Security Performance and Protocol Consideration in Optical Communication System with Optical Layer Security Enabled by Optical Coding Techniques

Xuhua Wang

Submitted for the Degree of Master of Philosophy

Heriot-Watt University
School of Engineering and Physical Sciences

March 2015

ABSTRACT

With the fast development of communication systems, network security issues have more and more impact on daily life. It is essential to construct a high degree of optical layer security to resolve the security problem once and for all.

Three different techniques which can provide optical layer security are introduced and compared. Optical chaos can be used for fast random number generation. Quantum cryptography is the most promising technique for key distribution. And the optical coding techniques can be deployed to encrypt the modulated signal in the optical layer.

A mathematical equation has been derived from information theory to evaluate the information-theoretic security level of the wiretap channel in optical coding schemes. And the merits and limitation of two coherent optical coding schemes, temporal phase coding and spectral phase coding, have been analysed.

The security scheme based on a reconfigurable optical coding device has been introduced, and the corresponding security protocol has been developed. By moving the encryption operation from the electronic layer to the optical layer, the modulated signals become opaque to the unauthorised users.

Optical code distribution and authentication is the one of the major challenges for our proposed scheme. In our proposed protocol, both of the operations are covered and defined in detail. As a preliminary draft of the optical code security protocol, it could be a useful guidance for further research.

DEDICATION

This thesis is dedicated to my parents, Aiguo Wang and Xinlian Zhang. Their continued support enabled the hours of research, contemplation, and writing necessary to complete this project. Words are just not expressive enough for their everlasting love.

This thesis is also in debt to Dr. Xu Wang, a mentor who showed great patience on me and who guided me to see the importance of working with consistency.

This thesis is dedicated to my friend, Yuxin Zhao, without her encouragement on the hardest moment, this thesis wouldn't have been possible to make.

ACKNOWLEDGEMENTS

I would like to gratefully acknowledge the guidance of my supervisor, Dr. Xu Wang, who has been abundantly helpful and has assisted me in numerous ways. I specially thank him for his infinite patience. The discussions I had with him were invaluable.

I would like to say a big thanks to my colleagues, Dr. Zhensen Gao, Dr. Bo Dai, Dr. Mumtaz Ali and Mr. Yu Liang. We had a good time together with lots of valuable discussions. Their ideas and solid working on the related subjects inspired me a lot.

I am particularly thankful for my friend, Yuxin Zhao, for her help and encouraging me to pursue my postgraduate studies.

Many thanks are due to all my friends for their support and kindness.

Last but not least, I would like to appreciate my family, especially my parents, for giving me their great love and support.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

3GPP	3rd generation partnership project
AEAD	Authenticated encryption with associated data
AES	Advanced encryptionstandard
AES	Advanced encryption algorithm
AH	Authentication header
AKA	Authentication and key agreement
CCMP	Counter mode cipher block chaining message authentication code protocol
CDMA	Code division multiplexing acess
CIA	Confidentiality, Integrity, Availabitliy
CSI	Channel state information
CSK	Code shift keying
DES	Data encryption standard
D-H	Diffie-Hellman exchange
DoS	Denial of service
DSA	Digital signature algorithm
DSS	Direct sequence spread
EAP	Extensible authentication protocol
ESP	Encapsulating payload
FH	Frequency hopping
HDR	Header
HTTPS	Hypertext transfer protocol secure
ID	Identity
IPsec	Internet protocol security
ISO	International standards organization
LAI	Location area identification
LTE	Long term evolution
MAC	Message authentication code

MD5	Message digest 5
MIC	Message integrity code
OC	Optical code
OCSP	Optical code security protocol
OFDM	Orthogonal frequency division multiplexing
OOK	On-off keying
PKI	Public key infrastructure
PMK	Pairwise master key
PRBS	Pseudo-random bit sequence
PRF	Pseudo-random function
PTK	Pairwise transient key
QKD	Quantum key distrbution
RAI	Routing area identification
RC4	Rivest cipher 4
RFC	Request for comments
RSN	Robust security network
SA	Security associations
SHA1	Secure hash algorithm 1
SPC	Spectral phase coding
SSL	Secure sockets layer
TDSS	Time domain spectral shaping
TKIP	Temporal key integrity protocol
TLS	Transport layer security
TPC	Temporal phase coding
UMTS	Universal mobile telecommunication system
VLR	Visited location register
WEP	Wired equivalent privacy

LIST OF PUBLICATIONS BY THE CANDIDATE

[1] X. Wang, Z. Gao, B. Dai, **X. H. Wang**, N. Kataoka, and N. Wada, "Fast optical code reconfigurable technique for secure optical communication", (Invited) 13th International Conference on Transparent Optical Networks (ICTON 2011), Sweden, July, 2011, Paper We. B1. 4.

[2] X. Wang, Z. Gao, **X. H. Wang**, N. Kataoka and N. Wada, "Bit-by-bit optical code scrambling technique for secure optical communication", Optics Express, Vol. 19 Issue 4, pp. 3503–3512 (2011).

Chapter 1 Introduction

As the network become more and more important in everyone's daily life, the security of the network draws increasing interest from the government to the public. In 2013, the PRISM program has been revealed by Snowden in Hong-Kong, which is considered as a big crisis in information privacy. The case shows the importance of the network security in many ways [1]. And in 2014, the world's largest and most popular mobile device provider – Apple involved in several data leakage cases, from user device ID (which can be used to track the phone user) to the data stored in iCloud. These big events remind us constantly of the importance of the network security [2].

The security of communication networks involves a fairly wide range of topics from system design, hardware and software implementation to the management, media and human behaviour etc. In spite of the fact that the network security has a very broad definition and the security requirement always varies for different networks, the ultimate objective is to protect the data safe, no matter what types of network we are in, how we configure our computer and firewall, patch our system, apply what kind of encryptions and security protocols. In other word, information security is the core of network security.

1.1 Information Security

The information security is always an issue about the balance under a certain amount of resources. Even when we start to define the scope of information security, a compromise has been made between the system complexity and security. Therefore, knowing the value of the information we are going to protect is quite important while developing a security strategy. Although in traditional cryptography, we always assume that the adversary has unlimited resources, it becomes unrealistic when the cost of hacking is higher than the value of the information.

In this section, the background of the information security is introduced, including the techniques used in the current security applications in communication networks.

1.1.1 Elements of information security

The general consideration of information security consists of three aspects: confidentiality, integrity and availability, which are often referred as CIA Triad by the definition from International Standards Organization (ISO) [3], as shown in Figure 1.1.

Confidentiality keeps the privacy of the data. It is the protection on the information from unauthorized access.

Integrity ensures the protected data cannot be modified or damaged by unauthorized parties, and if the modification on data (by authorized users) is unexpected, the original data can be recovered.

Availability refers to the data should be accessible by the demands of authorized entities. Either the access channels or the authentication mechanisms must be working properly when needed.

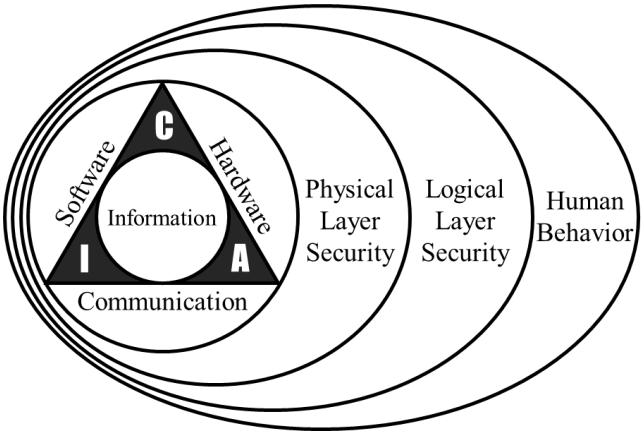


Figure 1.1 CIA triad and the onion model for information security.

The major concern of the CIA Triad is about the information security. And the concept of CIA Triad is continued being debated amongst security professionals. As a starting point of pursuing security, more and more considerations have been proposed and added into the original model, such as:

Authentication, which ensures both entities involved in the communication are who they claim to be.

Non-repudiation, which prevents the entities involved in communication denying the information transmission. The concept is original from the electronic commerce.

Accountability, which records and traces the behaviours of specific users.

It is important to note that although the considerations of the security are increasing, not all the elements are necessary at the same time. The development of the security service is always a result of needs. One thing is certain that each security technique always has its own limitations, and any formalized framework should never be treated as the end but the beginning to the new security approaches.

1.1.2 The hierarchy of network security techniques

The network security involves the techniques from many areas including, but not limited to, cryptography, network protocols, information theory, coding, switch and router, transmitter and receiver etc. In order to organize them in a structured map, it is convenience to categorize the technologies by their functionalities as below:

Elemental techniques: these techniques are primarily designed to fulfil one of the security elements. As the basic security measures, these techniques could be combined with each other or adopted by higher level implementations. The techniques are usually manipulated by system designer, and are not always known by the individual users.

Integrated techniques: these techniques are developed from one or more elemental techniques, and are designed to fulfil certain security requirements. These techniques are user oriented and usually can be used by any individual users directly.

Security Architectures: these techniques are independent security solutions, which contain bunch of lower level techniques and can be used as a security guidance or standard.

An example of the categorization is shown in Figure 1.2. Although not all the techniques could fit in the categorization perfectly, it is still very helpful when we

realized the functional level of each security techniques. It will provide us with a better understanding on how these techniques operate together or compete with each other.

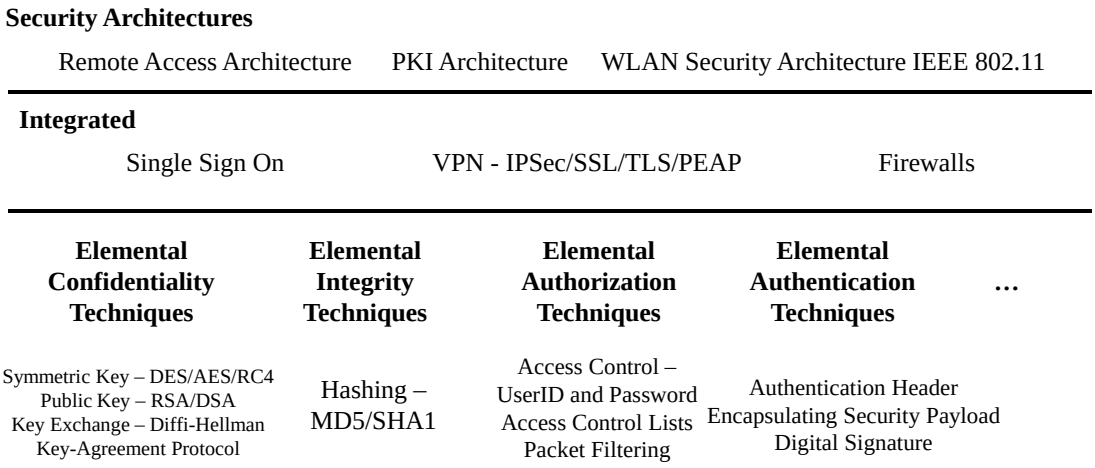


Figure 1.2 The hierarchy of network security techniques.

As shown in Figure 1.2, the elemental techniques in the same group have similar roles. For example, Data Encryption Standard (DES) [4], Advanced Encryption Standard (AES) [5] and Rivest Cipher 4 (RC4) are symmetric encryption algorithms and can be used as the options for data encryption. While the RSA [6] and Digital Signature Algorithm (DSA) [7] are asymmetric encryption algorithms which can be used to encrypt or to verify a digital signature. Message Digest Algorithm (MD5) [8] and Secure Hash Algorithm (SHA1) [9] are used to verify the integrity of the data. The integrated techniques consist of several elemental techniques. For instance, Internet Protocol Security (IPsec) adopts DES and AES for Encapsulating Security Payload encryption, SHA1 and AES for integrity verification, Diffie-Hellman group for secret key distribution [10]. Similarly, for different network environments, different elemental techniques may be selected to optimize the system performance.

1.1.3 The conceptual model of communication network and network security

Traditionally, the communication networks are divided into two broad types: One provides only unidirectional downstream capacity to diffuse information, which is referred as broadcasting network, and the other provides bidirectional upstream and downstream channels, which is referred as telecommunication networks.

With the rapid growth of the internet, the distinctions between broadcasting network and telecommunication network are converging. According to the research report on Science magazine [11], one fourth of broadcasting network had been digitalized by 2007. And the information transmitted on the Internet has accounted for 97% over the total amount of information exchange.

Meanwhile, there are still several types of communication networks working independently, such as the Internet, public switched telephone networks, mobile networks, global telex networks and interbank networks, as well as the private networks maintained by organizations, enterprises, universities and institutions that might not tend to open their resources to public access.

Since the services provided by these networks are different, the security requirements are also vary from one to another. To understand how the security techniques function in these networks, it is better to introduce a general model of communication networks.

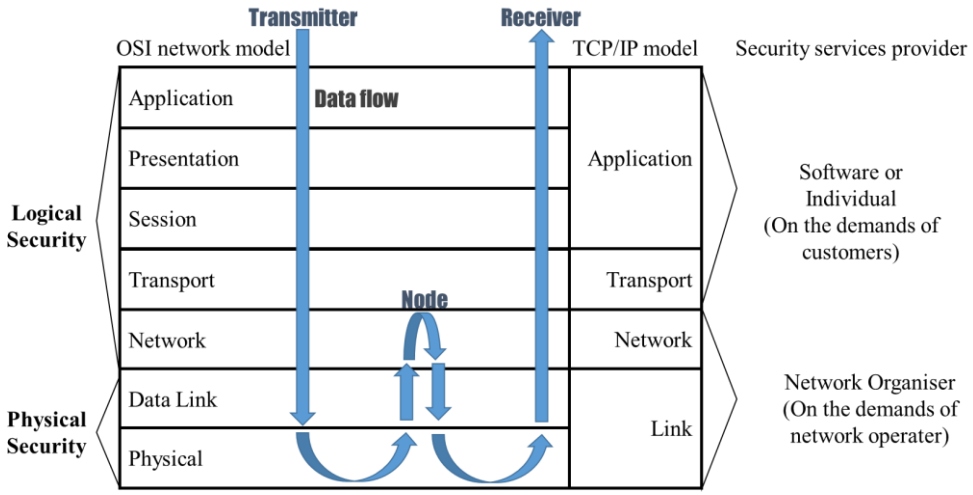


Figure 1.3 Network security and the network model.

Figure 1.3 shows the OSI model and the TCP/IP model of communication networks. The blue arrows indicate the data movement in the transmission. The data from various applications are encapsulated in the format of TCP/UDP packet in the transport layer. Then the packet is further encapsulated with an IP header to form an IP packet. The IP packets are further encapsulated into the format that is suitable for transmission on the channels which are defined according to the different physical

protocols, such as Ethernet, ATM, SONET, GSM and CDMA etc. At each network node, the IP header needs to be extracted for the purpose of routing the data packet to its destination. Similarly, the IP data packet is transparent to the node by the default TCP/IP protocols. Thus in order to keep the data packet safe, either secure physical protocols or the upper layer encryption is required. For the individuals without the knowledge of the network infrastructure, upper layer encryptions are the only choice for security purpose. Although the upper layer encryption may provide an end-to-end security, the obscurity of the data may cause compatibility problems in the bottom layers. In this case the network operators have to use the security approaches in the link layer/physical layer. Besides, elimination of the unnecessary O-E/E-O conversions will increase the throughput of the network significantly.

1.2 Network Security Threats

In this section, several common security threats in communication networks are introduced. These threats can be basically classified into two categories: passive attacks and active attacks, as shown in Table 1.1.

Table 1.1 Network security threats classification.

Network Security Threats	
Passive attacks	**Active attacks**
Sniffing	Denial-of-service attack
Eavesdropping	Spoofing
Passively Trojan	Man-in-the-middle attack

Generally, the objective of passive attacks is to collect the data information without the awareness of the legitimate user, for example, sniffing, eavesdropping, and even the passive Trojan. These operations do not disrupt the network operations or services, thus are usually difficult to be detected. However, as the nature of the passive attacks, these operations are usually aimless. The attacker cannot choose the objectives he wants to attack or the information he wants to collect, he needs to maintain the attack alive until the objective appears with targeted information.

On the other hand, active attacks usually cause an influence on normal network operations and services. One of the ultimate objectives of active attacks is to disrupt the network or the service temporarily. The other is to modify the information to deceive the users of the network or the service. Due to the interference caused by the attackers, active attacks are usually traceable and detectable. Hence the active attacks are only used for breaching the specific targets and services in an unpredictable way to avoid being countered.

1.2.1 Packet Sniffing and Eavesdropping

Packet sniffing is defined as the operations that monitor the network data flow and collect useful information. It can be used either in positive way or negative way. In fact, all the telecommunication service providers use sniffing techniques to monitor the traffic and locate the potential threats of the network, especially against Denial-of-service attack. The technique makes the traffic accountable. However, in a broadcasting network, such as Ethernet, all the packets are sent to every device in the network. In such network, it is easier for the attacker to capture all data packets by setting his/her Ethernet adapter to the promiscuous mode. Therefore, all the data without encryption is at the risk of exposure. There are several popular services such as telnet, FTP and POP3 that transmit the usernames and passwords in plain text. Such defects of the protocols cause severe security vulnerability in Ethernet. Since the sniffing is operated in the data-link layer, the current solution is to encrypt the data in the upper layers.

While the packet sniffing is usually operated at the nodes of the network, eavesdropping is the technique to listen the traffic secretly from the transmission media. The threat is considered as a physical layer attack. Another difference between sniffing and eavesdropping is the environment: sniffing can be applied when the network protocol is known to the attacker, so that he can use the related device to extract data; whereas the eavesdropping can be used to intercept the transmitted signals, no matter what the data format is, and the result can be further used for cryptanalysis. Increase the data confidentiality is the best way against packet sniffing and eavesdropping, while the physical access to the network nodes and links should be in control.

1.2.2 Denial of Service and Jamming

Denial-of-Service (DoS) attack is one of the simplest forms of network attack. Instead of trying to steal the information, the DoS attack simply disrupts the information services by exhausting the resources available to the legitimate users. Since the server is usually stronger than the personal terminals, a successful DoS attack technically requires the attacker to have the ability to control a large amount of terminals to perform the attacks in the same time. DoS attacks are usually considered as an application layer attack, since most of system flaws leading to DoS attack are tied to a certain program or service, and can be removed after software upgrading.

While DoS attacks are initiated to exhaust the resources of the service server, jamming is the technique to use up the bandwidth of the communication channels, hence is considered as a physical layer attack. Since the jamming signals are supposed to occupy all the channels of the network, the energy consumption of the attacks are remarkable and thus easily to be located. Although both the DoS attack and jamming are not the attacks in smart way, they do cause destructive influence: imagine the scenarios that the services of stock exchange or the World Cup are interrupted, or even worse in the case that a natural disaster happens while the entire communication network is jammed by the terrorist, the loss could be countless.

1.2.3 Spoofing and Man-in-the-middle attacks

Spoofing attack is the situation that an intruder successfully masquerades as a legitimate user by altering the transmitted data. Since many protocols in TCP/IP suite do not provide authentication mechanisms, the most common spoofing attack is IP spoofing. The destination of the packets is redirected by the attacker through the technique that falsifies the IP address. IP spoofing can be also used for good purpose, for example virtual users could be simulated by IP spoofing when the service requires a multi-user circumstance.

Man-in-the-middle-attack is the attack that the attacker directly relays or modified the content of the message on purpose without being aware between two parties who believe they are communicating with each other. The attack can be performed by the

clients and applications which are used by both of the parties but owned by the third party. Also the attack can be achieved by physically access a node between two communicating parties, such as the routers or the switches. Compared to eavesdropping, the man-in-the middle attack intercept all of the message exchanges between the two targets and has the ability to alter or even inject the new ones.

To prevent the spoofing and man-in-the-middle attack, the mutual authentication is required, which indicates both of the parties in the communication are real and as the ones they claim to be.

1.2.4 Viruses, Malwares and Trojans

Although viruses, malwares and Trojans are usually categorized to the computer security, they can also be used for cause the flaws in communication. As the most common attacks are targeted to the personal users, the impact of them can be controlled by the well-defined system rules. For example, make sure the users who don't have enough security awareness can only have limited authorities to the system. Since the viruses, malwares and Trojans are spread by exploiting system defects and inappropriate operations, it is suggested that only trust-worthy system and open-source software are used to avoid the threats comes from the application itself.

1.3 Examples of security approaches

In this section, several security measures undertaking in current communication networks are introduced. By studying these examples, it is easier to form a comprehensive understanding on the topic of security issues in practical security systems.

The first example is the Secure Sockets Layer/Transport Layer Security (SSL/TLS) protocol. The protocol is widely used in web security applications and is supported by most of the web browsers. The Hypertext Transfer Protocol Secure (HTTPS) protocol, which is popularly deployed on the Internet, is based on SSL/TLS protocol. It is used to secure the email services and the payment transactions on the web. At present, all types of websites use it for account managements.

The second example is the Universal Mobile Telecommunications System (UMTS) security architecture used in the “third generation” mobile cellular communication systems. It is derived from the “second generation” Global System for Mobile communications (GSM) system.

The third example is the 802.11i protocol, which is used to secure the wireless local area network (WLAN). Technically, WLAN is more susceptible to eavesdropping than wired network. Hence in the development of WLAN security, the protocol includes not only the strong encryption and authentication, but also a high level access control.

The last example is the Internet Protocol Security (IPsec) protocol, which is an end-to-end security scheme operating in the internet layer. Thus any application traffic over an IP network can be automatically secured by IPsec. Besides, the IPsec suite is an open standard. Various kinds of elemental security techniques are included in the protocols, and the security service provider can configure the protocols to achieve specific demand.

1.3.1 HTTPS based on SSL/TLS

Although Hypertext Transfer Protocol Secure (HTTPS) is not a top-level solution for network security, it is widely deployed on the Internet providing a bidirectional encryption of communication between specific client and the server, especially for the payment transactions on the web based application. The protocol is simply built on Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) including encryption algorithms, message digest functions and digital signatures. The current TLS version deployed is TLS 1.2 and is defined in RFC5246 [12].

The SSL/TLS session is started from a handshake between the client and the server, the basic information needed in secure transmission is synchronized during the hand shake, as shown in Fig. 1.4.

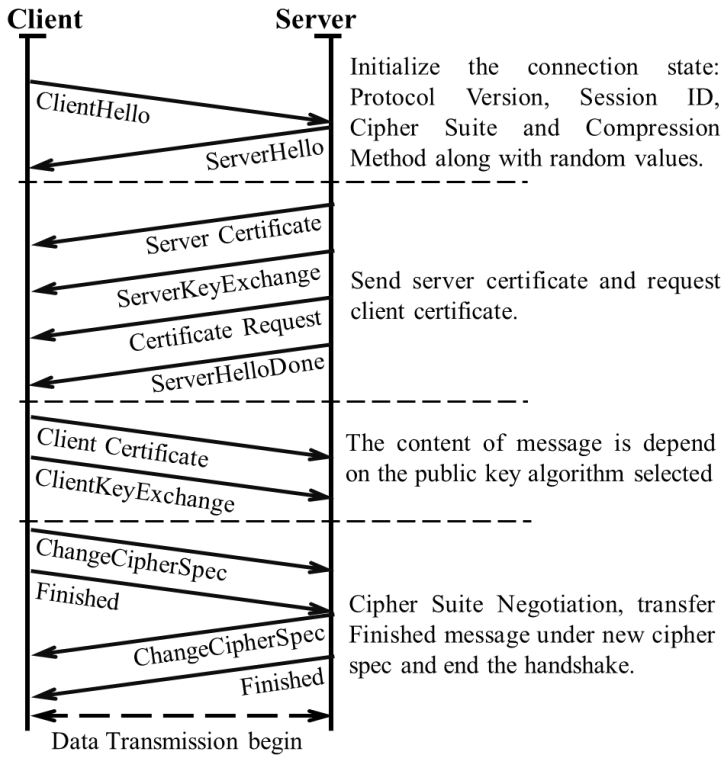


Figure 1.4 An example of TLS 1.2 handshake.

During the handshaking, the elements needed for secure communication are exchanged, including:

Exchange the certificates to authenticate client and server to each other.

Negotiate the cipher suite to be used for application data transmission.

Generate a master secret key that protecting cipher negotiation.

Establish and share a session key, declared as master secret which secures data used for cipher negotiation.

After handshake, the application data is exchanged under the encryption selected during Cipher Suite Negotiation, as shown in Figure 1.5.

The application data is firstly chunked into segments no larger than 2^{14} bytes, and then compressed by selected compression algorithms (TLS 1.2 supports 256 different compression methods). The result is then combined with a message authentication code (MAC). After that, the whole segment is encrypted by a selected encryption algorithm. TLS 1.2 provides four options on encryption: no encryption, stream cipher (RC4 etc), block cipher (3DES and AES etc) and Authenticated Encryption with Associated Data

(AEAD) cipher. Finally, all the encrypted segments are combined and enclosed as TCP packets.

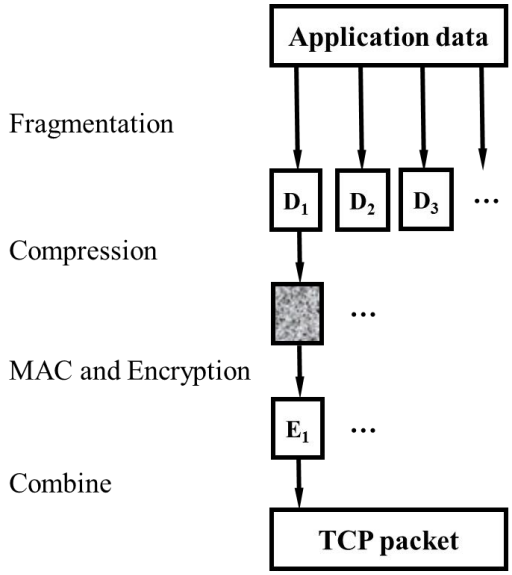


Figure 1.5 Data encryption process under TLS 1.2 protocol.

Both keys for MAC and encryption are calculated from the master secret which is always 48 bytes in length and generated by the Diffie-Hellman algorithm. To avoid any data modification and replay attacks, MAC is computed from the MAC key, the message length, the sequence number which indicates a particular session, and the message content. Hence any modification on message or repeated message will lead to a new encrypted result.

If the attacker does break an encryption key, all messages encrypted with it are revealed. Since MAC is also encrypted, the attacker needs to break both MAC and encryption keys to achieve a man-in-the-middle attack.

Generally, HTTPS based on TLS provides the integrity and confidentiality protection on data transmission via the use of symmetric encryption and authentication functions. It is proposed that the order of the encryption and authentication affects the security level eventually [13].

Denial-of-service attacks which attempt to bring the service down could be the real threats to TLS. Since TLS runs over TCP, DoS attacks on TCP connections cannot be avoided, besides the attacker can initiates a flood of handshake request to exhaust the server on RSA decryption.

Currently, there are five protocols in the SSL/TLS family, which are SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2. It has been revealed that all the SSL are not secure anymore especially as American NSA's PRISM programme revealed. In TLS, the public-key system with perfect forward secrecy has been adopted, making it much safer than previous versions. However, according to the survey from SSL labs, only 58.1% SSL-enabled web sites support the newest TLS 1.2 protocol by April 2015 [108].

1.3.2 Security architecture in UMTS mobile network

The technologies of the mobile networks are developed really fast driven by the needs of mobile communication. Hence there are quite a number of standards related to the security issues. Due to the limitation of space, here we only introduce several security features which are included in the 3rd Generation Partnership Project (3GPP) security architecture related to the Universal Mobile Telecommunication System (UMTS). UMTS is a 3G mobile cellular system adopted widely by the telecommunication operator all over the world. The full content of the security architecture is detailed in [14]. And for the security architecture developed by 3GPP for 4G (LTE) wireless communication standard, the full definition can be found in [15].

The security features defined in [14] that interested us can be categorized as the network access security, user domain security and configurability of security, as shown in Table 1.2.

There are two ways to identify a user on the serving network: identification by temporary identity (TMSI/P-TMSI) and identification by permanent identity (IMSI). And the association between the permanent and temporary user identity is kept by the Visited Location Register (VLR/SGSN) in which the user is registered. Normally, a TMSI is used to avoid the compromise of the user identity confidentiality. And it is valid only in the location area or routing area in which the user is registered. A Location Area Identification (LAI) or Routing Area Identification (RAI) is added if the TMSI is outside the area.

Table 1.2 Security features in UMTS security architecture.

Security features		Description
Network access security	User identity confidentiality.	The identity, the presence and the services of a certain user cannot be retrieved by eavesdropping.
	Entity authentication	Authenticate user and serving network to each other.
	Confidentiality	Algorithm negotiation, key agreement, data encryption, signal eavesdropping disproved
	Data integrity	Algorithm, key and data haven't been modified
User domain security	User-to-USIM authentication	USIM can only be accessed until the user has been authenticated to USIM.
	USIM-Terminal Link	A terminal or other user device can deny a USIM if USIM failed to provide a shared secret negotiated.
Security configurability		The security level can be configured by user.

The allocation of a TMSI is first initiated by the VLR, which generates the new TMSI randomly, and then both TMSI and LAI are sent to the user. After replacing the old TMSI with new one, the user sends a response to VLR. Hence the VLR can update the association between the user's IMSI and TMSI to its database. If the response is not received, both of the old and new association will be maintained. The whole process is encrypted by applying a key stream using a bit by bit XOR operation to the plaintext. The key stream is calculated by f8 algorithm from a time independent input, the bearer identity, the direction of transmission and the length of the key stream along with a 128-bit cipher key which is shared during UMTS AKA. Actually, UMTS AKA defines all the authentication procedures along with the cipher and integrity key. The strength of UMTS AKA has been analysed in [16] [17].

The data integrity is authenticated by f9 algorithm from a random value, the integrity sequence number, the direction bit, the signalling data and a 128-bit integrity key. While the user data is encrypted by f8 algorithm, the procedure is as the same as the encryption during identification message negotiation.

All the encryption algorithms used in UMTS are listed in Table 1.3.

Table 1.3 Encryption algorithms in UMTS.

Algorithm	**Description**
f0	Random challenge generation function
f1	Network authentication function to compute the message authentication code including authentication token
f2	Message authentication function to compute user response and expected response
f3	Cipher Key generating function
f4	Integrity Key generating function
f5	Anonymity Key generating function in normal procedures
f6	MAP encryption algorithm
f7	MAP integrity algorithm
f8	UMTS encryption algorithm
f9	UMTS integrity algorithm

Actually, f0 to f5 are the authentication algorithm which can be specified by the telecommunication operators. However, 3GPP does provide a set of algorithm called MILENAGE as a reference. The encryption and integrity algorithms in UMTS are all based on the Kasumi cipher, which is a block cipher with eight rounds of operation. The computational security of MILENAGE algorithm is analysed in [18], while the computational security of Kasumi algorithm is analysed in [19]. According to the evaluation, the computational strength of these algorithms is still efficient for security purpose.

1.3.3 Wireless local area network security

Today, more and more family and company choose wireless local area networks (WLANs) in a house or building for the flexibility it provides. This growing trend also raises the need for network security. Most of the current WLANs are originally based on IEEE 802.11 standard [20]. However, the basic security mechanisms in IEEE 802.11 standard have been proved to have large flaws and could be broken easily by skilful attackers. Therefore, a security enhanced version of the standard is developed called 802.11i [21]. The new standard not only improves the encryption and authentication procedures in original one, it also introduces the key management and Robust Security

Network (RSN) implementation. Along with the IEEE 802.1X standard as its authentication enhancement, 802.11i is supposed to be the security standard for novel WLAN setup. In this section, the core security improvements in IEEE 802.11i are introduced.

Generally, IEEE 802.11i standard defines two types of security framework for WLANs based on IEEE 802.11: RSN and pre-RSN, as shown in Table 1.4. The definition of the pre-RSN is basically a compatibility consideration on old firmware, and the definition of RSN contains all security improving aspects.

Table 1.4 Security framework of 802.11i.

<table>
<tr><td colspan="5">802.11i Security Framework</td></tr>
<tr><td colspan="3">RSN supported</td><td colspan="2">pre-RSN supported</td></tr>
<tr><td>Data Confidentiality</td><td>Authentication Enhancement</td><td>Key Management</td><td>Data Confidentiality</td><td>IEEE 802.11 entity authentication</td></tr>
<tr><td>TKIP</td><td rowspan="2">802.1X Authentication</td><td rowspan="2">802.1X Key Management</td><td rowspan="2">WEP</td><td>Open system authentication</td></tr>
<tr><td>CCMP</td><td>Shared key authentication</td></tr>
</table>

In order to enhance the data confidentiality, IEEE 802.11i introduces two types of encryption algorithms: Temporal Key Integrity Protocol (TKIP) and Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). TKIP can be viewed as an upgraded version of WEP, both of the algorithms are based on RC4 stream cipher. Although TKIP increased the length of Initialization Vector to 48-bit and the length of Secret Key to 128-bit, it has been later to be reported as “could be broken in one minute [22]”. While CCMP based on a stronger encryption Advanced Encryption Algorithm (AES) seems to be a long-term solution. Although several particular attacks against AES algorithms have been published [23-25], it is still provide a computational security with a enough length key.

802.11i replaces 802.1X as the authentication and key management solutions and the major improvements are based on 4-way handshake and group key handshake, as shown in Figure 1.6.

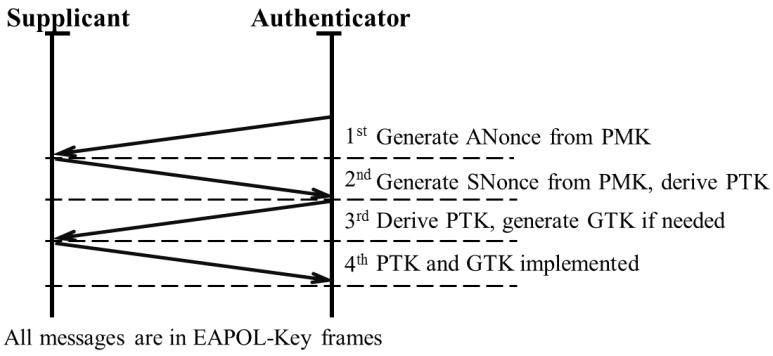


Figure 1.6 4-way handshake and group key handshake

In a 4-way handshake process, all the messages exchanged between the authenticator and the supplicant are in an Extensible Authentication Protocol (EAP) message format defined in IEEE 802.1X called EAP over LANs (EAPOL). The first message, which contains key information and a random value called key material (ANonce), is sent from the authenticator to the supplicant. Upon receiving the first message, the supplicant first checks the Replay Counter field of the message. Replay Counter is a sequence number which should be incremented by each message exchange. After successful validation on the Replay Counter, the supplicant generates a random value called SNonce, and derives a pairwise transient key (PTK) with SNonce, ANonce, a pairwise master key (PMK) and other information. Then the supplicant sends a message back to the authenticator containing: key information, SNonce, the supplicant's RSN information element (RSN IE) and the message integrity code (MIC). MIC is a cryptographic digest used to keep the integrity of the message. After the validation of the response message, the authenticator deploys the same algorithms and the same input value derives the same PTK and then sends the message including: key information, ANonce, MIC and the authenticator's RSN IE. After validating the message successfully, the supplicant sends the fourth message back to authenticator containing: key information and MIC. If the fourth message is validated by the authenticator, the four-way handshake is finished. And the PTK is used as the key to further encrypt the data. The group key handshake acts in a similar way to the 4-way handshake. And the group transient key (GTK) is sent to the supplicant for receiving broadcast messages.

Both GTK and MIC are encrypted by EAPOL-Key encryption key (KEK) and EAPOL-Key confirmation key (KCK) respectively. And both the KEK and KCK are part of the negotiated PTK.

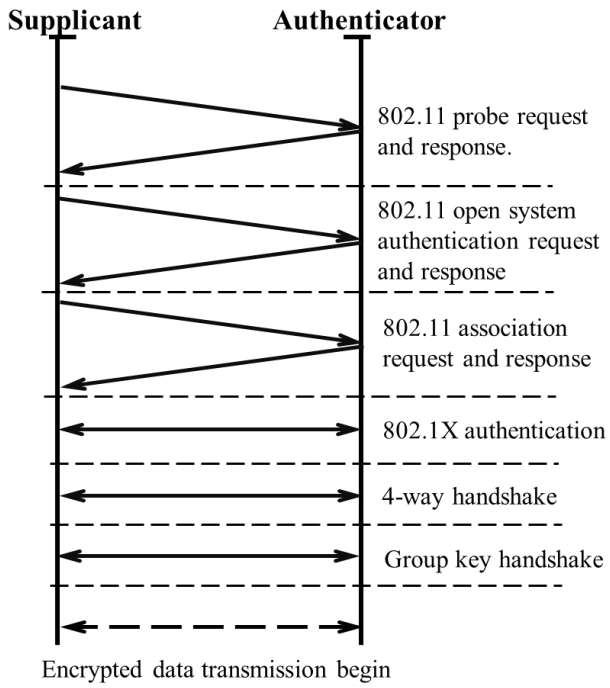


Figure 1.7 RSN establishment procedure.

The whole procedure of RSN establishment is shown in Figure 1.7. The connection session is first established following the original 802.11 association and authentication process. During the process, an RSN IE is used to distinguish pre-RSN connection and RSN connection. As shown in Table 1.5, RSN IE contains a list of authentication and cipher selector fields for connections. The value of the Element ID field should always be 48 in decimal. The Length field indicates the number of octets in the information fields excluding the Element ID and Length fields. The Version field shows the version number of the RSN protocol. The Pairwise Key Cipher Suite Count indicates the number of pairwise key cipher suites contained in the Pairwise Key Cipher Suite List field. The Pairwise field refers to two entities that are associated with each other. The Pairwise Key Cipher Suite, therefore is the cipher suite being or to be associated between communicating peers. Similarly, the Authentication and Key Management Suite Count indicates the number of authentication and key management suites contained in the Authentication and Key Management Suite List field. In the RSN Capabilities field, the requested or advertised capabilities are filled in. By using this

field, the receiver can know the security mechanisms the sender supports or is requesting.

Table 1.5 RSN information element format.

Element ID	Length	Version	Group Cipher Suite	Pairwise Cipher suite	Pairwise Cipher Suite List	AKM Suite Count	AKM Suite List	RSN Capabilities
1 octet	1 octet	2 octets	4 octets	2 octets	4m octets	2 octets	4n octets	2 octets

If the RSN IE is included, the 802.1X authentication is initiated. After successful authentication, both authenticator and supplicant generate a PMK independently. Then the PMK is used to derive and verify the PTK and GTK by 4-way handshake and group key handshake process respectively. And the PTK and GTK are used to encrypt point-to-point messages and broadcast messages respectively.

1.3.4 IPsec

Internet Protocol Security (IPsec) is a protocol suite to secure the IP based communications by applying authentication and encryption on each IP packet of a communication session. Since more and more wireless and wired network applications tend to be directly based on Internet layer, IPsec becomes an end-to-end security solution for a lot of applications, including 4G wireless network, interbank network, and VPNs.

IPsec can be implemented in two basic modes: tunnel and transport. In the tunnel mode, the entire IP packet is encrypted and encapsulated into a new IP packet with a new IP header. The mode is used to create VPN connection. In the transport mode, the header of original packet is preserved, only the payload together with a few header fields is encrypted. The mode is suitable for Encapsulating Security Payloads (ESP).

While the IPsec documents are too many, long and complex, the core functions are provided by: Authentication Headers (AH), ESP and Security Associations (SA). AH provides integrity protection, data origin authentication and the protection against replay attacks based on MAC algorithms. ESP provides similar services to AH along with confidentiality. SA provides solutions that protect the parameters required by AH/ESP operation, such as key management and identification.

The full definition of AH can be found in RFC 4302 [26]. By adding a bit sequence called Authentication Header to IP packet, AH provides integrity protection and authentication function. As shown in Figure 1.8, the Next Header field indicates the type of the payload following the AH. The Payload Len field indicates the length of the AH. The Reserved field must be set to “0” by the sender and is reserved for future use. SPI specifies the SA information related to inbound packet. The Sequence Number field contains a counter value that increases by one for each packet. And the ICV is computed from all the content which is supposed not to be changed during transmission. The algorithms used for authentication is defined in RFC 7321 [27], including the MAC algorithms based on SHA1 and AES.

<table>
<tr><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td colspan="8">Next Header</td><td colspan="8">Payload Len</td><td colspan="16">Reserved</td></tr>
<tr><td>32</td><td colspan="32">Security Parameters Index (SPI)</td></tr>
<tr><td>64</td><td colspan="32">Sequence Number</td></tr>
<tr><td>96</td><td colspan="32" rowspan="2">Integrity Check Value (ICV)
(variable length)</td></tr>
<tr><td>…</td></tr>
</table>

Figure 1.8 AH format.

The structure of ESP is declared in RFC 4303 [28]. The supported encryption algorithms are 128/192/256-bit AES-CBC [29], AES-CTR and 3DES-CBC. And the authentication algorithms are similar to AH authentication.

<table>
<tr><th>Bit</th><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>0</td><td colspan="32">Security Parameters Index (SPI)</td></tr>
<tr><td>32</td><td colspan="32">Sequence Number</td></tr>
<tr><td>64</td><td colspan="32" rowspan="3">Payload data</td></tr>
<tr><td>…</td></tr>
<tr><td>…</td></tr>
<tr><td>…</td><td colspan="32" rowspan="2">Padding (0-255 octets)</td></tr>
<tr><td>…</td></tr>
<tr><td>…</td><td colspan="16"></td><td colspan="8">Pad Length</td><td colspan="8">Next Header</td></tr>
<tr><td>…</td><td colspan="32" rowspan="2">Integrity Check Value (ICV)
…</td></tr>
<tr><td>…</td></tr>
</table>

Figure 1.9 Top-level format of an ESP packet.

Since IPsec only provides a security framework rather than a specific solution, the security of the systems based on IPsec really depends on the implementation.

1.4 Physical layer security

After taking a brief overview on the development of network security, it is easy to realize that the security issues are always driven by the awareness of the security flaws. As in the early days of the telecommunication network, the security issues of the network haven't draw enough concern for both the users and the system designers. Hence what we are trying to do now is more like to patch the system rather than to create something new. That is also the reason that the confidentiality enhancements are always made in the upper layer of networks.

Up to now, the physical layer of the networks is still the place where little security exists. Imagine that if there is a cost-effective measure to solve potential security threats at this fundamental level, it will make the things much easier for the end users and the services providers.

One may mix up the physical layer security (PLS) with the security of physical entities, such as the physical access to the media, router and server. In this thesis, these issues are categorised into environmental security and human behaviours, while the physical layer security we discussed is the information security based on the uncertainty principle in physics and the determination.

The first thing to do when we discuss the security of the physical layer is to introduce Shannon's information-theoretic notion of "perfect secrecy". The key point is that, unlike the security provided by the modern cryptography which based on mathematical problems, the physical layer security can rely on the physical uncertainties that are inherent during the transmission process, caused by noises, loss and gain, and most importantly, the different detection environments.

After the introduction to the information-theoretic security, the physical layer security techniques in wireless networks and optical networks are reviewed.

1.4.1 Shannon's information-theoretic secrecy theory

Consider the simplest transmission model in Figure 1.10, Alice (transmitter) wants to send a message X to Bob (legitimate user), and Eve (eavesdropper) can also access the message.

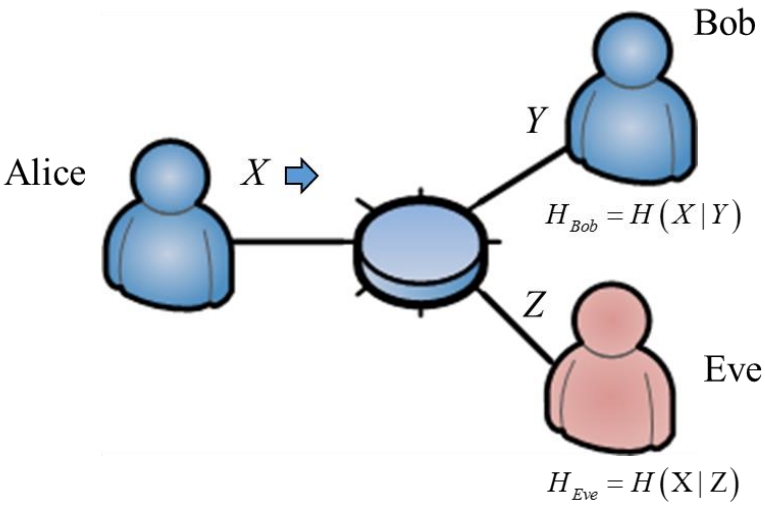


Figure 1.10 The simplest transmission model

The perfect secrecy can only be achieved when

$$H(X|Z) = H(X) \tag{1.1}$$

Equation (1.1) implies the observation of Z by Eve is statistically independent of transmitted message X. Although originally the equation was used to explain the Shannon's secrecy model, it leads to several definitions [109] we will use in later discussion: information entropy and mutual information.

Let X is the input ensemble of a noisy discrete channel, and Y is the ensemble of the output. The sample space of X and Y is $\{a_1,\ldots,a_k\}$ and $\{b_1,\ldots,b_j\}$ respectively. What we need is a quantitative measure of how much the occurrence of a particular case $y=b_j$ which can tell the possibility of the case $x=a_k$ has happened.

The definition of such a measure is derived from a priori probability $P_X(a_k)$ and a posteriori probability $P_{X|Y}(a_k|b_j)$ of X, which means the information provided about the event $x= ak$ by the occurrence of the event $y=bj$:

$$I_{X;Y}(a_k;b_j) \triangleq \log \frac{P_{X|Y}(a_k \mid b_j)}{P_X(a_k)} \tag{1.2}$$

The base of the logarithm in the definition determines the numerical scale used to measure information. The most common base is 2, which leads to the unit of information: bits.

It's easily to find

$$I_{X;Y}(a_k;b_j) = I_{Y;X}\left(b_j;a_k\right) \tag{1.3}$$

Hence $I_{X;Y}(a_k;b_j)$ is called *mutual information* between the events $x= a_k$ and $y=b_j$.

And the *self-information* of the event $x= a_k$ is:

$$I_X(a_k) \triangleq \log \frac{1}{P_X(a_k)} \tag{1.4}$$

It can be interpreted as the information required to resolve the uncertainty of event $x= ak$.

The *conditional self-information* of an event $x= a_k$ when the occurrence of $y=b_j$ is defined as:

$$I_{X|Y}(a_k \mid b_j) \triangleq \log \frac{1}{P_{X|Y}(a_k \mid b_j)} \tag{1.5}$$

It can be interpreted as the information that must be supplied to an observer to specify $x= a_k$ after the observer has observed the occurrence of $y=b_j$.

Hence, we have the relationship between mutual information, self-information and conditional self-information:

$$I_X(a_k) = I_{X;Y}(a_k;b_j) + I_{X|Y}(a_k \mid b_j) \tag{1.6}$$

Equation (1.6) stands for: Total Information of source = Information transmitted + Information needed to recover the source.

In fact, entropy is the statistic average of self-information, so we have

$$I(X;Y) = H(X) - H(X \mid Y) \tag{1.7}$$

where $H(X)$ is the *entropy* of X, defined as

$$H\left(X\right) \triangleq -\sum_{x \in X} p_X\left(x\right) \log p_X\left(x\right) \tag{1.8}$$

and $H(X|Y)$ is the *conditional entropy* of *X* given *Y*, defined as

$$H(X|Y) \triangleq -\sum_{x\in X}\sum_{y\in Y} p_{XY}(x,y)\log p_{X|Y}(x|y) \tag{1.9}$$

For a noise channel with given error probability, the average information lost can be estimated by Fano's inequality, which defined as follows:

Let $x \in X$ be a discrete random variable and let X' be the observation of *X*, and $p_e = P_{X'}\{x \neq x'\}$ is the probability of error obtained when estimating *X* with X'. Then

$$H(X|X') \leq H_b(p_e) + p_e \log(\|X\| - 1) \tag{1.10}$$

Where $H_b(p_e) \triangleq -p_e \log p_e - (1-p_e)\log(1-p_e)$ is the binary entropy function, and $\|X\|$ is the cardinality of ensemble X.

With the Fano's inequality, we can estimate the average information transmission rate of any channels with specific error probability. Thus with the model of wiretap channel introduced in Chapter 3, the information-theoretic security of a certain transmission scheme can be calculated.

1.4.2 PLS in wireless communications

It is fair to say that, due to the inherited broadcasting characteristics, the wireless communication is difficult to prevent adversaries from accessing transmitted signals. It is also the reason that the physical layer security draws more and more attention to compensate the situations.

According to the studies on information theory, perfect secrecy can be achieved using physical layer techniques in the condition that the channel of unauthorized users is more noisy that the authorized ones or the condition of the channels are unknown to unauthorized users [30]. Based on these two points, several techniques are developed to add built-in security features in wireless networks to aid the upper-layer security.

The major difference between the wireless physical layer security and the physical layer security in optical network is the channel state information (CSI). Due to the unstable environment of wireless networks, channel state information, which is used for

depicting known channel properties of a communication link, plays a critical role to achieve a reliable communication especially in multi-antenna systems.

Since the CSI contains the signal propagating characteristic from the transmitter to the receiver, which is unique and hardly to forge, it has been used to generate a “link fingerprint” for authentication purpose. An example is shown in [31], where the link fingerprint is used for the digital certificate generation. Another application is proposed in [32], where the coefficient of MIMO is used as the key only known to the transmitter and the receiver. It is difficult for the eavesdropper without corresponding coefficient to recover the effects of convolution on the mixed signals thus could not obtain a satisfying bit error rate (BER).

Although in as early as 1993, Maurer [33] expanded Wyner’s [30] conclusion about the wire-tap channel, and demonstrated a secret key agreement can be achieved as long as the received signals of the eavesdropper and the receiver are different, the techniques based on such theory are still under development. One of the successful examples is the spread spectrum technologies. It is first utilized in military applications, provides the transmitted signals the ability against jamming and unauthorized access, as well as the data confidentiality.

There are two major spread spectrum techniques: direct sequence spread (DSS) and frequency hopping (FH). DSS modulates the original signal with a pseudo-random bit sequence (PRBS) which is both known to transmitter and receiver. The modulated signal is noise like and could be recovered into original signal by applying the PRBS once again. Hence the good autocorrelation property of PRBS is required, and the synchronization on PRBS between transmitter and receiver is also important. Frequency hopping spread spectrum, instead of spreading the signal in time domain directly, spreads the signal by shifting it to different frequencies that are dictated by PRBS.

In practical application, spread spectrum techniques are used extensively in wireless networks both for the military and for the civilian applications, benefitting from the development of CDMA technologies. However, although the CDMA based mobile networks (3G) are performing well in security aspects, the “inherently less secure” mobile networks based on OFDM (4G) are commercialized on the increasing

demand of transmission capacity. For the absence of the physical layer security in 4G which is purely IP based, the security measures are mainly based on IPsec and Authentication and Key Agreement (AKA) protocol, both of which are applied in upper layers.

1.4.3 PLS in optical networks

The concept of the physical layer security in optical networks has just been formed very recently [34, 35]. However, the studies of the security issues in optical network have a longer history. Medard started the research on security issues in all optical networks in 1997 [36], and has continued her work on developing the information-theoretic security theory for optical network since then. And the studies on the related subjects are developed independently, such as the chaotic optical communication [37], the quantum cryptography [38], and the optical code division multiplexing techniques [39, 40].

Quantum cryptography uses quantum mechanical effects to achieve the security tasks. And the major application is the quantum key distribution. Since the quantum mechanics guarantees that measuring the data carried by quantum will disturb the data at the same time, any attempts on extracting the data from quantum exchange will be aware by comparing the detection result from the receiver to the original quantum status after quantum exchange. Thus, those quantum statuses that haven't been affected can be used for the secret key generation.

Chaotic optical encryption is based on the complexity of nonlinear dynamic behaviours of the optical laser. Since chaos is still a deterministic phenomenon, it is not as secure as the quantum cryptography. However, the difficulty on the chaos synchronization still provides a certain degree of information-theoretic security. To extract the data from a chaos carrier, precise synchronization is required. Even a minor difference between the transmitter and the receiver will result in poor BER performance. Therefore, the transmission imperfections induced by the optical medium have a great impact on overall performance. Another secure application of optical chaos is to generate the fast pseudo-random bit sequence by utilizing chaotic lasers. Kanter and his co-workers have demonstrated a true random number generator based on a chaotic

semiconductor laser [41], the single sequence rate can reach up to 12.5Gbps, which is much faster than the traditional physical electronic generators.

The concept of the optical code division multiplexing is firstly inherited from the spectrum spread techniques in wireless communication in 1980s [42, 43]. Afterwards, the techniques have been extensively explored in the optical communications, especially for its inherent security features [44-50]. However, as same as the optical chaos, the processes of optical encoding and decoding are also deterministic. As questioned in [51] by Shake, the security of the optical code multiplexing is not guaranteed. Later, several advanced code modulation schemes are proposed and demonstrated to solve the problem [52, 53]. However the limitation remains. By the merit of our proposed reconfigurable encoder and decoder, it is possible to design a robust secure system with the protection of dynamic optical code. Compared to the OCDM schemes which use relative static optical code, our scheme has the potentiality to utilize the optical code as the encryption key in the definition of cryptography, which can be any length, random chosen and easily to be reconfigured.

1.5 Objectives and outlines

After the review of the security issues in communication systems, it is clear that the physical layer security only takes a small fraction in today's security solutions which mainly relies on modern cryptography. However, due to its position in communication systems, it is still one of the most fundamental issues that can resolve the security problems once and for all.

With the development of the optical processing technologies, a lot of security schemes are proposed and claimed to be secure. Thus, there is a need to develop a standard mathematical tool to evaluate this physical layer security. Furthermore, since the security issue is a delicate and comprehensive problem, how to deploy the security techniques properly is also essential for the entire performance.

The objectives of the thesis are as follows:

To develop a standard mathematical tool derived from information theory which can be used to evaluate the information-theoretic security level of different optical layer security schemes.

To draft a security protocol that is compatible with our proposed reconfigurable optical coding device to provide full scope to optical layer security.

Following the introduction, Chapter 2 provides a review of the optical layer security approaches based on optical chaotic, quantum cryptography and optical coding techniques.

In Chapter 3, a simple and general method to evaluate the information-theoretic security level of optical coding schemes is introduced. Our proposed security scheme enabled by the reconfigurable optical coding device is also addressed and evaluated.

In Chapter 4, a security protocol based on the reconfigurable optical coding device is proposed, including the issue of distribution of optical code, mutual authentication, and the packet structures.

At last, a brief summary of the contributions of the presented works and suggestions for the future work are concluded in Chapter 5.

Chapter 2 Communication Security Approaches in the Optical Layer

Communication networks based on optical fibres, as the backbone of the Internet, are intuitively among the first communication infrastructures to embrace the physical-layer security. However, in the history of the development of the optical networks, the security consideration is mainly focused on the concept of "availability". Network management, optical monitoring and intrusion detection systems are the major concern to maintain the robustness of the networks, while the confidentiality of the data is usually guaranteed through the modern cryptography.

With the demands on the throughput of access networks increasing excessively, and the development of the optical signal processing technologies, the techniques which provide data confidentiality in real time in the optical layer are receiving more and more interest. Although compared to the wireless communications, optical fibres are difficult to be accessed by the potential attackers and there is only very little radiation leaked from the fibre, the unprotected data transmitted in it can be extracted quite easily by a sophisticated eavesdropper. Therefore, under the circumstances with high data confidentiality requirements, the security approaches realized in the optical layer become a crucial issue.

At the moment, there are several technologies as the candidates to secure the data in the optical layer, including optical chaos, quantum key distribution, and optical coding techniques. In this chapter, a brief overview of these techniques is introduced, with the comparison of advantages and the challenges of each technique.

2.1 Optical Chaos

Most devices in the current digital communication systems are essentially linear, especially for those electronic devices, and the performance of which follows the linear system theory. However, taking advantages of the intrinsic nonlinearity of optical devices, it is possible to achieve signal modulation, dispersion compensation, amplification, noise suppression and so on in the optical layer. One of the applications developed especially for security purpose is optical chaos. For such applications, the transmitter and the receiver are linked by a channel based on the synchronization of chaos, thus the performance of the transmission relies on the accuracy and robustness of

the chaos synchronization. In this section, we category these techniques into two major classes by function: data modulation and pseudo random sequence generation.

2.1.1 Data modulation based on nonlinear dynamics

There are several optical encryption methods proposed and demonstrated which utilize chaos related modulations: chaos shift keying, chaos masking, chaos modulation, and so on.

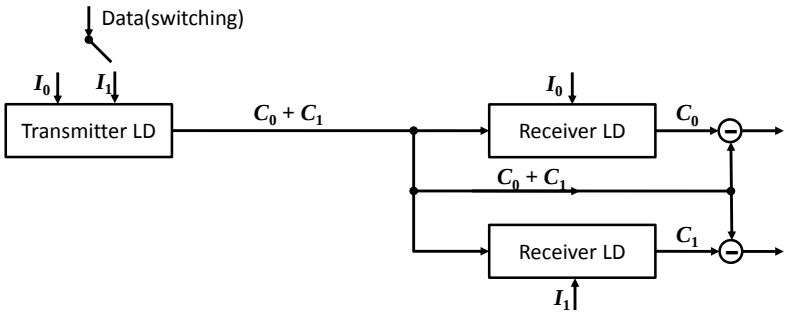


Figure 2.1 Schematic diagram of chaos shift keying [54].

Chaos shift keying is implemented by encoding the data through direct current modulation of the transmitter, as shown in Figure 2.1. I_0 and I_1 are injection current corresponding to data “0” and “1” respectively. C_0 and C_1 are chaos pattern generated from I_0 and I_1 respectively. The basic idea of the scheme is modulating the data with different chaos patterns. The receiver consists of two lasers driven by the selected parameters corresponding to transmitter’s “0” and “1” value (I_0 and I_1) independently. Decoding of the data is done by subtracting the output of the receiver from the signal received. In this situation, true chaos synchronization is infeasible since the transmitter is current-modulated with the data while the receiver is not. The chaotic state of the transmitter is determined by the data.

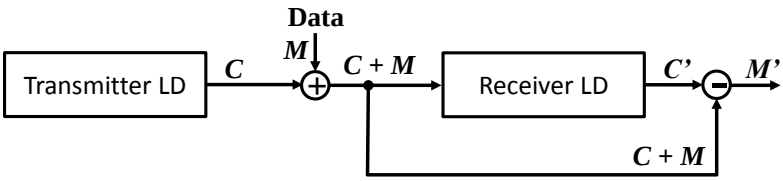


Figure 2.2 Schematic diagram of chaos masking [55].

The data modulation in chaos masking scheme is achieved by directly adding the data to the chaotic waveform, as shown in Figure 2.2. The demodulation operation is same as chaos shift keying, subtracting the output of the receiver from the received signal. In this case, the data is only injected to the receiver and is extracted from transmitted signal by subtracting a synchronized chaotic signal *C'*. However, it has not been mathematically proven whether the synchronized signal (*C'*) can be identically reproduced from the transmitted signal (*C*+*M*). As the result, the true synchronization is infeasible. Nevertheless, the chaotic state of the transmitter is not influenced by the data.

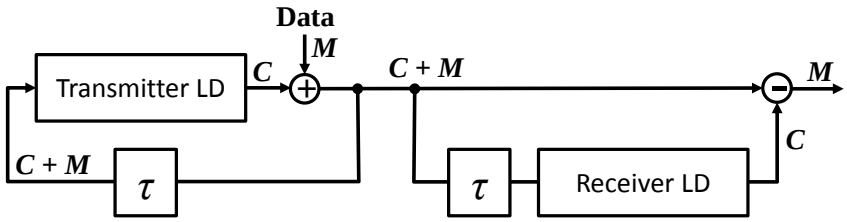


Figure 2.3 Schematic diagram of chaos modulation [56].

In the additive chaos modulation, the data is also added to the chaotic output of the transmitter. Meanwhile, the information about the data is sent both to the transmitter and the receiver so that the true synchronization is achievable. And the chaotic state of transmitter, as well as the complexity of chaos, is related with the data.

A general feature of communication based on optical chaos is that the recovered data is affected by the channel noise along with the synchronization error. Figure 2.4 shows the decoded waveform of the three different schemes. As we can see, data recovery is quite difficult to achieve in chaos shift keying scheme because the encoded signal has frequent desynchronized bursts. The performance is affected by the resynchronization time. According to the report [57, 58], resynchronization is hard to achieve when bit rate is over 10Gb/s. The performance gets better when the bit duration gets longer than the resynchronization time. In 2005, Argyris with his team demonstrated a chaos-based communication system on commercial fibre links [59] and the result is perfectly accordance with the theory analysis. The performance of the system is degraded significantly when the bit duration is approaching synchronization time.

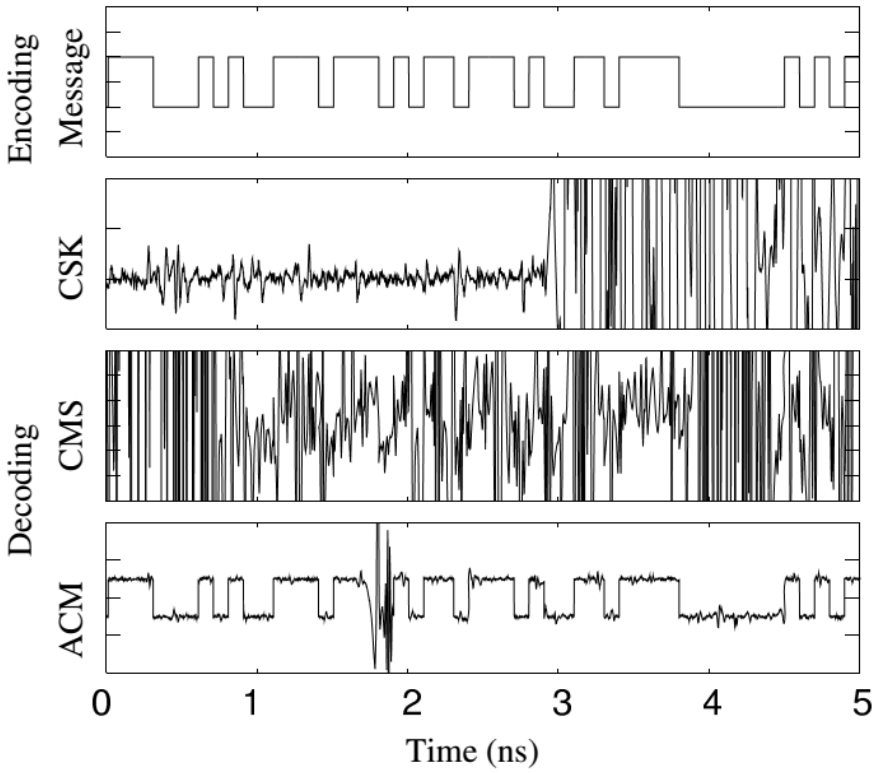


Figure 2.4 Decoded signals of chaos shift keying (CSK), chaos masking (CMS) and additive chaos modulation (ACM) [60].

In the case of chaos masking scheme, the synchronization error is mainly caused by the difference between the transmitter and the receiver. The influence of the data is weak comparing to the encoded signal, which is domiated by the chaos synchronization. The performance can be improved by deploying a low-pass filter to eliminate the interference from the chaos synchronization.

The performance of additive chaos modulation is greatly improved compared to the previous schemes since the true synchronization can be achieved. As the result, the synchronization noise is minimized, and the channel noise as well as the transmitter noise will be the main noise source. Since both the chaos shift keying scheme and the chaos masking scheme could not achieve true synchronization, the decoding waveforms are apparently noise like for a NRZ signal. In the example of the chaos shift keying scheme, it is quite easy to distinguish the two chaos patterns by observing the amplitude difference. Only the additive chaos modulation scheme which is truely synchronized can recover a good waveform. Still, the occurrence of the desynchronization bursts occurs will degrade the performance significantly, as the example shown in Figure 2.4.

The system performances measured by BER of these schemes are compared in Figure 2.5. The importance of the true chaos synchronization is revealed.

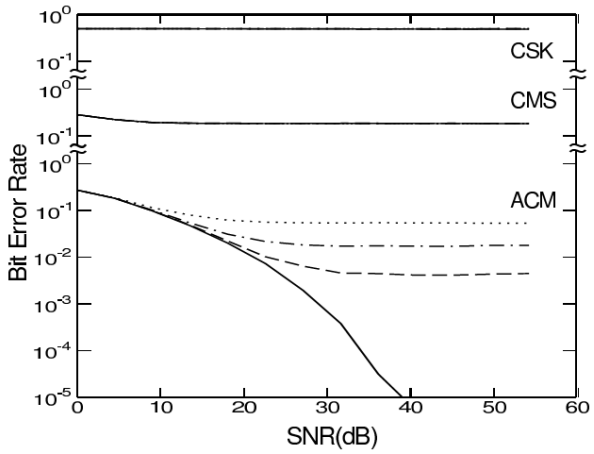


Figure 2.5. Performance comparisons of chaos shift keying (CSK), chaos masking (CMS) and additive chaos modulation (ACM) [60].

As a candidate in the optical layer for secure communication, although the optical chaos schemes have the comparable performance to traditional systems, they are too sensitive to the dispersion, distortion, nonlinear signal processing and noise. Besides, for any chaotic communication systems, the synchronization between the transmitter and the receiver is critical. It requires a good symmetry between the transmitter and the receiver to maintain high quality synchronization. Despite of these obstacles which prevent the optical chaos from commercial utilization, chaos-based secure communication scheme do have their advantages over the traditional encryption schemes. Optical chaos based schemes can be performed over continuous number fields. Both the chaos signal and data signal can be continuous signal rather than discrete digitized data. The encoded signal is noise-like and spectrum spread, which makes it difficult to perform a matched detection. Although the speed of optical chaos based scheme is limited by the time of synchronization, the coding process can still be implemented in all optical domain with high-speed analog signals.

The optical chaos based secure communication systems do have their weakness. It’s possible to break a chaos based system without searching for the secret key, as long as the encoded signals show low-order statistical characteristics corresponding to the data transmitted. In particular, transmission of binary data is risky, since even for the high-dimensional nonlinear dynamics, the transmitted signal pattern may be considered to reveal some information related data [61]. If the type of nonlinear dynamics is known

to the attacker, it is possible for him to use generalized synchronization to decode the data. In [62], an optical chaos based scheme on Chua's circuit is compromised by using generalized synchronization. The data is leaked from the variations in the synchronization error. In [63], an attack approach is proposed to break the optical chaos based system by reconstruct the secret chaotic dynamics completely without any knowledge about the type of the nonlinear dynamic. In this scheme, the attacker is using time delay to reconstruct the nonlinear dynamics part by part.

In summary, the security of a communication system is not only related to the data confidentiality, the availability of the system is also need to be considered and more important it is the first issue we should guarantee. It is still a long way to go for the chaotic secure communication before we mastered the chaos synchronization in optical layer and make it more feasible for practical application. After all, the security issues are highly bound to the practical implementation, and need time to evolve to prevent the attacks from every aspect.

2.1.2 Pseudo-random sequence generation from chaotic laser

Random number sequence generation is another promising application of chaotic lasers. The output of chaotic lasers naturally provides a fast temporal dynamic chaos pattern with a large spectral bandwidth. Unlike the traditional time multiplexed ultra-high speed sequence generation, the speed of chaotic laser is determined by the relaxation oscillation frequency, which can be over 20 GHz. With the proper setting, the rate of random bit sequences generation could reach up to the 480 Gbps [64].

The concept of random number generation of chaotic lasers is plain and simple. The output signals of a chaotic laser are detected by a photodetector and converted to a binary digital signal directly by an analog-to-digital converter (ADC). The ADC converts the analog signals into binary digital signals by comparing the amplitude with a threshold voltage. An example of random bit sequence generation from chaotic laser is shown in Figure 2.6, the output signals of two chaotic lasers are sampled (dots show sample point) and detected by certain threshold (black horizontal line). The outcome random bit sequence is obtained from the two detected sequences by the XOR operation.

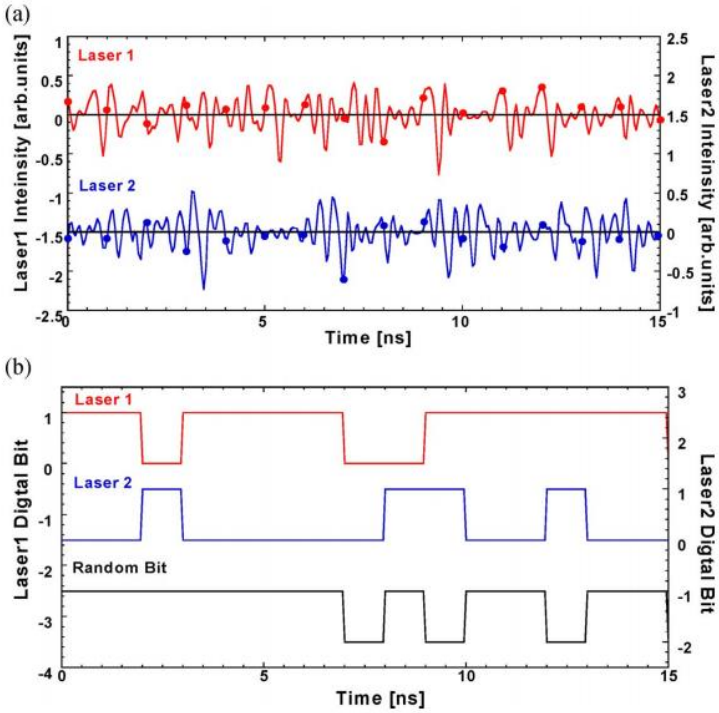


Figure 2.6 Concept of random number generation with chaotic lasers [65].

2.2 Quantum Key Distribution

In quantum physics, the unit of quantum information is the qubit. In a classical system, a bit would have to be in one state or the other. However, the qubit could be in a superposition of both states at the same time. Hence it is possible to encode one bit into a qubit. The two states in which a qubit may be measured are known as basis states. As a consequence, there would be different results when the sequence of qubits is measured by different basis combination. This basic quantum mechanism makes the quantum information system quite different from classical system.

Another interesting phenomenon in quantum physics is quantum entanglement, which occurs when pairs of particles are generated in a way that the quantum state of each particle cannot be described independently. Similar to the quantum states of individual particles, the state of an entangled system could also be expressed as a superposition of basis states. The action of measurement would break the entanglement. Therefore, the entangled system could also be used for transmitting information one time only, making it possible for security utilization.

In this section, the fundamental QKD protocols based on single-photon and quantum entanglement are introduced, along with the challenges for related practical applications.

2.2.1 Security in No-Cloning Theorem

The no-cloning theorem was first proposed by Wooters and Zurek [66] in 1982, it states a fundamental fact that it is impossible to create identical copies of an arbitrary unknown quantum state. Based on this theorem, the first QKD protocol was proposed in 1984 by Bennett and Brassard, known as BB84 protocol. Originally, the protocol depicts the quantum system transmitting information by photon polarization states, however, any two non-orthogonal states can be used for the protocol including phase, polarization and so on.

In BB84, two pairs of quantum states are used for information transmission, with each states-pair conjugate to the other, and the two states within a states-pair are orthogonal to each other. These pairs of orthogonal states are known as the basis. An example of key exchange in BB84 is shown in Figure 2.7.

Alice generates a random sequence of photons, whose polarization states depend on randomly selecting one of her basis. Hence the data is represented by four different polarization states. When these four polarization states are not all orthogonal, it's impossible to distinguish all of them and the only possible measurement is between any two orthogonal states. For example, if we measure the quantum states in "+" basis, the result can only be "→" or "↑", thus if the information is transmitted in "×" basis, all the information about its initial polarization state will be lost.

Since Bob does not know the basis of the photons chosen by Alice, all he could do is to select a random basis to measure each photon. After the measurement, Alice and Bob exchange their basis to each other over a public channel, thus both of them can discard the photon where Bob used a different basis, and the rest of the bits can be used as a shared key. If Eve without Alice's basis has gained any information from transmitted photons, errors will be introduced in Bob's measurements. Therefore, as long as Alice and Bob compare their shared bits, they will aware the existence of Eve when a difference is found.

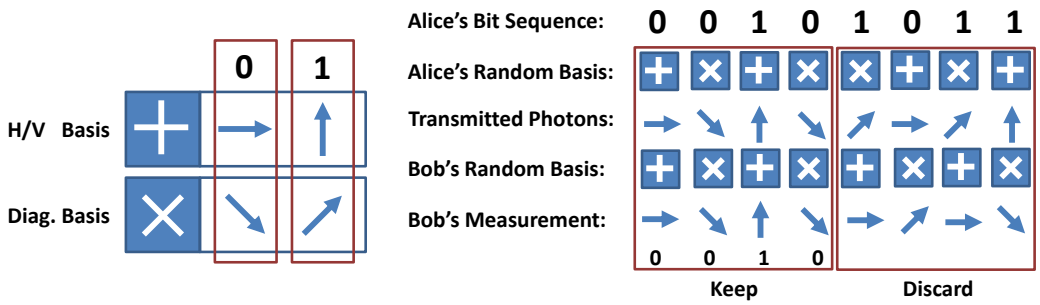


Figure 2.7 An example of QKD in BB84.

2.2.2 Security in Entanglement

The foundation for entanglement based quantum cryptography is involves the Einstein-Podolsky-Rosen paradox [67]. And the most famous protocol based on the theory is proposed by Ekert in 1991 [68], known as E91 protocol. The protocol uses entangled pairs of photons to achieve information exchange. The entangled photon pairs can be created by anyone including Eve. The photons are distributed to Alice and Bob, each of them own one photon from each pair. An experimental system based on the protocol is established in 2007 [69].

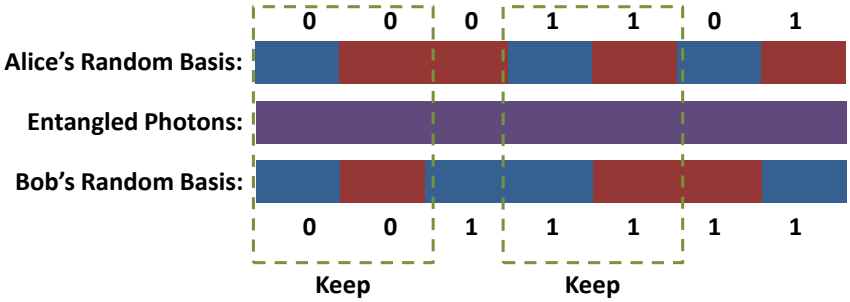


Figure 2.8 An example of QKD in E91.

Consider a source emitting two qubits in the entangled state, and one of them is sent to Alice while the other is sent to Bob. Alice and Bob can measure received qubits on any random basis independently. After the measurement, Alice and Bob exchange their basis on a public channel, hence they can discard the bits measured by different basis and the bits left can be used as a shared key, as shown in Figure 2.8. Although even Eve can be the one who generate the entangled qubits, the information contained in entangled photons is uncertain before the measurement. Suppose Eve prepares several pairs of photons by a certain basis, while Alice and Bob use random basis to measure them independently. They have 50% chance to measure the qubits with same

basis, and only half of the values can be predicted by Eve. However, the action results in 25% of errors when Alice and Bob test for entanglement by comparing their measurement in public channel, which is the same as the percentage of information Eve can predict. Hence the more information Eve has about the key, the more errors she creates.

2.2.3 Security in Quantum Fluctuation

A stream cipher protocol compatible to WDM transmission system is proposed by Yuen in 2000, known as Y-00 [70]. The protocol is based on quantum fluctuation of light. An example is shown in Figure 2.9.

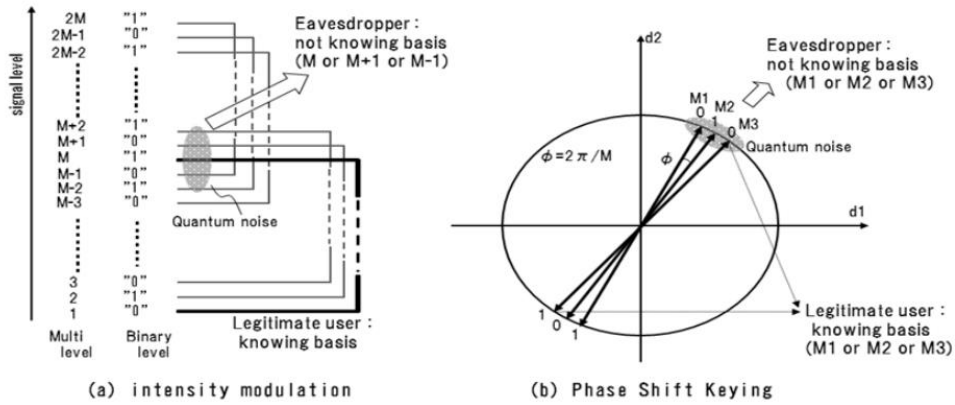


Figure 2.9 An example of QKD in Y-00 [71]

In this scheme, the information is modulated in multi-level phase or amplitude value. And the multi-value phase or amplitude information is arranged as closely as possible to achieve an overlapping in the range of quantum fluctuation. Thus only the receiver with corresponding multi-value modulation information can generate an optimized threshold to distinguish the value of “1” and “0”. The detection result of the eavesdropper is significantly interfered by the quantum noise.

2.2.4 Challenge from Practicality

Up to now, the information exchange relied on quantum mechanism is still the only way to achieve the theoretical unconditional security. However, although the quantum mechanism appears to provide an effective way to achieve unconditional security, it is still difficult to prove the information theoretic security level for a certain QKD system as stated in [72, 73], the author of which has proposed the Y-00 protocol.

In spite of this fundamental difficulty on the argument of "how secure the QKD system could be?" The quantum cryptography is still haunted by a several practical problem [74, 75]:

Difficulties in generation of pure single-photon pulses

The status of the laser used for single photon generation is not stable, by the fact that the number of photons in the pulse is random, with a Poisson distribution. Theoretically, only the pulses with one photon are secured since the extra photon may leak the information to the eavesdropper. Thus to provide the pulse required, the energy of signal is extremely small, which result in the reduction of the SNR of the system. Currently, only one out of ten attempts on single photon generation can be successful and we can't predict which attempt could succeed. Although a good single photon source seems feasible in technology, it still hasn't been achieved yet.

Response time of single-photon detection

At present, an InGaAs photon detector working at 1550 nm wavelength can detect photons in every 100 ns, thus limiting the bit rate of QKD system. The silicon detector working at ~800 nm wavelength is about 1000 times faster. However it is out of the range of current fibre communication system. Currently, the demonstrated QKD system working at 850 nm can achieve ~5 Mbps of data rate in the LAN area [76].

Incompatible with optical amplifier/optical signal processing devices

In traditional optical communication, optical pulses can be amplified by passive optical amplifier. Along with the suitable dispersion compensation, the long-haul transmission can be achieved. However things are getting changed when the signals go into the quantum world. The quantum channel not only requires the direct fibre link, but also no amplifier introduced. Thus it makes the environment of single-photon transmission extremely rigid. The facts also yield the development of QKD network, which is a costly solution to upgrade from the current fibre communication system.

2.3 Optical Coding Techniques

Optical coding techniques are originally enlightened by the spread spectrum (SS) techniques in military radio communication systems. However, due to the intrinsic differences between optical communication (digital) and radio communication (analog),

optical coding techniques are developed into an independent field. Generally, optical coding techniques can be used for multiplexing access, optical packet label switching, optical signal shaping and processing as well as the security purpose. In this section, two categories of optical coding techniques which are most promising for optical layer security are introduced.

2.3.1 Temporal Phase Coding

Temporal Phase Coding (TPC) is the technique to encode and decode optical signals by spreading the signals in time domain, the basic unit represents the code information is usually called chip, and each chip is phase encoded according to the optical code (OC). For the decoding, the encoded signal is processed similarly with the OC reversed to the encoding one. The principle of decoding can be explained by the aperiodic auto-correlation property [110] of the OC as:

$$C_{x,x}(k) = \sum_{n=k+1}^{N} x_n x_{n-k}^* = C_{x,x}(-k) \quad k=0, 1, \ldots, N\text{-}1 \tag{2.1}$$

where $C_{x,x}(\cdot)$ is the decoded output, k is the index of the time shift, N is the length of the OC, while x, x^* are the OC and OC reversed.

Although there are various devices to implement it, the basic model of TPC is equivalent to the structure with delay lines and phase shifts shown in Figure 2.10.

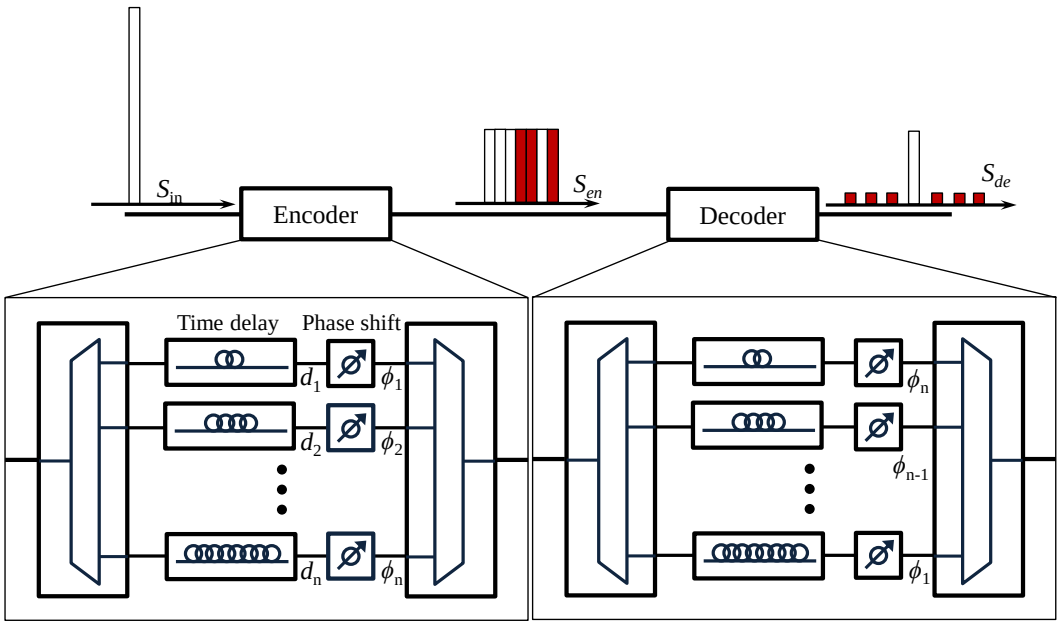


Figure 2.10 The schematic diagram of TPC encoding/decoding process.

Assume the complex electric field of input signal is [111]

$$S_{in}(t) = A(t)\exp(i\omega_c t), \tag{2.2}$$

where $A(t)$ is the complex field envelope and ω_c is the central frequency. And the OC $\mathbf{x} = (\phi_1, \phi_2, \cdots, \phi_N)$ is applied. Then the complex electric field of encoded signal can be modelled as the sum of N time spread chips

$$\begin{aligned} S_{en}(t) &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N} A(t - nt_c)\exp\left(i\omega_c (t - nt_c)\right) \cdot \exp(i\phi_n) \\ &= \frac{1}{\sqrt{N}} \sum_{n=1}^{N} S_{in}(t - nt_c) \cdot \exp(i\phi_n) \end{aligned}, \tag{2.3}$$

where N is the code length, t_c is the chip duration. Thus we can get the decoded signal:

$$S_{de}(t) = \frac{1}{\sqrt{N}} \sum_{m=1}^{N} S_{en}\left(t - (N - m)t\right) \cdot \exp(i\phi_m) \tag{2.4}$$

For the simplicity and without losing generality, we assume $S_{in}(t)$ has a rectangular pulse profile with unit energy and there is no in-phase noise. $A(t)$ and $\exp(i\omega_c t)$ can be safely neglected in this way. Then (2.4) is simplified to

$$S_{de}(t) = \frac{1}{N\sqrt{N}} \sum_{m=1}^{N} \sum_{n=1}^{N} \exp(i\phi_n)\exp(i\phi_m)\exp\left(i\omega_c \left(t - nt_c - (N - m)t_c\right)\right) \tag{2.5}$$

Hence the performance of TPC is strongly tied to the aperiodic correlation property of the OC. However, there is a major difference between time spread coding and aperiodic correlation property, as we can see from (2.5), the insertion loss of the decoder is increased proportional to the length of the OC. This fundamental structural limitation on the length of the OC has a negative effect on the information-theoretic security performance of the system, which will be discussed in detail in next chapter.

2.3.2 Spectral Phase Coding

Spectral Phase Coding (SPC) is the technique to encode and decode the OC directly on the spectrum of the signals. The principle is shown in Figure 2.11.

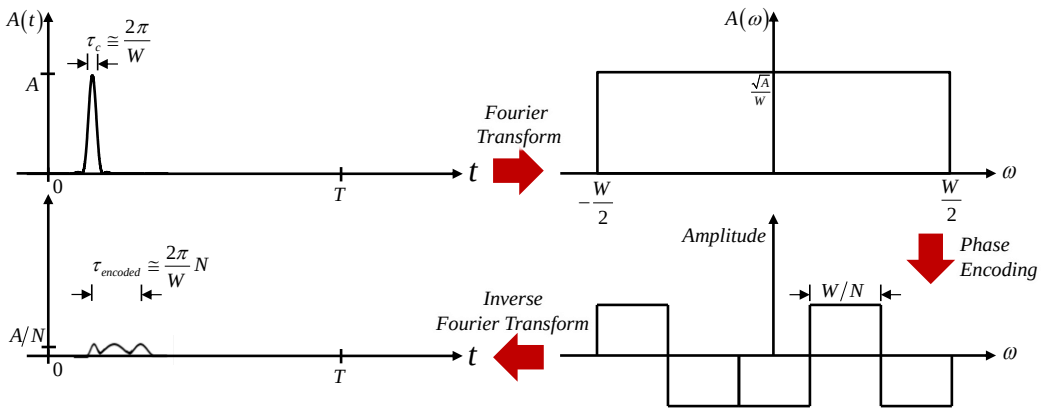


Figure 2.11 Basic principle of SPC encoding process.

To decode the encoded signals, we just need to apply a complementary phase shift according to the OC to recover the spectrum of the signals. Therefore, the OC could be any random sequence.

Assume the spectrum of the optical pulse is an ideal rectangle as shown in Figure 2.11, A is the peak power of the optical pulse and W is the total bandwidth, and thus the input signal can be modelled as:

$$S_{in}(t) = \sqrt{A}\,\mathrm{sinc}\left(\frac{W}{2}t\right) \tag{2.6}$$

where $\mathrm{sinc}(x) = \sin x / x$.

After the encoding, the spectrum of the signal is sliced into N chips, each of which is rectangle with the bandwidth $\Omega = W/N$. Thus for the OC $\mathbf{x} = (\phi_1, \phi_2, \cdots, \phi_N)$, the encoded signal can be modelled as the sum of N independent input signals corresponding to the rectangle spectrum with the width Ω,

$$S_{en}(t) = \frac{\sqrt{A}}{N}\mathrm{sinc}\left(\frac{\Omega}{2}t\right)\sum_{n=-\frac{N-1}{2}}^{\frac{N-1}{2}} \exp\left(-i\left(n\Omega t + \phi_n\right)\right) \tag{2.7}$$

Since each chip only has difference in phase, the average of encoded signal would be:

$$\left\langle S_{en}(t)\right\rangle = \frac{\sqrt{A}}{N}\mathrm{sinc}\left(\frac{\Omega}{2}t\right)\sum_{n=-\frac{N-1}{2}}^{\frac{N-1}{2}} \exp\left(-in\Omega t\right)\left\langle \exp\left(-i\phi_n\right)\right\rangle \tag{2.8}$$

In the schemes whose phase coding utilizing 0 or π for each chip, let the proportion of the "0" chip be α, the proportion of the "π" chip will be 1- α, and (2.8) can be simplified into:

$$\left\langle S_{en}(t)\right\rangle = (2\alpha-1)\frac{\sqrt{A}}{N}\operatorname{sinc}\left(\frac{\Omega}{2}t\right)\sum_{n=-\frac{N-1}{2}}^{\frac{N-1}{2}}\exp(-in\Omega t) \tag{2.9}$$

The peak value of the encoded signal occurs at time t=0, and the peak value of the intensity is:

$$\left\langle I(0)\right\rangle = A\left(\frac{1-(2\alpha-1)^2}{N}+(2\alpha-1)^2\right) \tag{2.10}$$

Thus when the OC utilized is balanced code, α=0.5, the energy is spread in the time duration $2\pi N/W$ evenly, and the average value is exactly equals to A/N. The fact indicates that although the OC utilized in SPC can be totally random, it's recommended to apply balanced code to hide the signal characteristic ultimately if we want to use SPC for security purposes. Further discussions will be given in next chapter.

2.4 Brief Summary

In this chapter, we introduced three classes of techniques which can be used for optical layer security application. Each of them covers a wide scope of researches and has a great impact on various fields. Due to the limitation of the space, only the basic principles of them are given with a few recent developments. A brief comparison of these techniques is given in Table 2.1.

Compared to the optical chaos and quantum cryptography, the solution with optical coding has the good compatibility to the current optical communication network, and is simple and easy to be implemented. The demonstrated applications based on optical coding techniques have already reached to ~40 Gbps for multiuser and over a few Tbps for backbone transmission [77, 79]. These practical and flexible benefits make the optical coding to be the most feasible candidate for providing security in the optical layer.

Table 2.1 Comparison between optical chaos, quantum cryptography and optical coding techniques.

	Chaos	Quantum	OC
Source carrier	Pulse	Photon	Pulse
Data Rate	~2.5Gbps [59]	~5Mbps [69]	>40Gbps [77]
Channel Requirement	Fibre – Tight Noise sensitive	Fibre/Free space – Harsh Quantum Channel	Fibre – Fair No Dispersion
Synchronization	Chaos Syn.	Delicate [78]	Asyn./Code Syn.
Security Criteria	Nonlinear dynamic	Quantum mechanics	Random Optical Code
Confidentiality	Dynamics [54]	Theoretically Perfect	Dynamics
Integrity	Fair	Fragile	Good
Availability	Fair	Fair	Good

Chapter 3 Security Performance Analysis for Optical Coding Techniques

In this chapter, we will discuss the security performance of the optical coding techniques from the following perspectives: code space against Brute-force attack, information-theoretic security against eavesdropping and the anti-jamming properties by adding artificial noise.

3.1 General wiretap channel

Consider the general model of wire-tap channel as shown in Figure 3.1, assuming that the eavesdropper could access the encoded signals as same as the authorized user, the information he can intercepted from the encoded signal can be denoted as $I(X;Z)$. And the information transmitted to the authorized user can be denoted as $I(X;Y)$, as indicated in section 1.5.1.

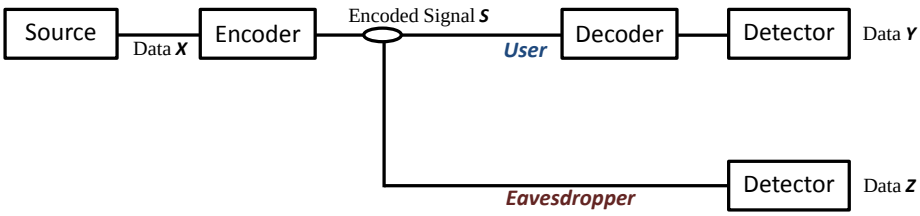


Figure 3.1 General wiretap channel for optical coding schemes.

According to Wyner's proof [30], when the channel input X, user's channel output Y, and eavesdropper's channel output Z satisfy the Markov chain X→Y→Z, then the perfect secrecy can be achieved and the secrecy capacity for the channel is defined as:

$$C_s = \max_X \left(I(X;Y) - I(X;Z) \right) \tag{3.1}$$

The result reveals one of the fundamental facts of the physical layer security that the secrecy is a relative concept which involves the difference of information transmission rate between the user and eavesdropper.

However, in the case of Figure 3.1, we could find that the user's output Y and the eavesdropper's output Z are determined independently by their own detection method. Instead of using the concept of secrecy capacity, we use the value $I(X;Z)/I(X;Y)$ to depict the ratio of the amount of information intercepted to the amount of information transmitted, denoted as α. Thus the value reflects the leakage level of the information under a certain physical environment.

$$\alpha = \frac{I(X;Z)}{I(X;Y)} \tag{3.2}$$

It's clear to see that, $\alpha = 0$ only if $I(X;Z) = 0$, which indicates the perfect secrecy is achieved, and the transmission capacity $I(X;Y)$ under the same condition is the secrecy capacity [30] for that specific physical setup. When $0 < I(X;Z) < I(X;Y)$, the eavesdropper can get partial information from encoded signals, however, the user can sacrifice the transmission rate to achieve the perfect secrecy by the information reconciliation and privacy amplification as depicted in [80]. When $I(X;Z) > I(X;Y)$, there is no information-theoretic security provided by optical coding process.

Assuming both the eavesdropper and the user can optimize their detection threshold, and the bit error rate for them are e_{ea} and e_u respectively, then α can be estimated by

$$\alpha = \frac{1+(1-e_{ea})\log_2(1-e_{ea})+e_{ea}\log_2 e_{ea}}{1+(1-e_u)\log_2(1-e_u)+e_u\log_2 e_u} \tag{3.3}$$

3.2 Temporal Phase Coding

3.2.1 Code Space Limitation

The maximum length of a temporal phase code is restricted by the pulse width t_p and the data transmission rate R:

$$L \le \frac{1}{R \cdot t_p} = \frac{t_b}{t_p} \tag{3.4}$$

where t_b is the bit duration.

Meanwhile, the code space of code-sets used in temporal phase coding is $\sim L$. Although the code space can be enlarged by applying poly-phase and multi-level code-set, there is no efficient way to construct such kind of codeset. Therefore, the code length is inverse proportional to the data rate. Assume the pulse width is ~20 fs, the code space is limited by data rate as shown in Figure 3.2.

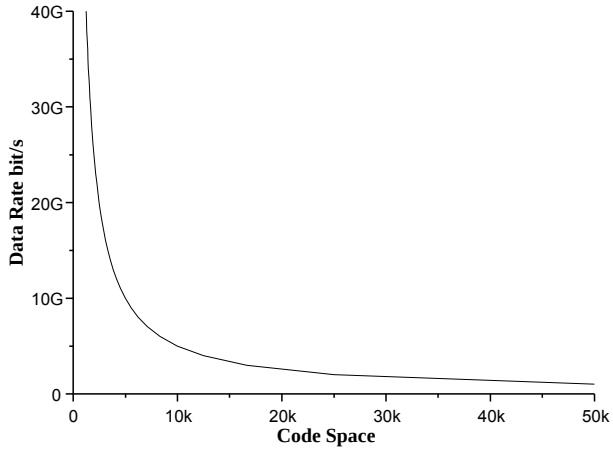


Figure 3.2 Code space limitation of temporal phase coding (t_p=20 fs).

If the time cost per code trial by the attacker approaches to the bit rate, the code can be cracked in a few seconds.

Another issue related to the Brute-force attack is that how many portions of code need to be correct before the eavesdropper can make a successful guess. In the most of the cases, the eavesdropper does not have to make every chip to be right to crack the system, which indicates that the actual searching space of the eavesdropper is smaller than the code space. Figure 3.3 shows an example of such partially decoding result when the length of the optical code is equal to 15.

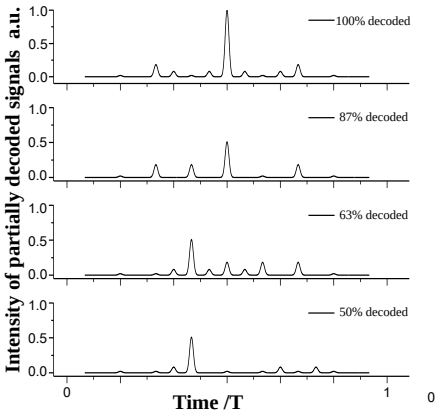


Figure 3.3 Partially decoding of TPC scheme.

In TPC scheme, each of the mismatched chips will reduce the autocorrelation peak power by ~2·*P*/*N* statistically, while the peak power of the side lobes is kept at a relative low level. *P* is the peak power of correct decoded signal, and *N* is the length of the optical code. Due to the large amount of side lobes exist, almost 50% of the bit energy is spread in the bit interval. Thus if the eavesdropper applies a proper optical thresholder to eliminate the interference from the autocorrelation wings, only over 60% correct chips are needed to observe a degraded autocorrelation peak for a temporal phase scheme with the length of the optical code equals to 511 with a chip-level detector.

3.2.2 Information-theoretic security

In this section, we consider three different modulation schemes as shown in Figure 3.4.

Modulation	Data	Code	Encoded Signal
OOK	0	N.A.	0 1
	1	C_1	
CSK	0	C_1	0 1
	1	C_2	
M-ary	000	C_1	000 ... 010
	...	...	
	111	C_8	

Code is dependent of data

Figure 3.4 Examples of different modulation formats of TPC schemes.

To optimize the performance of both the user and the eavesdropper, here we assume the user has an ideal optical thresholder which has infinite bandwidth and infinite output extinction ratio. Hence all the influence caused by side-lobes can be neglected including the cross-correlation peak. For the eavesdropper, we assume he can perform ideal chip level detection and 1-bit delay interferometer detection. However, the receiver noises are counted for both of them. Figure 3.5 shows the simplified model, where the rectangular temporal response function is used and the chip duration is assumed to be equal to the pulse width.

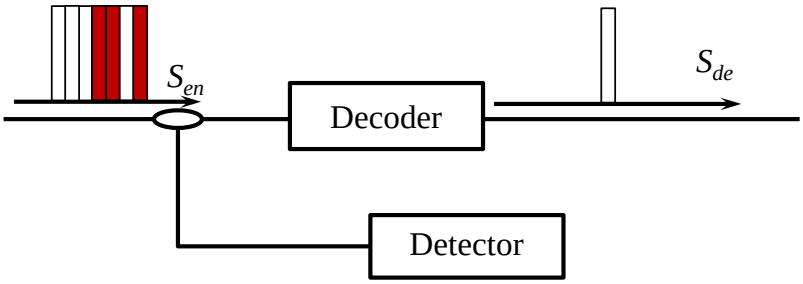


Figure 3.5 Eavesdropping structure of TPC schemes.

Assume the peak power of the encoded signal is $P_d = 1$, from equation (2.3) we have:

$$S_{en}(t) = \sum_{n=1}^{N} \exp\left(i\omega_c\left(t - nt_c\right)\right) \cdot \exp\left(i\phi_n\right) \tag{3.5}$$

Thus the decoded signal is

$$S_{de}(t) = \frac{1}{N}\sum_{m=1}^{N}\sum_{n=1}^{N} \exp\left(i\phi_n\right)\exp\left(i\phi_m\right)\exp\left(i\omega_c\left(t - nt_c - (N-m)t_c\right)\right) \tag{3.6}$$

The autocorrelation peak consists of contributions from all N chips of the encoded signals, while the n-th sidelobe from centre consists of contributions from N-n chips, which is suppressed completely by optical thresholder. Hence for the bit level receiver and chip level receiver, we have equation (3.7) for OOK modulation:

$$\begin{cases} P_{d-chip} = P_d = 1 \\ \sigma_{th}^2 = \dfrac{4k_B T B_{chip}}{R_L} = B_{chip} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{chip}\Re P_{d-chip} = 2eB_{chip}\Re \end{cases} \qquad \begin{cases} P_{d-bit} = P_d / N = \dfrac{1}{N} \\ \sigma_{th}^2 = B_{bit} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{bit}\Re P_{d-bit} = 2eB_{bit}\Re / N \end{cases} \tag{3.7}$$

where P_{d-chip} is the average power of received signal for chip-level detection, P_{d-bit} is the average power of received signal for bit-level detection, σ_{th} and σ_{sh} are the thermal and shot noise variances respectively. N_{th} is the thermal noise spectral density (typical value $N_{th} = 1pA^2 / Hz$ is used in the calculation), where k_B is Boltzman's constant, T is the absolute temperature, R_L is the load resistance, B_{chip} and B_{bit} are the receiver bandwidth corresponding to the chip-level detection and bit-level detection respectively. e is the elementary charge, $\Re$ is the responsivity of the photodetector.

Since the cross-correlation is assumed to be suppressed completely, the results of chip level detection for CSK and M-ary are the same, as well as the results of bit level detection.

Thus the error probabilities of the chip-level detection and bit-level detection for the user are:

$$\begin{cases} P_{e-chip}(1|0) = \dfrac{1}{2} erfc\left[\dfrac{P_{d-chip} D_{th}}{\sqrt{2}\sigma_{th}}\right] \\ P_{e-chip}(0|1) = \dfrac{1}{2} erfc\left[\dfrac{P_{d-chip}(1-D_{th})}{\sqrt{2\left(\sigma_{th}^2 + \sigma_{1-sh}^2\right)}}\right] \end{cases} \qquad \begin{cases} P_{e-bit}(1|0) = \dfrac{1}{2} erfc\left[\dfrac{P_{d-bit} D_{th}}{\sqrt{2}\sigma_{th}}\right] \\ P_{e-bit}(0|1) = \dfrac{1}{2} erfc\left[\dfrac{P_{d-bit}(1-D_{th})}{\sqrt{2\left(\sigma_{th}^2 + \sigma_{1-sh}^2\right)}}\right] \end{cases} \tag{3.8}$$

For the eavesdropper, we have equation (3.9) for OOK modulation:

$$\begin{cases} P_{d-chip} = P_d = 1 \\ \sigma_{th}^2 = \dfrac{4k_B T B_{chip}}{R_L} = B_{chip} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{chip}\Re P_{d-chip} = 2eB_{chip}\Re \end{cases} \qquad \begin{cases} P_{d-bit} = P_d = 1 \\ \sigma_{th}^2 = B_{bit} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{bit}\Re P_{d-bit} = 2eB_{bit}\Re \end{cases} \tag{3.9}$$

Since the average power of encoded signal for any optical code and any chip is equal to P_d, either the bit-level detection or the chip-level detection is not available for eavesdropper in CSK and M-ary modulation. However, the eavesdropper can apply 1-bit delay interferometer detection to recover the data. Assume the average distance for any pair of optical codes is d, we have equation (3.10) for CSK modulation:

$$\begin{cases} P_{d-chip-same} = P_d = 1 \\ \sigma_{th}^2 = \dfrac{4k_B T B_{chip}}{R_L} = B_{chip} N_{th} \\ \sigma_{diff-sh}^2 = 0 \\ \sigma_{same-sh}^2 = 2eB_{chip}\Re P_{d-chip} = 2eB_{chip}\Re \end{cases} \qquad \begin{cases} P_{d-bit-same} = P_d = 1 \\ P_{d-bit-diff} = P_d\left(N-d\right)/N \\ \sigma_{th}^2 = B_{bit} N_{th} \\ \sigma_{diff-sh}^2 = 2eB_{bit}\Re P_{d-bit-diff} = 2eB_{bit}\Re\left(N-d\right)/N \\ \sigma_{same-sh}^2 = 2eB_{bit}\Re P_{d-bit-same} = 2eB_{bit}\Re N \end{cases} \tag{3.10}$$

where the sub index $diff$ and $same$ indicates the situation when adjacent bits are same and different respectively.

The case for M-ary modulation is much more complex. Since the distance for any pair of optical codes is assumed to be same, the bit-level detection is not available for eavesdropper. It is possible that the information may be leaked by the position of phase difference for chip-level detection. For simplicity, we assume the eavesdropper can manage to locate the two phase differences corresponding to any pair of adjacent codes. Since the position of the phase differences are random, the eavesdropper needs to identify every chip correctly to reconstruct the M-ary modulation table. Hence the average error probability is

$$P_e = 1 - \left(1 - P_{e-diff}\right)^N \tag{3.11}$$

where P_{e-diff} is the error probability of a single chip difference.

3.3 Spectral Phase Coding

3.3.1 Code Space Limitation

The length of the spectral phase code is limited by the resolution of the spectrum chip, which is only a few hundred as reported [81].

$$L \le \frac{A_{T\times B}}{t_p \cdot \Omega} \tag{3.12}$$

where $A_{T\times B}$ is the time-bandwidth limitation of the optical pulse and Ω is the width of frequency chip. For a 40Gb/s system with ~20fs pulse and 10GHz chip width, the code length cannot exceed 220.

Although the code length of the spectral phase code is limited, the value of the chip can be set freely. From equation (2.10), we suggest that the binary code for spectral phase coding should be the balanced code. Thus for a given code length *N*, the maximum code space is

$$C = \binom{n}{\frac{n}{2}} \tag{3.13}$$

where $\binom{n}{k}$ is the number of *k*-combinations for a given set of *n* elements.

By applying Stirling's approximation $n! \approx \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$ to equation (3.14), we have

$$C = \sqrt{\frac{2}{\pi n}} \cdot 2^n \tag{3.14}$$

which is still quite a large number in the current physical environment. Thus the Brute-force attack seems inefficient against the spectral phase coding scheme.

Similar to the TPC scheme, the partial decoding of the SPC may also leak the information, as shown in Figure 3.6.

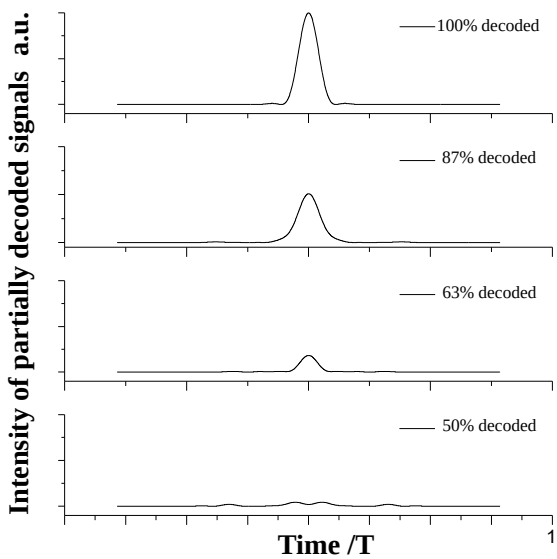


Figure 3.6 Example of partially decoding for SPC scheme.

In spectral phase OCDMA scheme, the peak power of the partially decoded signal is proportional to the percentage of chips recovered, as shown in Figure 3.7.

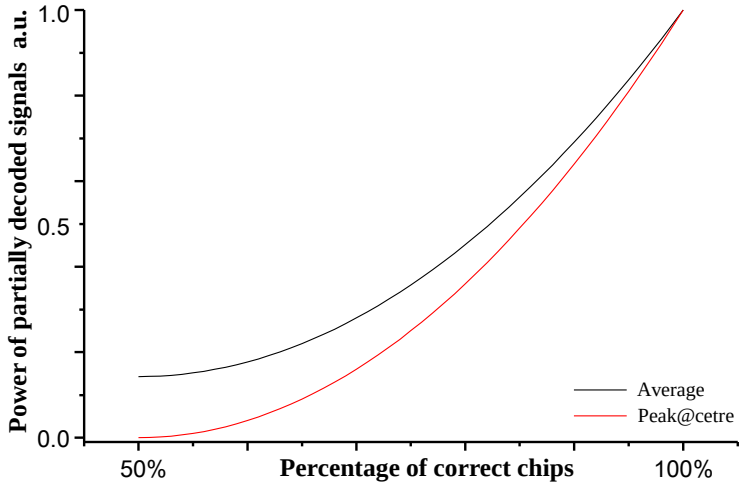


Figure 3.7 The power distribution of partially decoding in SPC.

The characteristic of partially decoding process in the SPC scheme is easier to be estimated with bit-level detector. And with about 70% of the chips are correct, the eavesdropper could obtain a degraded BER with a typical thresholder.

3.3.2 Information-theoretic Security

For the authorized user, the encoded signals can be recovered perfectly under the ideal numeric model as shown in Figure 2.11. However, for a code set with the length N, the average code distance between a pair of codes is $N/2$, thus the average beat noise induced by another code is

$$\begin{aligned}\langle I(0)\rangle &= A\left(\frac{1-(2\times 0.75-1)^2}{N}+(2\times 0.75-1)^2\right)\\ &= A\left(\frac{3+N}{4N}\right)\end{aligned} \tag{3.15}$$

Thus we have equation (3.16) for the authorized user in OOK modulation:

$$\begin{cases} P_{d-chip} = A = 1 \\ \sigma_{th}^2 = \dfrac{4k_B T B_{chip}}{R_L} = B_{chip} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{chip}\Re P_{d-chip} = 2eB_{chip}\Re \end{cases} \qquad \begin{cases} P_{d-bit} = A/N = \dfrac{1}{N} \\ \sigma_{th}^2 = B_{bit} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{bit}\Re P_{d-bit} = 2eB_{bit}\Re/N \end{cases} \tag{3.16}$$

And for CSK and M-ary Modulation, we have

$$\begin{cases} P_{d-auto} = A = 1 \\ P_{d-cross} = A\left(\dfrac{3+N}{4N}\right) \\ \sigma_{th}^2 = \dfrac{4k_B T B_{chip}}{R_L} = B_{chip} N_{th} \\ \sigma_{0-sh}^2 = 2eB_{chip}\Re P_{d-cross} = 2eB_{chip}\Re\left(\dfrac{3+N}{4N}\right) \\ \sigma_{1-sh}^2 = 2eB_{chip}\Re P_{d-auto} = 2eB_{chip}\Re \end{cases} \tag{3.17}$$

For the eavesdropper, the direct detection on balanced spectral phase code is not available in the ideal case. Instead, he can use a filter with the bandwidth equal to the chip width followed by a one bit delay interferometer to detect the OOK and CSK scheme. We have

$$\begin{cases} P_d = A/N = \dfrac{1}{N} \\ \sigma_{th}^2 = B_{chip} N_{th} \\ \sigma_{0-sh}^2 = 0 \\ \sigma_{1-sh}^2 = 2eB_{chip}\Re P_d = 2eB_{chip}\Re/N \end{cases} \tag{3.18}$$

Similar to the TPC scheme, to reconstruct M-ary modulation table in SPC also requires a fully recovery on chip information.

3.4 Reconfigurable Coding Device

According to the analysis in previous section, it is clearly that due to the inherent limitation of the phase encoding and decoding process, the guaranteed information-theoretic security couldn't be achieved with limited number of codes. However, for the

passive encoder and decoder, increase the number of codes supported by a single device means to increase the complexity of the system at both receiver end and the transmitter end, thus the cost for the entire system will be multiply increased. By developing from time domain spectral shaping (TDSS) techniques, our group proposed a reconfigurable coding device based on a dispersive device and a simple phase modulator. Compared to the spectral phase coding techniques introduced in the previous section, this time domain reconfigurable spectral phase coding device has several advantages especially for the secure utilization, as shown in Figure 3.8.

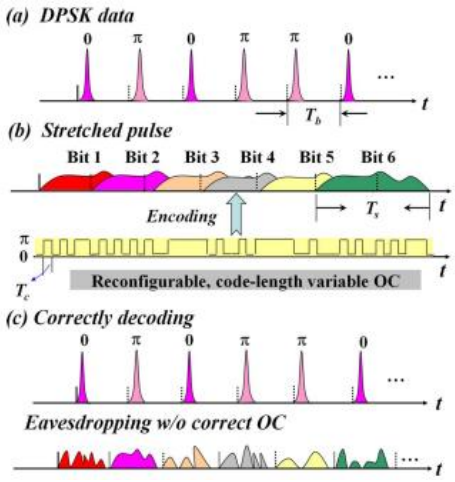
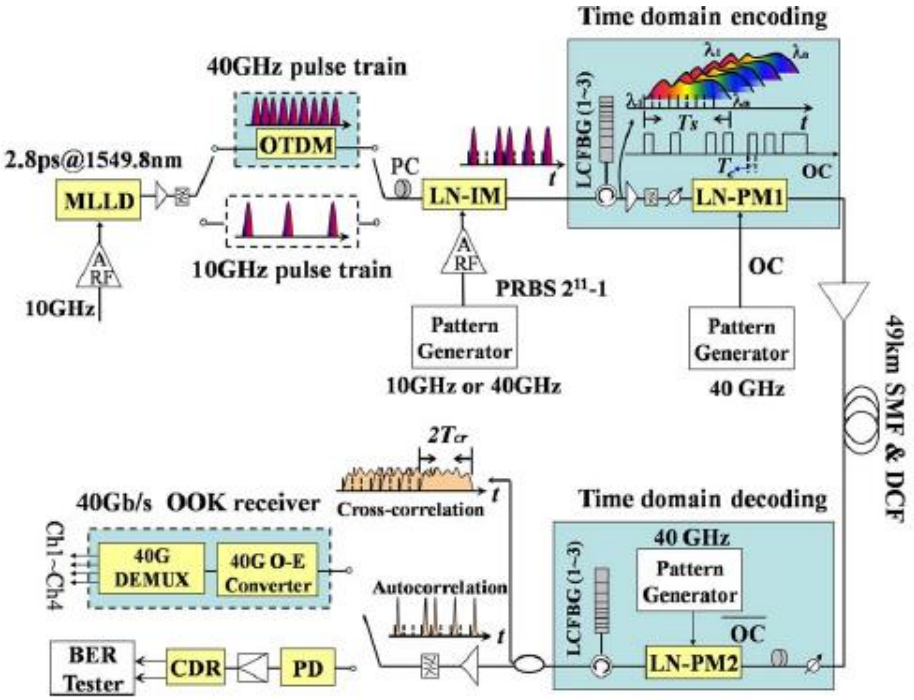


Figure 3.8 Principle of reconfigurable spectral phase coding device [82].

If the dispersion is sufficiently high, the dispersed temporal waveform is proportional to the pulse amplitude spectrum [83]. Since the individual frequency components will be distributed within the stretched envelop after the dispersion. Thus, either the amplitude or the phase of corresponding frequency components could be modulated independently without the use of optical filters. In our proposed scheme, the ultrashort pulse sequence is first modulated in the DPSK data format, and then the modulated signals are stretched by high dispersive device. The time duration of the stretched envelope T_s could exceed the bit duration. Therefore, the adjacent stretched pulses are temporally overlapped with each other. Then the overlapped signal is phase modulated by an ultra-long OC with the chip duration T_c lesser than the bit duration. In this way, each stretched pulse is encoded by a segment of OC with the effective code length T_s/T_c . Since adjacent stretched pulses are overlapped with each other, the effective code segment is iteratively applied on each stretched pulse. To decode the signals, a complementary OC is required with the code synchronization, followed by a reverse dispersion process to reconstruct the autocorrelation signal with high peak

power. If the eavesdropper doesn't know the entire OC sequences, it is impossible for him to extract the data from the noise like cross-correlation signals. Furthermore, due to the overlap of adjacent bits and the iterative use of the OC segment, the 1-bit delay interferometer is information-less. In our demonstration, the code reconfigurable rate can reach 40Gb/s, as shown in Figure 3.9. The laser source is an actively mode-locked laser diode (MLLD) producing nearly transform-limited 2.8 *ps* pulses at a repetition rate of 10 G*Hz* and spectrally centred at 1549.8 *nm*. The 40 G*Hz* pulse train is generated by multiplexing the 10 G*Hz* pulses using a four-stage planar lightwave-circuit-based optical time division multiplexer (OTDM). The pulse train is intensity modulated by a lithium-niobate intensity modulator (LN-IM) driven by a 40Gb/s pseudo-random bit sequence (PRBS). The sequence is generated from a pulse pattern generator and amplified by a radio frequency amplifier (ARF). After that, three identical cascaded linearly chirped fiber Bragg gratings (LCFBG) are used to significantly broaden the pulse train. Then, a 40 G*Hz* LN phase modulator (LN-PM) driven by a 40 Gchip/s, reconfigurable and code length variable pseudo-random OC generator to perform phase modulation on the stretched pulse. At the receiver side, similar configuration as the encoding part is utilized, but the phase modulator is driven by the complementary code patterns for spectral phase decoding.



recon

Figure 3.9 Experimental setup of the 40Gb/s secure optical communication system based on reconfigurable coding device. PC, polarization controller [84].

This scheme greatly extends the length of the OC with the ultimate flexibility on the code format. Since the optical code is active applying to the signals, unless the passive decoder, no more beat noise is induced. At the extreme situation, the length of the OC can be extended as same as the length of the signals, making the one-time pad achievable in optical layer.

For a signal encoded by a limited length (*N*) of OC, assume the length of encoded data is *M*, and the data rate is *R*, we have

$$T_c = M/NR \tag{3.19}$$

Thus effective code segment length *l* for one stretched pulse is

$$l = NRT_s/M \tag{3.20}$$

Then the average searching time for crack a single segment is

$$T_{trial} = 2^{NRT_s/M-1} \cdot T_s \tag{3.21}$$

From (3.21) we can see the duration of stretched pulse should be as large as possible to raise the average searching time for crack a single segment to the impractical range.

Assume the average probability for eavesdropper to crack a single segment is P_0, the probability for eavesdropper to crack a specific OC is

$$P_{crack} = P_o^{\frac{M}{RT_s}} \tag{3.22}$$

However, although the system has been demonstrated successfully for long-haul transmission, one of the most important issues hasn't been solved: the distribution of the ultra-long OC. In the next chapter, we will discuss the issue of OC distribution, along with the other aspects of the information security.

Chapter 4 Optical Code Security Protocol for Dynamic Optical Code Link Initiation

With the steep rise in growth of the optical communication network throughput, optical layer security has become quite promising for the ability to provide real time protection in ultrahigh data transmission. Various optical coding schemes enabling optical layer security have been proposed and demonstrated in different conditions and considerations [84-87], however, to the best of the author's knowledge, none of them consider protocol development. It is true that a trusted secure technique is important for the construction of a secured system, yet how to deploy it properly is also quite critical for system realization.

In this chapter, a primitive protocol of optical layer security based on optical coding techniques is presented. This is the first time a security protocol has been introduced for the reconfigurable optical coding techniques. The protocol encapsulates optical coding techniques into a feasible security module, and along with other security techniques, constitutes a brief model of an optical layer security solution.

4.1 Optical Code Security Protocol in Optical Communication System

The major motivation of Optical Code Security Protocol (OCSP) is to design a structure to enable optical layer security that is based on our proposed reconfigurable optical coding techniques. The protocol initiates a dynamic shared secret channel between the entities involved in the communication. This established dynamic shared secret channel, which is in accordance with specific optical code (OC), is called a secured OC link. From the security consideration, the OC information must be hidden completely from unauthorised users, inter nodes and malicious attackers. As a result, the design of a feasible security protocol to distribute the OC secretly is essential to fulfil the security requirement of the system.

To provide a full scale of network security, the protocol is designed to maintain the identity authentication, the data integrity checksum and the construction and the distribution of the dynamic OCs. Each security feature can be achieved by a separate module and operates together as long as the data is in the designed format. To maintain

the flexibility of the protocol, each security module is designed in similar structure and contains all the information that have to share between the entities involved in the communication. It should be noted that the proposed optical code security protocol is complete original. However, various open source algorithms are included as the supplements.

Before we consider the OCSP further, it is necessary to make a clarification about the terms we used, as shown in Table 4.1. A complete exchange always consists of a request and a response. The responder should only send a message when a request has been received. This strict rule is mainly for mutual authentication purposes. Thus after an OC link has been established, each entity can initiate the request for data transmission.

Table 4.1 Clarification of the terms.

Term	**Description**
Entity	The end involving the communication.
Message	The information sent from one entity to another.
Exchange	Consists of a pair of messages, a request and a response.
Requestor	The entity initiating the OC link. The message sent by the requestor is denoted with sub-index *q*.
Responder	The entity responds to the OC link request. The message sent by the responder is denoted with sub-index *s*.
Shared Secret	The information shared by the D-H key exchange, which is used for generating the key material.
Key Material	Generated from the shared secret and used for generating the OC and encryption keys.

In this section, two deployed scenarios are considered, and the necessary elements of OCSP are discussed.

4.1.1 Basic Point-to-Point Transmission

In this scenario, both entities involved in the communication are directly connected by an optical fibre, and there is no other form of O-E-O conversion needed during transmission. In other words, data transmitted can be hidden completely without causing

connection problems. Thus, all the messages can be encapsulated into OC link payloads, as shown in Figure 4.1. Once the OC link has been established in this scenario, a reliable channel is formed between two entities, to which the data transmitted is completely transparent. While the eavesdropper without the OC can neither extract the data nor modify them, the only ways he can interpose the communication is to crack the OC successfully in real time or to disable the OC link. Since the OC link is directly on the optical layer, the data in all kinds of formats is protected.

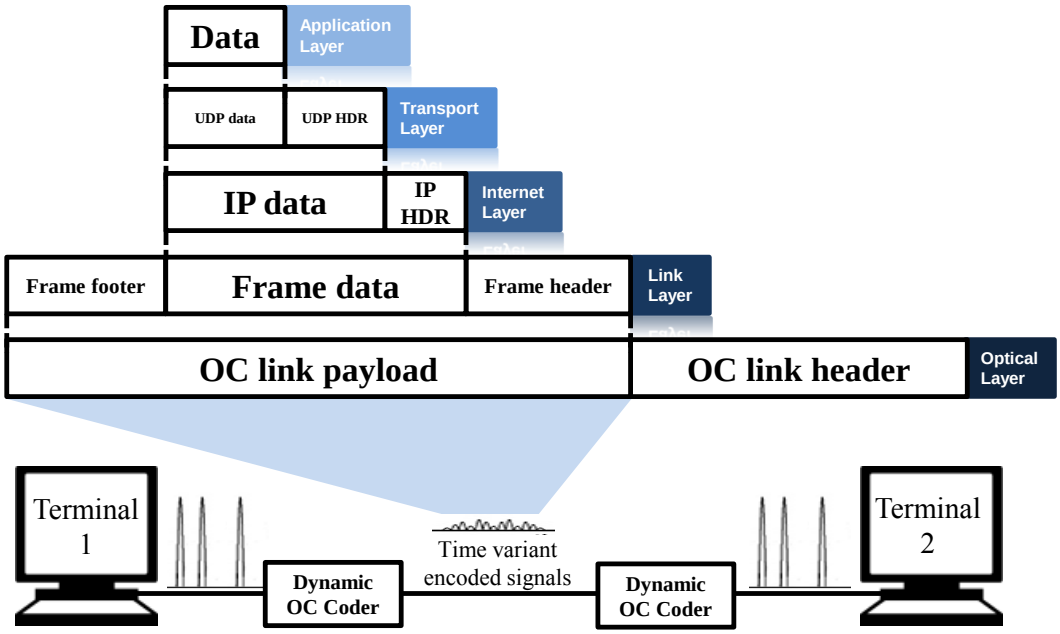


Figure 4.1 The position of the OC link in the TCP/IP network model for the point-to-point scenario.

The security of the OC link depends on the strength of the seed used for dynamic synchronized OC sequences generation. Also, the seed itself can be pre-shared between two entities by any secure method, including novel Quantum Key Distribution (QKD) protocol, traditional Diffie-Hellman (D-H) exchange and even a private offline exchange.

The schematic diagram of a basic back-to-back secure communication system enabled by OCSP is shown in Figure 4.2. Before the OC link establishment, the data is directly modulated onto the optical carrier, and the modulated signals are transmitted without protection. To establish an OC link, a D-H exchange is initiated on this public channel to generate a common shared secret between the transmitter and the receiver. Then the OC and the keys for other security purposes are generated by each peer

independently from the shared secret. After the D-H exchange, the data can first be protected by encryption algorithms and then encoded by OC. Thus, the energy of the optical pulse for each bit is spread into the entire bit interval according to the OC. At the receiver end, a complementary OC is used to decode the encoded signal to reconstruct the autocorrelation peak and recover the original data.

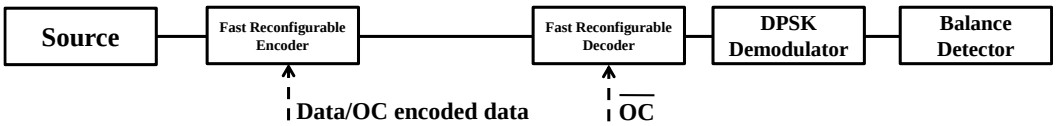


Figure 4.2 OCSP system schematic diagram.

4.1.2 Packet Switching Network

In this scenario both entities involved in the communication are in a scaled packet switching network, which can be any type of network supporting all optical transmission, such as Ethernet, TCP/IP network, and Multiprotocol Label Switching (MPLS) network etc. Other than encoding the entire data stream, the routing information, which is usually a header or label, needs to be accessible for the nodes in the packet switching network. As a result, only the payload can be encoded by OC, which leads to a mergence between OCSP and the packet switching protocol, as shown in Figure 4.3.

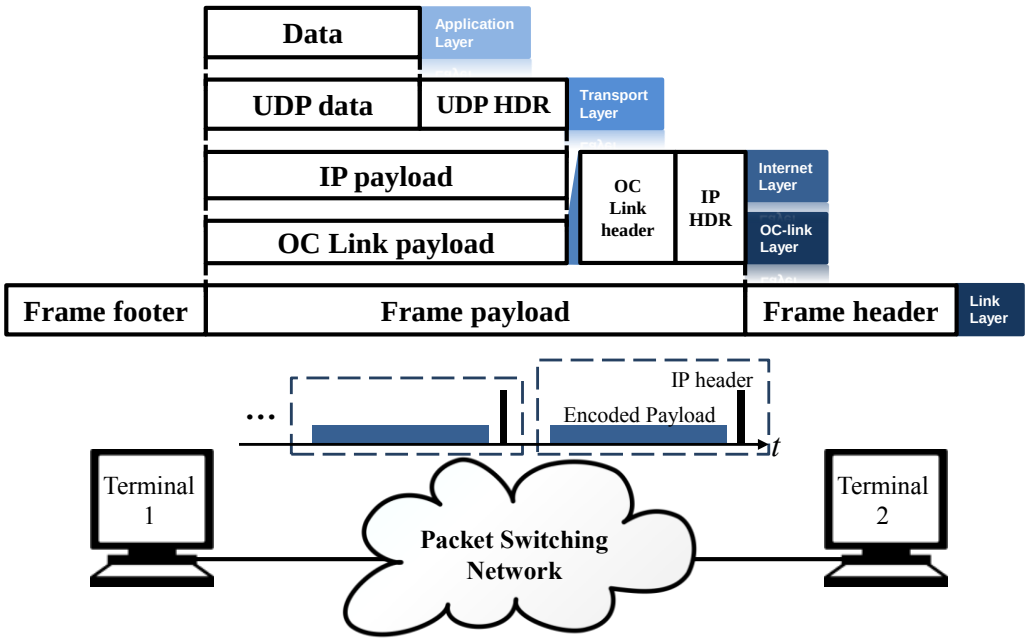


Figure 4.3 The position of the OC link in the packet switching (IP) network.

Apart from point-to-point transmission, where the OC link could be maintained all the time, the OC is deployed packet to packet in the packet switching network. Therefore, additional data exchange is required for OC link establishment. As a result, OCSP functions as part of the layer 2/layer 3 protocol, while providing a certain degree of optical layer security.

4.1.3 Discussion of Compatibility

Since our reconfigurable OC coder is based on coherent phase modulation techniques, the minimum requirement of OCSP is that the link must be phase insensitive and dispersion compensated. To be compatible with the packet switching network, it is necessary to insert an OC initiation header between the original header and the payload. As long as the OC initiation header is accessible, the OC encoded payload data is transparent to the upper layer services and applications for authorised users.

As analysed in previous sections, OC link mainly provides data confidentiality based on information-theoretic security along with a degree of integrity protection, Therefore, to achieve a comprehensive security level, additional security techniques must be included, especially for the authentication. The fact that dynamic OC synchronization requires a shared secret exchange makes OCSP quite extendible. The shared secret can be used to generate keys for authentication, integrity checking and even further encryption. In addition, this shared secret exchange happened before any upper layer applications, which indicates that OCSP has the potential to reduce the complexity of the upper layer security application procedure.

4.1.4 Modularity and General Procedure

It is a trend that a good security system should remain as simple as possible, as documented in the NIST's report on computer security [88]. On one hand, the more complex the mechanism, the more likely it is that it may contain exploitable flaws. On the other hand, the more complex the mechanism, the more likely it is that its security performance will be more difficult to evaluate, while the simpler mechanisms always require less maintenance and are easy to upgrade or replace. Therefore, in our proposed OCSP, we are trying to divide the entire security system into several less co-dependent

modules. Each module fulfils a specific security function and can be deployed on demand, leading to a vital security system with great flexibility and extensibility.

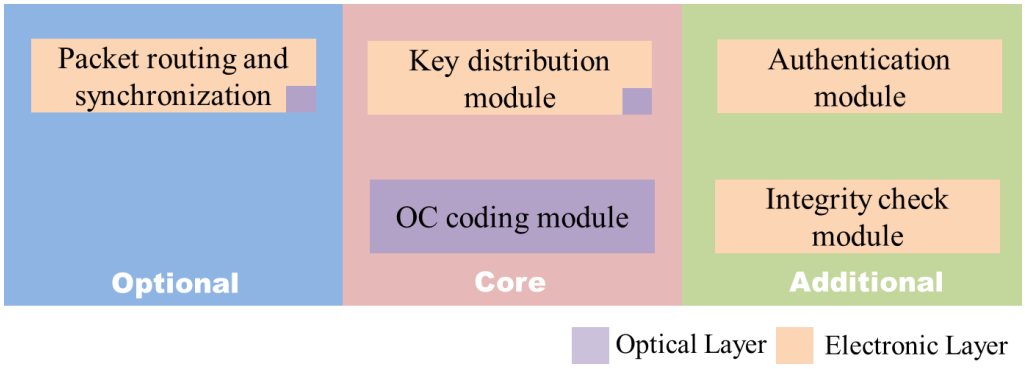


Figure 4.4 Functioning modules in OCSP

Figure 4.4 shows the major functioning modules in OCSP. The core module is the OC coding module which provides data confidentiality in the optical layer. Since maintaining this security feature requires a shared OC between the two entities of the communication, the key distribution module is also a must. Up to now, the most applied key distribution solutions are still based on computational complexity and processed in the electronic layer, for instance, the Diffie-Hellman key exchange (D-H) algorithm. As the patent of D-H has expired, it has already become a public algorithm and is still proving to be quite capable and efficient for key distribution. Moreover, the ephemeral Diffie-Hellman (DHE) which can provide perfect forward secrecy has been adopted in the newest version of Transport Layer Security (TLS) protocol [89]. For a mature TLS server, the ephemeral D-H key pair could be generated in one second (in the same D-H group) with only a very small fraction of computing power is used. When combined with our reconfigurable optical layer coding techniques, the D-H algorithm becomes much stronger. In [90], a typical way to evaluate the strength of public key algorithms is provided. Roughly, the computational time to crack a 1024bit MODP (More Modular Exponential [91]) D-H group is around one year, which is considered to be not secure enough in the electronic layer. However, things are very different in the optical layer. As reported in [92], even without the consideration of maintaining the features of the encoded signal, the maximum delay time of the novel optical buffer is only around 50,000 bits, which only lasts 5μs in a 10G communication system. In other words, if the attacker could not crack the OC in 5μs, he would never get an opportunity to test it. This limitation on the optical buffer also limited the ability of Brute-force attackers. Notice that, the value in Table 4.2 is calculated in the condition that the data rate is 700Gb/s, which indicates that the actual delay time is quite small.

Table 4.2 Comparison of different optical buffer approaches [92].

Technique	Slow Light			Delay Line	
	EIT-QD	CRS-Si	CRS-ideal	Silicon	Silica
Maximum Delay	28 bits	160 bits	700 bits	7000 bits	50,000 bits

The tiny purple block in the right corner of the module block in Figure 4.4 indicates that there are optical approaches instead of electronic approaches. However, as both Quantum Key Distribution and Multiprotocol Label Switching are still under development, our original OCSP will only contain mutual commercialized and open-sourced protocols and algorithms. Although in this section these all-optical related approaches will not be discussed, it must be pointed out that our reconfigurable OC coding techniques have the potential to be compatible with these protocols.

The packet routing and synchronization module is an optional module that depends on the network environment. While the authentication module is considered to be a must since shared time-varying OC does not provide any authentication features. As long as the OC link has been established, it is almost impossible for an attacker to modify the data transmitted on the link unnoticed without the right OC. Thus the impact of the integrity check algorithm is less important. Considering the transmission errors are the major source of impaired integrity, the preferable algorithms for the integrity check are Error-correcting codes (ECC), Forward error correction codes (FEC), Cyclic redundancy checks (CRC) or simply checksum.

The general procedure of OCSP is shown in Figure 4.5. Once the OC link is established, all the information is transmitted on the OC link including the authentication process and the new proposal for the renewal OC link. Thus without the OC, the potential attacker can barely perform any kind of traditional cryptanalysis attacks. Although it is not shown in Figure 4.5, each data packet can be further protected by the integrity checking module and other symmetric encryption algorithms if needed. However, considering the same function is also provided by the OC link, the related extension is only an optional choice rather than a necessary module. To reduce the threats of Denial-of-service attack, as we can see from Figure 4.5, the OCSP is unbalanced in design. The responder only acts when he receives a legal request, while

the requestor takes on the responsibilities of the transmission. Thus to maintain a connection, the requestor will use far more resources than the responder.

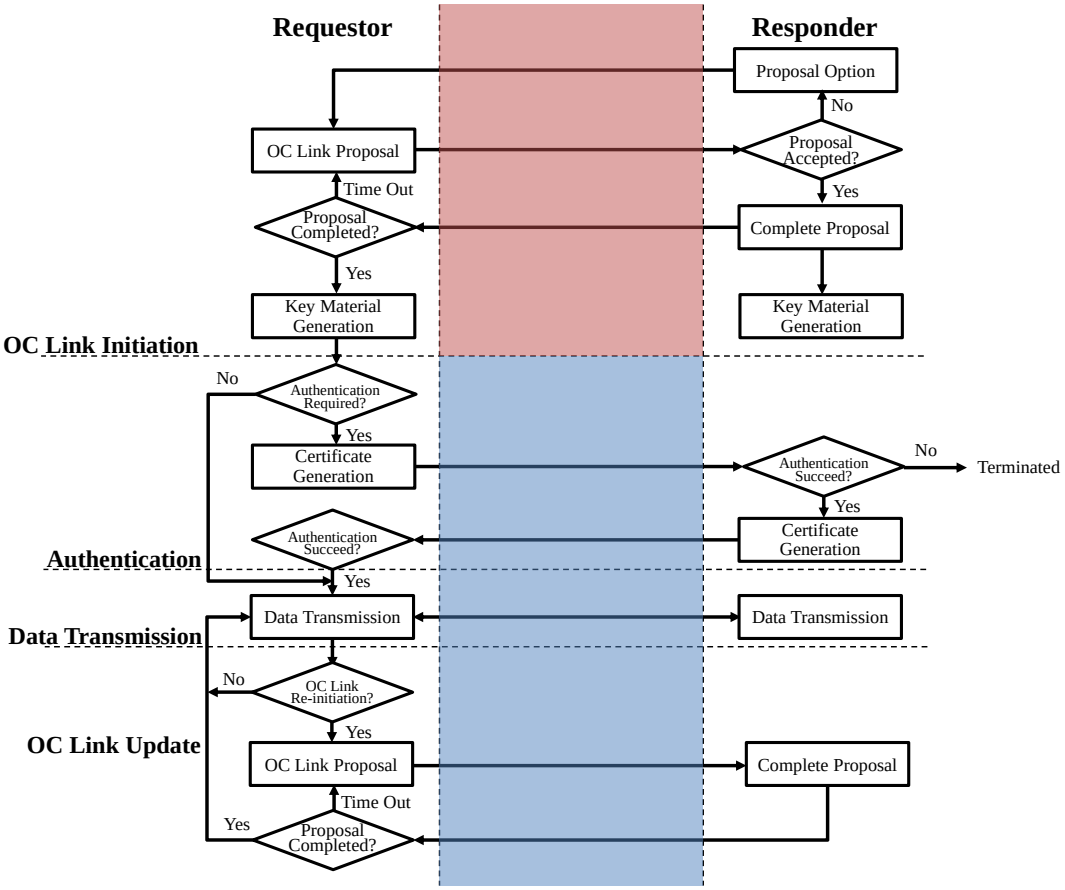


Figure 4.5 General procedure of OCSP.

To simplify the protocol, we managed to compress the entire OC link initiation procedure into few message exchanges as possible, as shown in Figure 4.6. The detailed definitions of the segments are given in section 4.3.

Basically, two exchanges are needed to establish a reliable OC link. The main purpose of the first exchange is OC distribution along with other configurable information related to other security aspects. The header segment contains the ID of both the entity for routing purpose. The link_E segment is the optical code link module and contains the parameters which are used for code generation, including: code generation algorithms, the length of the OC, and the chip rate of the OC. The D-H segment contains the Diffie-Hellman public key, which are used to generate the key material. The nonce segment is an arbitrary random number that used only once per

message. It prevents the replay attacks and is used to generate the unique key materials that correspond to the current session.

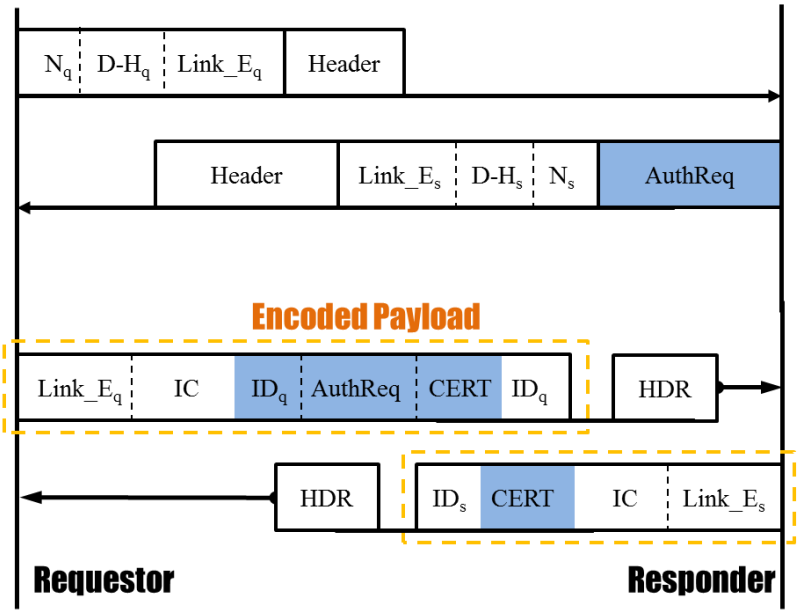


Figure 4.6 Message exchanges in OCSP for OC link initiation.
N: Nonce Segment, D-H: Diffie-Hellman Segment, Link_E: OC Link Segment, AuthReq: Authentication Request Segment, ID: Identity Segment, HDR: Header Segment, IC: Integrity Checking Segment, q/s: requestor/responder

It is true that the certificate exchange (identity authentication) could be done in either the first exchange or the second exchange. However, since the information in the first exchange is totally public, it is not wise to put important information there. Putting the identity authentication in the second exchange also exposes the first exchange to threats of Man-in-the-middle attacks, but due to the identity authentication in the following exchange, nothing valuable is leaked when the authentication fails. While there is a chance that the attacker uses his own ID to replace the requestor's ID and keeps everything else unmodified. In this case, the responder will consider the attacker as a legal requestor, and finishes the entire key exchange process. Thus the attacker could gain a shared secret with the responder and forward the secret to the requestor to make the requestor believe he is communicating with the responder. To eliminate this threat, it is critical to generate the key material with both entities' ID. In this case, although the attacker shares the secret with the responder, the shared secret received from the attacker will generate the wrong key and make the OC link terminate. Figure 4.7 shows an example of a Man-in-the-Middle attack against the first exchange.

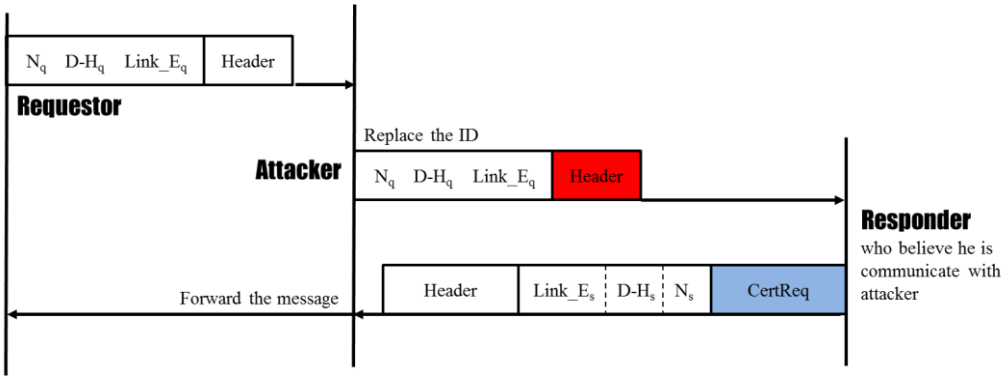


Figure 4.7 Man-in-the-Middle attack against the first exchange.

If the OC/key is only generated from the D-H shared secret, the attacker will access the D-H shared secret and generate any key he needs, while both the requestor and the responder will not be aware of the attack. The requestor believes he is communicating with the responder, while in the meantime the responder believes he is communicating with the attacker. When the second exchange begins, the attacker can just do the identity authentication with the responder and leave the requestor aside. Thus all the information sent from the requestor will be decrypted by the attacker.

If the OC/key is generated from the D-H shared secret combined with the ID, the requestor will time out since the key he holds is generated from the requestor-responder/requestor-attacker, while the key of the responder is generated from the attacker-responder. The key will never match, thus no useful information is leaked.

4.2 Consideration of the Secured Optical Code Link Initiation

As shown in Figure 4.5, it is quite important to initiate the OC link correctly to provide guaranteed security. On the other hand, after the OC link has been established, the data transmission process could be quite straightforward, providing a high transmission speed with sound optical layer security.

4.2.1 Features of Optical Code Link

As demonstrated in [82], our proposed reconfigurable OC coder supports totally random sequences, the variable length of the OC and variable chip rate. Therefore, at

least two parameters related to OC need to be negotiated during the initiated exchange: OC length and the chip rate.

OC length is the most significant parameter related to the strength of the OC link and is also the equivalent key length of the OC link. Technically there is no limitation on the chip rate. However, for simplicity, the clock signal of OC is usually generated by time multiplexing the clock signal of the data, therefore the chip rate is practically set to be an integer multiple of the data rate.

Apart from the inherited OC parameters, all security parameters related to the OC link have to be settled down, including:

- Diffie-Hellman Group
- Pseudo Random Function (PRF) algorithm
- Authentication method
- Integrity check algorithm

All the key lengths of these algorithms are suggested to be no less than the length of the OC to provide an equivalent computational complexity compared to the OC length. However, as explained in section 4.1.4, it is possible to use a shorter key as long as the computational time complexity is much longer than the life time of the optical encoded signals. Considering the fast configurable features of our optical coding devices, reliable security can be achieved when the computational time complexity of the related cryptography algorithm is longer than the life time of an OC.

4.2.2 Shared Secret and Optical Code Generation

Since the OC in our system could be a totally random sequence, it increases the flexibility when we choose the key distribution method. While the deployment of QKD is limited by the network environment, as indicated in Chapter 2, the Diffie-Hellman exchange has been developed mutually both in software and hardware implementation. Currently, the Diffie-Hellman Group is widely used as the shared secret algorithm in many security applications. In [91], several Diffie-Hellman Groups are defined for the Internet Key Exchange which can be inherited in the OCSP. The relative key length of each Diffie-Hellman Group is listed in Table 4.3.

Table 4.3 The relative key length of different D-H groups

Length of Prime	Relative Key Length
1536 bit	90~120
2048 bit	110~160
3072 bit	130~210
4096 bit	150~240
6144 bit	170~270
8192 bit	190~310

The basic concept of the Diffie-Hellman Key Agreement is defined in [93] and the D-H shared secret (DHs) is generated as follows:

$$\begin{aligned} DHs &= g^{x_q \cdot x_s} \bmod p \\ g &= h^{\frac{p-1}{q}} \bmod p \end{aligned} \tag{4.1}$$

where p and q are both large primes, h is any integer in the range of (1, p-1), and x_q, x_s are the private keys of the requestor and responder respectively.

However, instead of doing the calculation shown above, each entity performs the computations as follows:

$$\begin{aligned} DHs &= y_q^{x_s} \bmod p \\ &= y_s^{x_q} \bmod p \end{aligned} \tag{4.2}$$

where y_q and y_s are public keys for the requestor and responder respectively.

$$\begin{aligned} y_q &= g^{x_q} \bmod p \\ y_s &= g^{x_s} \bmod p \end{aligned} \tag{4.3}$$

An illustration of the process is shown in Figure 4.8.

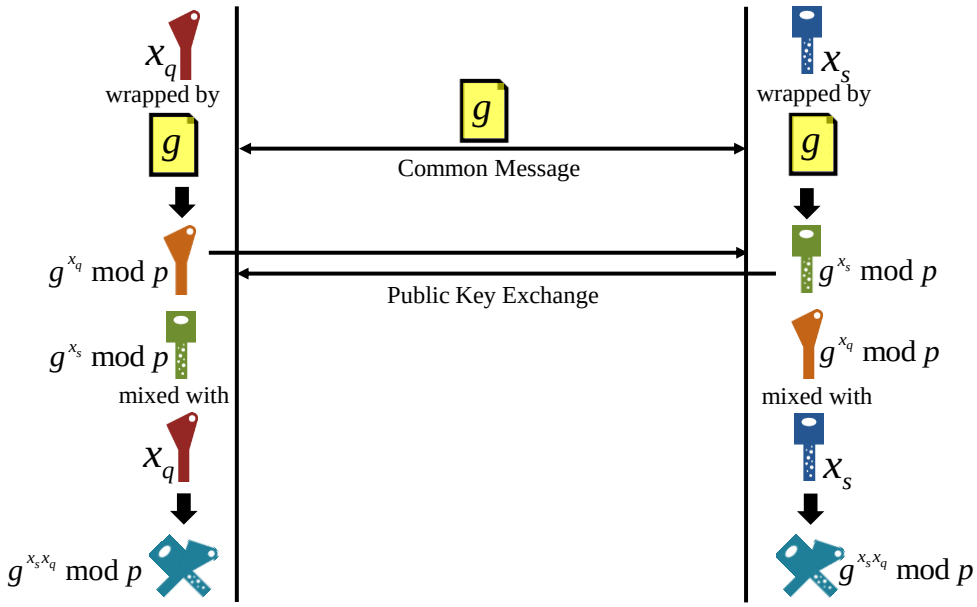


Figure 4.8 The process of the Diffie-Hellman key exchange

The length of the shared secret (*DHs*) is the same as the length of the prime *p*. For simplicity, the common message is 2 (*g* =2). Although usually there is no specific definition of the length of the private key of D-H algorithms, it is intrinsically in the range (1, *p*-1). If the length of the private key is defined as *l*, then the value should be in the range $x \in \left(2^{l-1}, 2^{l}\right)$.

After the Diffie-Hellman exchange, a required length of secret is shared between two entities. Each party can generate a seed derived from a D-H shared secret. The seed is also used for generating OC, along with keys that are used for authentication and integrity protection.

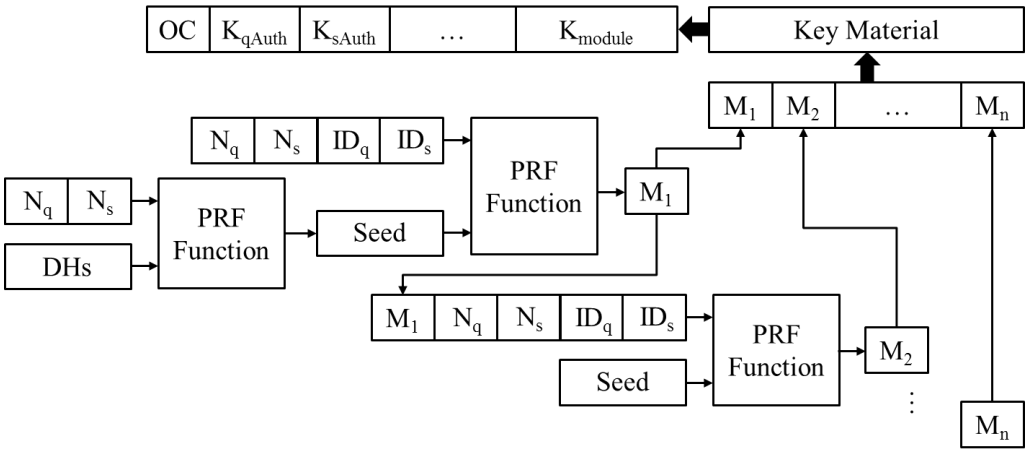


Figure 4.9 Key material generation

As shown in Figure 4.9, the key seed is generated from the output of the negotiated PRF algorithm. Since the PRF algorithm is fixed, when the required length of the key

material is greater than the length of the output of the PRF function, an iterative generation procedure can be used to create the rest of the key seed. The key material is a combination of the iteration results and each segment takes a fixed length of bits according to the negotiation. The meaning of nonces and link IDs will be explained in the following sections.

One of the merits of our reconfigurable optical coding scheme is that there is no specific requirement for the format of the code pattern. Thus our scheme is compatible with any pseudo random number generator. Currently, there are bunches of pseudo random function algorithms specified by a number of standard bodies including NIST, ANSI X9 committee and so on. Also, the software application can be easily supported by the open source project: OpenSSL library. Although the motivation for the project was originally to develop a robust, commercial-grade SSL/TLS protocol, the algorithms in its cryptography library are widely used for general security purposes.

Apart from the software based function, the hardware random number generator is also supported. Intel has embedded Secure Key Technology in their latest processors (Ivy Bridge) for random number generation, which means for most personal computer users, no additional hardware modules are needed for OC generation. However, for ultimate security consideration, a self-designed hardware or open source software is still preferable.

An extra coding function may be added to keep the OC for each bit balanced, leading to the maximum informatics-theoretic security. The question could be solved by applying a balanced code generating function [94] which uses the parameters from a shared secret based on Knuth's construction [95]. Here, the decoding of the balanced code is not required.

Define $C(M)=\binom{M}{M/2}$ as the total number of balanced numbers of length *M*. If we want to develop a balanced code-set that corresponds to *N* bits information, clearly we need to have enough parity bits *p* so that $C(N+p)\geq 2^N$. According to Stirling's approximation, p must follow $p>\frac{1}{2}\log_2 N+0.326$ in any balanced codes.

Hence a balanced code can be described with 2^p information bits and p parity bits, which means a 264 bits balanced code can be generated by a 256 bits random sequence with 8 parity bits. The procedure of balanced code generation is as follows:

Let $w(n)$ be the total number of '1' in the binary sequence n. Let $w_i(n)$ be the number of '1' in the first i bits of n. Let $n_{\bar{i}}$ be the binary sequence n with the first i bits complemented. For example, if n=10110, $w(n)$=3, $w_3(n)=2$, $n_{\bar{3}}=01010$. Thus we have

$$w(n_{\bar{i}}) = w(n) + i - 2w_i(n) \tag{4.4}$$

The relation leads to the fact that every sequence n can be associated with at least one i so that $n_{\bar{i}}$ is balanced. Hence the smallest i can be called as the balancing position of n. In other words, it is a way to produce balanced code from original sequence n. However, since the generated sequence can be conflicting, an extra identity should be added as a unique label for each balanced code. This can easily be achieved by encoding i into a balanced sequence u of length p. Therefore, $un_{\bar{i}}$ is the balanced code mapping from random sequence n.

Regardless of what data processing procedures are taken for OC and key generation, since the only source of secret entropy in this computation is DHs (N_q and N_s are unique but public), although the length of the key material could be much longer, the effective key length is still limited by the length of DHs.

The length of the key material is related to the length of the key we need for different security modules. For two directions of exchange, the key could be different.

4.2.3 Authentication

The most applied authentication methods are Extensible Authentication Protocol (EAP) and Digital Signature. Considering the physical accessible feature of our fast-reconfigurable coding devices, the Digital Signature issued by an Authentication Server

(AS) when any entities are added into the known network is preferable. Unlike a mobile network which requires the flexibility of network switching and transferring, the structure of optical connections is quite stable. Thus the issue of a Digital Signature would never become a problem. The procedure is shown in Figure 4.10.

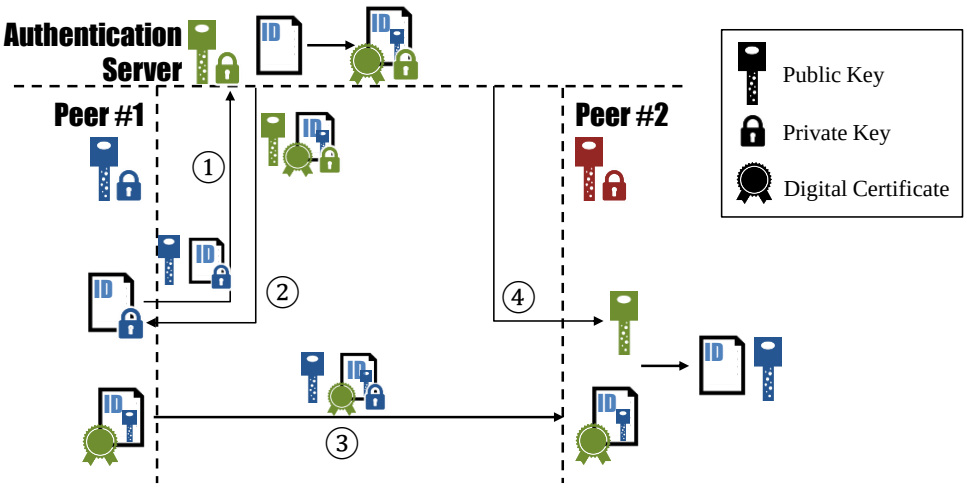


Figure 4.10 The identity authentication procedures.

- A node sends a certificate request to AS, including his identity, the public key related to the identity and encrypted by his private key (① in Figure 4.10).
- After verifying the identity of the node, AS issues a certificate to the node, which is generated from the identity of both the node and AS and encrypted by AS's private key (② in Figure 4.10). Hence the certificate cannot be forged by any entity. If the signed certificate or encrypted data are modified, the recovered identity will be changed unexpectedly.
- When other nodes request authentication from the node that has the certificate, the response message includes: the hash value of the last sent message and the signed certificate encrypted by his private key (③ in Figure 4.10).
- AS will issue the public key that corresponds to the signed certificate to the other node so the node can decrypt the signed certificate and validate the identity.

Since the authentication proceeds right after the OC link initiation and uses the content (part of which is random) of the OC exchange as validation, although an eavesdropper may eavesdrop the content of the OC exchange and store it, it is impossible for him to forge or modify an authentication message without a private key. He cannot perform a Man-in-the-middle attack either, since every message exchanged during the session is bound to the session and cannot be modified, thus it cannot work

for masquerading purposes by forwarding the message directly to another entity. The only opportunity that he could get a fake identity is when he joins the network by claiming to the AS that he has the same identity (Device ID/MAC address) as the target and gets a corresponding signed certificate. In this case, the attacker will be treated as the target user and will cause a network conflict when the target user is still online. This is the reason an offline method is suggested for securing this procedure.

Another way to break the system is to masquerade as the trusted AS. However, all the information issued by a real trusted AS is protected by its own private key and the corresponding public key is issued to every node when the AS is claimed to be trusted by them. Hence to masquerade as an existing AS means to crack the public key algorithm. An alternative way is to claim to be an AS and then issue fake certificates and corresponding public keys to other nodes. Hence in any circumstance, any operation related to modifying the trusted AS should be treated very carefully by users. This is also the reason an offline method is suggested when the new node wants to join the network. It is also important to keep AS activated all the time, in case any node in the network wants to pretend to be a fake AS when the real AS is offline, especially in a broadcasting network.

4.2.4 Integrity Checksum

After the OC link has been established, there is no way for a potential attacker to modify the encoded data without knowing the value of OC. Hence the integrity check module is only used for transmission error detection. Therefore, FEC could be introduced to replace the traditional integrity check hash function such as HMAC_MD5, HMAC_SHA1, DES_MAC, AES_XCBC. In extreme cases, the entire integrity check module can be replaced by a simple linear checksum segment without a cryptography hash function.

4.2.5 OC Link Renewal and Lifetime of the OC

Once the OC link is established, the renewal of the OC can be achieved in two ways. The first method is direct exchange. It is possible to exchange the information of the new OC publicly on the existing OC link as long as the link is considered to be secure. In this way, no time consuming algorithms are involved so the renewal of the

OC can be achieved at an ultra-high speed. The second method is renewing the OC with the new D-H shared secret. It is required to renew the OC with the new D-H shared secret when the OC link is considered to be compromised by a potential attacker. Although the security of the OC link is reliable, the original D-H value can be cracked. Since all the values used for key material generation are exchanged on the public link initially, it is possible for the attacker to synchronize the generation of the OC. In this scenario, the ephemeral D-H exchange is suggested to provide perfect forward security. However, the D-H algorithm is comparatively time-consuming, which will result in a sacrifice in the packet transmission rate.

Apart from exchanging the value of OC directly, a random value (in direct exchange mode) or a new D-H value (in new D-H mode) is exchanged for seed generation, and the new OC is generated following the method introduced in 4.2.2. Due to the fact that the chip rate is always higher than the bit rate, the length of the required OC is naturally longer than the value exchanged, which is the reason the OC should always be generated from a shorter seed.

To reduce the complexity of the OCSP, the lifetime of an OC is set by the requestor by default. The requestor should be responsible for setting a proper lifetime for OC considering the security level he requires. Generally, there are two factors that affect the lifetime of the OC, the strength of the OC and the strength of the D-H value. Although the computational complexity remains the same, the length of the OC can be extended on demand by using the pseudo-random function iteratively to make the signal analysis infeasible. Considering the physical limitation on real-time chip-level detection, the strength of the D-H value is essential for OC lifetime determination. The OC must be renewed in less time than the estimated time needed for D-H value cracking.

4.2.6 Packet Routing and Preamble Synchronization

As shown in Figure 4.11, the routing information is contained in a header/label outside the OC initiation packet. And the synchronization signals are right after the header of the OC link packet.

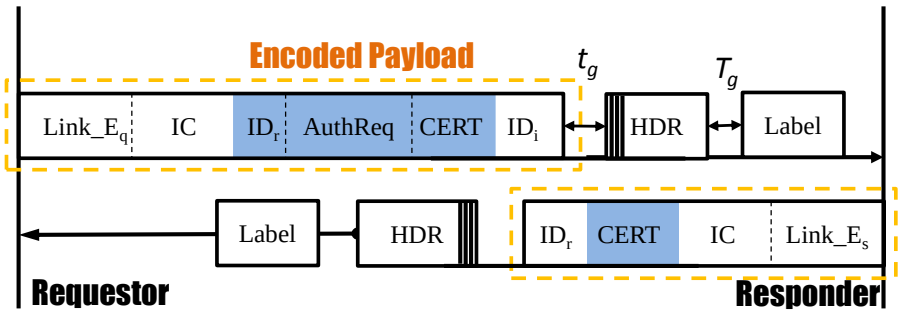


Figure 4.11 Packet routing label and preamble synchronization signals.

The label in Figure 4.11 is the original packet header, while from the HDR to Link_E is the packet of the OC link. The packet synchronization signal is right after the header of the OC link. T_g and t_g are the guard time of packet switching and OC generation.

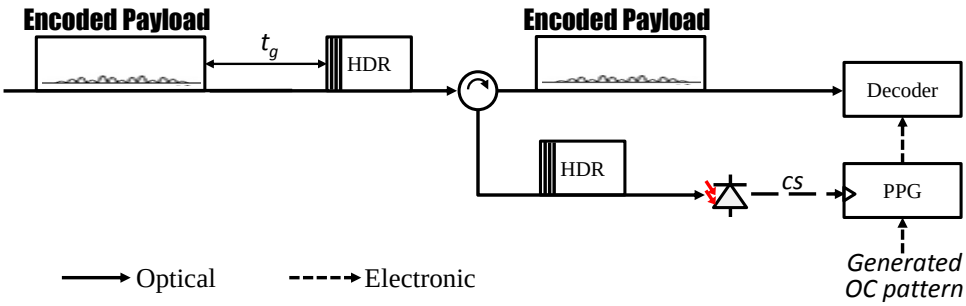


Figure 4.12 Schematic diagram of packet synchronization.

An example of packet synchronization is shown in Figure 4.12. Similar to the packet switching, the signals of the OC link header are also separated from the encoded payload signals by a simple reflective filter and the packet synchronization information is detected by a simple detector which provides a sequence of clock reference signals to the pulse pattern generator (PPG).

4.2.7 Packet Sequence, Nonces and Optical Code Link ID

The Packet Sequence is an identifier that indicates the retransmission of the packet. Each entity of the OC link maintains two active packet sequences: the next one to be used when sending a request and the next one it expects to see when receiving a request. The sequences increase every time a request is generated or received.

Each message of OC link negotiation contains a unique random value called a nonce. This is an indicator to make each negotiation unique. Also, to make sure the key seed for each negotiation is unique, the nonces involved in the OC link are also used as the input of the key seed generating function, as shown in Figure 4.9. After the OC link establishment, the nonces are not necessary as the channel has been isolated from potential attacks. However, if the renewal rate of the D-H exchange is slow, nonces can be used to add freshness to the generation of the key seed.

The OC link ID is a unique random number generated for an entity marking a specific OC link. It represents the ID of the entity on the OC link and is used for key material generation. After the OC link is established, the OC link ID only has the local meaning. It operates like an index of different OC links with different settings. By checking the OC link ID, the entity selects stored negotiated parameters to reconstruct the OC link until the link is terminated. This simplifies the procedure of OC redistribution/reconstruction, and is quite important for the packet switching network.

4.2.8 Retransmission

Since the initiation of the OC link required random information from both entities, a complete negotiation must consist of request/response pairs. Thus the responder only sends the response when a request is received. Therefore, the initiator is responsible for retransmission in the event of a timeout, and has to cache every request sent until it gets the response. On the other side, the responder has to cache each response until it receives a request whose packet sequence number is larger than the sequence number in the response plus its window size. After the OC link is established, each entity has the authority to initiate the request. While the request is being sent, unless a window size notification is received, the requestor has to wait for a response to each of its requests. Once a window size notification is received, the requestor is allowed to send multiple requests within the window. In other words, if the responder stated its window size is N, then when the initiator needs to make a request X, it MUST wait until it has received responses to all requests up through request X-N. If the window size supported is larger than one, the entity is required to process incoming requests out of order, since the arrival time of the requests in the same window is unpredictable.

4.3 Definition of Data Formats in OCSP

In this section, all the related data formats in the proposed optical coding security protocol are defined. It is the first time that we have a well-defined protocol to make our experimental setup more suitable for the practical applications. In the previous work, the data confidentiality which is guaranteed by the reconfigurable optical coding is the only thing we considered. However, in this new proposed protocol, the identity authentication, the data integrity checksum and the distribution of the dynamic optical codes are also included. Each security feature can be achieved by a separate module and operates together as long as the data is in the designed format. To maintain the flexibility of the protocol, each security module is designed in similar structure and contains all the information that have to share between the entities involved in the communication. It should be noted that the proposed optical code security protocol is complete original. However, various open source algorithms are included as the supplements.

4.3.1 Optical Code Link Header

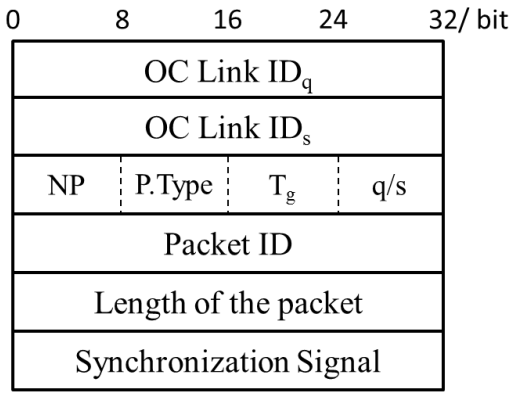


Figure 4.13 Format of the OC link header.

The format of the OC link header is shown in Figure 4.13.

- OC link ID (OLID): 8 octets, a value chosen by the entity to identify a specific OC link. The requestor's OLID is never zero while in the first request for OC link initiation, but the responder's OLID is left as zero. After the responder has received this request, a unique random value is generated and used as an OLID.

- NP (1 octet): Indicates the following type of module (1~255).

OC Link Module:	b10000000
OC Link Renewal Module	b11000000
D-H Module:	b01000000
IDq:	b00100000
IDs:	b00010000
Authentication Module:	b00001000
Authentication Req:	b00000100
Integrity check Module:	b00000010
Nonce:	b00000001
End:	b00000000

- P.Type (1 octet): Indicates the type of current payload.

OC link initiation:	b00100000
Identity Authentication:	b00000100
Data transmission:	b00000000

- tg (1 octet): Guard time of OC generation

The speed of the D-H algorithm is highly related to the environment, Diffie-Hellman groups and the length of p. For the 1024 bit ECDH group which can provide perfect forward secrecy in SSL/TLS, the operation per second is over 12000 [96].

A useful fact is that if we double the length of the D-H group, the operation we need increases by four times. Hence for a 32 bit ECDH group, the processing time is ~80 ns, which is equivalent to a packet rate ~12 Mpacket/s. However, since the responder gets all the information to generate the OC before he sends the response to the requestor, the setting of the guard time may be irrelevant to the time for the D-H exchange. In this case, the guard time equals to the overall time for synchronization signal processing.

- q/s (1 octet): Identifies the type of message.

Request:	b01000000
Response:	b00000010

• Packet ID (4 octets): Monotonically increased packet sequence, used for matching the requests and responses, controlling retransmission and preventing replay attacks.

• Length of Packet (4 octets): The total length of the OC link initiation message, including the OC link header and the total length of payload.

• Synchronization Signal (4 octets): A sequence of data “1” to provide a clock reference signal to the OC decoder.

4.3.2 Module Header

Each module of OCSP has the same header format, shown in Figure 4.14.

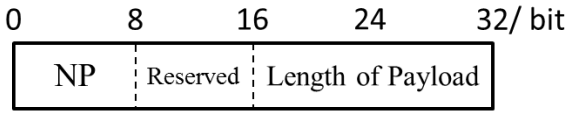


Figure 4.14 Format of the module header.

The module header provides the basic controlling information of a module: the next type of payload (see 4.3.1) and the length of the current module including the module header and the payload. Each module contains a module header, which indicates the next operation and where it starts.

4.3.3 Optical Code Link Module

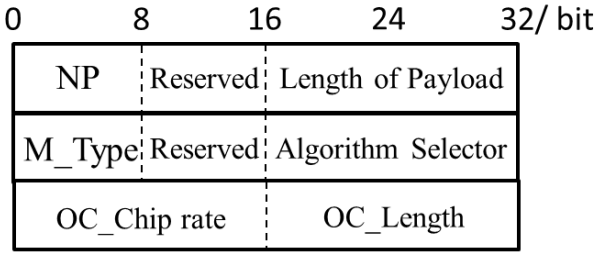


Figure 4.15 Format of the OC link module.

Each module consists of a module header and the payload. The payload of the OC link module includes the type of payload, the generation algorithm of OC, the chip rate of the OC link and the length of OC, which are defined as follows:

M_Type: Shares the same definition with NP, indicates the type of current module.

For the OC link module, the algorithm selector is defined as:

PRF_HMAC_MD5	b000000000000001
PRF_HMAC_SHA1	b000000000001000
PRF_HMAC_SHA256	b0000000100000000
PRF_USER_DEFINED	bXXXX000000000000

The default algorithms used for OC generation are MD5, SHA1 and SHA256 hash function, which are widely used for random number generation. However, users are allowed to define their own PRF function either by software or hardware.

The OC_Chip rate is defined as any multiple of bit rate. The highest chip rate supported by 16 bits is sufficient for any application.

OC_Length is the required length of the OC. Technically, the OC_Length can be set to any value, however it is suggested to be set at over 1024 bit against potential brute-force attacks.

4.3.4 Diffie-Hellman Exchange Module

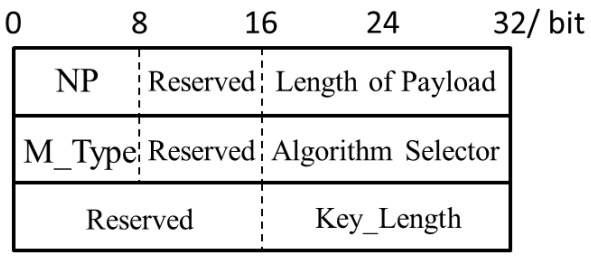


Figure 4.16 Format of the D-H exchange module.

The algorithm selector is defined as:

768 bit MODP D-H Group	b0000000000000001
1024 bit MODP D-H Group	b0000000000000010
1536-bit MODP D-H Group	b0000000000000100

2048-bit MODP D-H Group	b0000000000001000
3072-bit MODP D-H Group	b0000000000010000
4096-bit MODP D-H Group	b0000000000100000
6144-bit MODP D-H Group	b0000000001000000
8192-bit MODP D-H Group	b0000000010000000

The details of the above algorithms are defined in [91]. The key length is actually included in the algorithm selector. However, to construct a general format, it is required to be declared independently.

4.3.5 Authentication Module

As shown in the previous section, the identity authentication happens after the OC link is established. It starts from a CERTReq segment and ends with the exchange of the CERT segment. The formats of CERTReq and CERT are shown in Figure 4.17 and Figure 4.18, respectively.

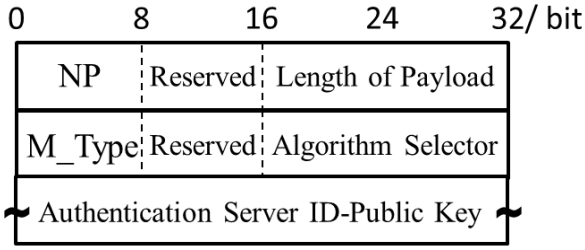


Figure 4.17 Format of the CERTReq segment.

The algorithm selector is defined as:

PKCS#1 [97]	d1
ECDSA [98]	d2
EIGamal Signature [99]	d3
X.509 Certificate – Signature [100]	d4
PGP Certificate [101]	d5
Kerberos Token [102]	d6
SPKI Certificate [103]	d7
Hash and URL of X.509 certificate [104]	d8
Reserved/User Defined	d9-65535

The authentication algorithms listed above are the most widely used algorithms and the protocol can be extended by the user.

The Authentication Server ID-Public key field contains an indicator of trusted AS, which consists of the corresponding ID and public key.

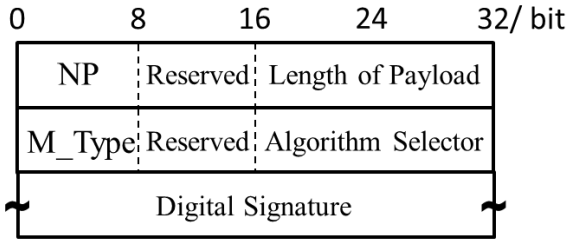


Figure 4.18 Format of the CERT segment.

Digital Signature is a variable length field filled with a signed certificate.

4.3.6 Integrity Checking Module

The format of the integrity checking module (data authentication) is shown in Figure 4.17.

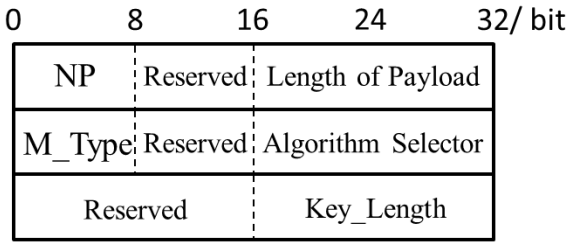


Figure 4.19 Format of the IC segment.

The algorithm selector is defined as:

IC_HMAC_MD5_96 [105]	d1
IC_HMAC_SHA1_96 [106]	d2
IC_AES_XCBC_96 [107]	d3
Reserved/User Defined	d4-65535

The default algorithms provide a degree of certificate function along with simple checksum. The simpler checksum such as BSD checksum could also be deployed since the OC link has already provided the protection on the data transmitted.

4.3.7 Data Transmission Module

The data transmission module simply consists of a module header and the data payload, as shown in Figure 5.20.

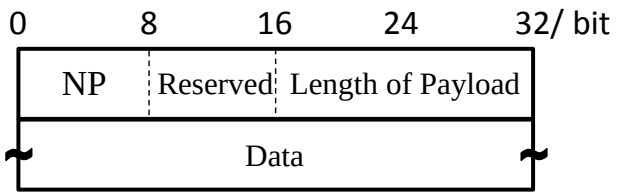


Figure 4.20 Format of the data transmission module.

The confidentiality of the data is related to the length of the data. If the length of the data is the same as the length of the OC, “one-time pad” can be achieved. If the length of the data is much longer than the length of the OC, then there is a risk that the eavesdropper could get the information without the knowledge of the OC, explained in section 4.4.2.

4.3.8 OC Link Renewal Module

The format of the OC link renewal module is defined as shown in Figure 4.21.

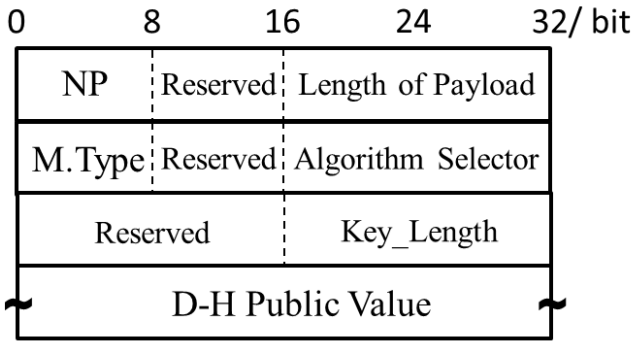


Figure 4.21 Format of the OC link renewal module.

The module consists of parameters of the D-H group and the new D-H public value. The only difference in the algorithm selector is, when the value is set to 0, a random sequence with required length is generated instead of the D-H public value, the value of which is used for key material generation.

The algorithm selector is defined as the same as the D-H exchange module with an additional definition about no D-H exchange being needed:

Direct exchange: b0000000000000000

4.3.9 D-H Exchange Segment

The D-H exchange segment is used to exchange the D-H public value between the requestor and the responder. The format is shown in Figure 4.22.

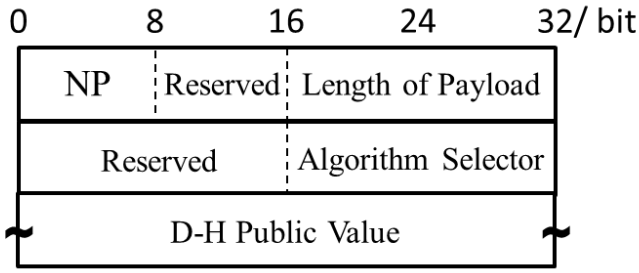


Figure 4.22 Format of the D-H segment.

The length of the D-H public value is equal to the length of the requested D-H group. If the request group is rejected by the responder, an acceptable option is sent back from the responder enabling the requestor to start a new initiation request. The generation of the D-H public value is introduced in section 4.2.2.

4.3.10 ID Segment

The ID segment is used to imply the identity of the entity. It is suggested that each message contains two IDs: IDi (identity of requestor) and IDr (identity of expecting responder). The format of the ID segment is shown in Figure 4.23.

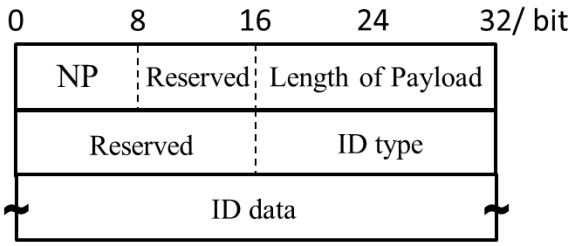


Figure 4.23 Format of the ID segment.

ID type is defined as:

ID_IPv4_Address	d1
ID_IPv6_Address	d2
ID_MAC_Address	d3
ID_Authorised_ID	d4

The ID can be the IP or the physical address of the entity, and the specific identity issued by the network operator. ID data segment is the value of the selected ID type.

4.3.11 Nonce Segment

The Nonce segment contains random data that is used to guarantee the uniqueness of the message. It is also used to generate the unique key materials that correspond to the current session. The format is shown in Figure. 4.24.

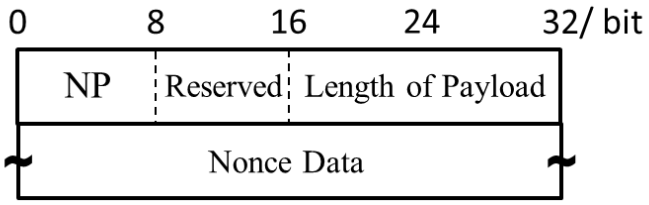


Figure 4.24 Format of Nonce segment.

Since the Nonce of both entities is used for key materials generation, the length of each Nonce is no less than half the length of the negotiated D-H Group length. Section 4.2.7 gives the explanation on how to generate the nonce data.

4.4 Security Consideration from Cryptanalysis Perspective

The major motivation of OCSP is to design a protocol that allows the data transmitted on a dynamic OC link to overcome the vulnerabilities of static OC schemes (M-ary modulation or OC aggregation for example). In cryptography, the information-theoretic secrecy is usually considered as a bonus and it is usually assumed that the attacker can obtain the information (especially encrypted) without error. Therefore, in this section, we analyse several attacking scenarios from the cryptanalysis perspective

without considering physical layer security. The results can be a good supplement to the secrecy provided in the optical layer. The scenarios are listed as follows.

4.4.1 Ciphertext-only Attack: Parallel Exhaustive OC Searching

One straightforward attack method against static OC schemes is the parallel exhaustive OC searching attack, as shown in Figure 4.25.

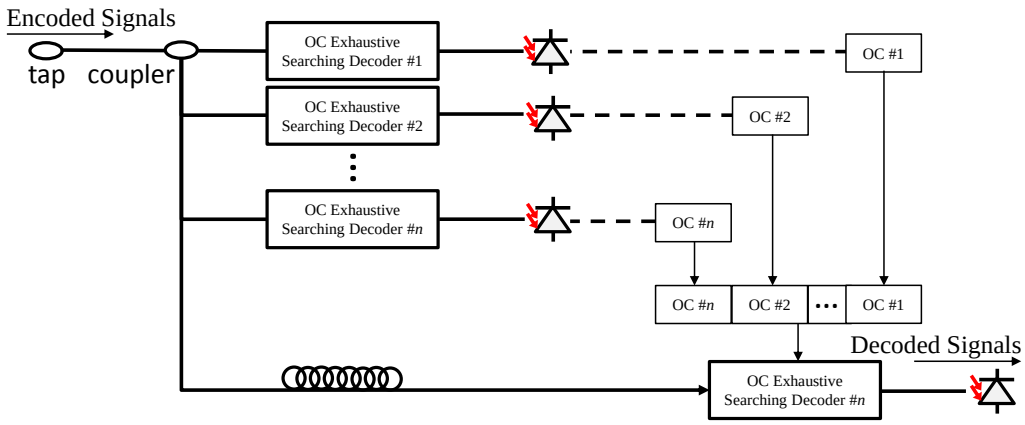


Figure 4.25 Parallel exhaustive OC searching.

When the length of OC is limited and used repeatedly, the eavesdropper can perform multiple exhaustive OC searching attacks in parallel simultaneously. Since the OC patterns are fixed, eventually the eavesdropper will get a good autocorrelation at each arm. Hence the total OC pattern can be determined and used for matched decoding.

The feasibility of the attack scheme depends on the average time spent cracking each OC, the optical buffer's ability to retain certain encoded signals and the lifetime of the OC. The first parameter is inversely proportional to the code space and the second parameter is determined by the ability of the optical buffer, while the last parameter is quite robust.

In traditional static OC schemes, the code space is fixed when the encoding/decoding device is selected, and the code reconfiguration operation usually involves delicate micro-mechanic techniques, which makes the system less flexible. In our reconfigurable OC coding scheme with OCSP, we provide a feasible way to generate ultra-long OC and in the meantime a reliable way to control the lifetime of OCs. Thus, this makes the system immune to the exhaustive OC searching.

4.4.2 Ciphertext-only Attack: Differential Analysis

Differential analysis is a common attack on the static OC scheme and is quite effective, especially when the signal is binary modulated by OC, as shown in Figure 4.26.

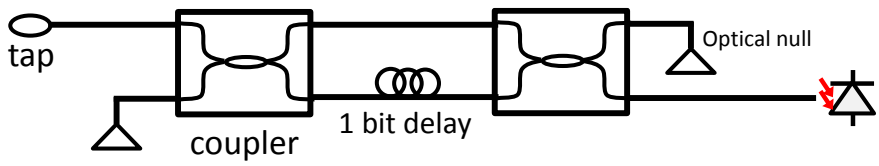


Figure 4.26 Schematic of a simple differential detector.

Instead of trying to extract the OC information, the scheme is designed to identify the differences between the code patterns. The feasibility of the scheme is inversely proportional to the number of codes used for modulation. In traditional static OC schemes, the encoder and the decoder are passive devices; hence the data is usually modulated by the limited number of OCs, making statistical analysis of the detection result feasible. In our reconfigurable OC coding scheme with OCSP, the data is totally independent from the OC, and the OC is generated from the shared secret which is unknown to the eavesdropper, thus the system is completely immune to the attacks.

4.4.3 Known Plaintext Attack: Phase Shifts Detection

From the perspective of cryptography, the encoding process is quite similar to the simple stream cipher. Instead of doing the XOR operation bit-by-bit, the optical encoding process uses a random pattern specified by multiple OC sequences (4 chips in this example) to replace each bit. Considering the chip-level detection is naturally more difficult than the bit-level detection, guaranteed information-theoretic secrecy is provided by the encoding process. However, the similar weakness of simple XOR encryption should also be avoided during the system design.

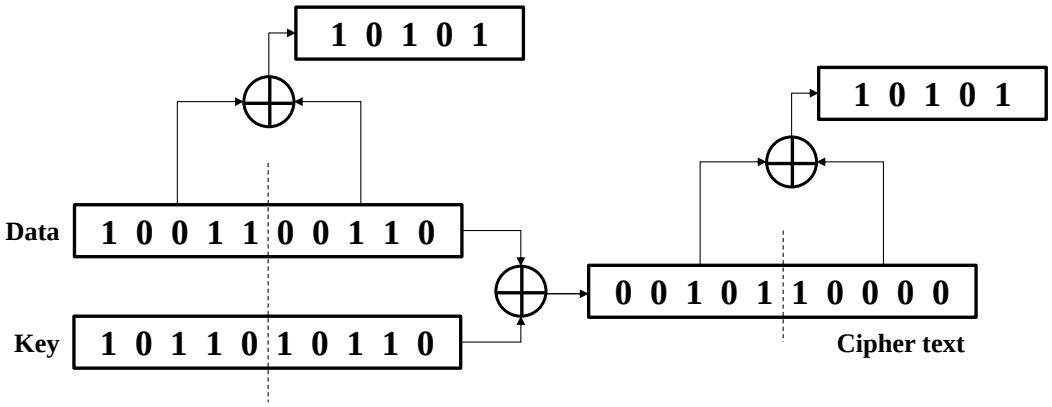


Figure 4.27 Weakness of simple XOR encryption.

The vulnerability of simple XOR encryption is shown in Figure 4.27. As long as the key length is limited and reused, the attacker who knows the length of the key can easily perform an XOR operation on cipher text to eliminate the influences of the key.

In ideal circumstances, a similar attack can be performed, as shown in Figure 5.28. The attacker can apply a delay line that is equal to the length of the key and then interfere the delayed signal with the original signal. In this way, the phase shifts induced by the OC will interfere destructively and will leave an interference signal caused by two sections of the original data. In other words, as long as the attacker knows part of the original data, the security of the system is compromised. Also, if he can manage to get enough information that is equal to the length of the OC, the security of the whole system is challenged.

The attacking scheme is specified against our proposed scheme because the traditional static OC scheme does not even have the concept of the “key”. To avoid the attacks, we defined an OC renewal module in OCSP to realize the management on the lifetime of the OC. With the proper setting on the length of the OC, the system can be strong enough against the attacks. If we set the time duration of each OC to be equal to the renewal rate and the length of the seed to be no less than the length of the data encoded by each OC, the “one-time pad” is achieved.

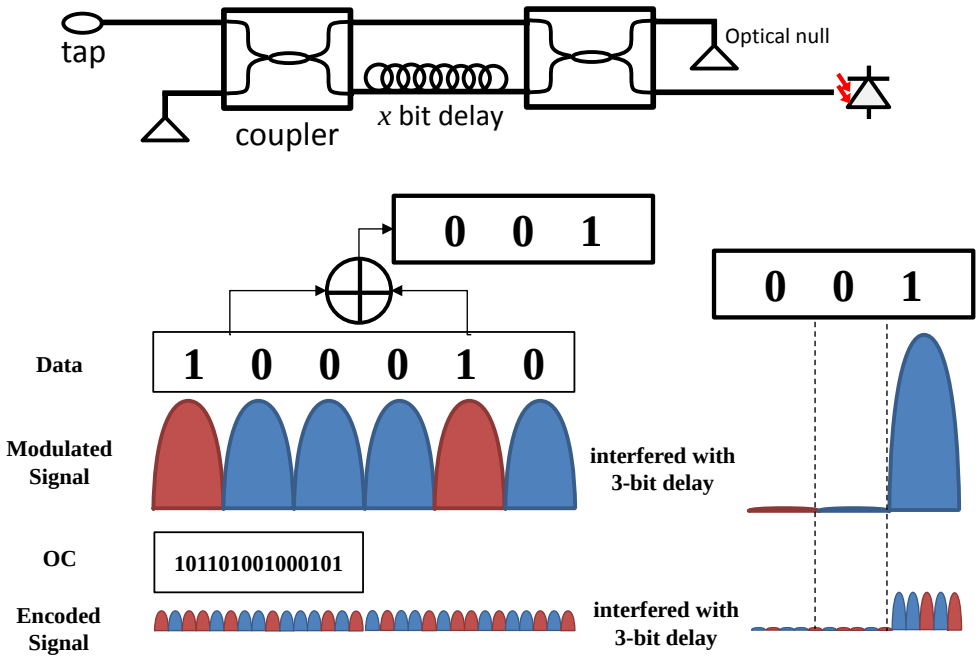


Figure 4.28 Potential threats when reusing OC with limited length.

Practically, due to the limitation of the optical buffer and the instability of the interference time of encoded signals, the scheme may not be feasible. However, it is still suggested to deploy a long OC with ephemeral D-H exchange to achieve perfect forward secrecy.

4.4.4 Chosen Plaintext Attack: Reconstruct the Transfer Function

A chosen plaintext attack is a very strong attack model that assumes the attacker can obtain ciphertext for arbitrary plaintext. The condition, at first glance, is an unrealistic model. However, in some special cases, the scheme may become feasible, for example, if the attacker manages to access the encoder physically. In this situation, the attack is feasible for static code schemes. Since the passive encoder is an LTI component, the attacker can get the output signals to correspond to any combination of inputs. Therefore, a mimic encoder can be synthesized by reconstructing the transfer function of the encoder. However, since the encoder in our scheme is an active encoder and the lifetime of the OC is session bounded, the attack is completely infeasible.

Besides these attacks, the strength of the encryptions applied in OCSP also affects the overall security performance. The most important is the strength of the D-H exchange because it is the only information transmitted outside of the protection of the

OC link and is used for OC link establishment. For security purposes, there are several security applications whose structure and algorithm are not fully public. On the contrary, in our OCSP, the security that is enabled by a dynamic OC link is fully transparent and stays in the physical layer rather than an obscure algorithm. Any user who adopts the OCSP can configure every detail of the system at their own demand, including selecting trustworthy algorithms, selecting required D-H groups, defining the type of OC and the chip rate. As long as the OC generation function is trustworthy and the outputs of which have high entropy, security can be guaranteed.

Chapter 5 Conclusion and Future Work

The security features of the coherent optical security communication systems enabled by optical coding techniques have been analysed in the thesis. Both the merits and the limitations of the temporal phase coding schemes and spectral phase coding schemes are addressed. The wiretap channel model for the optical coding schemes has been analysed and a brief equation, which can be used to evaluate the information-theoretic security level of the all kinds of optical coding channels, has been derived from information theory.

For our proposed reconfigurable optical coding device, a compatible security protocol has been drafted for the first time, which has been referred to as optical coding security protocol in the thesis. The protocol contains the guidance of optical code distribution, authentication through digital signature and the definition of all the security modules in the consideration. The protocol is designed to be extensible and can be configured on the specific demand. The encryption algorithms included are all open sources and trusted. It is believed that the use of the dynamic optical code to encrypt the signal will make the traditional cryptanalysis infeasible. Thus the security of the system can be guaranteed. The work in the thesis is still a preliminary result and can be further researched:

The system models that used in security evaluation are ideal models. In practice, the impairment of the device will induce much more noises than the thermal noise and the shot noise. Hence the result may be slightly different from the ideal case. However, the principle of the calculation is simple enough to be applied to any wiretap channel model. The security of the reconfigurable coding device can be proved by the information theory, yet the demonstration hasn't been done. In consideration of the compatibility, the proposed protocol has a redundant data structure. The size of the whole protocol could be reduced when the deployment environment is constant.

References

[1] R. Carroll, “Snowden used simple technology to mine NSA computer networks”, The Guardian, Feb. 2014.

[2] T. Groenfeldt, “Cybersecurity threats are rising– EY”, Forbes, Nov. 2013.

[3] ISO/IEC 2700:2014, “Information technology – Security techniques – Information security management systems – Overview and vocabulary”, Jan. 2014.

[4] W. Tuchman, “A brief history of the data encryption standard”, ACM Press Internet besieged, pp.275-280, 1998.

[5] United States National Institute of Standards and Technology, “Announcing the advanced encryption standard”, Federal Information Processing Standards Publication 197, Oct. 2012.

[6] R. Rivest, A. Shamir, L. Adleman, “A method for obtaining digital signatures and public key cryptosystem”, Communication of ACM, Vol. 21, No. 2, pp.120-126, Feb. 1978.

[7] United States National Institute of Standards and Technology, “Digital signature standard”, Federal Information Processing Standards Publication, FIPS.186-4, July 2013.

[8] R. Rivest, “The MD5 Message-Digest Algorithm”, RFC 1321, April 1992.

[9] United States National Institute of Standards and Technology, “Secure hash standard”, Federal Information Processing Standards Publication, FIPS.180-4, March 2012.

[10] P. Hoffman, “Cryptographic suites for IPsec”, RFC 4308, Dec. 2005.

[11] M. Hilbert, P. Lopez, “The world’s technological capacity to store, communicate, and compute information”, Science, Vol. 332, No. 6025, pp. 60-65, April 2011.

[12] E. Rescorla, “The transport layer security protocol”, RFC5246, Aug. 2008.

[13] Krawczyk, H., "The Order of Encryption and Authentication for Protecting Communications", Crypto 2001.

[14] 3GPP TS 33.102 V8.1.0 (2008-12) 3G security; Security architecture.

[15] 3GPP TS 33.401 V8.2.1 (2008-12) 3GPP System Architecture Evolution (SAE); Security architecture.

[16] Joe-Kai Tsay, Stig Mjølsnes, Computational Security Analysis of the UMTS and LTE Authentication and Key Agreement Protocols, Computer Science, Cryptography and Security

[17] Yu-Lun Huang, Chih-Ya Shen ; Shieh, S.W., S-AKA: A Provable and Secure Authentication Key Agreement Protocol for UMTS Networks, IEEE Transactions on Vehicular Technology, Vol.60 , Issue.9, pp. 4509-4519, Nov. 2011

[18] Hassan, Z.Z., Elgarf, T.A. ; Zekry, A., Modifying authentication techniques in mobile communication systems, 2014 Third International Conference on Cyber Warfare and Digital Forensic, Beirut, 2014.

[19] Rasheed, I., Amin, A., Chaudhary, M., Analyzing the security techniques used in LTE Advanced and their evaluation, 2013 Eighth International Conference on Digital Information Management, Islamabad, Sept. 2013.

[20] IEEE Standards Association, "IEEE 802.11: Wireless LAN medium access control and physical layer specifications", April 2012.

[21] IEEE Standards Association, "IEEE 802.11i-2004: Amendment 6: Media access control security enhancements", April 2010.

[22] T. Ohigashi, K. Mori, "A practical message falsification attack on WPA", Sept.2009.

[23] H. Gilbert, T. Peyrin, Super-Sbox Cryptanalysis: Improved Attacks for AES-like permutations, 2009.

[24] Vincent Rijmen, Practical-titled attack on AES-128 using Chosen-text relations, 2010.

[25] Andrey Bogdanov, Dmitry Khovratovich and Christian Rechberger, Biclique cryptanalysis of full AES, 2011.

[26] S. Kent, "IP Authentication Header", RFC 4302, Dec. 2005.

[27] P. Hoffman, "Cryptographic algorithm implementation requirements and usage guidance for Encapsulating Security Payload and Authentication Header", RFC 7321, Aug. 2014.

[28] S. Kent, "IP Encapsulating Security Payload", RFC 4303, Dec. 2005.

[29] R. Glenn, S. Frankel and S. Kelly, "The AES-CBC cipher algorithm and its use with IPsec", RFC 3602, Sept. 2003.

[30] A. D. Wyner, "The wire-tap channel," Bell System Technical Journal, Vol. 54, No. 8, pp.1355-1397, Oct. 1975.

[31] S. T. Ali, V. Sivaraman and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," Information Forensics and Security, Vol. 9, No. 12, pp.2193-2204, 2014.

[32] X. Li, E. P. Ratazzi, “MIMO transmission with information-theoretic secrecy for secret-key agreement in wireless networks,” Military Communications Conference, Vol. 3, pp. 1353-1359, 2005.

[33] U. M. Maurer, “Secret key agreement by public discussion from common information,” Information Theory, Vol. 39, No. 3, pp.733-742, 1993.

[34] P. R. Prucnal, M. P. Fok, and Z. Wang, “Physical layer security in fiber-optic networks using optical signal processing,” Communications and Photonics Conference and Exhibition, Asia, Vol. 2009-Supplement, pp.1-10, 2009.

[35] Xu Wang, “Optical layer security enabled by optical code based technology in optical communication systems,” International Conference on Optical Communications and Networks, China, M12.4, Nov. 2014.

[36] M. Medard, D. Marquis, and S. G. Finn, “Security issues in all-optical networks”, Network Magazine, Vol. 11, No. 3, pp.42-48, May 1997.

[37] P. D. Townsend, “Quantum cryptography on multi-user optical fibre networks”, Letters to Nature, Vol. 385, pp.47-49, Jan. 1997.

[38] J. Mork, B. Tromborg, J. Mark, “Chaos in semiconductor lasers with optical feedback: theory and experiment,” Journal of Quantum Electronics, Vol. 28, No.1, pp. 93-108, Jan. 1992.

[39] J. A. Salehi, “Emerging optical code-division multiple access communication systems”, Network, Vol. 3, No. 2, pp.31-39, 1989.

[40] K. Kitayama, H. Sotobayashi, and N. Wada, “Optical code division multiplexing and its applications to photonic networks”, Fundamentals of Electronics, Communications and Computer Sciences, Vol. E82-A, No. 12, pp. 7-19, Dec 1999.

[41] I. Kanter, Y. Aviad, and M. Rosenbluh, “An optical ultrafast random bit generator”, Nature Photonics, Vol. 4, pp.58-61, 2010.

[42] P. Prucnal, M. Santoro, F. Ting, “Spread spectrum fiber-optic local area network using optical processing,” J. Lightwave Technology, Vol. 4, No. 5, pp. 547–554, May 1986.

[43] A. M. Weiner, J. P. Heritage, J. A. Salehi, “Encoding and decoding of femtosecond pulses,” Optics Letters, Vol. 13, No. 4, pp. 300–302, April 1988.

[44] C. Yang, R. P. Scott, and S. J. B. Yoo, “Four-State Data Encoding for Enhanced Security Against Upstream Eavesdropping in SPECTS O-CDMA,” J. Lightwave Technology, Vol. 29, No. 1, pp. 62–68, Jan. 2011.

[45] Z. Gao, B. Dai, X. Wang, N. Kataoka and N. Wada, “Transparent transmission of secure time domain spectral phase encoding DPSK-OCDM signal over DWDM

network," J. Optical Communications and Networking, Vol. 3, No. 5, pp. 404–410, 2011.

[46] B. Dai and X. Wang, "Security Improvement Using ±π/2-Phase-Shifted SSFBG En/Decoder in Time-Spreading OCDMA", Photon. Technol. Lett., Vol. 22, No. 12, pp. 881–883, Jun. 2010.

[47] T. Kodama, N. Kataoka, N. Wada, G. Cincotti, X. Wang, T. Miyazaki, and K. Kitayama, "High-security 2.5 Gbps, polarization multiplexed 256-ary OCDM using a single multi-port encoder/decoder," Opt. Express, Vol. 18, No. 20, pp. 21376–21385, 2010.

[48] P. Bertarini, A. L. Sanches, B. V. Borges, "Optimal code set selection and security issues in spectral phase-encoded time spreading OCDMA systems", Journal of Lightwave Technology, Vol. 30, No. 12, pp. 1882-1890, June 2012.

[49] D. E. Leaird, Z. Jiang, A. M. Weiner, "Experimental investigation of security issues in OCDMA: a code-switching scheme", Electronics Letters, Vol. 41, No. 14, pp. 817-819, July 2005.

[50] Z. Wang, J. Chang, P. R. Prucnal, "Theoretical analysis and experimental investigation on the confidentiality of 2-D incoherent optical CDMA system", Journal of Lightwave Technology, Vol. 28, No. 12, pp. 1761- 1769, June 2010.

[51] T. H. Shake, "Security performance of optical CDMA against eavesdropping," J. Lightw. Technol., Vol. 23, No. 2, pp. 665–670, Feb. 2005.

[52] B. Dai, Z. Gao, X. Wang, N. Kataoka and N. Wada, "A novel optical orthogonal modulation format based on differential phase shift keying and code-shift keying", IEEE Photonic Technol. Lett., Vol. 23, No. 17, pp. 1210-1212, Sept. 2011.

[53] B. Dai, Z. Gao, N. Wada, and Xu Wang, "Orthogonal DPSK/CSK Modulation and Public-key Cryptography based Secure Optical Communication", IEEE Photonic Technol. Lett., Vol. 25, No. 19, pp. 1897–1900, Oct. 2013.

[54] U. Parlitz, L. O. Chua, and A. Shang, "Transmission of digital signals by chaotic synchronization," J. Bifur. Chaos, Vol.2, No.4 pp.973-977, Nov. 1992.

[55] Y. Z. Yin, "Experimental demonstration of chaotic synchronization in the modified chua's oscillators," Intern. Journ. of Bifur. and Chaos, Vol. 7, No. 6, pp.1401-1410, Nov. 1996.

[56] J. M. Liu, H. F. Chen and S. Tang, "Synchronized chaotic optical communications at high bit rates," IEEE Journal of Quantum Electronics, Vol. 38, No. 9, pp.1184-1196, Sept. 2002.

[57] J. Qhtsubo, “Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback,” Journal of Quantum Electronics, Vol. 38, No. 9, pp.1142-1154, Sept. 2002.

[58] S. Tang, J. M. Liu, “Chaos synchronization in semiconductor lasers with optoelectronic feedback,” Journal of Quantum Electronics, Vol. 39, No. 6, pp.708-715, June 2003.

[59] A. Argyris, D. Syvridis and K. A. Shore, “Chaos-based communications at high bit rates using commercial fibre-optic links,” Nature, Lett. Vol 438, No.17. pp. 343-346, Nov. 2005.

[60] L. E. Larson, L. S. Tsimring and J. M. Liu, “Digital communications using chaos and nonlinear dynamics,” Springer Science and Business Media, pp. 19, 2006.

[61] S. Li, G. Alvarez, G. Chen, “Breaking a chaos-based secure communication scheme designed by an improved modulation method,” Chaos, Solitons and Fractals, Vol.25, No. 1, pp.109-120, Sept. 2004.

[62] T. Yang, L. B. Yang and C. M. Yang, “Breaking chaotic switching using generalized synchronization: Examples,” IEEE Trans. On Circuits and Systems-I, Vol. 45, No. 10, pp. 1062-1067, Oct. 1998.

[63] K. M. Short and A. T. Parker, “Unmasking a hyper-chaotic communication scheme,” Phys. Rev. E, Vol.58, No.1, pp. 1159-1162, July 1998.

[64] N. Oliver, M. C. Soriano, and I. Fischer, “Fast random bit generation using a chaotic laser: approaching the information theoretic limit,” Journal of Quantum Electronics, Vol. 49, No. 11, pp.910-918, Nov. 2013.

[65] K. Hirano, K. Amano, and P. Davis, “Characteristics of fast physical random bit generation using chaotic semiconductor lasers,” Journal of Quantum Electronics, Vol. 45, No. 11, pp.1367-1379, Nov. 2009

[66] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” Nature 299, pp. 802-803, Oct. 1982.

[67] A. Einstein, B. Podolsky, N. Rosen, “Can quantum-mechanical description of physical reality be considered complete?” Physical Review, Vol 47, No. 10, pp. 777-780, May 1935.

[68] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. Vol. 67, No. 6, pp. 661-663, Aug. 1991.

[69] R. Ursin, F. Tiefenbacher, and A. Zeilinger, “Free-space distribution of entanglement and single photons over 144km,” Nature Physics, Vol. 3, pp. 481-486, June 2007.

[70] H. P. Yuen, “KCQ: A new approach to quantum cryptography I. General principles and key generation,” arXiv:quant-ph/0311061, July 2004.

[71] K. Harasawa, O. Hirota, and Y. Doi, “Quantum Encryption Communication Over a 192-km 2.5-Gbit/s Line With Optical Transceivers Employing Yuen-2000 Protocol Based on Intensity Modulation,” Journal of Lightw. Techno., Vol. 29, No. 3, pp. 316-323, Feb. 2011.

[72] H. P. Yuen, “Has quantum key distribution been proved secure?” arXiv: 1405.0457v2, Sept. 2014.

[73] H. P. Yuen, “Some physics and system issues in the security analysis of quantum key distribution protocols”, Journal of Quantum Information Processing, Vol. 13, No. 10, pp.1-27, Oct. 2014.

[74] G. Brassard, N. Lutkenhaus, and B. C. Sanders, “Limitations on practical quantum cryptography”, Phys. Rev. Lett. Vol. 85, No. 6, pp.1330-1333, Aug. 2000.

[75] M. Tomamichel, J. Mateo, and D. Elkouss, “Fundamental finite key limits for information reconciliation in quantum key distribution”, arXiv:1401.5194, Jan. 2014.

[76] H. K. Lo, M. Curty and K. Tamaki, “Secure quantum key distribution”, Nature Photonics, Vol. 8, pp.595-604, Aug. 2014.

[77] R. Matsumoto, T. Kodama, K. Kitayama, “40G-OCDMA-PON system with an asymmetric structure using a single multi-port and sampled SSFBG encoder/decoders,” Journal of Lightwave Technology, Vol. 32, No. 6, pp.1132-1143, March 2014.

[78] Q. Shen, S. Liao, and Q. An, “An FPGA-based TDC for free space quantum key distribution,” IEEE Trans. on Nuclear and Science, Vol. 60, No. 5, pp.3570-3577, Oct. 2013.

[79] N. Kataoka, N. Wada, K. Kitayama, “2.56 Tbps (40-Gbps × 8-wavelength × 4-OC × 2-POL) asynchronous WDM-OCDMA-PON using a multi-port encoder/decoder,” ECOC 37th, Geneva, pp.1-3, Sept. 2011.

[80] C. H. Bennett, G. Brassard, and U. M. Maurer, “Generalized privacy amplification”, Information Theory, Vol. 41, No. 6, pp.1915-1923, Nov. 1995.

[81] Andrew M. Weiner, Zhi Jiang, and Daniel E. Leaird, “Spectrally phase-coded O-CDMA”, Journal of Optical Networking. Vol. 6, Issue 6, pp. 728-755, May 2007

[82] Z. Gao, B. Dai, X. Wang, “Rapid programmable/code-length-variable time domain bit by bit code shifting for high speed secure optical communication”, Optics Letters, Vol. 36, No. 9, pp.1623-1625, May 2011.

[83] M. A. Muriel, J. Azana, and A. Carballar, “Real time fourier transformer based on fiber grating”, Optics Letters, Vol. 24, No. 1, pp.1-3, Jan. 1999.

[84] Z. Gao, X. Wang, and N. Wada, “40-Gb/s secure optical communication based upon fast reconfigurable time domain SPE/D with 40-Gchip/s optical code and symbol overlapping”, Optics Letters, Vol. 36, No. 22, pp.4326-4328, Nov. 2011.

[85] B. Dai, Z. Gao, and X. Wang, “Orthogonal DPSK/CSK modulation and public-key cryptography based secure optical communication,” Photonic Technol. Lett., Vol.25, No.19, pp.1897-1900, Oct. 2013.

[86] T. Kodama, N. Kataoka, and K. Kitayama, “High-security 2.5 Gbps, polarization multiplexed 256-ary OCDM using a single multi-port encoder/decoder,” Optical Express, Vol. 18, No. 20, pp. 21376-21385, Sept. 2010.

[87] Z. Wang, M. P. Fok and P. R. Prucnal, “Physical encoding in optical layer security,” Journal of Cyber Security and Mobility, Vol. 1, No. 1, pp.83-100, Jan. 2012.

[88] G. Stoneburner, C. Hayden, and A. Feringa, “Engineering Principles for Information technology security(A baseline for achieving security), revision A”, NIST Special Publication 800-27 Rev A, June 2004.

[89] RFC 5246, “The transport layer security protocol version 1.2,” Aug. 2008.

[90] RFC 3766, “Determining strength for public keys used for exchanging symmetric keys,” April, 2004.

[91] RFC 3526, “More modular exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE),” May, 2003.

[92] E. F. Burmeister, D. J. Blumenthal, J. E. Bowers, “A comparison of optical buffering technologies,” Optical Switching and Networking, Vol. 5, No. 1, pp. 10-18, July, 2008

[93] RFC 2631, “Diffie-Hellman key agreement method,” June, 1999.

[94] K. A. Schouhamer, J. H. Weber, “Very efficient balanced codes,” IEEE Journal on selected areas in communications, Vol.28, No.2, pp.188-192, Feb. 2010.

[95] D. E. Knuth, “Efficient balanced codes,” IEEE Trans. Inform. Theory, Vol. IT-32, No.1, pp.51-53, Jan. 1986.

[96] Emilia Kasper, “Fast Elliptic Curve Cryptography in OpenSSL”, Financial Cryptography and Data Security, Vol. 7126, pp. 27-39, Feb. 2012

[97] RFC 3447, “Public-key cryptography standards (PKCS) #1: RSA Cryptography specification version 2.1,” Feb. 2003.

[98] RFC 6979, “Deterministic usage of the digital signature algorithm (DSA) and elliptic curve digital signature algorithm (ECDSA)”, Aug. 2013.

[99] D. Pointcheval, J. Stem, “Security arguments for digital signatures and blind signatures,” J. Cryptology, vol.13, 361-396, 2000.

[100] ITU-T X.509, The Directory - Authentication framework.

[101] RFC 4880, “OpenPGP message format,” Nov. 2007.

[102] RFC 4120, “The kerberos network authentication service,” July, 2005.

[103] RFC 2693, “SPKI certificate theory,” Sept. 1999.

[104] RFC 4945, “The Internet IP security PKI profile of IKEv1/ISAKMP, IKEv2, and PKIX,” Aug. 2007.

[105] RFC 2403, “The use of HMAC-MD5-96 within ESP and AH,” Nov, 1998.

[106] RFC 2404, “The use of HMAC-SHA-1-96 within ESP and AH,” Nov, 1998.

[107] RFC 3566, “The AES-XCBC-MAC-96 Algorithm and its use with IPsec,” Sept, 2003.

[108] SSL Pulse, “Survey of the SSL implementation of the most popular web sites,” SSL Labs, April, 2015.

[109] R. G. Gallager, “Information theory and reliable communication,” New York: John Wiley, 1968.

[110] L. R. Welch, “Lower bounds on the maximum cross correlation of signals,” Information Theory, Vol. IT-20, pp. 397-399, May 1974.

[111] J. C. Diels, W. Rudolph, “Ultrashort laser pulse phenomena – fundamentals, techniques, and applications on a femtosecond time scale,” Academic Press of Elsevier, 2006.