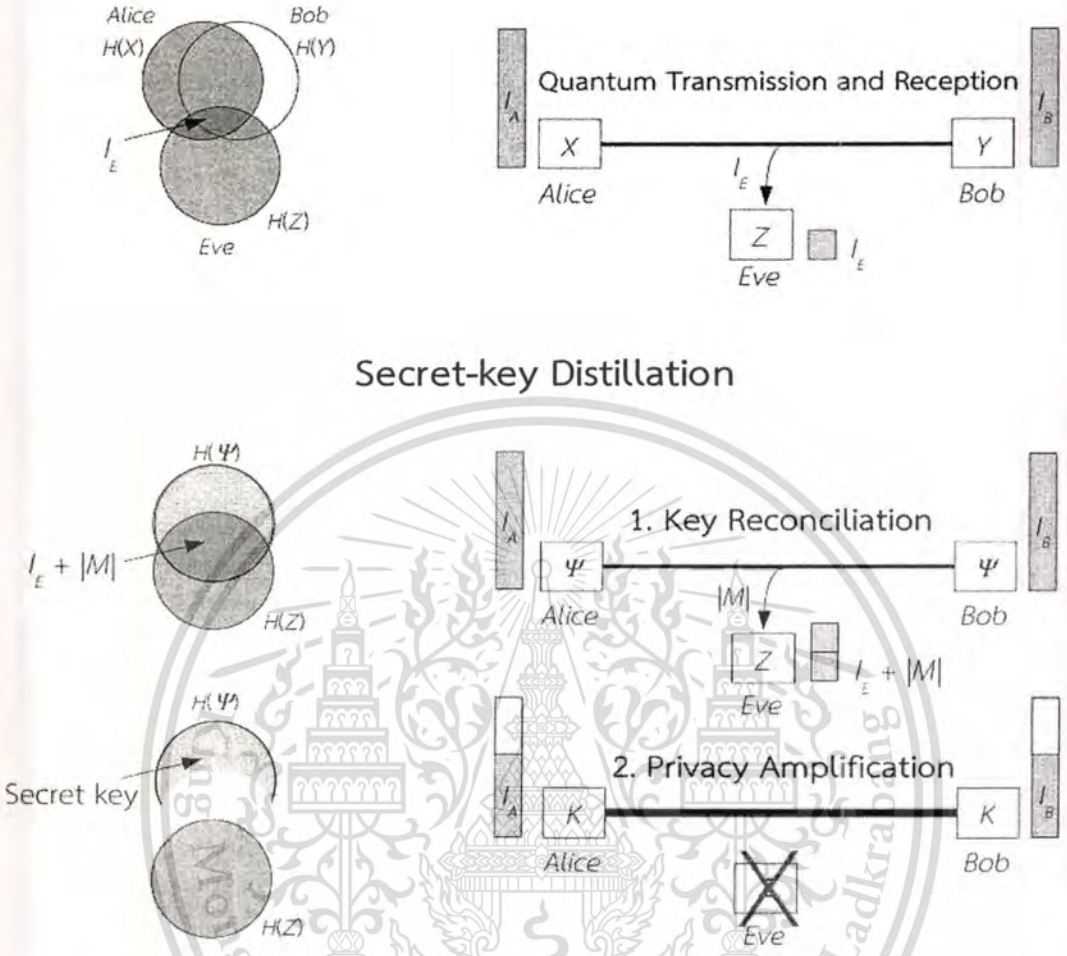


Fig 2.2 Two steps for secret-key distillation: quantum key reconciliation and privacy amplification

in [*Maurer, 1993*]. It is known as *secret-key distillation*. This scenario can explain the QKD system without the knowledge of quantum theory when the classical noisy channel is replaced by the quantum noisy channel.

The overview of the two-step approach for secret-key distillation is shown in Fig 2.2. After the quantum transmission and reception step, *Alice* and *Bob* have the binary strings modeled by the random variables X and Y respectively, and the random variable Z models the eavesdropper's knowledge I_E bits which wipes out from the quantum channel. In the first step of secret-key distillation, *Alice* and *Bob* share some of their information which is denoted as M. It is for agreeing on a common string Ψ, that ensure the sifted keys of *Alice* and *Bob* into a fully correlated string. However, the number of bits M is the leaked information during the reconciliation process which can be monitored by *Eve*, and it will be then taken into

account of *Eve*'s knowledge becoming the variable Z' ($Z' = l_E + |M|$). Finally, privacy amplification is the last step to transform this partially secured *Eve*'s information into a highly secret key K by reducing the knowledge of *Eve* from Ψ.

2.2 Quantum Key Reconciliation

Reconciliation is the one of classical parts in a QKD protocol, and aims at correcting the transmission error after the distribution of quantum informations over a quantum channel. In this step, a classical interactive communication is necessary to use for a practical reconciliation scheme.

In this section, the definitions of a general reconciliation scheme and an alternative reconciliation scheme based on channel coding are firstly reviewed for a discrete-variable[3] QKD protocol in Section 2.2.1 and 2.2.2, respectively. These are mostly described from [*Renner, 2005*].

2.2.1 One-Way Reconciliation Scheme

A typical reconciliation scheme is a *one-way communication* where only *Alice* needs to send the least number of partial correlated information to *Bob* to be able to correct a value of sifted keys at *Bob*'s side. This is illustrated in Fig. 2.3, where they have the classical inputs $x \in \mathcal{X}$ and $y \in \mathcal{Y}$, respectively, and let $\mathcal{H}$ be a two-universal family of hash functions from $\mathcal{X}$ to $\mathcal{Z}$, which f is chosen uniformly at random from $\mathcal{H}$ ($f \in \mathcal{H}$). Then, the main procedures of this scheme can be described by following step:

Step 1.) Sender: *Alice* computes the correlated information z by $z = f(x)$, where $z \in \mathcal{Z}$. Then, she communicates f and z to *Bob*.

Step 2.) Receiver: *Bob* calculates an output value x', where $x' \in \mathcal{X}$. This scheme is successfully concluded when the function f of an output value x' matching with the *Alice*'s correlated information z ($f(x') = z$). Otherwise, the abortion must happen.

It is noted that the transmission of reconciliation scheme contains the useful information on sifted keys of *Alice* and *Bob*, which might be leaked to *Eve* whenever the communication channel is insecure. For any pair of inputs x and y, and for any communication (f, z), the minimum leakage of one-way reconciliation scheme

3 Discrete-variable QKD (DV-QKD) is that the modulation of quantum states in discrete variables, such as polarization or phase. Meanwhile, continuous variables QKD (CV-QKD) represents quantum states in continuous Hilbert spaces, which the most notable examples of coherent or squeezed states.

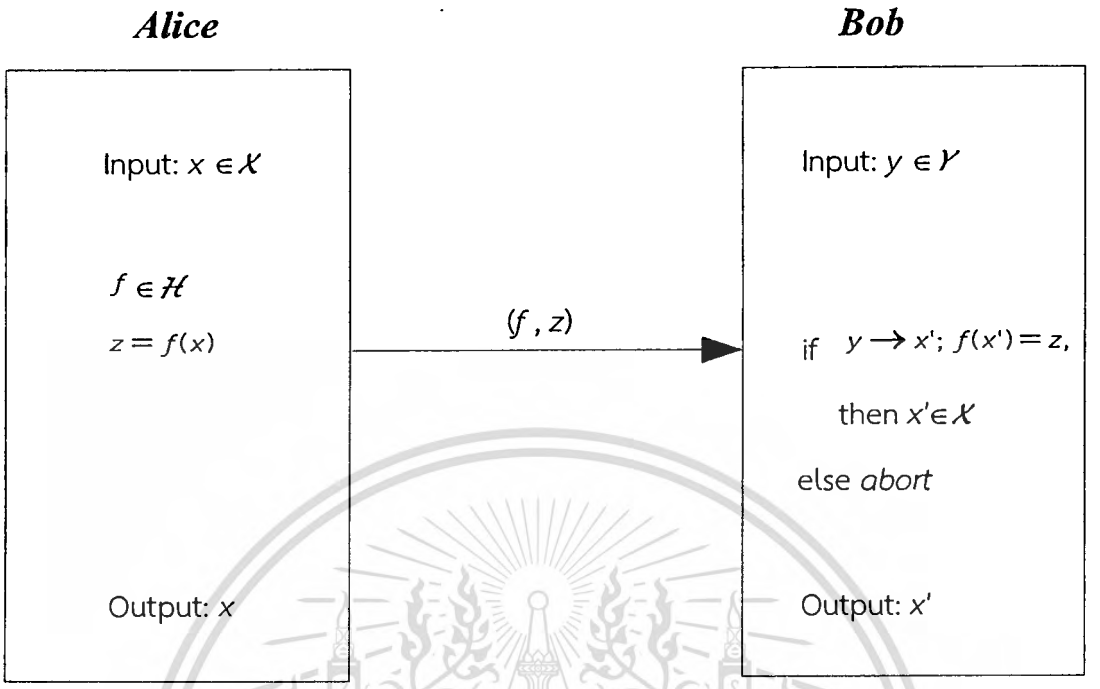


Fig. 2.3 One-way reconciliation scheme

replies on the maximum joint entropy $H_{max}^{\varepsilon}(X|Y)$, where this reconciliation scheme is ε-secure on the joint probability distribution $P_{XY}(x,y)$, if x and y are chosen according to $P_{XY}(x,y)$.

The bound on the leaked information of one-way reconciliation scheme ($leak_{recon(X,H)}$) are previously proved by **[*Renner, 2005*]**, which Alice must send her correlated information z to Bob for agreeing on their common key (x = x') satisfying the following inequality

$$leak_{Recon}\{\mathcal{X}, \mathcal{H}\} \leq H_{max}\left(P_{XY}(x,y)|Y\right) + \log\left(2/\varepsilon\right). \qquad (2.1)$$

2.2.2 Reconciliation Scheme based on Channel Coding

Error-Correcting Code (ECC) is a technique used for controlling errors in classical data transmission over unreliable or noisy communication channels. It can be adapted for an alternative reconciliation by the fundamental of channel coding theorem.

For a reconciliation scheme based on error-correcting codes, it can be specified by Fig 2.4, where the inputs of *Alice* and *Bob* are the strings

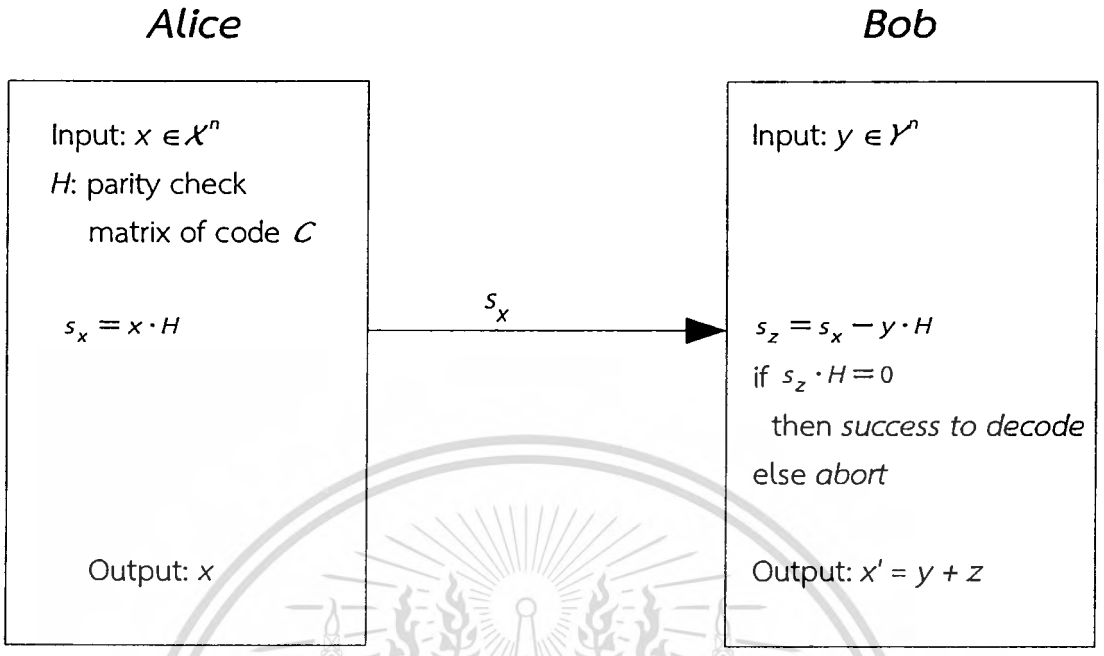


Fig. 2.4 Reconciliation scheme based on error-correcting codes

$x = \{x_1, x_2, \ldots, x_n\}$ and $y = \{y_1, y_2, \ldots, y_n\}$, respectively. This scheme is secure if the inputs x and y are distributed according to a joint probability distribution $P_{xy}(x,y)$, where $x \in \mathcal{X}^n$ and $y \in \mathcal{Y}^n$. Let C be a code containing a parity check matrix H defined over GF(q) (GF is called a *Galois Field*). The main procedures of this scheme is described by the following steps:

Step 1) **Encoder:** *Alice* first compresses x to the syndrome $s_x = x \cdot H$, and sends s_x to *Bob*.

Step 2) **Decoder:** *Bob* then calculates the syndrome of z by $s_z = s_x - y \cdot H$, where s_z is an indicator of the error position on y. This scheme would success when $s_z \cdot H$ is "0". Next, z can be estimated by the error pattern estimator of code C, and *Bob*'s output value x' are finally calculated by $x' = y + z$.

Since the communication of s_x are sent over a public channel, which *Eve* can also obtain whenever this channel is insecure. For the channel coding scheme, the amount of s_x must depend on the rate of code C which close to the correlation of channel capacity (Section 3.1.3). Let $P_{xy} \in \mathcal{P}(\mathcal{X} \times \mathcal{Y})$ be a probability distribution, and let $\delta > 0$. Then, the minimum leakage of reconciliation scheme based on channel coding is given by [*Renner, 2005*]

$$leak_{Recon\{C\}} = H(X|Y) + \delta . \tag{2.2}$$

2.3 Reconciliation Protocols

Many various quantum key reconciliation protocols have been proposed in literature which the binary interactive reconciliation schemes are traditionally used for QKD protocols. In this section, the examples of existing reconciliation protocols are presented. They are for using in discrete-variable QKD, where *Alice* and *Bob* have the binary key elements of n-bit X and Y (X, $Y \in GF(2)^n$), respectively.

2.3.1 BBBSS

C. H. Bennett *et al*. first proposed a binary interactive reconciliation protocol for using in their experiment which published in the paper titled "*Experimental quantum cryptography*", called *BBBSS* [***Bennett_2, 1992***]. It requires *Alice* and *Bob* to exchange parities of subsets of their key elements in each block. If the parities between two parties are not matched, they then use a binary searching to locate the position of errors in their key elements and correct them. This protocol requires a certain number of iterations with the bit interleaving between two parties.

For iteration *i*, *Alice* and *Bob* disclose their parities of a block $\mathcal{B}_j^{(i)}$ which are defined by

$$Par_{X,j}^{(i)} = \sum_{t \in \mathcal{B}_j^{(i)}} X_t , \text{ and } Par_{Y,j}^{(i)} = \sum_{t \in \mathcal{B}_j^{(i)}} Y_t \tag{2.3}$$

respectively. If the parities are wrong $Par_{X,j}^{(i)} \neq Par_{Y,j}^{(i)}$, it means that there is an odd number of errors in the block $\mathcal{B}_j^{(i)}$. Then, the binary searching process will be begun until these errors can be located and corrected by simply flipping bits. This protocol ends when the parities are disclosed enough for error correction corresponding to the observed error rate.

2.3.2 Cascade

Cascade is the well-known interactive reconciliation protocol based on *BBBSS*. It was proposed by G. Brassard and L. Salvail in the publication paper titled "*Secret key reconciliation by public discussion*" [***Brassard, 1994***]. This protocol improved the efficiency of reconciliation in term of the number of disclosed bits by keeping the track of all investigated block of their key elements. Then, it takes advantage of this information to reduce the number of iterations, while *BBBSS* does

not keep this tracking. In the traditional *Cascade* [***Brassard, 1994***], the number of disclosed bits (d) depends on the parity informations which are exchanged over the public classical channel. It can be estimated as

$$d \approx l(1.1+e)h(e) \quad , \tag{2.4}$$

where l is a size of sifted key, e is a quantum bit error rate (*QBER*), and $h(e) = -e\log_2 e - (1-e)\log_2(1-e)$. Relevant works on the optimization of block size for *Cascade* are also discussed in [***Sugimoto, 2000***] [***Yamazaki, 2000***]. Its objective is to minimize the number of disclosed bits during the reconciliation process to be the closest to the theoretical limit.

2.3.3 Winnow

Winnow is the one of interactive reconciliation protocols similar to *BBBSS* and *Cascade*. It was proposed by W. T. Buttler *et al.* in publication titled *"Fast, Efficient Error Reconciliation for Quantum Cryptography"* [***Buttler, 2003***]. Unlike *BBBSS* and *Cascade*, *Winnow* uses the syndrome from a Hamming code [***Hamming, 1950***] as the property of forward error correcting to locate and correct the error in a block with a different parity between *Alice* and *Bob* instead of correcting errors by iterative binary search. If the parities of each block between *Alice* and *Bob* are not matched, the Hamming syndromes are calculated in following

$$S_X=\left(\sum_{j=1}^{N_h} X_i h_{i,j}^{(m)}\right)(mod\,2) \in\{0,1\}^m \quad \text{and} \quad S_Y=\left(\sum_{j=1}^{N_h} Y_i h_{i,j}^{(m)}\right)(mod\,2) \in\{0,1\}^m \tag{2.5}$$

respectively, where $h^{(m)}_{i,j}$ is the parity check matrix of Hamming code. Then, the syndrome matching is computed by $S_d = S_X \oplus S_Y$. The position of errors can be located and corrected by this syndrome matching S_d, whenever the syndrome between *Alice* and *Bob* are different $S_d \neq \{0\}^m$.

The advantage of this protocol is much less requirement on interactive communication than that of binary searching protocols. However, the property of Hamming code allows *Winnow* to correct only single error per block, otherwise, this protocol can not produce accurate result when the block contains more than single-bit error. Therefore, the block size of *Winnow* should be chosen on the error correcting capability of Hamming syndrome. The optimization in [***Yan, 2009***] gives the optimal block size on *Winnow* for using in different cases of error rate.

2.4 Bound of Secure Secret Key Rate and Reconciliation Efficiency

The concepts of coding theorem (information theory) can be used to prove the security of secret key rate in QKD system. This section is actually devoted the bound of secure secret key rate to be guaranteed the security for QKD system, where *Eve* is assumed to possess a purification of *Alice* and *Bob*'s informations.

In the perfect secret-key distillation, the theoretical secure secret key rate (r_{th}) can be defined in terms of only on simple entropic quantities **[*Devetak, 2005*]** by

$$\begin{aligned} r_{th} &= I(X;Y) - I(X;Z), \\ &= \big(H(X) - H(X|Y)\big) - \big(H(X) - H(X|Z)\big), \\ &= H(X|Z) - H(X|Y), \end{aligned} \tag{2.6}$$

where $H(.|.)$ is the conditional von Neumann entropy. However, in the case of secret-key distillation, it actually occurs on classical communication system, which the conditional von Neumann entropy can be transformed into the conditional Shannon entropy. Therefore, $H(X|Z)$ depends on the uncertainty of *Eve*'s information on the *Alice* and *Bob*'s secret key bits, and $H(X|Y)$ represents the minimum information needed by *Bob* to recover his sifted keys in the key reconciliation step. It is noted that these notations are used to quantifies the uncertainty associated with respect to random variables which are the basic concept of information measurements in classical information theory (Section 3.1)

In a practical realization, the term of $H(X|Y)$ corresponds to the minimum information that ensures *Alice* and *Bob*'s sifted keys are equal. It is certainly greater than in Eq (2.6). Consequently, the actual secure secret key rate (r_{real}) can be defined as

$$r_{real} = H(X|Z) - f \cdot H(X|Y). \tag{2.7}$$

In the following Eq (2.7), f is the parameter of reconciliation efficiency that significantly uses to evaluate the efficiencies of different reconciliation schemes in Chapter 5. For the perfect reconciliation scheme, f is equal to one, and the maximum *QBER* acceptable to guarantee the security for any QKD system is 11%, which certainly obtain a positive value of secure key rate as shown in Fig. 2.5.

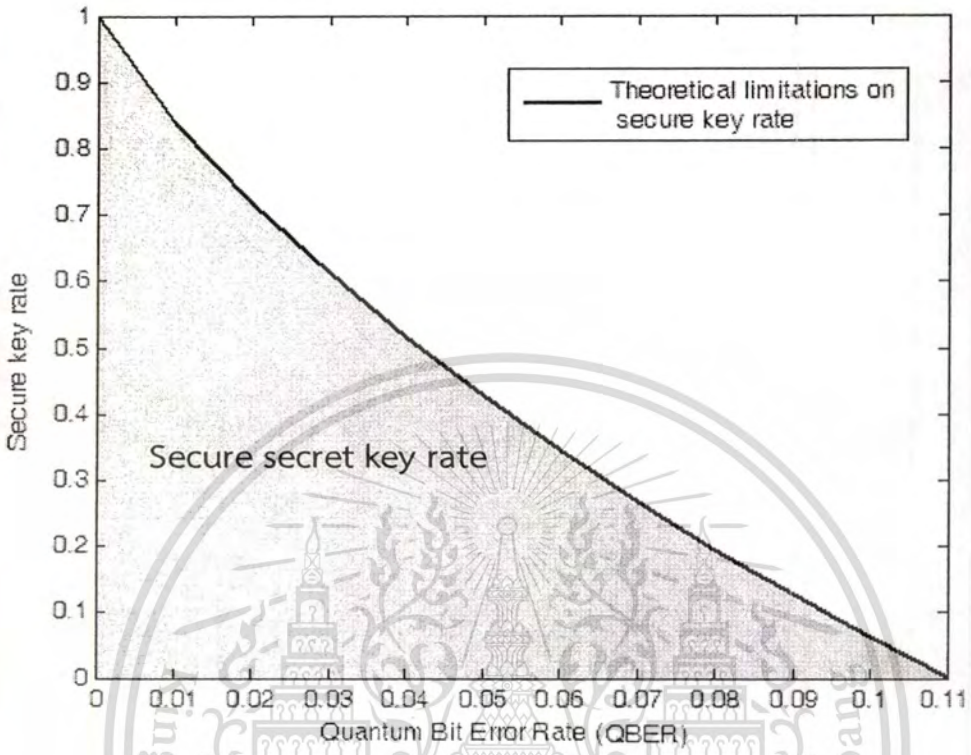


Fig. 2.5 Theoretical limitations for secure secret key rate (r_{th}) as a function of *QBERs*

Chapter 3
Basics of Classical Information Theory and Coding

This chapter presents the useful preliminaries of classical information and coding theory needed in the study of quantum key reconciliation. The brief introduction of classical information theory is first reviewed in Section 3.1, which is a consequence of original work published by Claude E. Shannon **[*Shannon, 1948*]**. In section 3.2, the principles of error-correcting code and its applications are briefly introduced for the main methodology to improve the reconciliation efficiency. Those are Hamming code **[*Hamming, 1950*]**, BCH code **[*Bose, 1960*]** **[*Hocquenghem, 1959*]**, convolutional code **[*Elias, 1955*]**, and Low-Density Parity-Check code (LDPC) **[*Gallager, 1963*]**, respectively. Finally, Section 3.3 discusses the definition of Slepian-Wolf coding with the main focus on its construction for solving the quantum key reconciliation problem, and also its relationship to channel coding in order to apply the error-correcting code schemes based on the Slepian-Wolf system.

3.1 Information Theory

Classical information theory is a important concept for QKD post-processing. It is accurately used to describe the key elements of *Alice* and *Bob* in classical values after the quantum transmission and reception process. In particular, key reconciliation mostly requires the concepts of classical information theory and information-theoretic security.

Claude E. Shannon proved that two theorems deal with the fundamental principles of communications in journal publication titled "*A Mathematical Theory of Communication*" **[*Shannon, 1948*]**. There are the *source coding* and the *channel coding* theorems, which respectively concern with the limit for data compression of a source and information transfer rate in a given communication channel.

3.1.1 Source Coding

In this research, source coding is only focused for binary discrete sources that use to describe the key elements on discrete-variable QKD protocol. A discrete source are assumed to produce a sequence of symbols x_i each of which is drawn from a finite set of symbols, called an alphabet $\mathcal{X}$. It can be defined by the random variable X on $\mathcal{X}$, according to the probability distribution function $P_X(x)$.

The *Shannon entropy* (or *entropy*) is the basic concept of information measurements which quantifies the average information gain per use with respect to

an information source, or equivalently, a random variable.

By convention, all logarithms are in base 2, unless otherwise specified. For a discrete random variable X with the alphabet $\mathcal{X}$ on the probability distribution $p(x_1), p(x_2), \ldots, p(x_n)$, the entropy of X (denoted by $H(X)$) can be defined as

$$H(X) = H(p(x_1), p(x_2), \ldots, p(x_n)) = -\sum_{i=1}^{n} p(x_i)\log(p(x_i)). \quad (3.1)$$

Noted that the entropy is always positive ($H(X) \geq 0$). If one of the probabilities $p(x_j)$ is 1, the entropy then achieves its minimum value as equal to zero ($H(X) = 0$).

Traditionally, the entropy of a binary random variable are expressed with probability distribution p, and $1-p$ for $0 \leq p \leq 1$, denoted by $h_{bin}(p)$, in following equation as

$$h_{bin}(p) = -p\log p - (1-p)\log(1-p). \quad (3.2)$$

In the source encoder, the entropy of a random variable implies the average number of bits per symbol called the *compression rate* R_S. The expected R_S that possible to construct of any all source codes, must be satisfied by following inequality

$$H(X) \leq R_S \leq H(X) + 1. \quad (3.3)$$

Thus, the minimum number of bits per symbol is not lower than that entropy ($R_S \geq H(X)$). This inequality actually indicates the information rate to achieve uniquely extendable codes such as *Huffman coding* [**Huffman, 1952**].

3.1.2 Joint and Conditional Entropies

The entropy of a single random variable is previously introduced in Section 3.1.1. In case of two random variables X and Y with the alphabets $\mathcal{X}$ and $\mathcal{Y}$ respectively, they may be correlated on the joint probability distribution $P_{XY}(x,y)$ ($P_{XY}(x,y) \neq P_X(x)P_Y(y)$). Then the *joint entropy* of both X and Y ($H(X,Y)$) is defined as

$$H(X,Y) = -\sum_{x\subset X}\sum_{y\subset Y} P_{X,Y}(x,y)\log P_{X,Y}(x,y), \quad (3.4)$$

where $H(X,Y) \leq H(X) + H(Y)$, when X and Y are independent.

The joint entropy $H(X,Y)$ quantifies the amount of uncertainty in random variables X and Y. However, if this definition is extended to n random variables $X_1, \ldots, X_n$, their joint entropy can be defined as

$$H(X_1,\ldots,X_n) = -\sum_{x\subset X_1} \cdots \sum_{x\subset X_n} P_{X_1,\ldots,P_{X_n}}(x_1,\ldots,x_n)\log P_{x_1,\ldots,P_{x_n}}(X_1,\ldots,X_n). \quad (3.5)$$

For two discrete random variables X and Y with the alphabets $\mathcal{X}$ and $\mathcal{Y}$ on the joint probability distribution $P_{XY}(x,y)$, the *conditional entropy* of X given Y, denoted by $H(X|Y)$, can be defined as

$$H(X \mid Y) = -\sum_{x\subset X}\sum_{y\subset Y} P_Y(y) P_{X|Y}(x \mid y)\log P_{X|Y}(x \mid y), \quad (3.6)$$

where $P_{X|Y}(x \mid y)$ is the conditional probability distribution of X given Y.

The conditional entropy $H(X|Y)$ quantifies the remaining uncertainty of a random variable X, if the value of another random variable Y is known. It is noted in two cases that if X and Y are independent, then $H(X|Y)$ is $H(X)$. Meanwhile, if X is a function of Y, then $H(X|Y)$ is "0", More specifically, it is always true that $H(X|Y) \leq H(X)$.

3.1.3 Channel Coding

In the communications over a channel, *channel coding* is the important concept to find the theoretical maximum information transfer rate over a noisy channel. Its main objective is to optimize the transmission rate constrained by the transmission reliability.

A discrete channel is characterized by a finite input alphabet $\mathcal{X}$ which is the symbols that sender transmits to channel. Meanwhile, a finite output alphabet $\mathcal{Y}$ is the symbols that the receiver obtains. For simplicity, the *Discrete Memoryless Channel* (DMC) is only discussed for channel behavior, which the output of DMC depends only on the input at the same instant. In this case, all these transition probabilities from x_i to y_j are gathered in a transition matrix. It can be defined as n-dimensional conditional distribution $p(y^n \mid x^n)$.

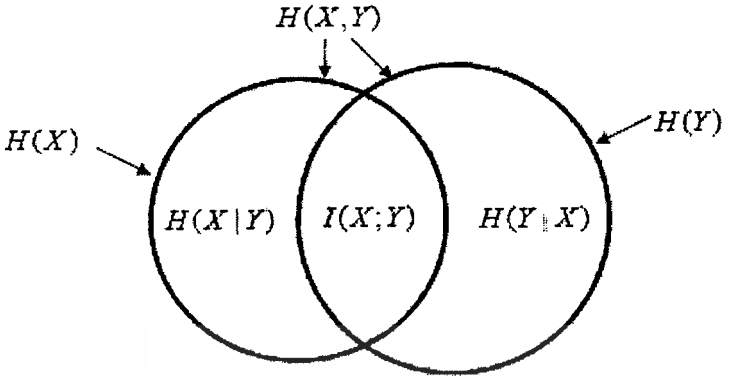


Fig. 3.1 The relation between the entropy of two random variables X and Y, and their mutual information, joint and conditional entropies.

In the channel coding, the *mutual information* is an important quantity between two random variables. The mutual information between X and Y is denoted by $I(X;Y)$. It can then be defined as

$$I(X;Y) = H(X) + H(Y) - H(X,Y) \tag{3.7}$$

or in term of the conditional entropy as

$$I(X;Y) = H(X) - H(X \mid Y) = H(Y) - H(Y \mid X), \tag{3.8}$$

where $I(X;Y) = I(Y;X)$, and it satisfies $I(X;Y) \geq 0$ when X and Y are independent.

The mutual information $I(X;Y)$ quantifies the amount of information that Y provides about X. In other words, it is the reduction in the uncertainty about X from the knowledge of Y. It is also noted in two cases that if X and Y are independent or the knowledge of Y does not provide any information about X, then $I(X;Y) = H(X) - H(X)$ is 0. Meanwhile, if X is a function of Y or X and Y are a pair of fully correlation, then $I(X;Y) = H(X) - 0$ is $H(X)$.

The relation of these quantities (an entropy, joint and conditional entropies, and a mutual information) on two random variables X and Y are illustrated in Fig 3.1.

Because the transmission error may occur over a discrete memoryless channel as the conditional probability distribution $p(y|x)$. Therefore, *Alice* wishes to transmit the information to *Bob* reliably through this channel. The limitation on the rate of transmission is proved by Shannon called the *channel capacity* that can be

defined by

$$C = \max_{P_X(x)} I(X;Y), \tag{3.9}$$

where $I(X;Y)$ denotes the mutual information between X and Y. This definition implies the upper bound of the transmission rate $I(X;Y)$ bits per channel use.

For example, the two common channels for binary input alphabets are reviewed as follows:

- **Binary Erasure Channel (BEC)** models the information was not received over the transmission (*erased*), such as a packet losses over a network connection. In this model, the input and output are $X = \{0, 1\}$, and $Y = \{0, 1, \#\}$, respectively, where # denotes the erasure symbol. Erasure # happens with a probability e, independently of the input symbol. The model for BEC is shown in Fig. 3.2, where is characterized by the conditional probabilities as

  $$p(0|0) = p(1|1) = 1 - e,$$
  $$p(\#|0) = p(\#|1) = e, \text{ and}$$
  $$p(1|0) = p(0|1) = 0.$$

  Note that the capacity of a BEC (C_{BEC}) is $1 - e$ bits per channel use, where e is the probability of erasure.

- **Binary Symmetric Channel (BSC)** models the transmission errors that it will be flipped with a probability e (*crossover probability*), but no erasures happen. Fig. 3.3 shows the channel model for BSC, where is characterized by the conditional probabilities as

  $$p(0|0) = p(1|1) = 1 - e, \text{ and}$$
  $$p(1|0) = p(0|1) = e.$$

  The binary input X and output Y are both {0,1}, and the crossover probability is e. It is noted that the capacity of a BSC (C_{BSC}) is $1 - H(e)$ bits per channel use, where $H(e)$ is the binary entropy function in Eq. (3.2).

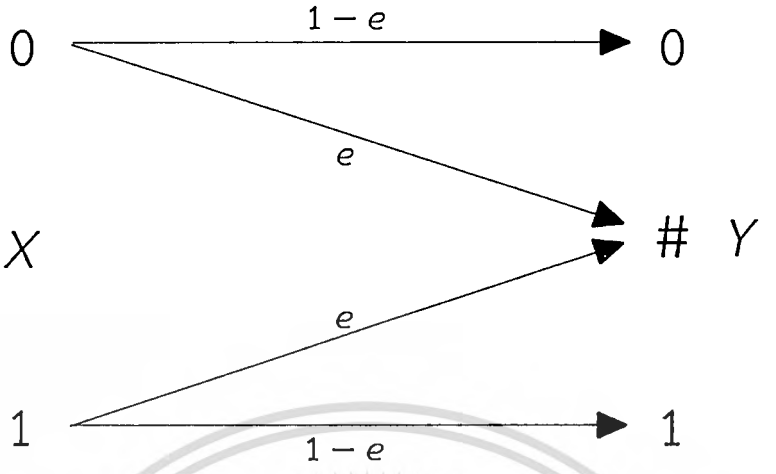


Fig. 3.2 Channel model for the binary erasure channel (BEC)

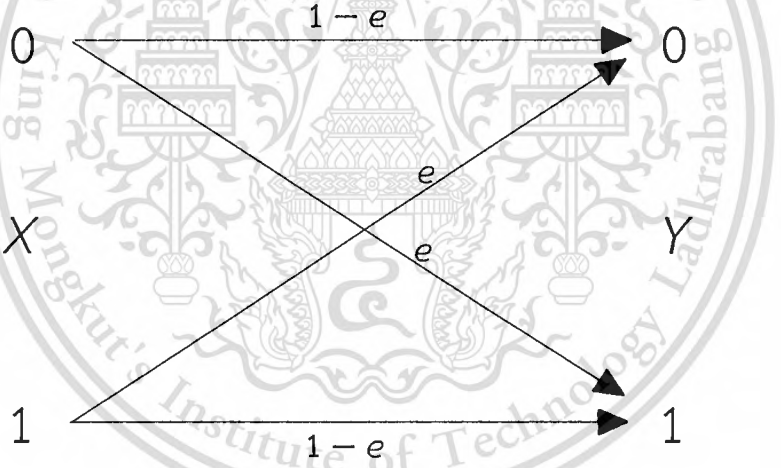


Fig. 3.3 Channel model for binary symmetric channel (BSC)

3.2 Overview of Error-Correcting Codes and the Examples of Codes

Communication channels may suffer from many factors, for instance, due to noise, interference, distortion, and the imperfect hardware configuration. The *Error-Correcting Code* (ECC) aims at developing methods for encoding information in such a way that even if the channel (or storage medium) introduces errors, the receiver can correct the errors and recover the original transmitted information by decoding process. Moreover, it also reduce the consumption of transmitted power that are very critical for long distance communications such as deep-space and satellite communications.

The history of error-correcting code started with the introduction of information theory by *Claude E. Shannon* in 1948 [***Shannon, 1948***]. He showed the prediction of the arbitrarily reliable communications are achievable by redundant in channel coding, known as *Shannon's limit*. It became as the motivation to the communications community which need to develop the coding schemes in order to achieve higher reliability in communications over noisy channels as close to the Shannon's limit as possible. All error-correcting code schemes are based on the same concept that the information bit is encoded by adding the *redundancy* to be the *codeword* in order to retrieving detection and correction capability. This codeword is transmitted through communication systems or stored in the devices as its purpose. Then it will be recovered to be the original form by decoding related to the encoding process. For example, the illustration of principle concept that obtained by the systematic block encoding and decoding are shown in Fig. 3.4. The systematic encoding means that the information symbols always appear in k positions of a codeword, and the remaining $n - k$ symbols in a codeword can be used for error detection and correction purposes. The set of all code sequences is an error-correcting code which is denoted by C.

It is obvious for more than fifty years, the error-correcting code plays an important role which has been developing and adopting to many communication systems such as mobile communications, satellite communications, and digital video broadcasting systems.

In this section, some applications of error-correcting codes are introduced. Those are *Hamming code*, *BCH code*, *convolutional code*, and *Low-Density Parity-Check code (LDPC)*, respectively. They are the mainly contributed to this research for improvement the efficiency of the key reconciliation schemes.

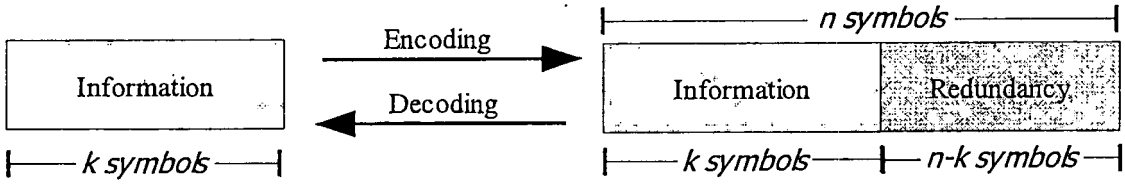


Fig 3.4 Systematic block encoding/decoding for error correction

3.2.1 Hamming Code

After C. E. Shannon proved the theoretical reliable communications in 1948, the earliest error-correcting code was found in 1950 by *Richard Hamming* known as the *Hamming code* [***Hamming, 1950***]. The generalization of Hamming code ((*7,4*)-*Hamming code*) allows the pattern of parity checking to correct the single error along with the detection of double errors. In mathematical terms, Hamming codes are a family of linear block codes *C* that can be expressed in term of (*n*, *k*, *t*) for a code with *k* input symbols, *n* output symbols, and the error capability *t*. Let *u* be an input vector of *k* symbols, and *G* is a generator matrix *k* x *n* over GF(*q*). Then, the codeword is computed by

$$\bar{v} = \bar{u}G, \tag{3.10}$$

where $\bar{v}$ is a codeword vector of *n* symbols that any codeword $\bar{v} \in C$. Because *C* is a *k*-dimensional subspace of the set of all *n*-tuples, there is an $(n-k)$-dimensional *dual space*, denoted by C^T, which generated by the rows of a parity-check matrix ***H***. Therefore, $\bar{v}$ satisfies

$$\bar{v}H^T = \left[0\right]_{1,n-k}. \tag{3.11}$$

Note that the rows of *G* are all legal codewords, then $G \cdot H^T = \left[0\right]_{k,n-k}$.

A codeword vector $\bar{v}$ are assumed to transmit over a BSC, and errors occur on a received vector as $\bar{r} = \bar{v} + \bar{e}$. Then, the syndrome of $\bar{r}$ is computed by

$$s = \bar{r}H^T = (\bar{v} + \bar{e})H^T = \bar{e}H^T. \tag{3.12}$$

where *s* is a set of syndrome vector. It could indicate the error position on $\bar{r}$ corresponding to column of ***H***, but not depend upon the transmitted codeword $\bar{v}$.

The columns of H are binary vector of length m, where $m \geq 2$. Therefore, the important parameters for Hamming code are as following

- Code length: $n = 2^m - 1$,
- number of information symbols: $k = 2^m - m - 1$,
- number of parity symbols: $n - k = m$,
- Error correcting capability: $t = 1$.

Consequently, any code that achieving these parameters are called as Hamming code.

It should be noted that the Hamming code had been adopted for the reconciliation protocol, known as *Winnow* [***Buttler, 2003***]. Hamming syndrome is utilized to locate and correct the error position in the block of sifted keys between two legitimate parties.

3.2.2 BCH Code

The Bose, Chaudhuri, and Hocquenghem (BCH) codes were independently discovered by Alexis Hocquenghem in 1959 [***Hocquenghem, 1959***], and Raj Chandra Bose and Dijen Ray-Chaudhuri in 1960 [***Bose, 1960***]. They are a class of multiple error correcting codes over GF(q) that can be used to correct several error bits per block. Generally, BCH codes are a family of linear block codes. It can be expressed in term of (n, k, t) which correspond to their generator polynomials $g(x)$ of degree $n - k$, when block length $n = 2^m - 1$, and number of parity symbols $n - k \leq mt$, where $m \geq 3$.

This code is a t-error-correcting that actually correct t or fewer random errors over n bits. The generator polynomial $g(x)$ of t-error correcting BCH code is constructed in term of its roots from GF(2^m). Let α be a primitive element in GF(2^m), the generator polynomial $g(x)$ of the t-error correcting BCH code of length $2^m - 1$ is the lowest-degree polynomial over GF(2) which α^b, α^{b+1}, ... , α^{b+2t-1} are roots of the generator polynomial $g(x)$. Let $\Phi(x)$ be the minimal polynomial of α^i, then $g(x)$ is computed by

$$g(x) = \text{LCM}\{\Phi_b(x), \Phi_{b+1}(x), \ldots , \Phi_{b+2t+1}(x)\} \tag{3.13}$$

where LCM$\{\Phi_b(x), \Phi_{b+1}(x), \ldots , \Phi_{b+2t+1}(x)\}$ defined as the least common multiple of $\Phi_b(x), \Phi_{b+1}(x), \ldots , \Phi_{b+2t+1}(x)$.

For any code, the generator matrix relates to the parity-check matrix. They are assumed that $h(x)$ is associated with the parity-check matrix of the t-error

They are assumed that $h(x)$ is associated with the parity-check matrix of the t-error correcting BCH code, called the parity-check polynomial. Then, the connection between the generator polynomial and the parity-check polynomial can be expressed as

$$g(x)\,h(x) = x^n + 1. \tag{3.14}$$

Note that α^b, α^{b+1}, ... , α^{b+2t-1} are roots of the generator polynomial $g(x)$, and every codeword polynomial $v(x) \in C$, Then

$$v(\alpha^b) = v(\alpha^{b+1}) = \ldots = v(\alpha^{b+2t-1}) = 0. \tag{3.15}$$

Since $vH^T = 0$, the parity-check matrix H can be written by

$$H = \begin{bmatrix} 1 & \alpha^{b} & \alpha^{2b} & \cdots & \alpha^{(n-1)b} \\ 1 & \alpha^{b+1} & \alpha^{2(b+1)} & \cdots & \alpha^{(n-1)(b+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+2t-1} & \alpha^{2(b+2t-1)} & \cdots & \alpha^{(n-1)(b+2t-1)} \end{bmatrix}. \tag{3.16}$$

In the BCH encoding, let $u(x)$ is associated with a message to be encoded. Then, the codeword polynomial $v(x)$ can be computed by

$$v(x) = x^{n-k}u(x) + \left[x^{n-k}u(x) \bmod g(x)\right]. \tag{3.17}$$

There are many decoding algorithms for BCH codes. It mains idea is to use the elements of GF(2^m) for numbering the positions of codeword. Let $r(x) = v(x) + e(x)$ be the polynomial associated with a received codeword, where the error polynomial is denoted by $e(x)$. Then, the decoding procedure of BCH codes can be divided as following steps

Step 1) Compute the syndrome sequence S_1, S_2, ... , S_{2t} by evaluating on the received codeword polynomial at the zeros of the code in following

$$S_i = r(\alpha^i) = v(\alpha^i) + e(\alpha^i) = e(\alpha^i),\ 1 \le i \le 2t \tag{3.18}$$

Step 2) Find the coefficients Λ_1, Λ_2, ... , Λ_v of the error-locator polynomial, that $\Lambda(x)$ is defined as

$$\Lambda(x)=1+\Lambda_1(x)+\Lambda_2(x^2)+...+\Lambda_v(x^v), \quad v\leq t. \tag{3.19}$$

Step 3) Determine the error locations α^{j1}, α^{j2} , ... , α^{jv} by finding the inverse of the roots of error-locator polynomial $\Lambda(x)$

Step 4) Determine the error values e_{j1} , e_{j2} , ... , e_{jv} , and correct the received codeword $\bar{r}$ with the error locations and the error values.

It should be noted that the set $\{\alpha^{j1}, \alpha^{j2}, ..., \alpha^{jv}\}$, and $\{e_{j1}, e_{j2}, ..., e_{jv}\}$ are the error positions and the error values respectively, where $e_j \in \{0, 1\}$ for BCH codes, and $\alpha \in GF\{2^m\}$.

This code may not produce the accurate results of BCH decoding (decoding failure) when the number of errors in block length n (n_{err}) more than the t-error correcting capability of BCH code ($n_{err} > 1$). This failure can be declared whenever one of following events occurs [*Sarwate, 1990*];

- Unable to compute the coefficients of the error-locator polynomial,
- The error locations are not v distinct roots of unity,
- Some of the error values are either zero, or do not belong to the symbol field.

In this research, the BCH codes is adopted to the one of methodology for reconciliation improvement in Section 4.2, due to their quite flexibilities in choice of parameters, in particular code rates, properly to optimize for different case of error rates in QKD system.

3.2.3 Convolutional Code

Convolutional code is the one of the popular binary error-correcting codes that first introduced by Peter Elias in 1955 [***Elias, 1955***]. Unlike linear block codes, convolutional codes work on a stream of data instead of segmenting data into distinct blocks which the encoders add the redundant bits to a continuous stream of input data by using a linear shift register. Generally, convolutional codes can be denoted in term of (n, k, m), where output bits n are generated whenever input bits

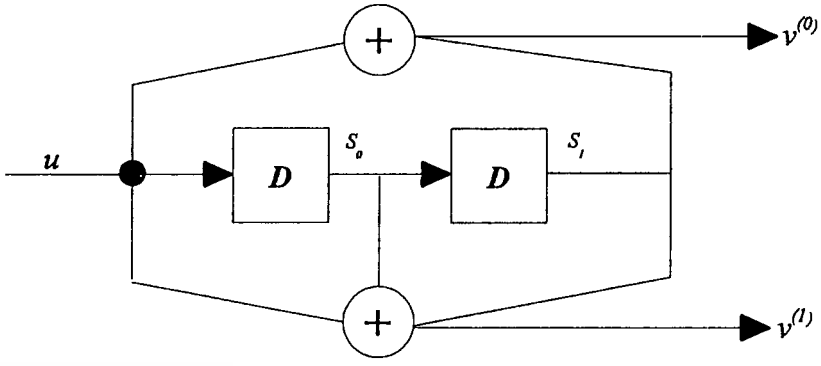


Fig. 3.5 An encoder for (2, 1, 2) convolutional code

k are received, and m is the number of previous k-bit input blocks that must be memorized in the encoder, called as the memory order of convolutional code. In the contents of the shift register, the current outputs n are linear combinations (i.e. with exclusive-OR gates) of the present k input bits, and the previous $m \times k$ input bits.

The example of a convolutional encoder is depicted in Fig 3.5, where is a memory-2 convolutional encoder (m = 2), and the coding rate (R_C) is equal to ½ because every one input bit (k = 1) produces two output bits (n = 2), defined as $R_C = k/n$.

The encoder of a memory-m rate-1/n convolutional code can be represented by discrete *linear time-invariant* (LTI) system, with impulse responses given by the code generators $g_0(D)$, $g_1(D)$, ... , $g_n(D)$, where $g_j(D)$ is defined as

$$g_j(D) = g_j[0] + g_j[1](D) + g_j[2](D^2) + \ldots + g_j[m](D^m) \tag{3.20}$$

and the output sequences can be computed by

$$v^j = u * g_j = \sum_{l=0}^{m} u[i-l]g_j[l], \quad 0 \le j \le n, \tag{3.21}$$

where * is the *discrete convolutional* operation. These impulse responses are called generator sequences of the encoder.

From (3.21), the output of convolutional codes v^j can be generated by a generator matrix in the time domain as

$$\bar{v} = \bar{u}G, \tag{3.22}$$

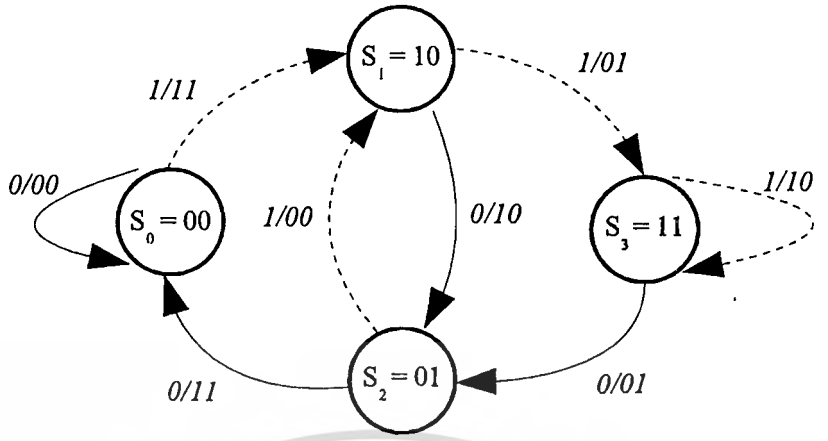


Fig. 3.6 State transition diagram for (2, 1, 2)-convolutional encoder.
The transition links for each time step are labeled as input / output bits ($u_t / v_t^{(0)} v_t^{(1)}$).
The solid lines (——) correspond to transitions with input bit "0", and
the dashed lines (------) correspond to transitions with input bit "1".

where G is a generator matrix of the convolutional code. For example, the generator matrix of a memory-m rate-1/2 convolutional code is defined as

$$G = \begin{bmatrix} g_{(0)}[0]\,g_{(1)}[0] & g_{(0)}[1]\,g_{(1)}[1] & \cdots & g_{(0)}[m]\,g_{(1)}[m] & & \\ & g_{(0)}[0]\,g_{(1)}[0] & g_{(0)}[1]\,g_{(1)}[1] & \cdots & g_{(0)}[m]\,g_{(1)}[m] & \\ & & g_{(0)}[0]\,g_{(1)}[0] & g_{(0)}[1]\,g_{(1)}[1] & \cdots & g_{(0)}[m]\,g_{(1)}[m] \\ & & \ddots & \ddots & & \ddots \end{bmatrix}, \quad (3.23)$$

where these blank entries represent zero.

According to the transform domain, the convolutional codes can be described by a polynomial form. Let $v(D) = v^{(0)}(D) + Dv^{(1)}(D) + \ldots + D^{n-1}v^{(n-1)}(D)$, the convolutional relation of transform domain $\{u, g_j\}$ can be written as

$$\overline{v}(D) = \overline{u}(D)G(D), \quad (3.24)$$

where $G(D)$ is a polynomial generator matrix that are referred to a generators of a rate-1/n convolutional code.

A convolutional encoder can be represented by a finite state machine (FSM) know as the *state transition diagram*. Each state is labeled by the register contents (S_t, S_{t+1}, ...) which the output informations $v_t^{(0)}, \ldots, v_t^{(n-1)}$ at time t depend on the current state S_t, and the input information u_t. For the convolutional encoder in Fig. 3.5, the state transition diagram is shown in Fig. 3.6.

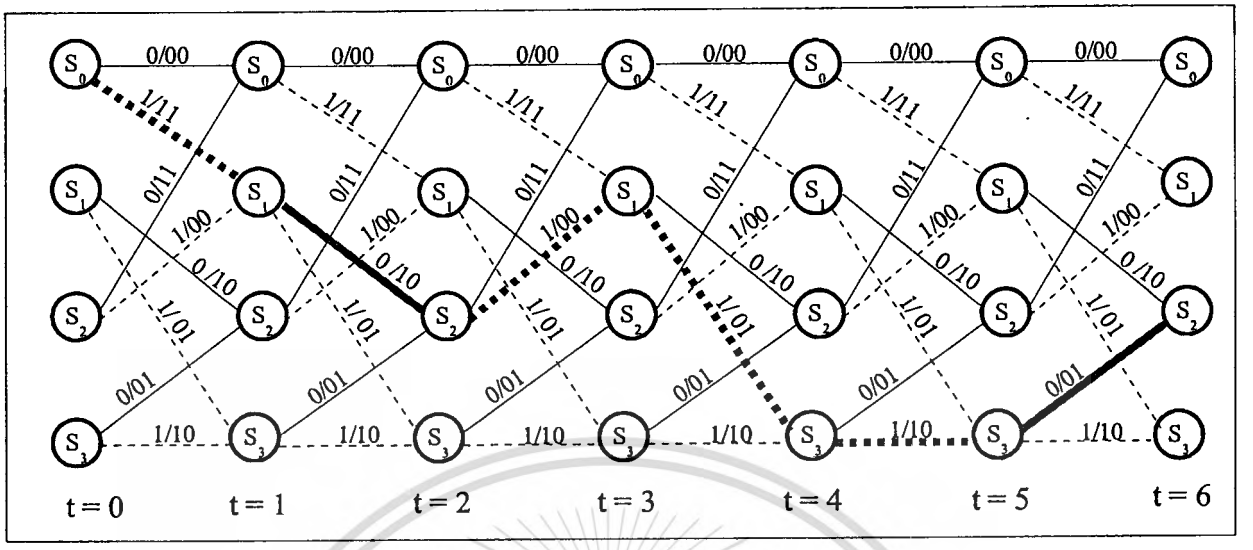


Fig. 3.7 Trellis diagram for (2, 1, 2)-convolutional encoder. A path in this trellis diagram corresponds with the encoded bits v = (11, 10, 00, 01, 10, 01), when given the six input sequences u = (101110).

In Fig 3.6, there are 2^m states that each change of state $S_t \rightarrow S_{t+1}$ is associated with the input u_t and the output $v_t^{(0)}, \ldots, v_t^{(n-1)}$. The possible transitions of each state are labeled by $u_t / v_t^{(0)}, \ldots, v_t^{(n-1)}$.

Another way to represent a convolutional encoder is to use the *trellis diagram*, which is essentially the state transition diagram with the states at different time steps drawn separately. Consider the encoder in Fig. 3.5 and the input sequence u = (101110). Then, the encoded bit sequence corresponds to a path in the trellis diagram, as shown in Fig. 3.7. From the link labels along the path, the encoded bits v = (11, 10, 00, 01, 10, 01).

Several classes of algorithms exist for convolutional decoding. An efficient solution for the convolutional decoding problem is a dynamic programming algorithm known as the *Viterbi algorithm*. It is a well-known and an optimal in the sense of maximum-likelihood algorithm that was proposed by Andrew J. Viterbi [***Viterbi, 1967***]. This is possible to take advantage of trellis diagram to compute the accumulated distances on the branches of the trellis, which come from the received sequence r to the possible transmitted (encoded bit sequence) v by maximizing the probability $p(r|v)$. Generally, A Viterbi algorithm for convolutional decoding consists of the following three major steps:

Step 1.) Branch metric computation—the "*branch metric (BM)*" is a distance of the received codeword from the possible

transmitted bit associated with that branch (called *Hamming* distance in case of a BSC or *Euclidean* distance in case of AWGN). In the first step, all the branch metrics of all the states are determined by

$$BM_{i,j,t} = \sum_{l=0}^{n} r_t \oplus v_{i,j}\,, \tag{3.25}$$

where $BM_{i,j,t}$ is the branch metric from state i to j at time t on trellis diagram.

Step 2.) Path metric update and survivor path—the "path metric (PM)" is the accumulated metrics of all branches in the path. The present path metrics can be calculated by adding the previous path metrics with the corresponding branch metrics in following

$$PM_{j,t} = PM_{i,t-1} + BM_{i,j,t}\,, \tag{3.26}$$

where $PM_{j,t}$ is the present path metric at state j, and $PM_{j,t-1}$ is the previous path metric at state i, which move to present state j.

Next, only one of the lowest-cost paths that entering into a present state j is chosen as the "*survivor path* (*SP*)" for the state j. It can be defined by

$$SP_{j,t} = \min\{(PM_{l,t-1} + BM_{i,j,t}), (PM_{i+1,t-1} + BM_{i+1,j,t}), \ldots\}. \tag{3.27}$$

Step 3.) Optimum Paths Trace Back—At the end of viterbi decoding, the optimum decoding path is determined with the minimum survivor path. Because the history of a survivor path is maintained by the state appropriately. Then, the corrected output sequence can be found by tracing back the history of the path associated with this state to identify the codeword tagged to the first branch of this path.

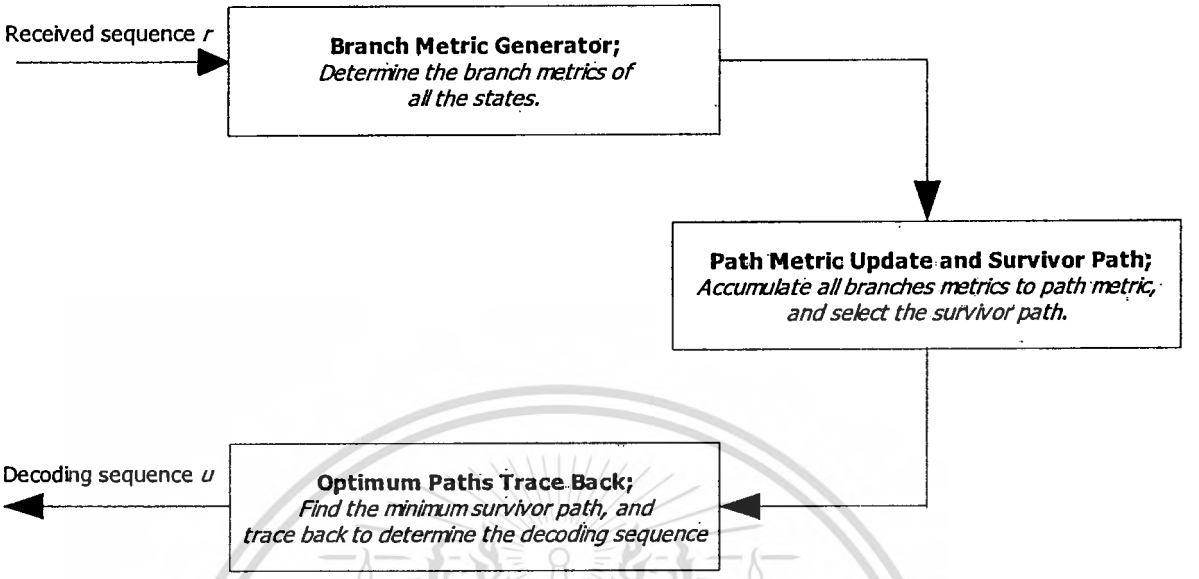


Fig. 3.8 Block diagram of a Viterbi decoding procedure

The block diagram of a Viterbi decoder can be depicted in Fig. 3.8. In these viterbi decoding procedures, the important parameters called the *decoding depth* L, which is a range of L received output bits per state transition. The value of L must be such that $L > 5m$, and it should be considerably large for the capability of covolutional decoding

For the convolutional encoder in Fig. 3.5, the encoded bits are assumed as v = (11, 10, 00, 01, 10, 01, 00). These are transmitted over a *BSC* and the receiver can get the received sequence r = (11, **00**, 00, **11**, 10, 01, 00) (The bold symbol is the position of the two errors). Then, the Viterbi decoder can be corrected these errors as depicted on the trellis in Fig. 3.9. This decoding is finalized at the end of the transmission (the 14 received data bits) by selecting the state at the last stage having the minimum survivor path (SP = 2), and traversing backward along this path to indicate the beginning of the trellis. Then, the corresponding decoding sequence can be recovered by the decoding transition of this minimum survivor path (bold lines) as u = (1 0 1 1 1 0 1).

In this research, the convolutional code is adopted to an alternative quantum key reconciliation method in Secton 4.1. Its objective is to improve the performance of error detection in *Winnow*.

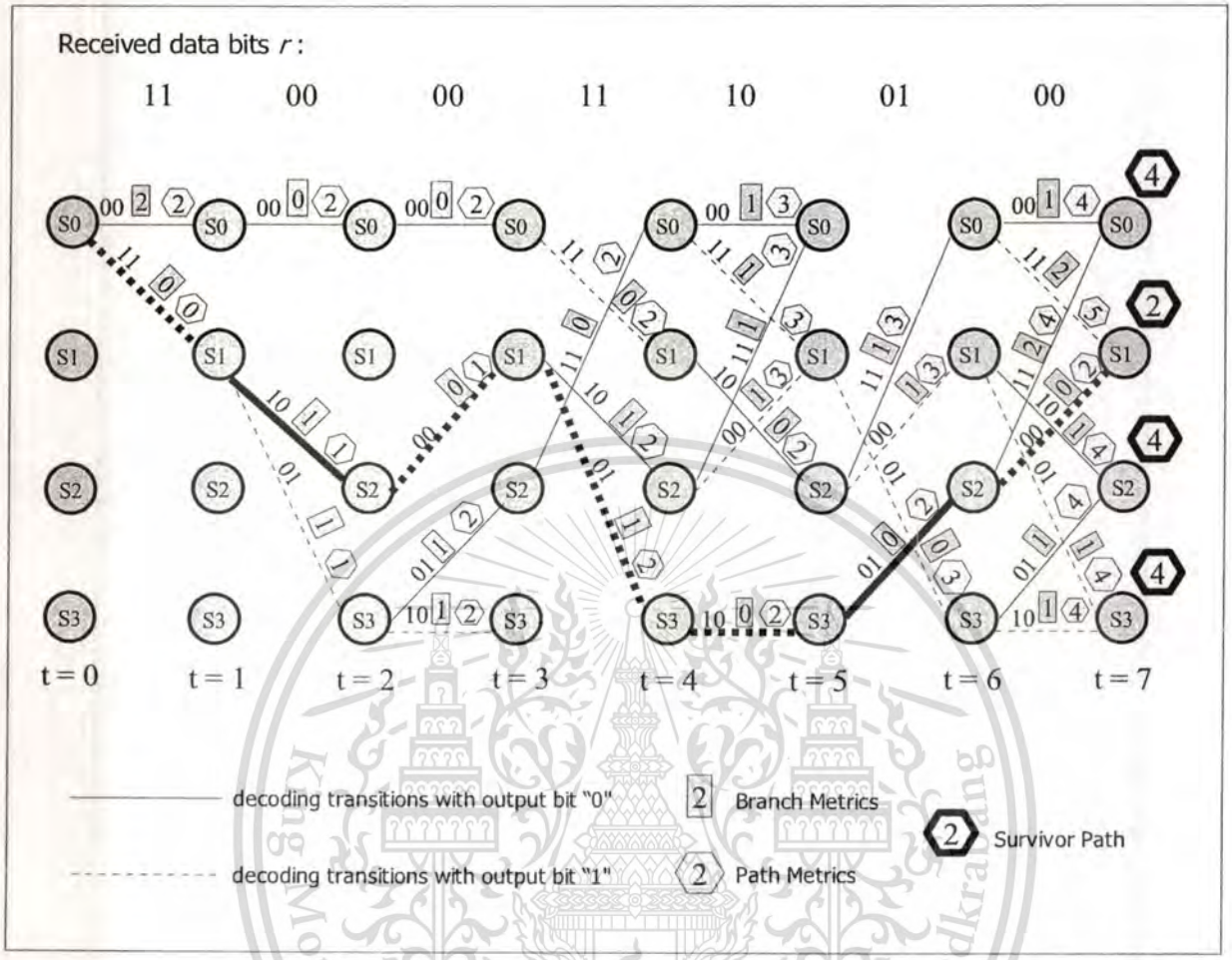


Fig. 3.9 Viterbi algorithm for (2, 1, 2)-convolutional encoder.

3.2.4 Low-Density Parity-Check Code

Low-Density Parity-Check codes were originally proposed in 1962 by Robert Gallager in his PhD thesis [***Gallager, 1963***]. However, they were forgotten due to the hardware at that time could not support effective decoder implementations, and LDPC codes remained largely unstudied for over thirty years. Until they have been strongly promoted, beginning with the work of MacKay [***MacKay_1, 1996***] [***MacKay_2, 1999***] that LDPC codes are rediscovered to achieve a remarkable performance with iterative decoding as close to the Shannon limit. Later in 2001, Richardson *et al.* [***Richardson_2, 2001***] have developed irregular LDPC codes that perform even better than turbo codes in approximately the same length and code rate for very large block lengths. After that the performance of LDPC codes were the best rate-1/2 binary code by Chung *et al.* [***Chung, 2001***] which achieved a record 0.0045 dB away from the Shannon limit for the binary transmission over AWGN channel using a block length of 10^7.

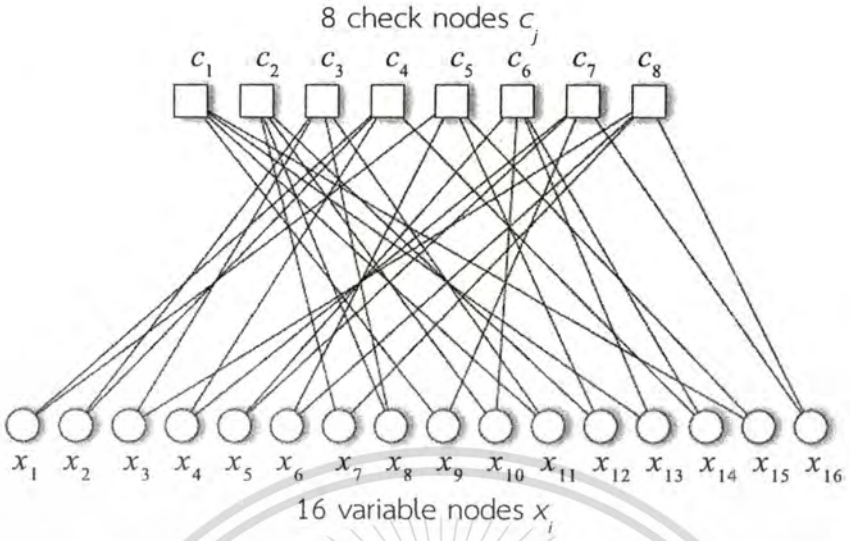


Fig. 3.10 Tanner graph of a (16, 8) LDPC code with N = 16 variable nodes, and M = 8 check nodes.

LDPC codes are binary linear block codes which can be described by a sparse (low-density) parity-check matrix H. This parity-check matrix can be represented as a bipartite graph know as *Tanner graph*. The nodes of Tanner graph of a code are associated with two kinds of variables which are the *variable nodes* and the *check nodes*. A variable node represents an element of the codeword, whereas a check node represents a row of the parity-check matrix. If H has a dimensions $M \times N$, so there are N variable nodes and M check nodes in the graph. For $H_{j,i} \neq 0$, there is an *edge* connecting between check node j and variable node i. The *degree* of a node is defined as the number of connecting edges. The example of a Tanner graph is depicted in Fig 3.10, where is a (16, 8) LDPC code. It has the parity check matrix H as

N

$$H = \begin{bmatrix} 0&0&0&0&0&0&0&0&1&0&1&0&1&0&1&0 \\ 0&0&0&0&0&0&1&1&0&1&0&1&0&0&0&0 \\ 0&1&1&0&0&0&0&1&0&0&1&0&0&0&0&0 \\ 1&1&0&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ 1&0&0&0&0&1&0&0&0&0&0&1&0&0&1&0 \\ 0&0&0&0&1&0&0&0&0&1&0&0&1&1&0&0 \\ 0&0&0&1&1&0&0&0&1&0&0&0&0&0&0&1 \\ 0&0&1&0&0&1&1&0&0&0&0&0&0&0&0&1 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \\ \\ \\ \end{matrix} \begin{matrix} \\ \\ \\ \\ \\ d_c \\ \\ \\ \end{matrix} \quad \Big\} M$$

d_v

The edge connecting between check nodes and variable nodes is dictated by the rows of the parity check matrix. The number of ones per column and per row are denoted by d_v and d_c, respectively, which correspond to the degree of the variable and check nodes in this graph. If every type of node has the same degree such as $d_v(i) = d_v$ and $d_c(j) = d_c$, then the code is called *regular*. Otherwise, it is called *irregular* when there are check or variable nodes with different degrees.

For irregular codes, the fraction of edges must be specified which are connected to nodes of a certain degree. Let the maximum degree of a variable node, and a check node be $d_v^{\max}$ and $d_c^{\max}$, respectively. Then, the degree distribution polynomial for the variable nodes $\lambda(x)$ and for the check nodes $\rho(x)$ can be defined by

$$\lambda(x) = \sum_{i=2}^{d_v^{\max}} \lambda_i x^{i-1}, \tag{3.28}$$

and

$$\rho(x) = \sum_{j=2}^{d_c^{\max}} \rho_j x^{j-1}, \tag{3.29}$$

respectively. It is noted that the check nodes with degree one would correspond to a parity-check equation with only one digit and are not used. Therefore, the summation for the check node distribution must be started from $j = 2$.

The code rate of LDPC codes can be calculated from the degree distribution polynomial in following equation

$$R_C = \frac{N-M}{N} = 1 - \frac{M}{N} = 1 - \frac{\sum_{j=2}^{d_c^{\max}} \frac{\rho_j}{j}}{\sum_{i=2}^{d_v^{\max}} \frac{\lambda_i}{i}} \tag{3.30}$$

The LDPC encoding deals only with binary values. Because it is defined by a large block length. Therefore, the complexity of LDPC encoding is linear with respect to the size of block length. Basically, there are two possibilities of LDPC

encoding similar to a linear block code. The first one is the LDPC encoding with the generator matrix *G*. It can be formulated as $\bar{v} = \bar{u}G$, where the generator matrix *G* is converted from the parity-check matrix *H* in a systematic form. If the dimension of *G* is $k \times n$, then the relation between the generator matrix and the parity-check matrix can be expressed as

$$H=\begin{bmatrix} P & I_{n-k} \end{bmatrix} \rightarrow G=\begin{bmatrix} I_k & P^T \end{bmatrix} \tag{3.31}$$

where *I* is the identity matrix, and *P* is the matrix $k \times (n - k)$ for generating the parity bits.

This LDPC encoding requires $O(n^2)$ for a computational complexity, where *n* is the block length of the LDPC code that is *quadratic* with the block length. Since the characteristic of the LDPC's parity-check matrix is sparse, but after the generator matrix is converted in a systematic form. The sparseness of the generator matrix is lost. This quadratic behavior is very significant to affect with the encoding complexity. Therefore, it is not suitable for LDPC encoding.

Another possible method for LDPC encoding is the relation of $\bar{v} \cdot H^T = [0]_{1,\, n-k}$, where v = [p_m p_{m-1} ... p_1 u_k u_{k-1} ... u_1]. From this relation, the codeword $\bar{v}$ can be computed by the parity-check matrix which is the computation of *m* parity bits (p_m p_{m-1} ... p_1). This method is preferred to use for the LDPC encoding because it can exploit the sparseness of the parity-check matrix. It is noted that every row of the matrix contains d_c ones. Therefore, the computation of *m* parity digits is $O(m \cdot d_c)$, where $O(n)$ are achieved for encoding complexity.

For LDPC decoding, there are some algorithms operating on the Tanner graph. The *sum-product algorithm* is the one of iterative message-passing decoders based on *belief propagation* [*MacKay_2, 1999*]. It is usually called belief propagation when the messages represent beliefs.

In this section, the sum-product algorithm are introduced for applying to the LDPC decoding over binary symmetric channel (BSC). Before introducing this algorithm, given the parity-check matrix *H* has a dimensions $M \times N$ corresponding to a LDPC code with *M* check nodes and *N* variable nodes, and some denotations are provided as following:

- $N(j)$ denotes the set of variable nodes adjacent to the check node c_j by $N(j) = \{i: H_{j,i} = 1\}$, and $M(i)$ be the set of check nodes adjacent to the variable node x_i by $M(i) = \{j: H_{j,i} = 1\}$.

- $N(j)\backslash\{i\}$ denotes the set $N(j)$ with including bit i, and $M(i)\backslash\{j\}$ be the set $M(i)$ with including bit j.
- $q_{i\to j}$ be a message sent by the variable node x_i to the check node c_j , and $r_{j\to i}$ be a message sent by the check node c_j to the variable node x_i, where $q_{i\to j}$ and $r_{j\to i}$ associated with each nonzero element in H that are iteratively updated.

The processes of LDPC decoding with the sum-product algorithm can be divided into four steps as following **[*Qi, 2006*]**:

Step 1) Initialization: Let $p_i^0 = \Pr\{x_i = 0\}$, and $p_i^0 = \Pr\{x_i = 1\} = 1-p_i^0$. For the BSC, let ε be the crossover probability over the BSC. Then, p_i^0 and p_i^1 are initialized to $1-\varepsilon$ and ε respectively. For every edge in the Tanner graph (i, j), such that $H_{j,i}$, $q_{i\to j}^0$ and $q_{i\to j}^1$ can be initialized as

$$q_{i\to j}^0 = p_i^0 = 1-\varepsilon, \tag{3.32}$$

and

$$q_{i\to j}^1 = p_i^1 = \varepsilon. \tag{3.33}$$

Step 2) Horizontal step: Let $r_{j\to i}^0$ and $r_{j\to i}^1$ be the probability of the observed value of c_j, where $x_i = 0$, and $x_i = 1$, respectively. This step run through the check nodes and it computes the corresponding messages $r_{j\to i}$ from check nodes to variable nodes in following

$$r_{j\to i}^0 = \sum_{x_{i'}:i'\in N(j)\backslash\{i\}} Pr\left(c_j | x_i=0, x_{i'}:i'\in N(j)\backslash\{i\}\right) \prod_{i'\in N(j)\backslash\{i\}} q_{i'\to j}^{x_{i'}}, \tag{3.34}$$

$$r_{j\to i}^1 = \sum_{x_{i'}:i'\in N(j)\backslash\{i\}} Pr\left(c_j | x_i=1, x_{i'}:i'\in N(j)\backslash\{i\}\right) \prod_{i'\in N(j)\backslash\{i\}} q_{i'\to j}^{x_{i'}}. \tag{3.35}$$

The conditional probabilities of $\Pr(c_j \mid x_i = 0, x_{i'} : i' \in N(j)\backslash\{i\})$ and $\Pr(c_j \mid x_i = 1, x_{i'} : i' \in N(j)\backslash\{i\})$ in Eq (3.34) and (3.35), respectively, are either zero or one, depending on the observed c_j which corresponding to the parity-check equation.

Step 3) Vertical step: This step run through the variable nodes. For each i, it computes the corresponding messages $q_{i\to j}$ from variable nodes to check nodes in following

$$q_{i\to j}^{0}=\sigma_{j,i}p_i^{0}\prod_{j'\in M(i)\setminus\{j\}}r_{j'\to i}^{0}, \tag{3.36}$$

$$q_{i\to j}^{1}=\sigma_{j,i}p_i^{1}\prod_{j'\in M(i)\setminus\{j\}}r_{j'\to i}^{1}, \tag{3.37}$$

where $\sigma_{j,i}$ is chosen that $q_{j\to i}^{0}+q_{j\to i}^{1}=1$. Then, the posterior probabilities for each variable q_i^{0} and q_i^{1} can be computed by

$$q_i^{0}=\sigma_i p_i^{0}\prod_{j\in M(i)}r_{j\to i}^{0}, \tag{3.38}$$

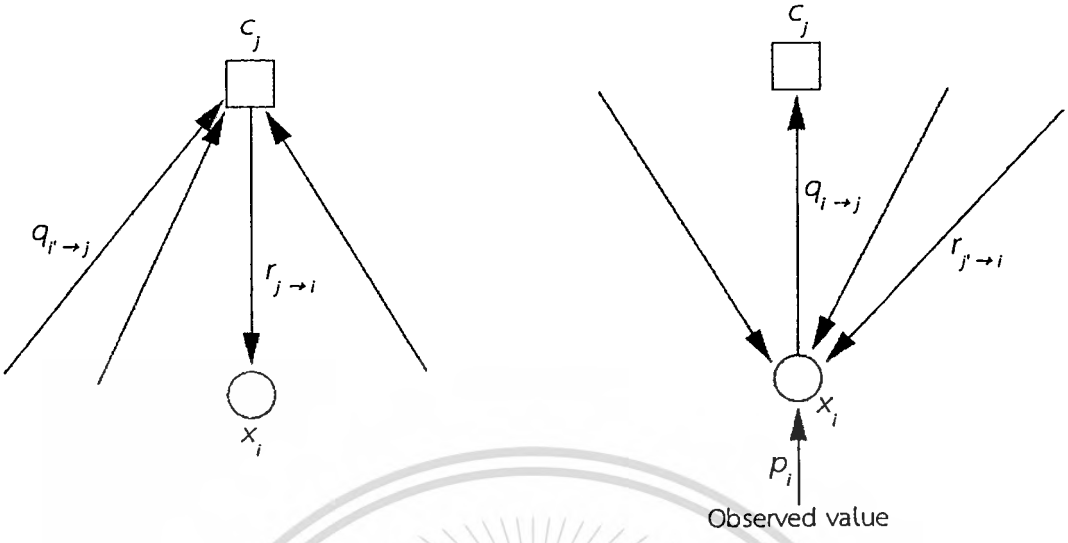
and

$$q_i^{1}=\sigma_i p_i^{1}\prod_{j\in M(i)}r_{j\to i}^{1}, \tag{3.39}$$

respectively, where σ_i is chosen from $q_i^{0}+q_i^{1}=1$.
These computations produce a tentative value of decoding, where the information from every variable node $\hat{x}_i$ is updated as

$$\hat{x}_i=\begin{cases}1 & q_i^{1}>q_i^{0},\\ 0 & else\end{cases} \tag{3.40}$$

The decoding algorithm are terminated if every check node is satisfied by $Hx^{T}=0$. All the informations that used to compute on both horizontal and vertical steps are depicted in Fig. 3.11.



(*a*.) Message from check to variable nodes

(*b*.) Message from variable to checks nodes

Fig. 3.11 Observed values and messages exchanging between (*a*.) check to variable nodes $r_{j \to i}$, and (b.) variable to check nodes $q_{i \to j}$ under the sum-product algorithm.

Step 4) Repeat horizontal step: This algorithm must goes back to the horizontal step again until every check node is successfully satisfied by $Hx^T = 0$ within a maximum number of iteration. Otherwise, the decoding is terminated when the maximum number of iteration has been reached, that is the failure of LDPC decoding.

In this research, LDPC codes are also adopted to the methodology for reconciliation improvement in Section 4.3, which the main advantage is capable of approaching capacity limit (Shannon's limit) by using message-passing decoding such as sum-product algorithm. In case of reconciliation with binary key strings (DV-QKD), the LDPC codes need to be specifically optimized for the BSC which the cross-over probability distribution obviously corresponds directly to the various error rates in QKD system.

3.3 Slepian-Wolf Coding and Its Application to Reconciliation

The problem of *Slepian-Wolf coding* deals with the lossless compression of two or more correlated sources, known as *source coding with side information* [***Slepian, 1973***]. It is the main contribution for solving the key reconciliation problem of this work.

First, the problem formulations of Slepian-Wolf coding are discussed. Its main focus is on the original Slepian-Wolf compression with two correlated sources. By convention, the main information X is statistically correlated with the side information Y on the joint probability distribution P_{XY}, when Y is known only to the receiver side, but not known by the sender. In this system at the sender side, X is compressed into an encoder and the encoder output $|M|$ is sent to the receiver. $|M|$ is a binary sequence in which a compression rate R_S bits not lower than the conditional entropy of X given Y, denoted by $H(X|Y)$. At the receiver side, Y and $|M|$ are used to decompress for producing the final result that will eventually become the recovered information X'.

It should be noted that the minimum information needed by receiver is under the condition of Slepian-Wolf lower bound as $R_S \geq H(X|Y)$. In this scheme, the encoder knows only the joint probability distribution P_{XY}, but it does not know the value of the outcome of Y when encoding X.

The problem of key reconciliation is returned to discuss, which it can be solved by the Slepian-Wolf coding scheme as illustrated in Fig. 3.12. In this scheme, *Alice* and *Bob* have sifted keys modeled by binary random variables X and Y respectively, which it can be described by following two major steps:

Step 1.) **Encoding**: First, *Alice* encodes X and communicates the resulting $|M|$ to *Bob* over the classical channel.

Step 2.) **Decoding**: Then, *Bob* recovers X by using Y and $|M|$, which are both fed into the decoder.

The objective of this scheme is to transform X and Y into a pair of fully correlation, where the $Pr[X'=X]$ equal to one. However, it is noticed that the information $|M|$ are sent over the communication channel, which *Eve* can obtain whenever this channel is insecure. Therefore, the efficiency of reconciliation must also depend on the amount of information $|M|$ which correspond to the compression rate R_S.

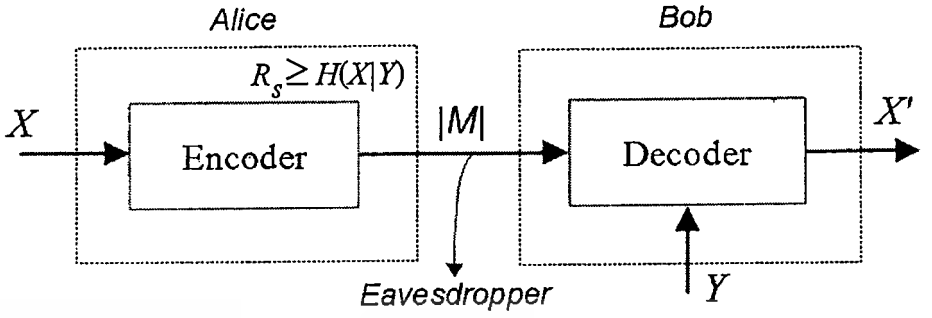


Fig. 3.12 Quantum key reconciliation based on Slepian-Wolf coding scheme

Generally, the channel coding scheme can be applied to the Slepian-Wolf system for various applications such as wireless sensor networks [***Sartipi, 2005***] and multimedia systems [***Weerakkody, 2006***]. It is noted that the Slepian-Wolf coding is closely related to the channel coding. For this reason, X and Y can be seen as the input and the output over GF(2) of a binary symmetric channel (BSC) respectively. Let C be a linear block code which has a parity check matrix H of size $M \times N$. In the Slepian-Wolf scheme, the syndrome S can be calculated by compression of main information X^N, where $S = X^N H^T$. Correspondingly in Slepian-Wolf Coding, the compression rate (R_S) is the rate of syndrome denoted as $\frac{M}{N}$, which is equivalent to the channel coding rate (R_C) of linear code C, where R_S is $\frac{N-M}{N}$. Therefore, the connection between Slepian-Wolf compression rate and channel coding rate can be expressed as

$$R_s = 1 - R_c. \tag{3.41}$$

In the quantum key reconciliation scheme, the channel coding rate R_C must be optimized to the Slepian-Wolf lower bound $R_S \geq H(X|Y)$. Then, it can be rewritten as

$$\begin{aligned} 1 - R_c &\geq H(X|Y), \\ &\geq H(e), \end{aligned} \tag{3.42}$$

where e is the cross-over probability distribution among X and Y. In the case of QKD system, e is equivalent to *QBER* which can determine the joint probability distribution among correlated information from *Alice*, and *Bob*, as well as *Eve*.

Chapter 4
Reconciliation with Proposed Error-Correcting Codes

The quantum key reconciliation is an essential step of QKD protocol. It is invented to eliminate the problem of transmission error after the key distribution over the quantum communication channel. Generally, the several existing reconciliation protocols have been invented using the interactive error correction based on a binary searching, such as the first *BBBSS* [***Bennett_2, 1992***] (Section 2.3.1) and the well-known *Cascade* (Section 2.3.2) [***Brassard, 1994***][***Sugimoto, 2000***] [***Yamazaki, 2000***]. The *Cascade* is certainly the most widely used reconciliation protocol in practical QKD system. It has a good reconciliation efficiency by keeping the track of all investigated block of their key elements. However, *Cascade* still requires a lot of interactive communications between two legitimate parties which slow down the process in practice. That is not suitable for high-speed QKD applications. Other quantum key reconciliation protocol, *Winnow* [***Buttler, 2003***] [***Yan, 2009***] (Section 2.3.3) have been proposed to improve the cost of interactive communication than that of *BBBSS* and *Cascade*. Unfortunately, the ability of its error detection and correction is also hampered with the Hamming code by only single-error correcting.

This chapter presents the alternative quantum key reconciliation methods based on channel coding scheme for discrete-variable QKD protocol. In order to overcome these research objectives, the applications of error-correcting codes play a significant role to improve the reconciliation efficiency. Specifically, the using of convolutional, BCH, and LDPC codes are adapted in the technique of source coding with side information (Slepian-Wolf coding). Its main objectives is to achieve a good error-correcting performance, to improve the reconciliation efficiency for different cases of error rates, and to minimize the leaked information during the reconciliation step.

In this chapter, methodologies for reconciliation improvement are organized by the following three main proposed schemes. Section 4.1 presents the first scheme by using *½-rate convolutional code with side information*. This scheme uses the fixed ½-rate convolutional code adapting on source coding with side information in order to correct any error in a block with a different parity between *Alice* and *Bob* instead of using the Hamming syndrome in *Winnow*. In Section 4.2, the second proposed *BCH-based Slepian-Wolf Coding* with the optimal set of binary BCH code

rates are presented. In this scheme, the BCH decoder is based on syndrome decoding and also modified by adding one-bit feedback to detect the failure of decoding process. Its objective is to discard the uncorrectable errors in a block of key in order to produce no remaining bit error in the final reconciled key after reconciliation step. Finally, the proposed *rate-compatible irregular LDPC codes based on the Slepian-Wolf Coding* is presented for interactive reconciliation scheme in Section 4.3. The rate-compatible LDPC codes are optimized for the binary symmetric channel (BSC). The success of this scheme is expected by the feedbacks of syndrome decoding when decoder produces its new syndrome matching to the syndrome received form encoder.

4.1 ½-Rate Convolutional Code with Side Information

This section presents the proposed reconciliation method by using convolutional code (Section 3.2.3). It deploys the fixed ½-rate code based on the technique of source coding with side information (Slepian-Wolf coding) to achieve a good error-correcting performance. In original *Winnow*, only block containing a single bit error can be detected and corrected by the Hamming syndrome. Nevertheless, it can not produce accurate results whenever more than one of the error are found in the block of key elements. Consequently, the goals of this proposed schemes is to correct any error in a block with a different parity between *Alice* and *Bob* by mean of ½-rate convolutional code with side information, instead of the Hamming syndrome in *Winnow*.

The deployment of convolutional code with side information is shown in Fig 4.1. This scheme can be seen as the side information source coding when the sifted keys of *Alice* are the main input information statistically correlated with the side information of *Bob*'s sifted keys. They are on the joint probability distribution P_{xy} which correspond directly to the observed value of *QBER*. For this ½-rate systematic convolutional encoder, the two output bits can be generated whenever every one input bit x_i is fed into the encoder. They consist of a part actual input bit x_i and a part of parity information bit p_i. After that, *Alice* transmits only the parity information p_i. through the classical communication channel where the compression rate (R_S) is 0.5 ($R_S = 1 - R_C$, Eq. 3.41). Then, *Bob* uses the parity information bit p_i that received from *Alice* and his side information y_i (*Bob*'s sifted key) to calculate an estimate of x'_i by the convolutional decoder. This proposed scheme can be divided into four steps as;

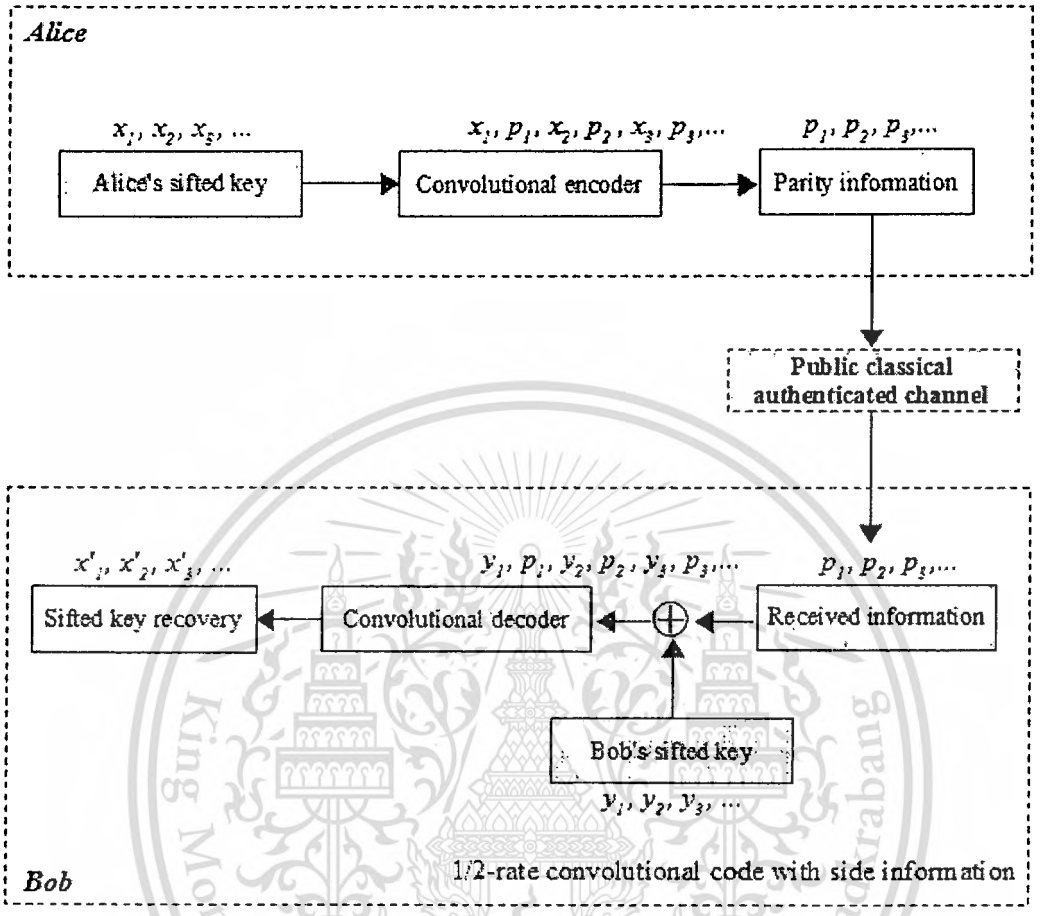


Fig. 4.1 Flow diagram of ½-rate convolutional code with side information.

Step 1) **Computation for optimal block size:** First, *Alice* and *Bob* arrange their sifted keys in blocks of *N* bits which the optimal block length *N* is determined by the quantum bit error rate (*QBER*) and the remaining bit errors (*k*). For the quantum bit error rate *e*, the probability for *k* wrong bits in a block of *N* bits is given by the binomial distribution in following

$$P_k(N) = \binom{N}{k} e^k (1-e)^{N-k}. \tag{4.1}$$

Step 2) **Parity bit comparing:** *Alice* and *Bob* then compare their parities in each block of N bits over the classical authenticated channel. If the parities mismatch, these blocks are only considered to reconcile the errors by ½-rate convolutional code with side information.

Step 3) **Encoding:** *Alice* concatenates the bits of each block with different parities into a stream of x_i and feeds it into the ½-rate convolutional encoder, where its code generator (G) is [100, 171], and memory of convolutional encoder (m) is 6 (Section 3.2.3). Then, the redundancy bits (parity information p_i) from the ½-rate convolutional encoder are only transmitted to *Bob* over the public classical channel.

Step 4) **Decoding:** The Viterbi algorithm (Section 3.2.3) is adopted to decode *Bob*'s codewords. These codewords correspond to the parity informations p_i received from *Alice*, and his sifted keys y_i along with their positions. Finally, *Bob* has a new reconciled keys (sifted key recovery x'_i) of each block with different parity bits x'_i, and then arrange them back to the original sequences.

It is noted that the parities of each block can be transmitted in a single-message communication from *Alice* to *Bob*, and then from *Bob* to *Alice*. After that, the the stream of redundancy bits from ½-rate convolutional encoder is also sent in the single-message from *Alice* to *Bob*. Therefore, this proposed scheme requires only three times-message per iteration, which actually reduce the cost of interactive communications than that of *BBBSS* and *Cascade*.

4.2 BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding

The BCH codes (Section 3.2.2) are a class of multiple error correcting over GF(q). They can correct several error bits per each block which are possible to select the compatible code rate depending on *QBER*. In this section, the BCH-based Slepian-Wolf coding is proposed to be an alternative key reconciliation method. The chosen optimal set of BCH code rates has been adopted for various possible cases of error rates in QKD system. Moreover, the BCH decoder is based on the syndrome decoding. It is modified by adding one-bit feedback in order to detect and discard uncorrectable errors in a block of key whenever the decoding process fails.

The deployment of BCH-based Slepian-Wolf coding with feedback syndrome decoding is depicted in Fig. 4.2. It is a one-way reconciliation scheme which can be described by the following four steps:

Step 1) **Selecting of BCH parameters:** *Alice* and *Bob* arrange their sifted keys in the optimal blocks size. The parameters of BCH codes (n, k, t) (Section 3.3.2) can be selected properly on observed value of *QBER* for producing the code rate close to the lower bound of Slepian-Wolf coding (Eq. (3.42)). The selections of BCH parameter for this proposed scheme are shown in Table 5.2.

Step 2) **Encoding:** The sequences of X^n (*Alice*'s sifted key) are fed into the BCH-based Slepian-Wolf encoder for calculating her syndromes by $S_x^{n-k} = X^n H^T$. After that, *Alice* transmits the syndrome information bits S_x^{n-k} over the classical authenticated channel to *Bob* along with their positions.

Step 3) **Syndrome comparing**: *Bob* calculates his sifted keys Y^n to produce his syndromes S_y^{n-k}. Then, it is compared with the received syndrome from *Alice* to find the syndrome matching S_{diff}^{n-k} in following

$$S_{diff}^{n-k} = S_x^{n-k} \oplus S_y^{n-k}. \tag{4.2}$$

In this proposed scheme, the error is only reconciled by the BCH-based Slepian-Wolf decoder whenever the syndromes matching are different ($S_{diff}^{n-k} \neq \{0\}^{n-k}$). Otherwise, this proposed scheme is successfully where $S_{diff}^{n-k} = \{0\}^{n-k}$ ensure that *Alice* and *Bob*'s sifted keys of this block are equal.

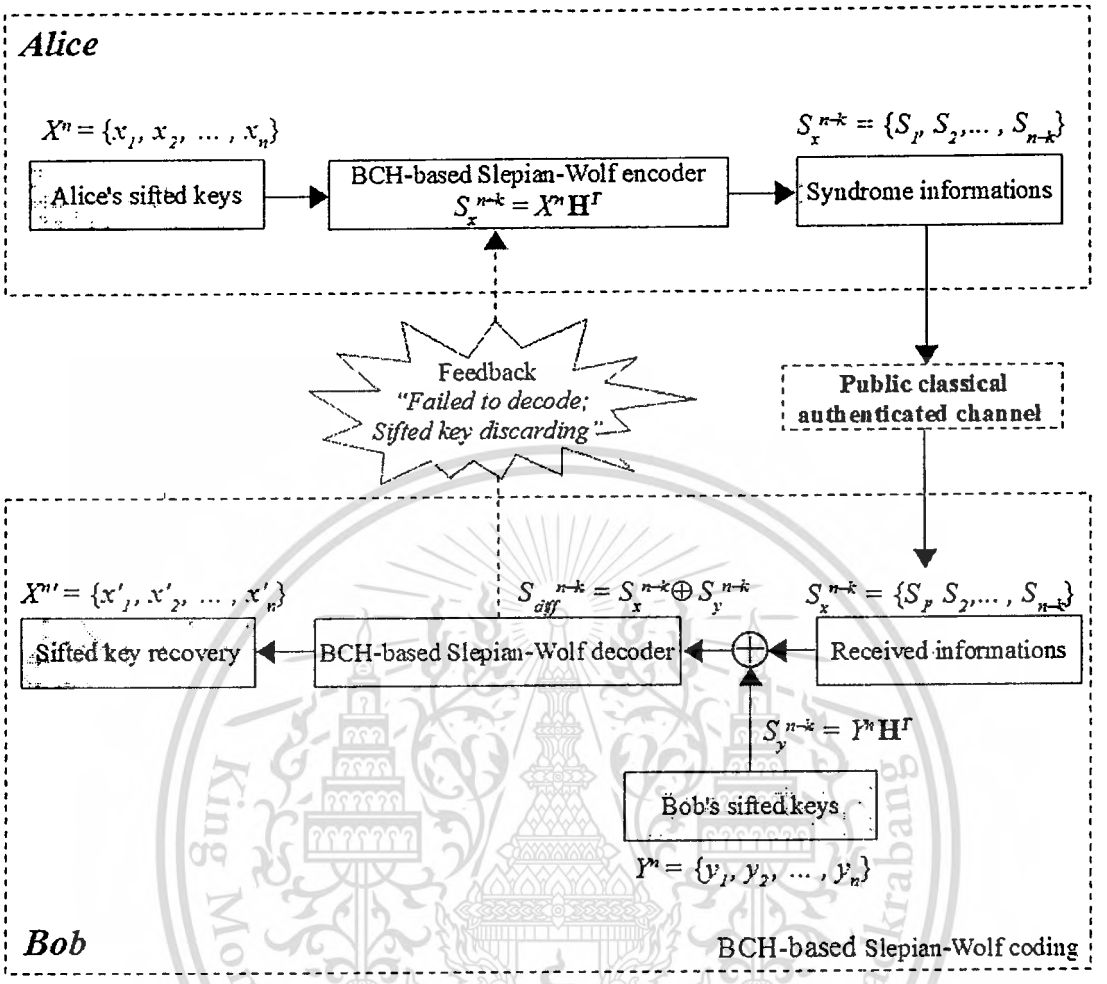


Fig. 4.2 Flow diagram of quantum key reconciliation with feedback by using BCH-based Slepian-Wolf coding.

Step 4.) Decoding: If the syndrome matching is different ($S_{diff}^{n-k} \neq \{0\}^{n-k}$), *Bob* then feeds S_{diff}^{n-k} into the decoder based Slepian-Wolf coding in order to find the error-locator polynomial of BCH. This polynomial are used to estimate the error pattern of *Bob*'s sifted key in each block. Finally, the error is identified and corrected by the BCH error-locator polynomial to calculate $x^{n'}$.

In this scheme, if the decoder declares uncorrectable errors whenever the number of error bits in the block length *n* of sifted keys more than *t*-error capability of BCH code **[Sarwate, 1990]**. Then, *Bob* sends one-bit feedback to *Alice* for agreeing to discard their uncorrectable errors of sifted key in this block. Its main objective is to produce no remaining bit error in the final reconciled key between *Alice* and *Bob* after reconciliation step.

4.3 Interactive Reconciliation with Rate-Compatible Irregular LDPC codes

The irregular LDPC codes have been shown in **[*Chung, 2001*] [*Richardson_2, 2001*]** which are capable of transmitting information over noisy channels close to the Shannon limit. In this section, the proposed reconciliation scheme, rate-compatible irregular LDPC codes are presented. It serves for application to discrete-variable QKD by adapting on the Slepian-Wolf coding system. In the case of binary reconciliation scheme, LDPC codes are specifically optimized for the binary symmetric channel (BSC) where the introduced *QBER* corresponds directly to the cross-over probability distribution of a BSC.

The deployment of LDPC codes based on the Slepian-Wolf coding scheme is depicted in Fig. 4.3. Its main idea is similar to that of BCH-based Slepian-Wolf Coding in Fig. 4.2, which is also based on the syndrome decoding. Nevertheless, since LDPC codes is defined by a large of code block length (block length is 10^5), the key discarding process would not be able to use whenever the LDPC decoding cannot produce the accurate *Bob*'s syndromes matching to *Alice*. Therefore, the code rate will be determined to decrease in each additional step until the successful decoding is finally achieved.

The procedures of reconciliation scheme by rate-compatible irregular LDPC codes can be described by the following three steps based on Slepian-Wolf coding scheme:

Step 1) **Encoding**: *Alice* encodes the sequences of X^n for calculating her syndromes informations by $S_x^{n-k} = X^n H^T$, where the compression rate is optimized by the observed *QBER* from the channel parameter estimation step in QKD (Section 2.2). Then, the syndromes of *Alice* S_x^{n-k} are transmitted to *Bob* over the classical authenticated channel. The optimal set of LDPC code rates used in this proposed scheme through various possible cases of *QBER* can be found in Table 5.3.

Step 2) **Decoding**: The sum-product algorithm (Section 3.2.4) is adopted to find and to correct the position of errors in *Bob*'s sifted keys. The reconciled keys will eventually become the recovered information $X^{n\prime}$.

Generally, the belief propagation of sum-product algorithm is defined on the channel coding scheme. In order to apply in the Slepian-Wolf system, the update equations for the messages-passing

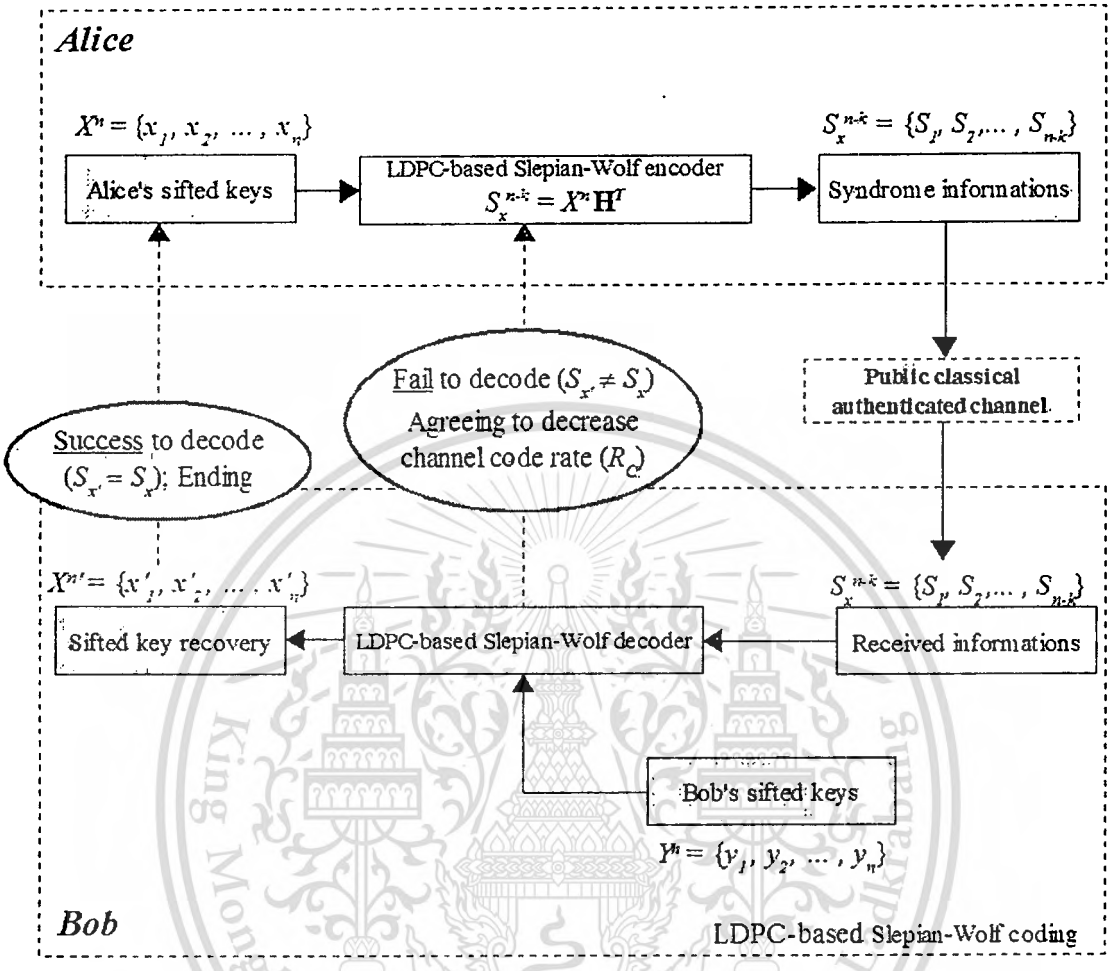


Fig. 4.3 Flow diagram of interactive quantum key reconciliation by using LDPC-based Slepian-Wolf coding.

under the belief propagation [*Chen, 2007*] can be described in following

$$q_{i\to j}^{(l)} = \begin{cases} p_i, & \text{if } l=0 \\ p_i + \sum_{j' \in M(i)\setminus\{j\}} r_{j'-i'}^{(l)}, & \text{if } l>0 \end{cases}, \tag{4.3}$$

and the operation at check nodes is defined by

$$r_{j\to i}^{(l)} = (-1)^s \gamma^{-1}\left(\sum_{i' \in N(j)\setminus\{i\}} \gamma(q_{i'\to j}^{l-1}) \right) \tag{4.4}$$

where s is the syndrome value corresponding to the check node c. It associates with the parity-check equation defined by the j-th check node. The expression of $\gamma(.)$ can be found in [*Richardson_3, 2001*].

Step 3) Confirmation: The advantage of syndrome decoding is to determine whether the LDPC decoder is a success or a failure. By convention, The success of this scheme is expected when *Bob* can produce his syndrome matching to the received syndrome within a maximum number of iteration ($S_{x'}^{n-k} = S_x^{n-k}$), and he then sends a feedback for reconciliation ending to *Alice*. Otherwise, the feedback for decoding failure is sent for their determination in order to decrease the channel code rate R_C, and they then return to Step 1 again until the successful decoding is achieved.

Chapter 5
Results and Calculations

In order to verify the proposed methods and to evaluate these performance characteristics, the validation of the proposed methods are studied by working on simulation, and observed the various system parameters in terms of error-correcting performance, reconciliation efficiencies, and number of disclosed informations used in reconciliation step. These are also compared to the binary interactive reconciliation protocols, *Cascade* and *Winnow*, which are implemented in most QKD systems.

5.1 Results of ½-Rate Convolutional Code with Side Information

In this section, the simulation results of the proposed ½-rate convolutional code from Section 4.1 are evaluated together with the well-known *Cascade* and *Winnow*. They are subjected to comprehensive simulation setups as follows:

- All the initial sifted keys are generated randomly according to quantum bit error rate (*QBER*) with its size is 100,000 bits.
- Simulation results are averaged from 100 routines.

5.1.1 Error-Correcting Performance

The error correction capability of the proposed ½-rate convolutional code with side information are shown in Table 5.1. The objective of this proposed method is to eliminate the final bit error rate (*Final BER*) in reconciled keys less than 10^{-3} by using a several number of iterations. In this table, the final bit error rate (*BER*) for the proposed ½-rate convolutional are compared with the traditional *Winnow* at the same conditions. They are composed of introduced *QBER*, size of block length, and number of iterations.

Fig. 5.1 shows the results comparison of the error correction capability between the proposed method by ½-rate convolutional code and *Winnow*. In this case, the results have been simulated in only first iteration whereas the two parties (*Alice* and *Bob*) arrange their sifted keys in optimal block sizes depending on *QBER* by the the binomial distribution (Eq. (4.1)).

Table 5.1 Error correcting capability achieved by the original *Winnow* and the proposed ½-rate convolutional code.

QBER (%)	Block length size (bits)	Number of iterations	Final BER	
			Winnow	The proposed method
1	32	2	4.43×10^{-4}	1.64×10^{-4}
5	16	3	1.52×10^{-3}	3.50×10^{-4}
10	8	3	2.13×10^{-3}	6.99×10^{-4}

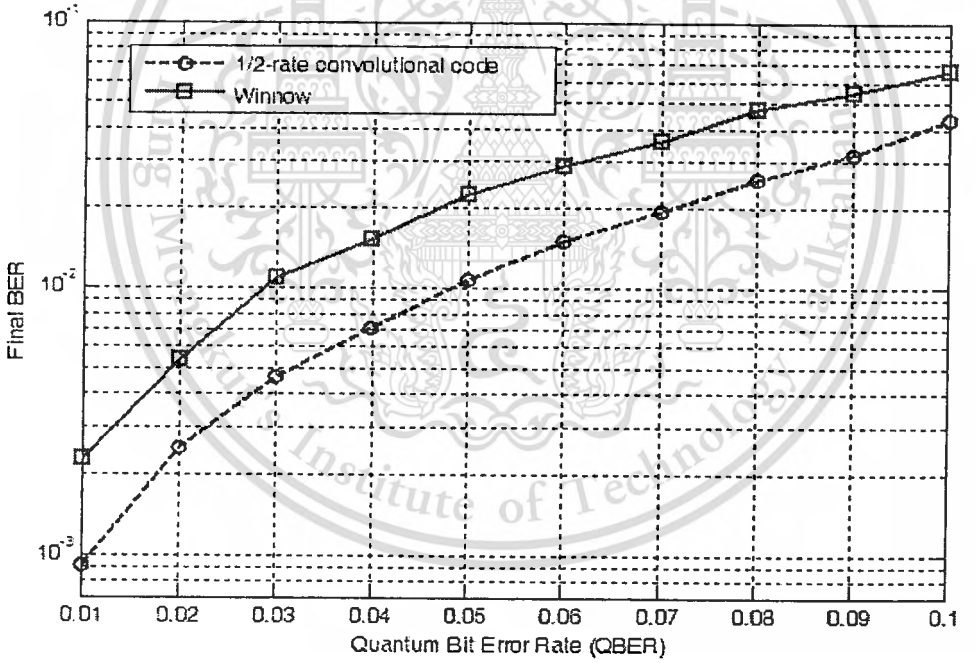


Fig. 5.1 Final bit error rate (*Final BER*) in reconciled keys achieved by the proposed ½-rate convolutional code with side information and *Winnow* as a function of *QBER*.

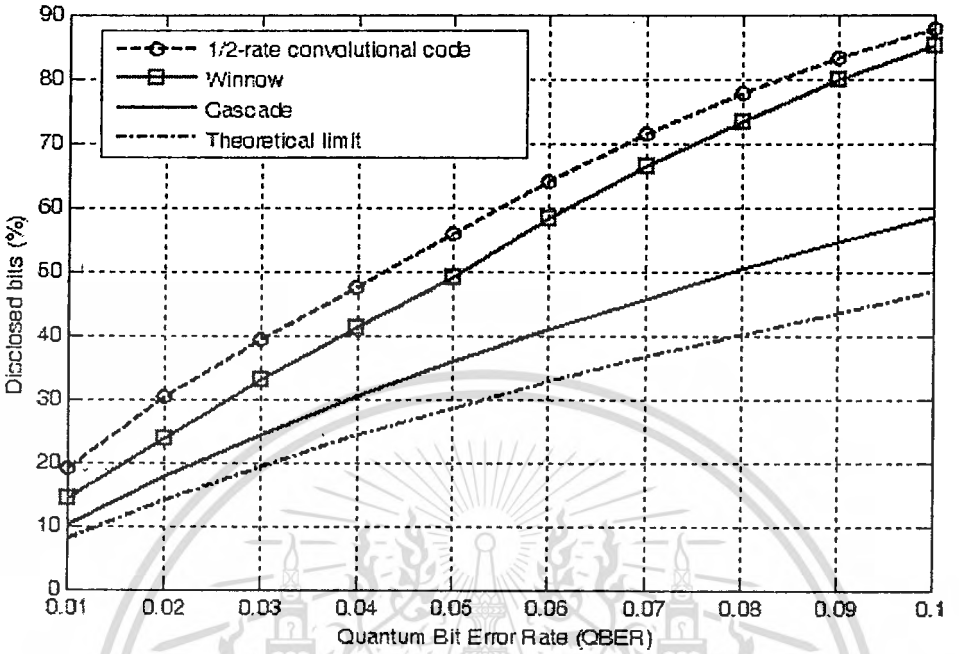


Fig. 5.2 Number of disclosed bits achieved by the proposed ½-rate convolutional code and the binary interactive reconciliation protocols as a function of *QBER*.

5.1.2 Disclosed Informations for ½-rate Convolutional code

The graphical interpretation of the number of disclosed bits during the reconciliation step is shown in Fig. 5.2 as the function of quantum bit error rate (*QBER*). The simulated number of disclosed bits for the proposed ½-rate convolutional code are compared with the 10^5 bit-length strings of *Cascade* and *Winnow*, and also the theoretical limit. In the perfect reconciliation scheme (theoretical Shannon limit), the number of disclosed bits (d_{th}) can be calculated by

$$d_{th} = 1 - I(e), \tag{5.1}$$

where e is a quantum bit error rate (*QBER*), and $I(e) = 1 + e \log_2 e + (1-e) \log_2(1-e)$.

These simulated results show that the proposed ½-rate convolutional code with side information is a good error-correction alternative to original *Winnow*. It achieves the lower *Final BER* after reconciliation comparable to *Winnow* in various cases of good to very bad *QBER* (1% – 10%). Furthermore, this proposed scheme communicates only three-message per iteration, which it can actually reduce the

cost of interactive communications between *Alice* and *Bob* than that of *BBBSS* and *Cascade*. Therefore, it is suitable to use in high-speed QKD applications. Although, this proposed ½-rate convolutional code requires a large number of disclosed bits, but it can be reduced the amount of disclosed bit by optimizing the code rate at the minimum information needed by *Bob* (Slepian-Wolf bound, Eq. (3.42)).

5.2 Results of BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding

This section presents the simulation results of the proposed BCH-based Slepian-Wolf coding from Section 4.2. which are subjected to comprehensive simulation setups as follows:

- All the initial sifted keys are generated randomly according to quantum bit error rate (*QBER*) with its size greater than 100,000 bits.
- The attainment of the proposed method is to get no remaining error bit in the final reconciled key with averaged values of 100 routines.
- The maximum size of final reconciled keys is set not less than 80% of initial size of sifted keys (key discarding < 20%).

5.2.1 Reconciliation Efficiency for BCH-based Slepian-Wolf coding

In order to compare with the best known reconciliation protocols, *Cascade*, the efficiencies of different reconciliation schemes can be evaluated by the expression of actual secure secret key rate in Eq. (2.7) ($r_{real} = H(X|Z) - f \cdot H(X|Y)$). However, the term of $f \cdot H(X|Y)$ is the practical compression rate R_S. It guarantees the sifted keys of *Alice* and *Bob* are equal after the reconciliation step. Consequently, the parameters for reconciliation efficiency f can be defined by

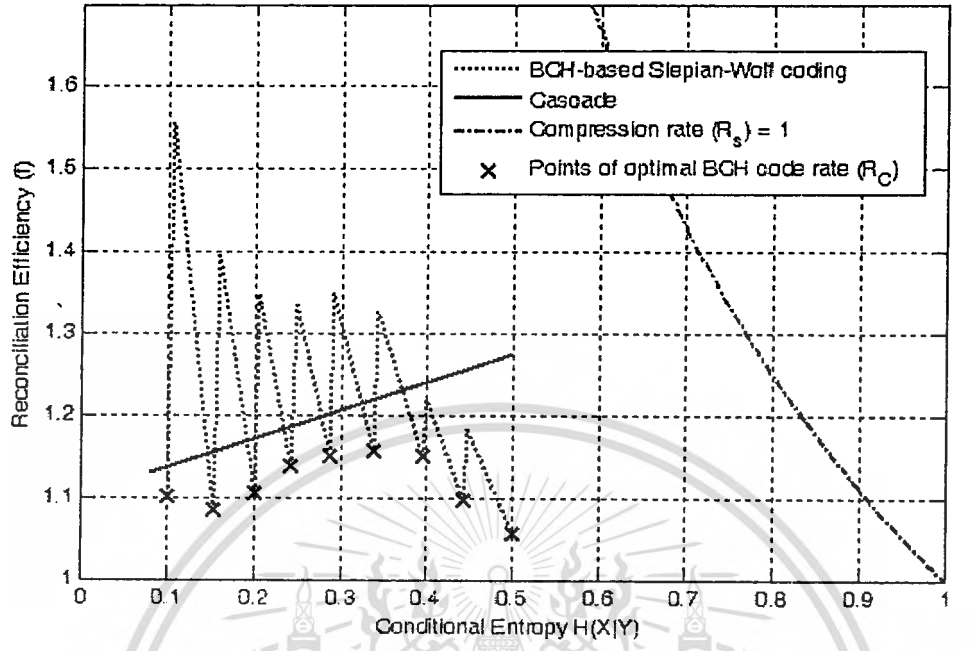
$$f = \frac{R_s}{H(X|Y)} = \frac{1 - R_c}{H(X|Y)}. \tag{5.2}$$

Table 5.2 shows the selections of BCH parameter for the different case of error rate using in the proposed scheme. They are optimized as close to the lower bound of Slepian-Wolf coding corresponding to the *QBER* (Eq. (3.42)). The left column shows the highest error rate (critical *QBER*) for each particular code rate. This table also includes the optimal BCH code rates (R_c) corresponding to the Slepian-Wolf compression rates (R_s) that is used to calculate the reconciliation efficiency f as defined in Eq. (5.2) in the right column.

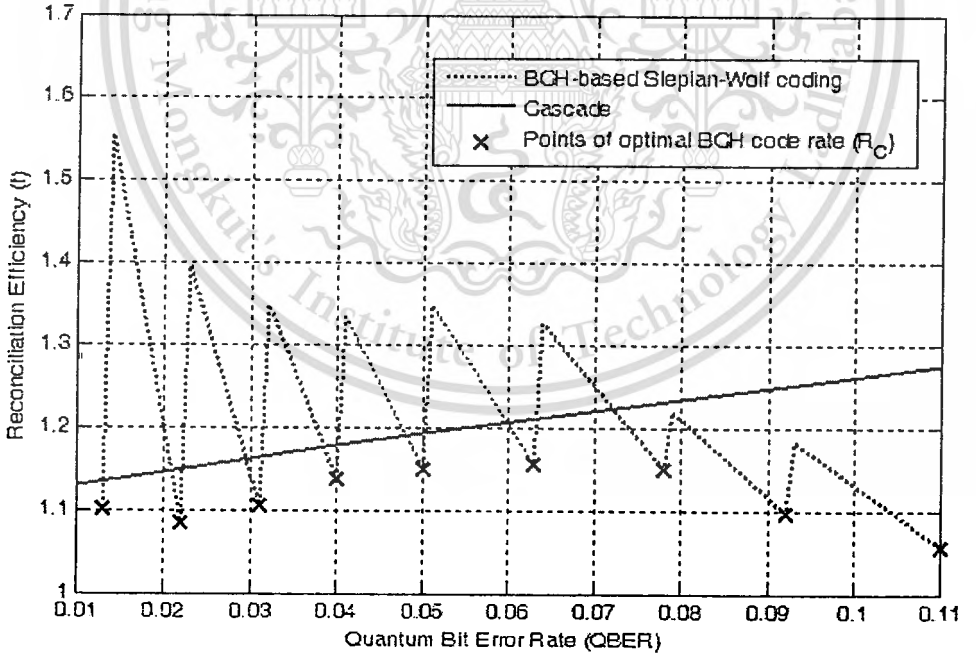
Table 5.2 Parameters of BCH codes used in different case of *QBER* for quantum key reconciliation, and the calculation of reconciliation efficiency (*f*)

Critical *QBER*	Parameters of BCH codes (n,k,t)	BCH code rates (R_c)	Slepian-Wolf compression rates (R_s)	Reconciliation efficiency (f)
0.013	(127,113,2)	0.88976	0.11024	1.1015
0.022	(127,106,3)	0.83465	0.16535	1.0841
0.031	(127,99,4)	0.77953	0.22047	1.1058
0.040	(127,92,5)	0.72441	0.27559	1.1374
0.050	(255,171,11)	0.67059	0.32941	1.1502
0.063	(255,155,13)	0.60784	0.39216	1.1560
0.078	(255,139,15)	0.54510	0.45490	1.1514
0.092	(255,131,18)	0.51373	0.48627	1.0974
0.110	(512, 241, 36)	0.47162	0.52838	1.0569

The graphical interpretation of the reconciliation efficiency f as the function of the conditional Shannon entropy $H(X|Y)$, and quantum bit error rate (*QBER*) are shown in Fig. 5.3*a* and 5.3*b* respectively. The efficiency of the proposed BCH-based Slepian-Wolf coding are simulated by optimizing 9 BCH code rates based on the Slepian-Wolf system (R_c = 0.88976, 0.83465, 0.77953, 0.72441, 0.67059, 0.60784, 0.54510, 0.51373, 0.47162). They are covered the range of error rates (*QBER*) in QKD system. These codes are compared by the 10^5 bits of *Cascade*. In the theoretical reconciliation scheme, the reconciliation efficiency equals "1".



(*a.*)



(*b.*)

Fig. 5.3 Efficiency of reconciliation f achieved by BCH-based Slepian-Wolf coding and *Cascade*; (*a*) as the function of conditional Shannon entropy $H(X|Y)$, and (*b*) as the function of *QBER*.

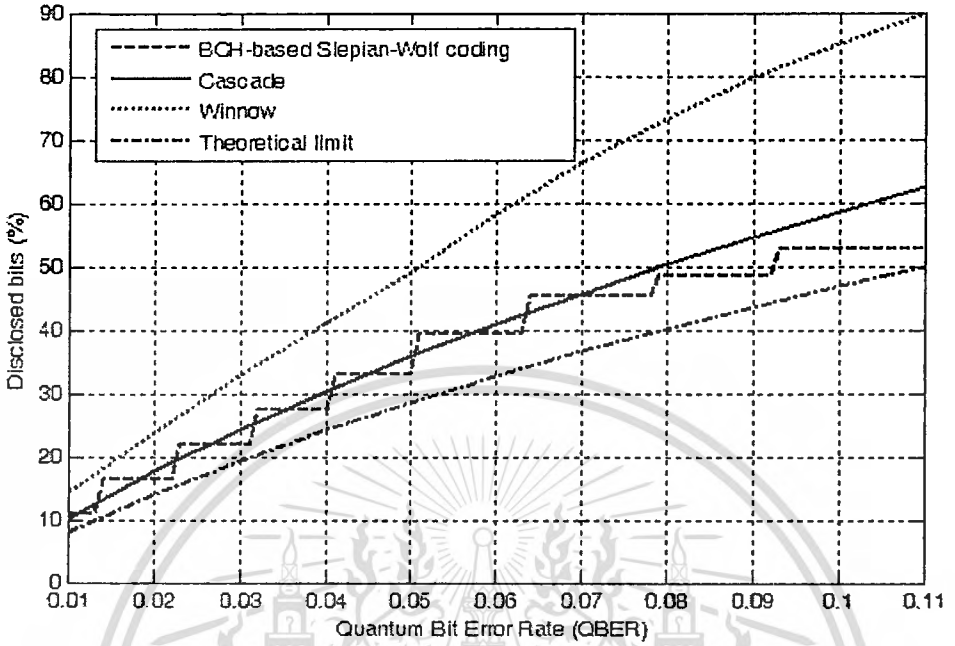


Fig. 5.4 Number of disclosed bits achieved by BCH-based Slepian-Wolf coding and the binary interactive reconciliation protocols as a function of *QBER*.

5.2.2 Disclosed Informations for BCH-based Slepian-Wolf coding

The disclosed bit is one of the important parameters to be evaluated the efficiency of reconciliation schemes. Because, it indicates the amount of leaked informations, which can be monitored by *Eve* during the reconciliation step. The number of disclosed bits of this proposed scheme is the syndrome information bits that sent over the public classical authenticated channel during reconciliation step. In Fig. 5.4, the number of disclosed bits of the proposed BCH-based Slepian-Wolf coding are compared with those of *Cascade* and *Winnow* protocols in the subject of quantum bit error rate (*QBER*). For the perfect reconciliation scheme (theoretical limit), the number of disclosed bits are also calculated as Eq. (5.1).

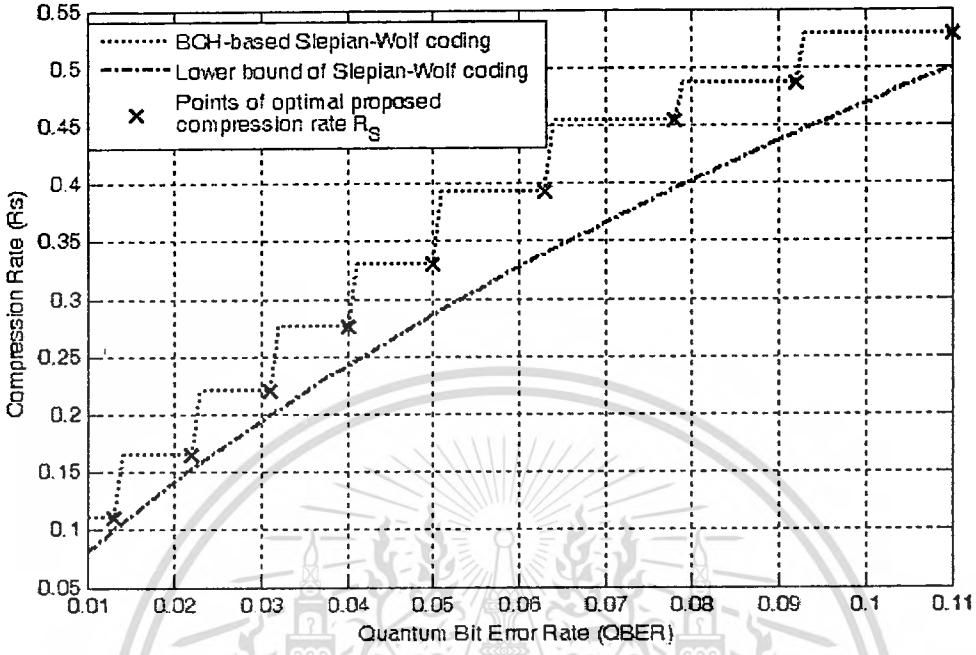


Fig 5.5 Compression rates of the proposed BCH-based Slepian-Wolf coding and the Slepian-Wolf lower bound as a function of *QBER*.

5.2.3 BCH-based Slepian-Wolf Compression Rate

The optimized 9 compression rates of BCH-based Slepian-Wolf coding (R_s = 0.11024, 0.16535, 0.22047, 0.27559, 0.32941, 0.39216, 0.45490, 0.48627, 0.52838) are shown in Fig. 5.5. These are for covering the error rate range in QKD, and are compared with the theoretical Slepian-Wolf lower bound ($R_s = H(X|Y)$) as the function of quantum bit error rate (*QBER*).

The simulation results show that the proposed BCH-based Slepian-Wolf coding is an alternative reconciliation method to the well-known conventional binary interactive reconciliation protocols, *Cascade* and *Winnow*. It can improve the reconciliation efficiency in every critical point of *QBER* which the optimal set of BCH code rates has been optimized for various possible cases of error rates in QKD system. Moreover, the BCH-based Slepian-Wolf coding requires less number of disclosed bits than that *Cascade* at the points of optimal BCH code rates, and always less than *Cascade* when the *QBER* is approximately above 7%. In term of

communication resources, the proposed BCH-based Slepian-Wolf coding uses only two-message communication for carrying the syndrome informations from *Alice* to *Bob*, and the another single-message for feedback detection from *Bob* to *Alice*. Therefore, it can actually reduce the cost of interactive communication than the other binary interactive reconciliation protocols. That is also attractive to implement for high-speed QKD applications.

5.3 Results of Interactive Reconciliation with Rate-Compatible Irregular LDPC codes

This section presents the simulation results of the proposed rate-compatible irregular LDPC codes from Section 4.3. They were also simulated in order to compare with the other interactive reconciliation protocols in the terms of reconciliation efficiency as defined in Eq. (5.2), and the number of disclosed bits during the reconciliation step. They are subjected to simulation setups as follows:

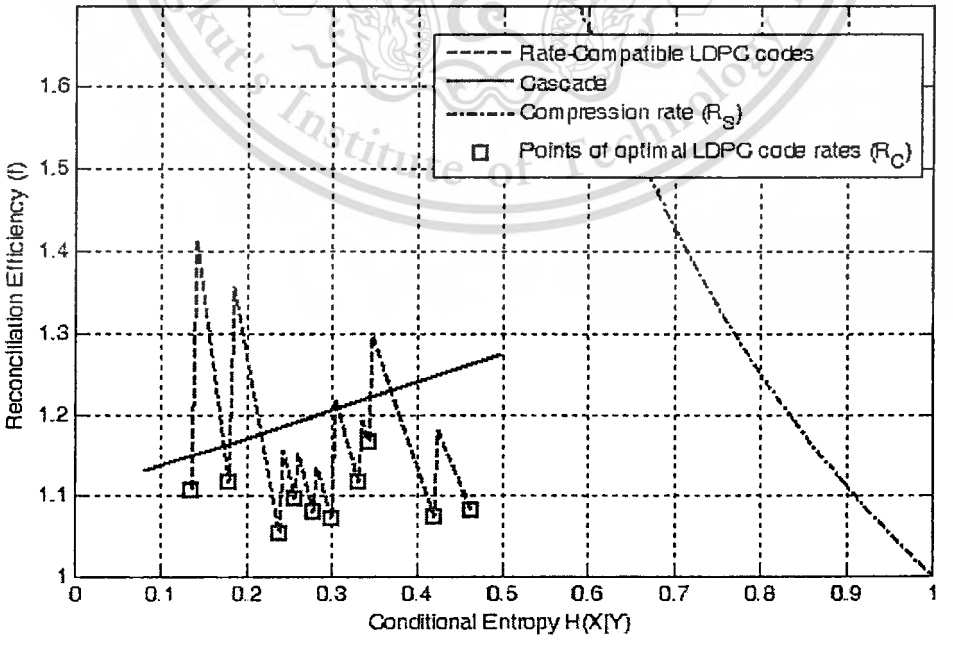
- All the initial sifted keys are generated randomly according to quantum bit error rate (*QBER*) with its size greater than 100,000 bits.
- Block length of LDPC codes are defined with 10^5 bits.
- Maximum number of iterations for LDPC decoding are set at 200 rounds.
- The attainment of the proposed method is to get no remaining error bit in the final reconciled key with averaged values of 100 routines.

5.3.1 Reconciliation Efficiency for Rate-Compatible Irregular LDPC codes

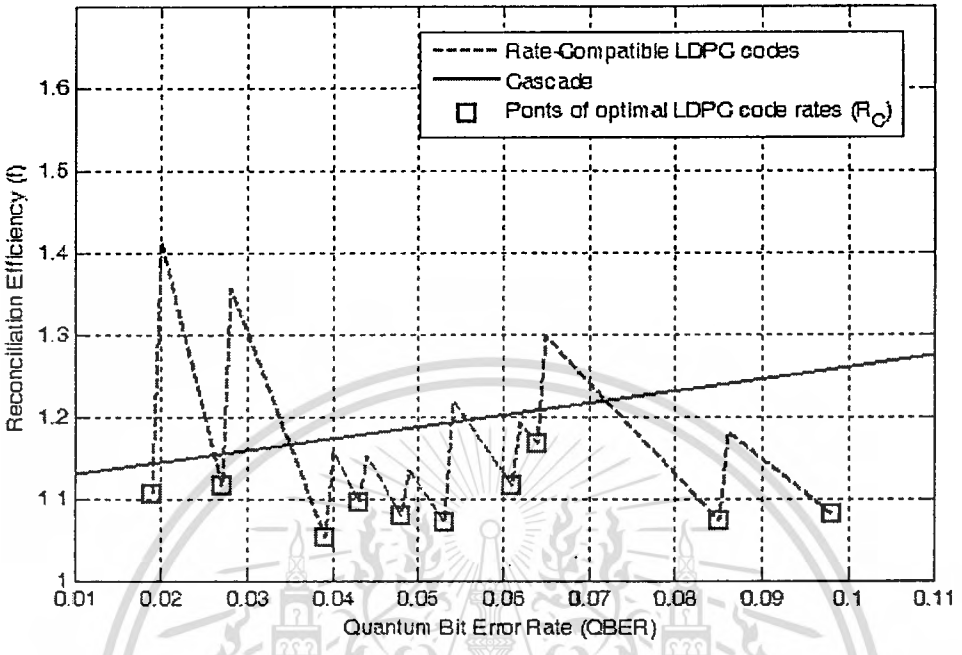
The fixed set of irregular LDPC code rates R_C (rate-compatible codes) are shown in Table 5.3 in order to cover various possible cases of error rates in QKD system. In this case, the LDPC codes are specifically optimized for the binary symmetric channel (BSC) which the cross-over probability distribution obviously corresponds directly to introduced *QBER* in the left column. For this proposed scheme, the rate-compatible irregular LDPC codes have been applied into the Slepian-Wolf system. The relationship between these LDPC code rates R_C and compression rate of Slepian-Wolf coding R_S were also defined by Eq. (3.41). This table also includes the reconciliation efficiency f in the right column. It can be calculated by using $R_S\ (1 - R_C)$ together with the critical *QBER* for each code rate, as defined in Eq. (5.2).

Table 5.3 LDPC code rates used in different case of *QBER* for quantum key reconciliation, and the calculation of reconciliation efficiency (*f*).

Critical *QBER*	LDPC code rates (R_C)	Slepian-Wolf compression rate (R_S)	Reconciliation efficiency (f)
0.019	0.85	0.15	1.1047
0.027	0.80	0.20	1.1166
0.039	0.75	0.25	1.0518
0.043	0.72	0.28	1.0943
0.048	0.70	0.30	1.0798
0.053	0.68	0.32	1.0702
0.061	0.63	0.37	1.1165
0.064	0.60	0.40	1.1658
0.085	0.55	0.45	1.0726
0.098	0.50	0.50	1.0808



(*a.*)



(*b.*)

Fig. 5.6 Efficiency of reconciliation *f* achieved by rate-compatible irregular LDPC codes and *Cascade*; (*a*) as the function of conditional Shannon entropy *H*(*X*|*Y*), and (*b*) as the function of *QBER*.

Fig 5.6 shows the graphical interpretation of reconciliation efficiency as the function of the conditional Shannon entropy, and quantum bit error rate (*QBER*) in Fig. 5.6*a* and 5.6*b* respectively. The simulated efficiency of the rate-compatible irregular LDPC codes, as proposed in Table 5.3, were compared by the 10^5 bits of *Cascade*.

5.3.2 Disclosed Informations for Rate-Compatible Irregular LDPC codes

The number of disclosed bits of the proposed rate-compatible irregular LDPC codes are shown in Fig 5.7, which are also compared with those of *Cascade* and *Winnow* in the subject of quantum bit error rate (*QBER*). The disclosed bits of the proposed rate-compatible irregular LDPC codes has been calculated from the syndrome information bits which are sent over a classical communication channel.

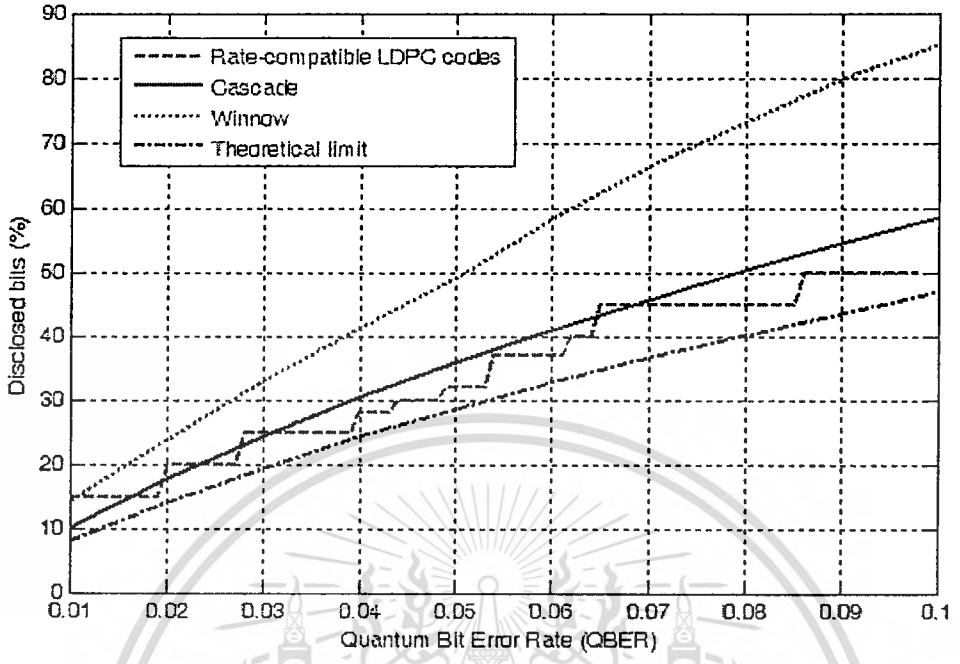


Fig. 5.7 Number of disclosed bits achieved by rate-compatible irregular LDPC codes and the binary interactive reconciliation protocols as a function of *QBER*.

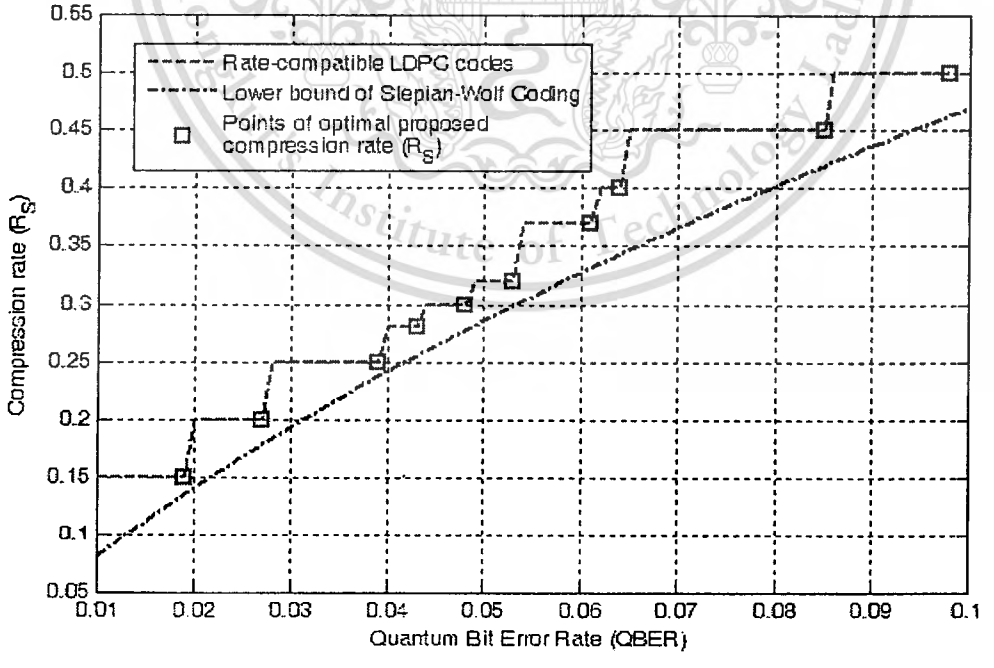


Fig 5.8 Compression rates of the proposed rate-compatible irregular LDPC codes and the Slepian-Wolf lower bound as a function of *QBER*.

5.3.3 LDPC-based Slepian-Wolf Compression Rate

The optimized 10 compression rates of LPDC-based Slepian-Wolf coding (R_s = 0.15, 0.20, 0.25, 0.28, 0.30, 0.32, 0.37, 0.40, 0.45. 0.50) are finally compared with the theoretical Slepian-Wolf lower bound as the function of quantum bit error rate (*QBER*) in Fig 5.8.

The simulation results show that the efficiency of the proposed rate-compatible irregular LDPC codes are a good alternative to *Cascade*. In term of reconciliation efficiency, the optimized LDPC codes perform better than *Cascade* when the quantum bit error rates (*QBER*) is approximately over 3.5%. Furthermore, the proposed rate-compatible irregular LDPC codes actually require the less number of disclosed bits than *Winnow* in every point of possible *QBER* range, and always less than *Cascade* when the *QBER* is approximately above 3%. Although in term of communication overhead, this proposed scheme is an interactive reconciliation method similar to *Winnow* and *Cascade*, but the success of LDPC decoding mainly achieves in the first round approximately 88%, in the second round approximately 9%, and less than 3% in the third round. Therefore, it allows the two parties to be distilled a significantly higher secret key rate in the QKD system.

5.4 Result Comparison

In this section, the simulated efficiency of the three main proposed reconciliation schemes are compared together with the existing interactive reconciliation protocols, *Cascade* and *Winnow*. There are in terms of reconciliation efficiency, number of disclosed informations, and the security of secret key rate in QKD.

5.4.1 Comparison for Reconciliation Efficiency

The graphical interpretation of reconciliation efficiency f as the function of the quantum bit error rate (QBER) are presented in Fig 5.9. The reconciliation efficiency for the proposed schemes are compared to Cascade which is probably the most widely used reconciliation protocol in the QKD systems. These results are interpreted as follows:

- *Cascade* is really simple to implement with a good efficiency approximately from 1.13 to 1.28 along with the possible cases of *QBER*.

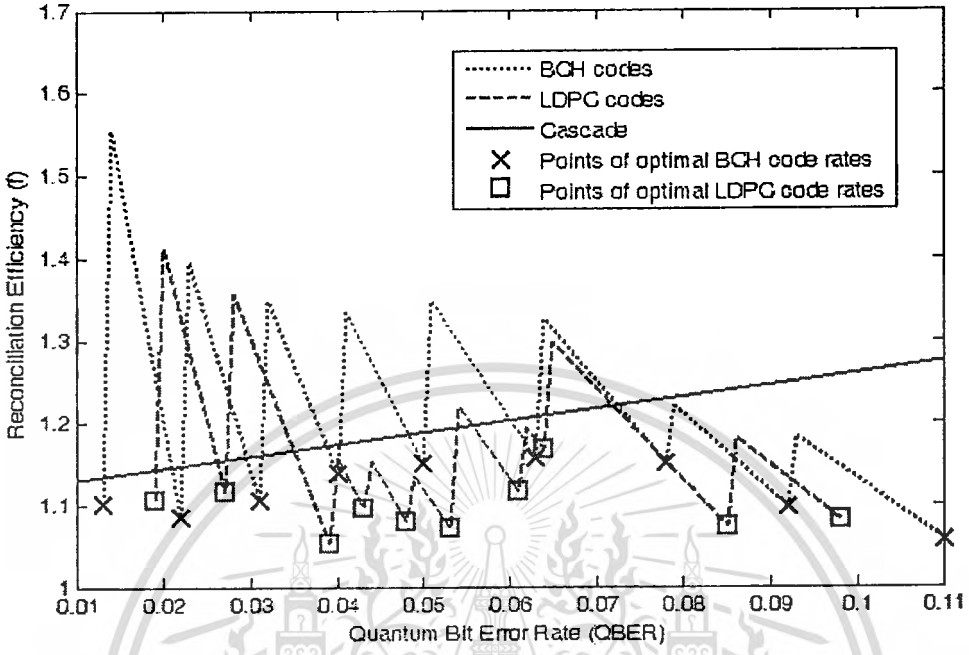


Fig. 5.9 Graphical comparison of reconciliation efficiency for the proposed rate compatible LDPC codes, BCH-based Slepian-Wolf coding, and *Cascade* as the function of *QBER*.

- In case of *Winnow*, its efficiency does not appear in Fig 5.9 because it is approximately above 1.76 that is far away from the theoretical limit.
- The proposed *BCH-based Slepian-Wolf coding* and *rate-compatible irregular LDPC codes* are a good alternative to the existing *Cascade*. Their reconciliation efficiencies are achieved better than *Cascade* in every points of optimal code rates.
- In case of BCH-based Selpian-Wolf coding, it is always better than *Cascade* when the *QBER* is approximately above 7%, while for the rate-compatible LDPC codes, they are also always better than *Cascade* when the *QBER* is approximately above 3.5%.

The gain of reconciliation efficiency can significantly impact on the achievable secret key generation rate in the QKD system. Therefore, the proposed BCH-based Slepian-Wolf coding and rate-compatible irregular LDPC codes are an alternative practical reconciliation protocols to be performed in higher-speed QKD applications.

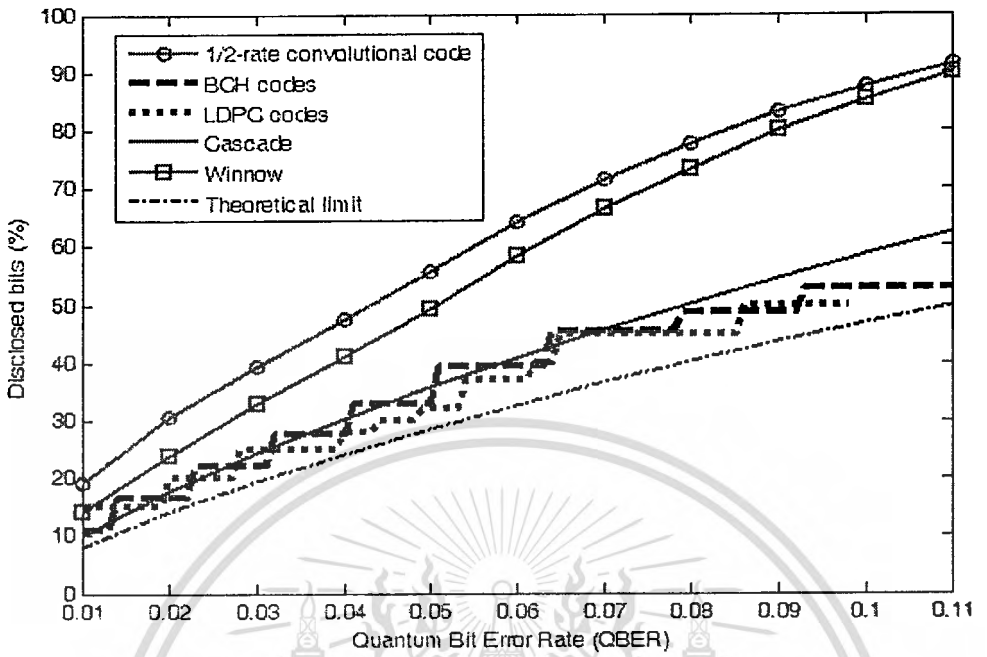


Fig. 5.10 Graphical comparison of disclosed informations for the three main proposed schemes and the binary interactive reconciliation protocols as the function of *QBER*.

5.4.2 Comparison for Disclosed Informations

In order to achieve the goals for reconciliation, the two legitimate parties need to disclose some of their correlated informations over the public classical channel for agreeing on the common reconciled keys. Because, the disclosed informations have the relationship with the sifted keys of Alice and Bob, and also might be leaked to Eve to be cloned her new secret key for breaking cryptographic systems. For this reason, the disclosed informations of different reconciliation schemes are necessary to compare for the performance evaluation in the function of QBER, as shown in Fig 5.10. In these comparison, the proposed BCH-based Slepian-Wolf coding and rate-compatible irregular LDPC codes actually require the less number of disclosed bits than Winnow in every possible cases of QBER. In case of LDPC codes, the required number of disclosed bits is closest to the theoretical limit and always less than Cascade when the QBER is approximately above 3%. In case of BCH-based Slepian-Wolf coding, it also require the less number of disclosed bits than Cascade at the points of optimal BCH code rates and always less than when the QBER is approximately above 7%.

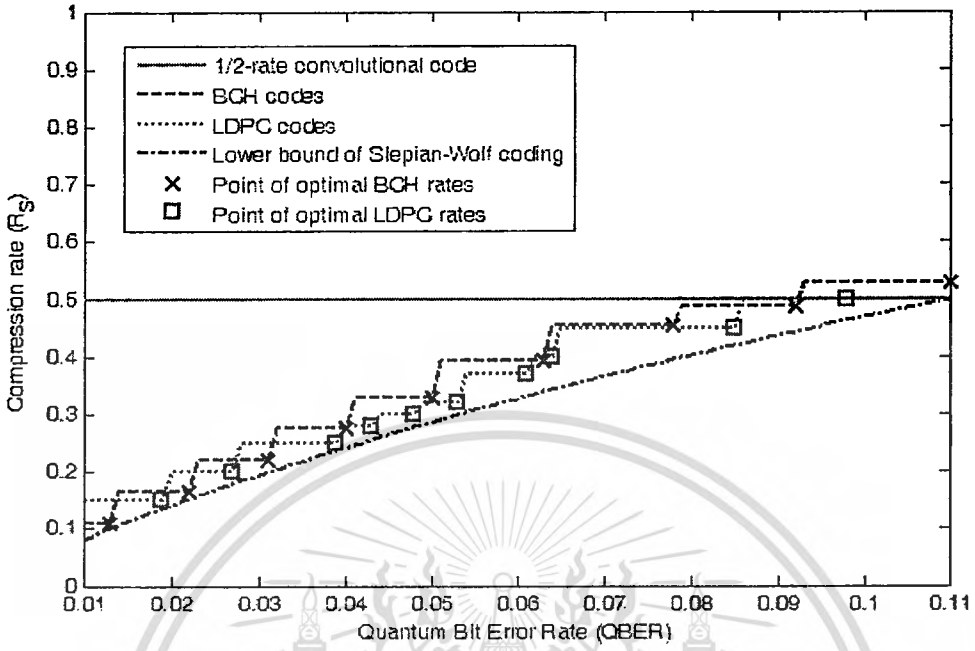


Fig. 5.11 Graphical comparison of Slepian-Wolf compression rate achieved by the three main proposed schemes and the lower bound of Slepian-Wolf coding as the function of *QBER*.

However, in case of the proposed ½-rate convolutional code, the large number of disclosed bits are required more than that of *Cascade* and *Winnow*. It is due to the compression rate for convolutional code with side information is fixed only to rate-1/2 for covering the range of *QBER* ($R_S = 1 - R_C$), Eq. (3.41)). That is not generally optimized as close to the Slepian-Wolf lower bound (Eq. (3.42)), similar to the proposed BCH (R_S = 0.11024, 0.16535, 0.22047, 0.27559, 0.32941, 0.39216, 0.45490, 0.48627, 0.52838) and LDPC codes (R_S = 0.15, 0.20, 0.25, 0.28, 0.30, 0.32, 0.37, 0.40, 0.45. 0.50), as shown in Fig. 5.11. It is noted that the efficiency of reconciliation with channel coding also depend on the number of disclosed informations, which correspond to its channel coding rate R_C equivalent to $1 - R_S$.

5.4.3 Security for Secret Key Rate

For the expression of secure secret key rate in Eq. (2.6), it is one of the most important parameters to be proved the security of secret key rate in QKD system. In this perspective, the efficiency of the different reconciliation schemes is directly related to the security of secret key rate. It can be done with getting a positive secure key rate, when the privacy amplification was assumed to be perfect.

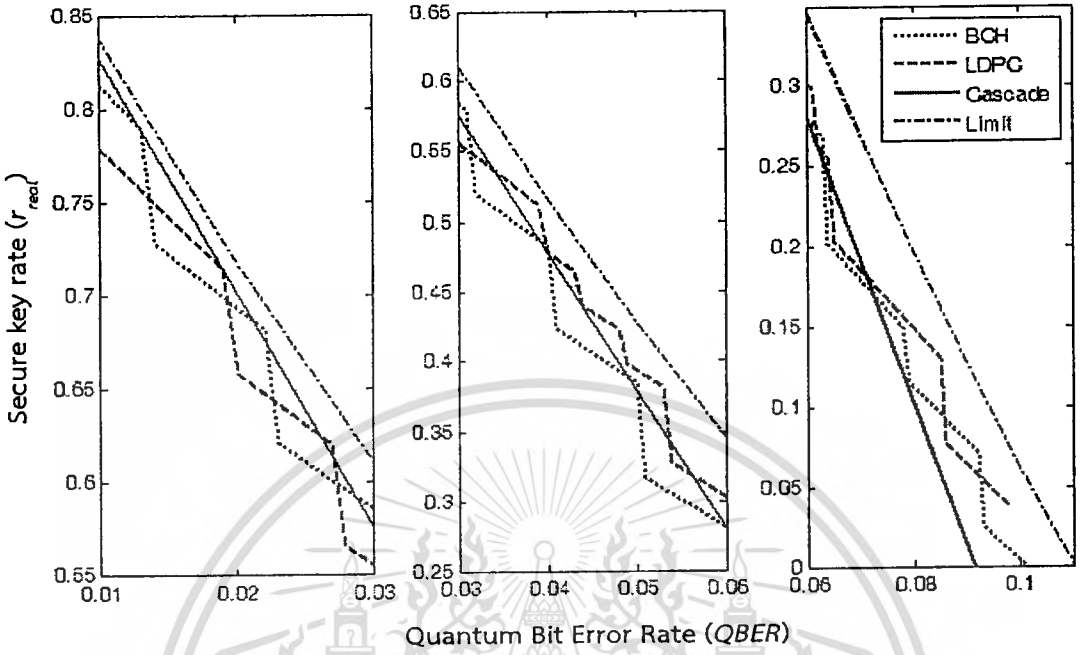


Fig 5.12 Graphical comparison of secure secret key rate for the proposed rate compatible LDPC codes, BCH-based Slepian-Wolf coding, and *Cascade* as the function of *QBER*.

Fig 5.12 shows the simulated efficiency for actual secure reconciled key rate (r_{real}) in Eq. (2.7) of the proposed reconciliation with BCH and LDPC codes. They are compared with *Cascade* and the theoretical limitations on secure key rate as the function of *QBER*. These comparisons can interpret as similar to the graphical interpretation of reconciliation efficiency f in Fig. 5.9. The advantage of the proposed reconciliation with BCH and LDPC codes can be achieved the maximal admissible error rate as close to the theoretical limit of 11% than approximately 9.2% of *Cascade*. The gain of this parameter significantly impact on the security of secret key generation rate in the QKD system. It can implies that the maximum distance of secret key distribution is possible to extend in practice when the proposed reconciliation protocols are used.

Chapter 6
Conclusions

In this chapter, the conclusion are discussed in order to summarize the results of this work, and also point out for the future work. In any Quantum Key Distribution (QKD) system, the key reconciliation is an essential step of QKD protocol. It uses a classical interactive communication in order to correct the transmission error after a key distribution of quantum objects. Its main objective is to agree on the common key of two legitimate parties (*Alice* and *Bob*) into a fully correlated string. Generally, the several quantum key reconciliation protocols have been done using the interactive error correction based on a binary searching, such as the first *BBBSS* and the well-known *Cascade*. However, the speed of these protocols are fundamentally limited by the network latency in their high interactivity which are not suitable for high-speed QKD applications. In this work, the novel quantum key reconciliation methods have been proposed by the mean of channel coding schemes. In order to overcome the research problem of key reconciliation, the error-correcting codes play a significant role by applying into the technique of source coding with side information based on Slepian-Wolf coding, where the classical information theory can be utilized for modeling and solving this problem in the context of theoretically key agreement corresponding to QKD protocol.

6.1 Reconciliation Improvement with Proposed Error-Correcting Codes

This work have shown the methodologies for reconciliation improvement by the three main contributions of convolutional, BCH, and LDPC codes. The performance of the proposed methods has been obtained by working on simulation, and important parameters have been considered in terms of error-correcting capability, reconciliation efficiencies, and number of disclosed informations. The first proposed scheme has been developed by ½-rate convolutional code with side information. It has deployed the fixed ½-rate convolutional code based on source coding with side information to correct any error in blocks with a different parity between *Alice* and *Bob* instead of using the Hamming syndrome in *Winnow*. The simulated results have shown that this proposed method is a good error-correction capability. It achieves the lower final bit error rate in reconciled keys comparable to *Winnow* at the same conditions. Furthermore, this method actually reduces the cost of communication overhead than that of the interactive protocols with *BBBSS* and

Cascade. It uses only three-message communication per iteration. However, a large number of disclosed bits is required by this method. It is suggested that the amount of disclosed bits can be minimized by optimizing the code rate according to the lower bound of Slepian-Wolf coding.

In second proposed reconciliation scheme, the BCH codes have been applied on the Slepian-Wolf coding system. It has adopted the optimal set of BCH code rates as close to the Slepian-Wolf bound depending on the different cases of error rates in QKD system. This method uses the advantage of syndrome decoding to be declared and discarded the uncorrectable blocks of key whenever decoding process fails. The numerical results show that the reconciliation efficiency can be improved at every points of optimal proposed BCH code rates than the well-known conventional *Cascade*. In term of communication resources, it is attractive to achieve in higher-speed secret key generating by using only two-message communication with minimal number of disclosed informations.

The proposed interactive reconciliation by rate-compatible irregular LDPC codes is also the main contribution for reconciliation improvement. This method also uses the advantage of syndrome decoding in order to confirm the successful conclusion when *Bob* can produce his new syndrome matching to the syndrome received from *Alice*. Otherwise, its channel coding rate is determined to decrease in each additional step until successful decoding is achieved by interactivity. The simulated results have shown that this method is a good alternative for practical reconciliation protocol. Its ability has performed reasonably well in terms of reconciliation efficiency with minimal amount of disclosed informations that also outperform *Cascade* in certain regions of *QBER*. Moreover, this method can be done without a knowledge of error rate estimation that is beneficial to avoid the waste of a relevant part of sifted key. It is achievable to get the longer final secret-key sizes after QKD post-processing. As a result, this method can also provide the exact error rate form the amount of corrected error bit in final reconciled key that is precisely for the security analysis of finite length keys.

6.2 Remark for Reconciliation with Channel Coding

The development of efficient reconciliation schemes with error-correcting codes was mainly focused of this work. Even though the proposed methods have been performed equally good, or better than the existing protocols by the simulated observation in the most important aspects of reconciliation parameters.

Nevertheless, there are the points to be discussed for the future work. One of the criticisms mentioned by Matsumoto [*Matsumoto, 2009*], is due to a general model of binary symmetric channel (BSC) has been used to characterize the transmission errors in quantum communication channel. It has also used to optimize the error-correcting codes scheme in this work. However, a BSC might not actually perform like the perfect quantum communication channel whether the transition probabilities of quantum channel is asymmetric with $p(y=1|x=0) \neq p(y=0|x=1)$, where y be the output of quantum channel with the input x. Consequently, this problem may have to solve for the novel reconciliation protocol with error-correcting code scheme in order to become more favorable as an alternative to the *Cascade* in the practical QKD system.

In case of the security perspective, the risk of this system may happen for the breaking of QKD protocol completely. It is due to eavesdropper (*Eve*) can clone the new key in such a way that she can always introduce enough errors in quantum channel, and acquire enough correlated informations in a classical post-processing, in particular during the key reconciliation step. It is conceivable that if she could know the use of error-correcting code to be reconciled by the two legitimate parties. However, the security of practical QKD post-processing, or more precisely, key reconciliation, can be taken an information-theoretic security (ITS) to be authenticated the secured classical channel as granted from the communication environment. For this reason, the bound of secure secret key rate is the most important parameters to be proved the security for QKD system. It is directly related to the parameter of reconciliation efficiency. Therefore, the security of reconciliation with error-correcting code schemes can be guaranteed with always getting a positive value of secure key rate.

In order to achieve the practical high-speed QKD secret key generation rate, the computation and communication times are also the main argument for the reconciliation improvement. In fact, these significant advances should be replied on the practical implementation of directly comparing in different reconciliation schemes. Since the speed of interactive reconciliation protocols such as *Cascade* are fundamentally limited by the network latency from their interactive communications, while modern error-correcting codes based on LDPC codes are just limited by the computational complexity of the decoding algorithm. However, the reconciliation schemes with low-decoding complexity such as BCH codes could be alternatively implemented on the practical QKD system. That is the challenging problem for the development of the reconciliation scheme based on error-correcting codes, where

the high throughput rates with minimal interactive communications is needed for the next generation QKD systems in the 1 Gbps data encryption regime [*Eraerds, 2010*].

In the future work, the proposed methods would be promising for the practical reconciliation schemes in order to be implemented as the software libraries, and to be integrated in commercial QKD devices. That is needed to be achieved in the generating rate of secret key for higher-speed QKD applications.

References

[Bennett_1, 1984] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", *Proceedings of IEEE International Conference on computers, Systems & Signal Processing*, Bangalore, India, pp. 175-179, December 1984.

[Bennett_2, 1992] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. "Experimental quantum cryptography," *J. Cryptol*, 5:328, 1992.

[Bennett_3, 1988] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy amplification by public discussion," *SIAM Journal on Computing*, 17(2):210–229, 1988.

[Bose, 1960] R. Bose and D. Ray-Chaudhuri, "On Class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, 1960.

[Brassard, 1994] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," *Advance in Cryptology Proc. EUROCRYPT 93*, pp. 410423, 1994.

[Buttler, 2003] W. T. Buttler, S. K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue and C.G. Peterson, "Fast, Efficient Error Reconciliation for Quantum Cryptography," *Physical Review A (Atomic, Molecular and Optical Physics)*, vol. 67, 052303, 2003.

[Chen, 2007] J. Chen, D. He, A. Jagmohan, "The equivalence between slepian-wolf coding and channel coding under density evolution". *IEEE Transactions on Communications*, vol. 57, no, 9,pp 2534-2540, 2009.

[Chung, 2001] S. Y. Chung, D. Forney, T. Richardson, and R. Urbanke, "On the design of low-density parity- check codes within 0.0045 dB of the Shannon limit," *IEEE Communication Letters*, vol. 5, pp. 58-60, 2001.

[Devetak, 2005] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," *Proc. R. Soc. Lond. A*, vol. 461, pp 207–235, 2005.

[Elias, 1955] P. Elias, "Coding for noisy channels." *IRE Convention Record*, Part 4, pp. 37-47, 1955.

[Elkouss_1, 2009] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," *in Proc. 2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, Jul. 2009.

[Elkouss_2, 2010] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate Compatible Protocol for Information Reconciliation: An application to QKD," *in IEEE Information Theory Workshop*, pp. 145–149, Jan. 2010.

[Eraerds, 2010] P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 gbps data encryption over a single fibre," *New Journal of Physics*, vol 12, 063027, 2010.

[ETSI-QKD, 2010] ETSI GS QKD 005, "Quantum Key Distribution (QKD); Security Proofs", *DGS/QKD-0005_SecProofs*, V1.1.1 (2010-12).

[Gallager, 1963] R. Gallager, "Low-density parity-check codes". *PhD thesis, Massachusetts Institute of Technology*, 1963.

[Hamming, 1950] R. W. Hamming, "Error detecting and error correcting codes." *The Bell System Technical Journal*, vol. 29, pp. 147-160, April 1950.

[Heisenberg, 1927] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik" *In: Zeitschrift für Physik*, pp. 172–198, vol. 43, 1927.

[Hocquenghem,1959] A. Hocquenghem, "Codes correcteurs d' erreurs," *Chiffers(Paris)*, vol 2, pp. 147–156, Sept. 1959

[Huffman, 1952] D. A. Huffman, "A Method for the Construction of Minimum-Redundancy Codes", *Proceedings of the I.R.E.*, pp 1098–1102, September 1952.

[ID Quantique, 2012] ID Quantique SA. A fast and secure solution: high speed encryption combined with quantum key distribution [Online]. Viewed 2012 January 21. Available: http://www.idquantique.com

[Kerckhoffs, 1883] A. Kerckhoffs, "La cryptographie militaire," *Journal des sciences militaires*, vol. IX, pp. 5–83, Jan. 1883, pp. 161–191, Feb. 1883.

[MacKay_1, 1996] D. MacKay and R. Neal, "Near Shannon limit performance of low density parity check codes," *IEE Electronics Letters*, vol. 32, no. 18, pp. 1645-1655, 29th Aug. 1996.

[MacKay_2, 1999] D. MacKay, "Good error correcting codes based on very sparse matrices," *IEEE Trans. Information Theory*, pp. 399-431, March 1999.

[Makkaveev, 2005] A. P. Makkaveev, S. N. Molotkov, D. I. Pomozov and A. V. Timofeev, "Practical Error-Correction Procedures in Quantum Cryptography," *Journal of Experimental and Theoretical Physics*, vol. 101, pp 230-252, 2005.

[Matsumoto, 2009] Ryutaroh Matsumoto, "Problems in application of LDPC codes to information reconciliation in quantum key distribution protocols", *arXiv:0908.2042v2*, 13 Sept 2009.

[Maurer, 1993] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[Pearson, 2004] D. Pearson, "High-speed QKD Reconciliation using Forward Error Correction," *QCMC2004*, pp. 299, 2004.

[Qi, 2006] L. Qi, G. Chen, C. Huijuan, and T. Kun, "Channel Mismatch Effect on Performance of Low Density Parity Check Codes", *IMACS Multiconference on "Computational Engineering in Systems Applications"(CESA)*, pp. 1600 – 1604, October 4-6, 2006.

[Renner, 2005] R. Renner, "Security of Quantum Key Distribution", *PhD thesis, ETH Zurich (Swiss Federal Institute of Technology)*, 2005.

[Richardson_1, 2008] T. Richardson and R. Urbanke, "Modern Coding Theory", *Cambridge University Press*, 2008.

[Richardson_2, 2001] T. Richardson and R. Urbanke, "The Capacity of Low-Density Parity Check Codes under Message-Passing Decoding," *IEEE Transactions on Information Theory*, vol. 47(2), pp. 599-618, 2001.

[Richardson_3, 2001] T. Richardson, A. Shokrollahi, and R. Urbanke, "Design of capacity approaching irregular low-density parity-check codes," *IEEE Trans. Inform. Theory*, vol. 47, pp. 619-637, Feb. 2001.

[Sartipi, 2005] M. Sartipi, F. Fekri, "Distributed source coding in wireless sensor networks using LDPC coding: the entire Slepian-Wolf rate region," *WCNC2005*, pp. 1939–1944, Mar. 2005.

[Sarwate, 1990] D. V. Sarwate, R. D. Morrison, "Decoder malfunction in BCH decoders," *IEEE Transactions on Information Theory*, vol 36, no. 4, pp 884–889, 1990.

[Shannon, 1948] C.E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27, pp. 379–423 & 623–656, July & October, 1948.

[Slepian, 1973] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[Sugimoto, 2000] T. Sugimoto and K. Yamazaki, "A study on secret key reconciliation protocol "cascade". *In IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. E83-A, pp 1987–1991, 2000.

[van Dijk, 1997] M. van Dijk and A. Koppelaar, High rate reconciliation, *Proc. of ISIT'97*, June 28 - July 4, p. 92, 1997.

[Viterbi, 1967] A. Viterbi, "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm." *IEEE Transactions on Information Theory*, vol. IT-13, pp. 260-269, April 1967.

[Weerakkody, 2006] W.A.R.J. Weerakkody, W.A.C. Fernando, A.B.B Adikari, R.M.A.P Rajatheva, "Distributed video coding of Wyner-Ziv frames using Turbo Trellis Coded Modulation," *ICIP2006*, pp. 257–260, 2006.

[Yamazaki, 2000] K. Yamazaki and T. Sugimoto, On secret reconciliation protocol–modification of ''Cascade'' protocol, *International Symposium on Information Theory and Its applications*, Honolulu, Hawaii, pp. 223–226, Nov.5–8, 2000.

[Yan, 2009] H. Yan, X. Peng, X. Lin, W. Jiang, T. Liu, and H. Guo. "Efficiency of Winnow protocol in secret key reconciliation." *In Computer Science and Information Engineering, WRI World Congress on*, vol. 3, pp. 238 – 242, 2009.

Index

Curriculum Vitae

Personal

Name:	Mr. Patcharapong Treviriyanupab
Birth date:	25 April 1987
Address:	112 Thailand Science Park, Paholyotin Rd., Klong 1, Klong Luang, Patumthani, Thailand 12120
Phone:	(662) 5646900 Ext. 2553
E-mail:	patcharapong.treeviriyanupab@nectec.or.th

Education

2005	Science-Math Program, Sarakhampittayakhom School, Mahasarakham, Thailand
2009	B.Eng. in Computer Engineering, King Mongkut's Institute of Technology Ladkrabang (KMITL), Bangkok, Thailand.

Working experience

2009 – Present Research Assistant, Optical and Quantum Communications Laboratory (OQC), National Electronics and Computer Technology Center (NECTEC), Thailand's Science Park, Patumthani. Thailand

Publication

- Conference proceedings

1.) P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "Performance of ½-Rate Convolutional Code on Winnow Protocol for Quantum Key Reconciliation" *International Symposium on Communications and Information Technology (ISCIT2010)*, Tokyo, Japan, October, 2010.

2.) K. Sripimanwat and P. Treeviriyanupab, "Investigation of Error Control Coding for Quantum Key Reconciliation on Q-Ti Network", *Updating Quantum Cryptography and Communications (UQCC2010)*, Tokyo, Japan, October, 2010.

3.) P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding for Quantum Key Reconciliation", *ECTI-CON 2012*, Thailand, May 16-18, 2012.

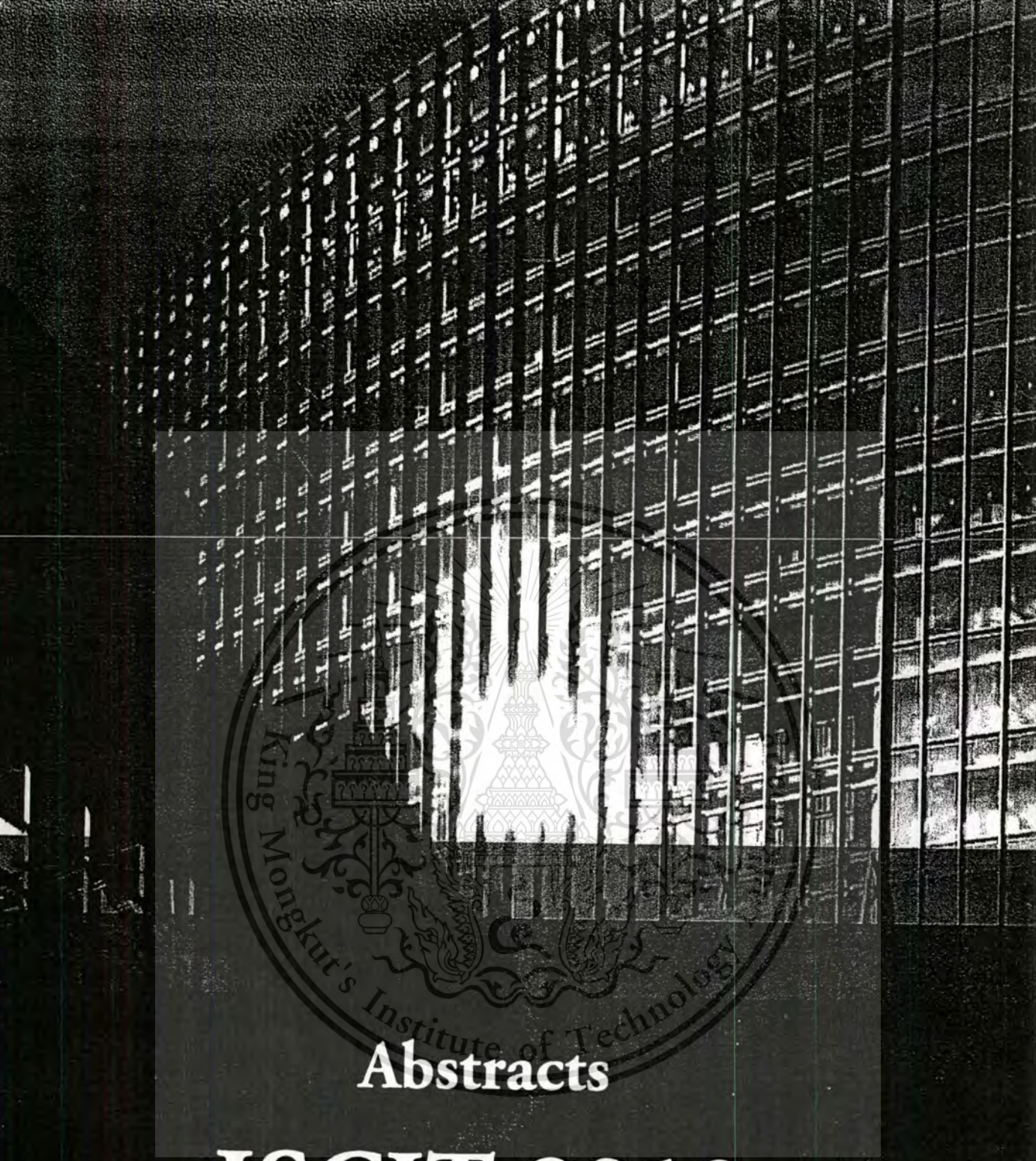
4.) P. Treeviriyanupab, P. Sangwongngam. and K. Sripimanwat, "Improved Reconciliation Efficiency with Channel Coding for Quantum Key Distribution", *Conference on Quantum Cryptography (QCRYPT2012)*, Singapore, Sept 10-14, 2012.

- Talks in workshops

1.) P. Treeviriyanupab, P. Sangwongngam, K. Sripimanwat, and O. Sangaroon, "Performance of Slepian-Wolf Coding with Convolutional and BCH Codes for Quantum Key Reconciliation", *QKD Post Processing Workshop 2011; Towards a secret key rate of 100Mbit/s*, Vienna, Austria, July, 2011.

- Book

1.) P. Treeviriyanupab, P. Sangwongngam, O. Sangaroon, and K. Sripimanwat (Editor) "World Health Information System Survey for Thailand's Smart Health Project 2010", ISBN : 978-616-12-0161-6, July, 2011.



Abstracts

ISCIT 2010

2010 10th International Symposium on Communications and Information Technologies

October 26-29, 2010
Meiji University, Tokyo, Japan

alog Number: CFP10830-PRT
8-1-4244-7008-2

Performance of ½-Rate Convolutional Code on Winnow Protocol for Quantum Key Reconciliation

Patcharapong Treeviriyanupab [1], Paramin Sangwongngam [2], Keattisak Sripimanwat [2] and Ornlarp Sangaroon [1]
[1] Department of Information Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand.
s2611310@kmitl.ac.th, ksornlar@kmitl.ac.th
[2] Optical and Quantum Communications Laboratory
National Electronics and Computer Technology Center (NECTEC), Thailand.
keattisak.sripimanwat@nectec.or.th

Abstract— The quantum key reconciliation is an essential step of Quantum Key Distribution (QKD) systems for correcting error in the raw keys which happens after the transmission over a quantum channel, where two legitimate parties make their correlated bits identical by exchanging messages over the public channel. This paper presents an alternative method for error correction of quantum key reconciliation by using ½-rate convolutional code, a class of forward error correcting (FEC) on Winnow for discrete-variable QKD protocol. The convolutional code can be applied to source coding with a side information problem which uses to describe quantum key reconciliation process. In the proposed scheme, it focuses on the performance evaluation of ½-rate convolutional code in quantum key reconciliation. In order to reduce an amount of interactive communication via error-free public channel for high-speed QKD applications, this proposed method is that the suitable solution.

I. INTRODUCTION

The quantum key distribution (QKD) protocol, first proposed in 1984 [1], is one of the quantum information processing technologies. The objective of QKD protocol is to enable two parties (*Alice* and *Bob*) to share a random bit string known as a secret key to keep confidential information from eavesdroppers (*Eve*). QKD system separates communication into two channels, a quantum channel and a public channel. In the first step, quantum states such as the polarization or phase of single photons are transmitted and received between *Alice* and *Bob* on the quantum channel. This process gives the two legitimate parties correlated classical bits of the same length called "shifted key". *Alice* and *Bob* then use a public channel to compare a few bits of their shifted keys for the estimation of a quantum bit error rate (QBER), which they can use to determine the amount of information, that *Eve* may have acquired possibly correlates to shifted keys. In the practical QKD system, even if there exists no eavesdropper existed, some quantum bit error may occur due to imperfect system configuration and noise.

The second process, occurs in the public channel is the secret key distillation which is the agreement of the secret keys [2] and usually splits into two steps. The first one, called reconciliation, is that *Alice* and *Bob* reconcile their shifted keys by exchanging information over the public channel for each party to correct errors and to get the same shifted key as that of the other party. The information transmitted on the public channel is also considered as it is opened to *Eve*. The second step, called privacy amplification [3], is for *Alice* and *Bob* to reduce the relevance of their shifted keys on *Eve*'s information. That is the art of transforming this partially secured *Eve*'s information into a highly secret key by public discussion.

A general model of correlated two random variables sharing is known as the channel-type model for secret key agreement between two parties. This model is available to *Alice* and *Bob* when they generate common random keys and use a secure communication between them as discussed in [4]. Therefore, this model can explain the QKD system without basics of knowledge in the quantum theory when the classical noisy channel is replaced by the quantum noisy channel.

In the reconciliation process, there are several protocols which have been proposed to correct errors such as the earliest BBBSS protocol [5] and the well-known Cascade protocol [6]. In these two protocols, *Alice* and *Bob* divide their shifted keys into blocks and exchange the parity of each block. Then, it is to find a block with a different parity and use a binary search to locate and correct the position of errors in the shifted keys. So the binary search process requires many interactive communications between *Alice* and *Bob*, which slow down the process in practice and not suitable for high-speed QKD applications. The other well-known protocol, Winnow [7], uses the syndrome from a hamming code, the property of forward error correcting to correct the error in a block with a different parity between *Alice* and *Bob*. Although Winnow requires much less interactive communication than that of Cascade and BBBSS, but the performance of error detection and correction is also limited with the hamming code. Other applications of forward error correcting codes such as LDPC codes [8] can be used in reconciliation process with side information system. LDPC codes used in reconciliation process help to reduce the number of interactive communications and improve the

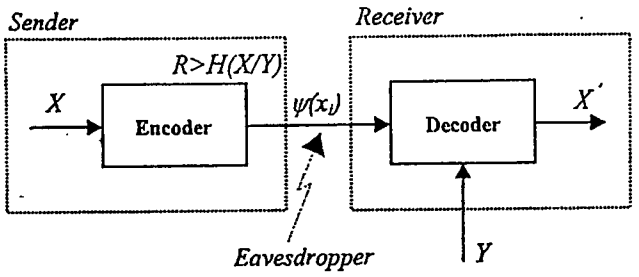


Fig. 1. Reconciliation as side information source coding

efficiency of error corrections. However, LDPC codes are defined by a huge sparse parity-check matrix, so this method requires more memory to store the parity-check matrix. In addition, security issues must be concerned with the designed parity-check matrix, if the standard or optimized matrices in literature are adopted.

The motivation of this paper is to present an alternative quantum key reconciliation method by using classical error correction technique, a ½-rate convolutional code, to correct the error on Winnow protocol instead of using the hamming syndrome for discrete-variable QKD protocol. This proposed method can be used in high-speed QKD efficiently by using side information source coding to reduce the cost of interactive communication between *Alice* and *Bob*.

This paper is organized as follows. Section II shows the principle of source coding with side information and how it can be used in the reconciliation process. In Section III, the proposed method is presented, ½-rate convolutional code with side information on Winnow protocol, used for error correction in the quantum key reconciliation. Section IV gives simulation results, and the conclusions are presented in Section V.

II. Source Coding with Side Information

Source coding with side information, known as Slepian-Wolf coding [9], is near-lossless compression of correlated sources. Given the communication system shown in Fig.1, the main information X is statistically correlated with the side information Y when the encoder does not know Y. At the sender side, X is compressed into an encoder and the encoder output, $\psi(x_i)$ called a side information source coding, is sent to the receiver. $\psi(x_i)$ is a binary sequence in which a compression rate R bits must be greater than $H(X|Y)$. At the receiver side, Y and $\psi(x_i)$ are used to decompress for the final result that will eventually become the recovered information X'. The minimum information needed by receiver is under the condition $R>H(X|Y)$.

Source coding with side information can be used in the key reconciliation process when *Alice* and *Bob* have shifted key X and Y respectively. First, *Alice* encodes X and sends $\psi(x_i)$ to *Bob*, then *Bob* recovers X using the source coding with side information at the decoder with Y and $\psi(x_i)$, which are both

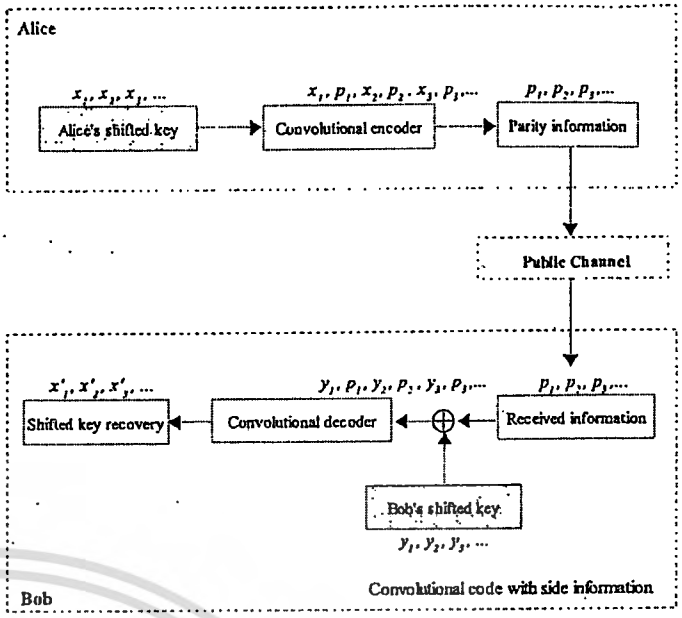


Fig. 2. Schematic block diagram of convolutional codes with side information

fed into the decoder. The amount of information leaked to *Eve* can be estimated from the number of bits in the side information source coding. Therefore, the amount of leaked information depends on the compression rate, R.

III. Secret Key Reconciliation with Convolutional Code on Winnow Protocol

In this section, the proposed method using ½-rate of convolutional code with side information on Winnow protocol for quantum key error correction is presented.

The deployment of convolutional code with side information is shown in Fig. 2. This system can be used for side information source coding when the input bit sequences x_i (*Alice*'s shifted keys) are encoded by ½-rate systematic convolutional code. For this ½-rate systematic convolutional encoder, every one input bit gives two output bits that consist of a part actual input bit and a part of parity information bit. After that, *Alice* transmits only the parity information bit through the authenticated public channel, resulting in compression rate (R) = 1. Then, *Bob* uses the parity information bit received from *Alice* and the side information y_i (*Bob*'s shifted key) and to calculate an estimate of x_i by the convolutional decoder.

In the proposed procedure, *Alice* and *Bob* arrange their shifted keys in blocks of N bits. The optimal block length N is determined by the quantum bit error rate and the remaining bit errors (k). For a bit error rate e, the probability for k wrong bits in a block of N bits is given by the binomial distribution, following equation (1).

$$P_N(k) = \binom{N}{k} e^k (1-e)^{N-k} \qquad (1)$$

Then, the parities from both *Alice* and *Bob* in the public channel are compared. If the parities do not match, it can be considered that the error correction of those blocks is as same as Cascade and Winnow. In the case of Winnow, the error can be found and corrected by the hamming syndrome when a block contains only one error. Therefore, this protocol can not produce accurate result for every error correction when the block contains more than one error. Therefore, the proposed scheme, ½-rate convolutional code, is used to correct any error associated with the block containing more than one error. This can be done by feeding the bits of each block with different parities into the convolutional encoder by using ½-rate, the convolutional code generator (G) is [100, 171], and the constraint length (K) is 7.

In the decoding process, the Viterbi algorithm (VA) is adopted to decode *Bob*'s codeword into the corresponding redundancy bits (parity information bits) received from the public channel along with his shifted keys. Finally, *Bob* has a new shifted key block with different parity bits. The objective of this method is to eliminate the final shifted key bit error rate to be less than 10^{-3}

IV. Simulation Results

This section is shown with the simulation results of the proposed method, quantum key reconciliation by the ½-rate convolutional code on Winnow protocol of the previous section.

In the simulation results, all the initial shifted keys are generated randomly according to quantum bit error rate, with the size set of 100,000 bits. These results are averaged values of 100 routines. Table I shows the error correction performance simulation results of the proposed method when comparing the final bit error rate (BER) with that of Winnow protocol in the same conditions which composed of QBER, block length, and number of passes.

Fig. 3 shows the error correcting simulation results of the proposed method when *Alice* and *Bob* arrange their keys in optimal block sizes depending on QBER.

Fig. 4 The results are compared with those of Cascade and Winnow protocols in the subject of disclosed bits (leaked information) and QBER. As illustrated in Fig. 4, a graph of the proposed method consists of three parts with different values of reconciliation process passes employed to achieve final shifted key bit error rate (Final BER) value of less than 10^{-3}. The first part of 1% QBER, the second between 2% and 6%, and the third between 7% and 10% were obtained via 1, 2, and 3 passes respectively.

TABLE I
THE PERFORMANCE OF ERROR CORRECTION

QBER (%)	Block length (bits)	Number of Passes	Final BER	
			Winnow	The proposed method
1	32	2	4.43×10^{-4}	1.64×10^{-4}
5	16	3	1.52×10^{-3}	3.50×10^{-4}
10	8	3	2.13×10^{-3}	6.99×10^{-4}

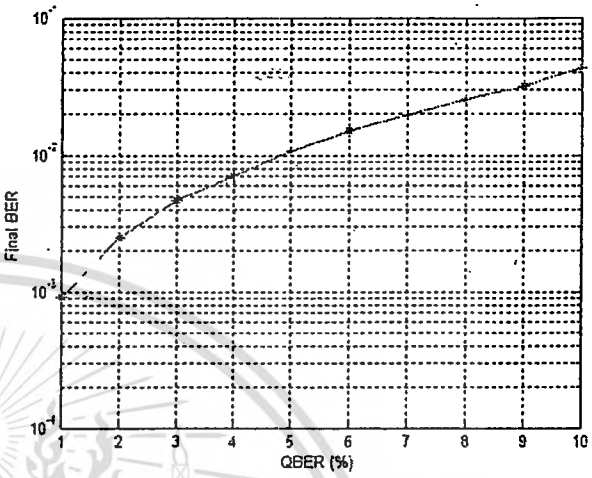


Fig. 3. Final bit error rate as a function of the quantum bit error rate

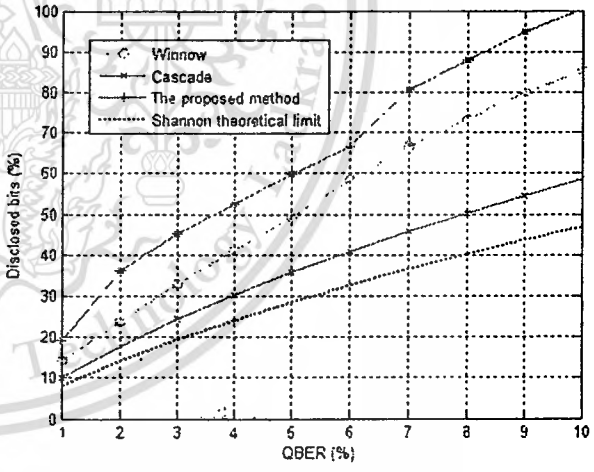


Fig. 4. Number of disclosed bits as a function of the quantum bit error rate

V. Conclusions & Discussion

The method of reconciliation by applying ½-rate convolutional code on Winnow protocol has been proposed in this paper. The results show that ½-rate convolutional code is a good error-correction alternative to Winnow protocol. Moreover, this method can reduce the interactive communications between *Alice* and *Bob* and is suitable to using in high-speed QKD applications. Even this method requires a large number of disclosed bits, it can be reduced the amount of disclosed bit by optimizing the code rate at the minimum information needed by *Bob*. In the future, it would be implemented in a real quantum key distribution network system.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179, 1984.

[2] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy amplification by public discussion." *SIAM Journal on Computing*, 17(2):210–229, 1988.

[4] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography-Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. it-39, pp. 1121–1132, 1993.

[5] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. "Experimental quantum cryptography." *J. Cryptol*, 5:3–28, 1992.

[6] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion", *Advance in Cryptology Proc. EUROCRYPT 93*, pp. 410–423, 1994.

[7] W.T Buttler, S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue and C.G. Peterson, "Fast, Efficient Error Reconciliation for Quantum Cryptography", *Physical Review A(Atomic, Molecular and Optical Physics)*, Vol. 67, 052303, 2003.

[8] D. Pearson, "High-speed QKD Reconciliation using Forward Error Correction," *Proc. 7th International conference on Quantum Communication, Measurement and Computing (QCMC)*, pp. 299, 2004.

[9] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, July 1973.

BOOKOFABSTRACTS

16-18 May 201
Phetchaburi, THAILAN

IEEE IEEE THAILAND SECTION ECTI Association KMUTT

BCH-Based Slepian-Wolf Coding with Feedback Syndrome Decoding for Quantum Key Reconciliation

Patcharapong Treeviriyanupab [1,2], Paramin Sangwongngam [2], Keattisak Sripimanwat [2] and Ornlarp Sangaroon [1]
[1] Department of Information Engineering, Faculty of Engineering
King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand.
s2611310@kmitl.ac.th, ksornlar@kmitl.ac.th
[2] Optical and Quantum Communications Laboratory
National Electronics and Computer Technology Center (NECTEC), Thailand.
keattisak.sripimanwat@nectec.or.th

***Abstract*—The quantum key reconciliation is an essential step of QKD protocol. Its main objective is to correct the transmission error after the distribution of quantum objects over a quantum channel, where two legitimate parties use a classical interactive communication for agreeing on their common key. This paper presents an alternative quantum key reconciliation method based on the Slepian-Wolf coding scheme with the chosen optimal set of BCH code rates as close to the Slepian-Wolf bound. In the proposed scheme, the BCH decoder is modified by adding one-bit feedback based on syndrome decoding to detect uncorrectable errors whenever the decoding process fails. The performance evaluation of this proposed scheme can achieve the reconciliation efficiency and reduce the cost of interactive communication via an error-free public channel comparable to the well-known reconciliation protocols. It is then suitable to apply for higher-speed discrete-variable QKD applications.**

Keywords- Key reconciliation; BCH code; Slepian-Wolf coding; Quantum key distribution.

I. INTRODUCTION

The quantum key distribution (QKD) was first proposed in 1984 [1]. It is one of the quantum information processing technologies based on classical cryptography and quantum physics. The QKD protocol employs the properties of quantum mechanics to guarantee the secure secret key exchanging between two parties (*Alice* and *Bob*) for cryptographic purpose. Generally, the QKD system consists of four steps. In the first one that occurred on the quantum channel, quantum states such as the polarization or phase of single photons are transmitted and received between *Alice* and *Bob*. This process gives a list of raw key of the two legitimate parties. Second, *Alice* and *Bob* then use the key sifting procedure over the public classical authenticated channel to obtain correlated classical bits of the same length called "*sifted key*". Then, it is to reveal a part of their information to each other in order to estimate the error rate in the quantum channel or quantum bit error rate (*QBER*). This quantity can determine the joint probability distribution among *Alice* and *Bob* as well as eavesdropper (*Eve*) which cannot be known within the classical key agreement. The third step is key reconciliation. It is the technique needed to ensure that *Alice* and *Bob*'s sifted keys are equal. Finally, privacy amplification [2] is the last step to transform this partially secured *Eve*'s information into a highly secret key by public discussion. Basically, the last two steps (reconciliation and privacy amplification) are the same as a scenario of theoretically secret-key agreement by public discussion from correlated randomness discussed in [3], known as secret-key distillation. This scenario can explain the QKD system without basics of knowledge in the quantum theory when the classical noisy channel is replaced by the quantum noisy channel.

The QKD protocol is already possible to use in the practical system as found in the commercial QKD product [4]. Even if no eavesdropper exists, some quantum bit error may occur from many other reasons as these in the classical communication systems. For example, it is due to the imperfect system configuration and noise. Therefore, the key reconciliation process was invented to solve this problem in the practical QKD system. The several existing key reconciliation protocols are the first BBBSS [5] and the well-known Cascade [6] protocols. They are binary interactive error correction, which imply that *Alice* and *Bob* exchange parities of subsets of their keys over the public classical authenticated channel. These parities help two parties to locate and correct the position of errors in their sifted keys by using a binary searching. However, these protocols require a lot of interactive communications between *Alice* and *Bob* for the binary search process, which perform a high latency over these communications and is then not suitable for high-speed QKD applications.

Apart from above protocols, the other protocols have been also proposed in the literature. For instance, the existing Winnow [7] uses the syndrome from a Hamming code as the property of forward error correcting to correct the error in a block with a different parity between *Alice* and *Bob*. Although Winnow requires less interactive communication during the reconciliation process that is significantly faster than that of BBBSS and Cascade protocols, but unfortunately the performance of error detection and correction is also limited with the Hamming code. In [8], the practical reconciliation scheme by mean of BCH codes is proposed. These codes can be used to correct the several error bits in a block of key. However, [8] shows only the BCH parameters for using in the different cases of *QBER* while does not provide the optimal code rates to achieve the best efficiency of reconciliation scheme. Furthermore, the applications of modern coding theory [9] were addressed in the key reconciliation problem such as the using of LDPC codes [10][11][12]. These proposed schemes can reduce the cost of communication resources, and to improve the efficiency in the reconciliation process. However, LDPC code reply on the message-passing decoder which are defined by a huge sparse parity-check matrix, so it

978-1-4673-2025-2/12/$31.00 ©2012 IEEE

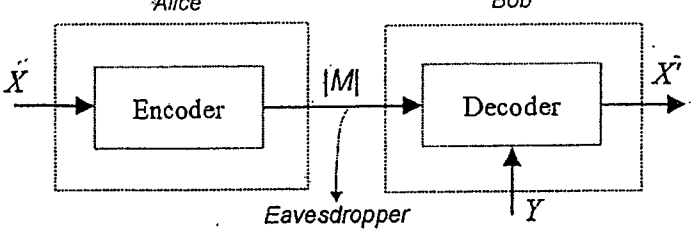


Figure 1. Quantum key reconciliation as Slepian-Wolf coding scheme.

requires more memory to operate during the reconciliation process. In addition, LDPC codes use a large of code block length [11] [12]. Therefore, it cannot discard any block of keys whenever the LDPC decoding fails.

The goal of this paper is to present an alternative quantum key reconciliation method by optimizing the code rate of BCH codes in the lower bound of Slepian-Wolf coding according to the quantum bit error rate (*QBER*). This method is based on the syndrome decoding that the BCH decoder was modified with one-bit feedback. Its main objective is to discard a block of key whenever the decoding process is not successful in order to produce no remaining bit error in the final reconciled key after reconciliation process. This proposed method can be served in high-speed QKD applications by applying the Slepian-Wolf technique to achieve the reconciliation efficiency for various cases of good to very bad *QBER*. In comparing with the other binary interactive error correction protocols, it can also reduce the cost of interactive communication.

The rest of this paper is organized as follows. Section II reviews the Slepian-Wolf coding and its scenario for solving the key reconciliation problem. Next, the theoretical secure sifted key capacity is also discussed to evaluate the efficiency of reconciliation schemes. In Section III, the proposed method, BCH-based Slepian-Wolf coding with feedback syndrome decoding for quantum key reconciliation is presented. Section IV gives simulation results of the proposed method which are compared with the well-known reconciliation protocols in term of reconciliation efficiency and number of disclosed bits. Finally, the conclusions are presented in Section V.

II. PRELIMINARIES

A. Slepian-Wolf Coding

The problem of Slepian-Wolf coding [13] deals with the near-lossless compression of two correlated sources, known as source coding with side information. By convention, the main information X is statistically correlated with the side information Y on the joint probability distribution P_{XY}. At the sender side, X is compressed into an encoder and the encoder output $|M|$ is sent to the receiver. $|M|$ is a binary sequence in which a compression rate R_S bits not lower than the conditional entropy of X given Y, denoted by $H(X|Y)$. At the receiver side, Y and $|M|$ are used to decompress for producing the final result that will eventually become the recovered information X'. It should be noted that minimum information needed by receiver is under the condition of Slepian-Wolf lower bound ($R_S \geq H(X|Y)$). In this scheme, the encoder knows only the joint probability distribution P_{XY}, but the value of the outcome of Y isn't known when encoding X.

The problem of reconciliation process can be seen as the Slepian-Wolf system as illustrated in Fig. 1. In this scheme, *Alice* and *Bob* have sifted keys modeled by binary random variables X and Y respectively. First, *Alice* encodes X and sends resulting $|M|$ to *Bob*, then *Bob* recovers X by using Y and $|M|$, which are both fed into the decoder. The objective of the key reconciliation process is to transform X and Y into a pair of fully correlation, where $Pr[X=X]$ equal to one. However, it is noticed that the information $|M|$ are sent over the communication channel during the reconciliation process, which *Eve* can obtain whenever this channel is insecure. Therefore, the efficiency of reconciliation must depend on the amount of information $|M|$ which corresponds to the compression rate R_S.

Generally, the channel coding scheme can be applied to the Slepian-Wolf system for various applications such as wireless sensor networks [14] and multimedia systems [15]. It should be noted that the Slepian-Wolf coding is closely related to the channel coding. For this reason, X and Y can be seen as the input and the output over $GF(2)$ of a binary symmetric channel (BSC) respectively. Let C be a linear block code which has a parity check matrix H of size $M \times N$. In the Slepian-Wolf scheme, the syndrome S can be calculated by compression of main information X^N, where $S^M = X^N\mathbf{H}^T$. Correspondingly in Slepian-Wolf coding, the compression rate R_S is the rate of syndrome denoted as $\frac{M}{N}$, which is equivalent to the channel coding rate R_C of linear code C, where R_C is $\frac{N-M}{N}$. Therefore, the connection between Slepian-Wolf compression rate and channel coding rate can be expressed as

$$R_S = 1 - R_C. \tag{1}$$

In the reconciliation scheme, the channel coding rate R_C must be optimized close to the Slepian-Wolf lower bound ($R_S \geq H(X|Y)$). Then, it can be rewritten in following

$$\begin{aligned} 1 - R_C &\geq H(X \mid Y) \\ &\geq H(e), \end{aligned} \tag{2}$$

where e is the cross-over probability distribution among X and Y. In the case of QKD system, e is equivalent to *QBER* which can determine the joint probability distribution among correlated information from *Alice*, *Bob* and *Eve*.

B. Theoretical Secure Sifted Key Rate

In the perfect key reconciliation process, the theoretical secure sifted key rate (r_{th}) can be defined by

$$\begin{aligned} r_{th} &= I(X;Y) - I(X;Z), \\ &= H(X \mid Z) - H(X \mid Y), \end{aligned} \tag{3}$$

where $H(.|.)$ is the conditional von Neumann entropy. In this case, the key reconciliation process occurred on classical system. Therefore, the conditional von Neumann entropy becomes the conditional Shannon entropy which $H(X|Z)$ depends on the uncertainty of *Eve*'s information on the sifted key bits, and $H(X|Y)$ represents the minimum information needed by *Bob* to recover his sifted keys.

In a practical realization, the term of $H(X|Y)$ corresponds to the minimum information that ensure *Alice* and *Bob*'s sifted keys are equal. It is certainly greater than in (3). Therefore, the actual secure reconciled key rate (r_{real}) can be rewritten as

$$r_{real} = H(X \mid Z) - f \cdot H(X \mid Y). \tag{4}$$

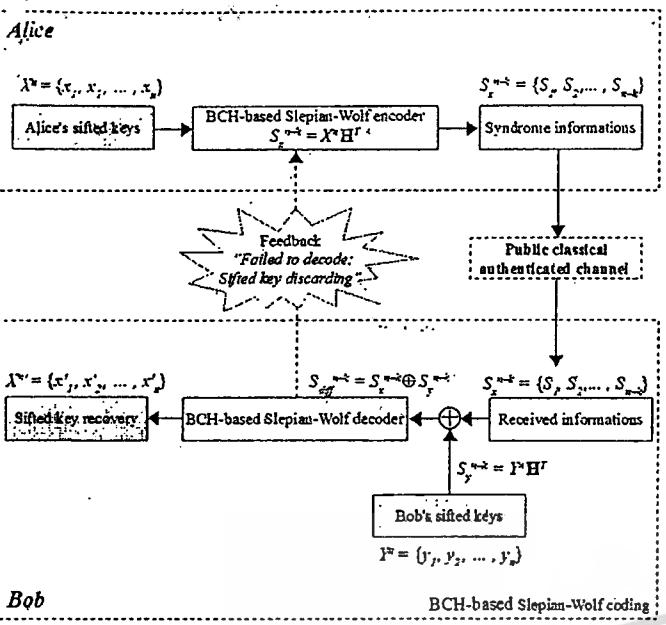


Figure 2. Schematic diagram of feedback reconciliation by using BCH-based Slepian-Wolf coding.

In the following (4), f is the parameter of reconciliation efficiency that can be evaluated the efficiencies of different reconciliation schemes. For the perfect reconciliation scheme, f is equal to "1", and the maximum *QBER* acceptable to achieve a reconciled key rate must be lower than 11%.

III. Reconciliation with Binary BCH Codes on the Slepian-Wolf System

In this section, the proposed reconciliation method using BCH-based Slepian-Wolf coding is presented. BCH codes [16][17] are a class of multiple error correcting codes over $GF(q)$ that the code rates can be selected properly on *QBER* for various cases of reconciliation scheme. The construction of BCH codes can be expressed in term of (n, k, t) where n is the codeword length, k is the number of information bits, and t is the error capability of BCH code. Generally, BCH codes are defined by a corresponding generator polynomial $g(x)$ of degree $n-k$, where $n=2^m-1$ and $mt \geq n-k$ $(m \geq 3)$.

The deployment of BCH-based Slepian-Wolf coding with feedback syndrome decoding for one-way reconciliation is shown in Fig. 2. It is described by the following four steps:

1.) Selecting of BCH parameters: Alice and *Bob* arrange their sifted keys in the optimal blocks size by selecting the parameters of BCH codes (n, k, t) for producing the code rate as close to the lower bound of Slepian-Wolf coding. In the proposed scheme, the selections of BCH parameter are shown in Table I, which corresponding to the *QBER*.

2.) Encoding: The sequences of X^n are fed into the BCH-based Slepian-Wolf encoder for calculating her syndromes by $S_x^{n-k} = X^n H^T$. After that, *Alice* transmits the syndrome information bits S_x^{n-k} over the public classical authenticated channel to *Bob* along with their positions.

3.) Syndrome comparing: Bob uses his sifted keys Y^n to calculate S_y^{n-k}. Then, it is compared with the syndrome of *Alice* that received from public classical authenticated channel to find the syndrome matching S_{diff}^{n-k} in following

$$S_{diff}^{n-k} = S_x^{n-k} \oplus S_y^{n-k}. \quad (5)$$

TABLE I. Parameters of BCH codes used in different case of *QBER* for Quantum Key Reconcilation

Critical *QBER*	Parameters of BCH codes (n,k,t)	R_C	R_S	f
0.013	(127,113,2)	0.88976	0.11024	1.1015
0.022	(127,106,3)	0.83465	0.16535	1.0841
0.031	(127,99,4)	0.77953	0.22047	1.1058
0.040	(127,92,5)	0.72441	0.27559	1.1374
0.050	(255,171,11)	0.67059	0.32941	1.1502
0.063	(255,155,13)	0.60784	0.39216	1.1560
0.078	(255,139,15)	0.54510	0.45490	1.1514
0.092	(255,131,18)	0.51373	0.48627	1.0974
0.110	(511, 241, 36)	0.47162	0.52838	1.0569

In this proposed scheme, the error is only reconciled by the BCH-based Slepian-Wolf decoder when the syndromes are different $(S_{diff}^{n-k} \neq \{0\}^{n-k})$. Otherwise, this proposed method is successfully where $S_{diff}^{n-k} = \{0\}^{n-k}$ is that ensured *Alice* and *Bob*'s sifted keys of this block are equal.

4.) Decoding: If the syndrome is different $S_{diff}^{n-k} \neq \{0\}^{n-k}$, then *Bob* feeds S_{diff}^{n-k} into the BCH-based Slepian-Wolf decoder to find the error-locator polynomial for estimating the error pattern of *Bob*'s sifted keys. Finally, the error is identified and corrected by the error-locator polynomial of BCH code to calculate X^n'. For this scheme, if the decoder declares uncorrectable errors whenever the number of error bits in the block of sifted keys more than t-error capability of BCH code [18]. Then, *Bob* sends one-bit feedback to *Alice* for agreeing to discard their sifted key of this block. Its main objective is to produce no remaining bit error bits in the final reconciled key between *Alice* and *Bob* after this reconciliation process.

The efficiency of reconciliation scheme can be evaluated from the actual reconciled key rate (r_{real}) expression in (4), where the compression rate R_S is $f \cdot H(X|Y)$. Therefore, the reconciliation efficiency f can be defined by

$$f = \frac{R_S}{H(X|Y)} = \frac{1-R_C}{H(X|Y)}. \quad (6)$$

IV. Simulation Results

In this section, quantum key reconciliation by BCH-based Slepian-Wolf coding with feedback syndrome decoding is presented in order to compare with the binary interactive reconciliation protocols [6][7], which are currently implemented in most QKD systems.

In the simulation setups, all the initial sifted keys are generated randomly according to *QBER*, with the size set of information greater than 100,000 bits. The attainment of the proposed method is to get no remaining error bit in the final reconciled key after reconciliation process with averaged values of 100 routines. The maximum size of final reconciled keys is set not less than 90% of initial size of sifted keys (key discarding < 10%).

Fig. 3 presents the reconciliation efficiency f as the function of the conditional Shannon entropy $H(X|Y)$. The blue line shows the reconciliation efficiency of the proposed method with optimized 9 BCH code rates based on the Slepian-Wolf system (R_C = 0.88976, 0.83465, 0.77953, 0.72441, 0.67059, 0.60784, 0.54510, 0.51373, 0.47162). It is compared with 10^5 bits of Cascade protocol shown as the red line. In the

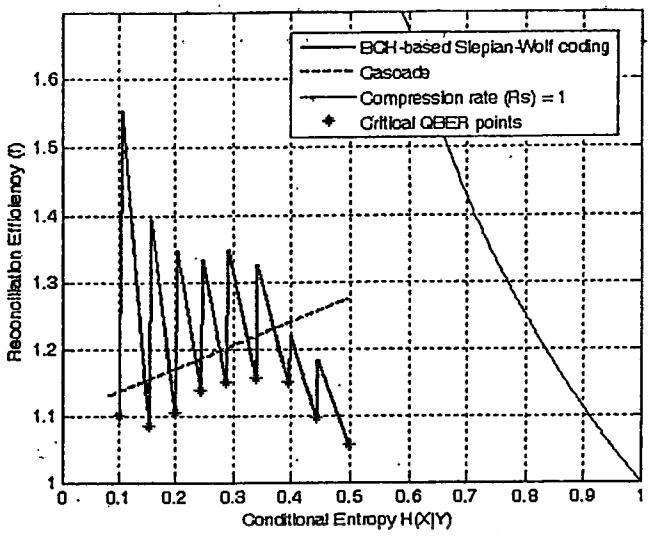


Figure 3. Efficiency of reconciliation (f) achieved by set of 9 BCH code rates based on the Slepian-Wolf coding and Cascade protocol with 10^5 bits as the function of conditional Shannon entropy $H(X|Y)$.

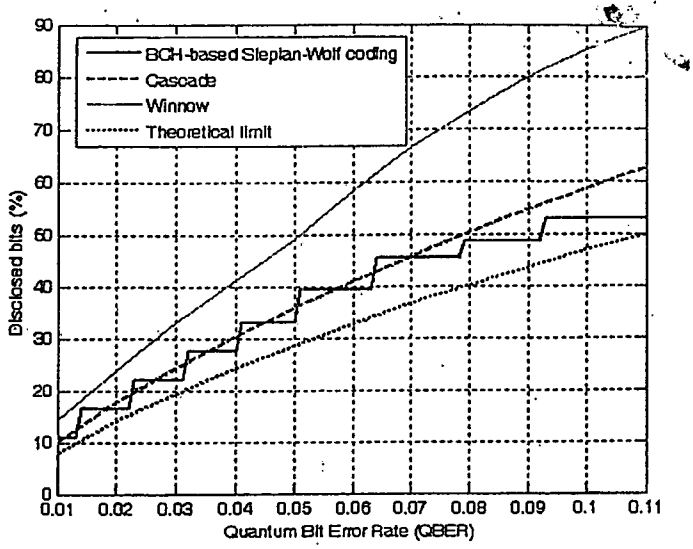


Figure 4. Number of disclosed bits achieved by set of 9 BCH code rates that compared with 10^5 bits of Cascade and Winnow protocol as a function of quantum bit error rate ($QBER$).

theoretical reconciliation scheme, the reconciliation efficiency equals "1".

In Fig. 4, the number of disclosed bits of the proposed method is compared with those of Cascade and Winnow protocols in the subject of quantum bit error rate ($QBER$). The disclosed bit is the one of parameters for evaluating the efficiency of reconciliation schemes because it is the leaked information, which can be monitored by *Eve* during the reconciliation step. The number of disclosed bits of this proposed scheme is the syndrome information bits that sent over the public classical authenticated channel during reconciliation step. In the perfect reconciliation scheme (theoretical Shannon limit), the number of disclosed bits (d_{th}) can be calculated by $d_{th} = 1-I(e)$, where e is quantum bit error rate ($QBER$), and $I(e) = 1+e\log_2 e+(1-e)\log_2(1-e)$.

V. Conclusions

Quantum key reconciliation method by applying BCH-based Slepian-Wolf coding has been proposed in this paper for using in discrete-variable QKD. The optimal set of BCH code rates has been adopted for various possible cases of error rates in QKD system. The proposed method uses the advantage of syndrome decoding to modify the BCH-based Slepian-Wolf decoder by declaring one-bit feedback whenever the decoding process fails. The numerical results show that the proposed method is an alternative reconciliation scheme to the well-known conventional Cascade and Winnow protocols. It improves the reconciliation efficiency in every critical point of quantum bit error rates. In term of communication resources, BCH-based Slepian-Wolf coding can reduce the cost of interactive communication between *Alice* and *Bob* in the key reconciliation step. Therefore, the proposed scheme is attractive to use in high-speed QKD applications.

Acknowledgment

The authors would like to thank Ryutaroh Matsumoto for their helpful comments and suggestions. The authors also would like to thank Christoph Pacher for valuable discussion.

References

[1] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York, 1984), pp. 175–179, 1984.

[2] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy amplification by public discussion," *SIAM Journal on Computing*, 17(2):210–229, 1988.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[4] ID Quantique SA. A fast and secure solution: high speed encryption combined with quantum key distribution [Online]. Viewed 2011 August 21. Available: http://www.idquantique.com

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. Smolin. "Experimental quantum cryptography," *J. Cryptol*, 5:3–28, 1992.

[6] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," *Advance in Cryptology Proc. EUROCRYPT 93*, pp. 410–423, 1994.

[7] W. T. Buttler, S. K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue and C.G. Peterson, "Fast, Efficient Error Reconciliation for Quantum Cryptography," *Physical Review A (Atomic, Molecular and Optical Physics)*, vol. 67, 052303, 2003.

[8] A. P. Makkaveev, S. N. Molotkov, D. I. Pomozov and A. V. Timofeev, "Practical Error-Correction Procedures in Quantum Cryptography," *Journal of Experimental and Theoretical Physics*, vol. 101, pp 230-252, 2005.

[9] T. Richardson and R. Urbanke, "Modern Coding Theory", *Cambridge University Press*, 2008.

[10] D. Pearson, "High-speed QKD Reconciliation using Forward Error Correction," *Proc. 7th International conference on Quantum Communication, Measurement and Computing (QCMC)*, pp. 299, 2004.

[11] D. Elkouss, A. Leverrier, R. Alléaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," *in Proc. 2009 IEEE International Symposium on Information Theory*, pp. 1879–1883, Jul. 2009.

[12] D. Elkouss, J. Martinez, D. Lancho, and V. Martin, "Rate Compatible Protocol for Information Reconciliation: An application to QKD," *in IEEE Information Theory Workshop*, pp. 145–149, Jan. 2010.

[13] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[14] M. Sartipi, F. Fekri, "Distributed source coding in wireless sensor networks using LDPC coding: the entire Slepian-Wolf rate region," *In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1939–1944, Mar. 2005.

[15] W. A. R. J. Weerakkody, W.A.C. Fernando, A.B.B Adikari, R.M.A.P Rajatheva, "Distributed video coding of Wyner-Ziv frames using Turbo Trellis Coded Modulation," *Proceedings of International Conference on Image Processing (ICIP)*, pp. 257–260, 2006.

[16] A. Hocquenghem, "Codes correcteurs d' erreurs," *Chiffers(Paris)*, vol 2, pp. 147–156, Sept. 1959.

[17] R. Bose and D. Ray-Chaudhuri, "On Class of error correcting binary group codes," *Information and Control*, vol. 3, pp. 68–79, 1960.

[18] D. V. Sarwate, R. D. Morrison, "Decoder malfunction in BCH decoders," *IEEE Transactions on Information Theory*, vol 36, no. 4, pp 884–889, 1990.