World Academy of Science, Engineering and Technology
International Journal of Electronics and Communication Engineering
Vol:2, No:12, 2008

Speech Encryption and Decryption Using Linear Feedback Shift Register (LFSR)

Tin Lai Win, and Nant Christina Kyaw

***Abstract*—** This paper is taken into consideration the problem of cryptanalysis of stream ciphers. There is some attempts need to improve the existing attacks on stream cipher and to make an attempt to distinguish the portions of cipher text obtained by the encryption of plain text in which some parts of the text are random and the rest are non-random. This paper presents a tutorial introduction to symmetric cryptography. The basic information theoretic and computational properties of classic and modern cryptographic systems are presented, followed by an examination of the application of cryptography to the security of VoIP system in computer networks using LFSR algorithm. The implementation program will be developed Java 2. LFSR algorithm is appropriate for the encryption and decryption of online streaming data, e.g. VoIP (voice chatting over IP). This paper is implemented the encryption module of speech signals to cipher text and decryption module of cipher text to speech signals.

***Keywords*—** Linear Feedback Shift Register.

I. Introduction

As speech communications become more and more widely used and even more vulnerable, the importance of providing a high level of security is dramatically increasing. As such, a variety of speech encryption techniques have been introduced. The Linear Feedback Shift Register (LFSR) has been one of the most popular encryption techniques widely used in speech communication.

LFSR is suitable for speech because speech is continuous streaming data. They encrypt individual character (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time.

Stream cipher which used LFSR is algorithm that encrypts plaintext one bit at a time. Key stream generator generates outputs stream of bits k_1, k_2, ..., k_n. Cipher text is obtained by XORing this key stream bits with plain text bits p_1, p_2, ..., p_n.

$$c_i = p_i \oplus k_i$$

In synchronous stream ciphers, key stream is generated independent of the message being encrypted (decrypted). One key stream generator generates key stream of bits at the encryption side, another key stream generator generates the identical key stream of bits at the decryption end.

For this method, the two key stream generators must be synchronized. If the key stream generators are not synchronized or one of cipher text bits is lost in transmission then every cipher text bit is decrypted incorrectly. If this happens, sender and receiver must resynchronize the key generators.

One advantage of synchronous stream ciphers is that they do not propagate transmission errors. If a bit is garbled during transmission only, that bit is decrypted incorrectly. If any active attacker inserts a bit into the cipher text stream and then it can be detected, the cipher text cannot be decrypted correctly after that inserted bit.

Ms. Tin Lai Win is with the Department of Information Technology, West Yangon Technological University, Yangon, Myanmar (e-mail: tinlai83@ gmail.com)

Nant Christina Kyaw is with PACT Myanmar, Yangon, Myanmar (e-mail: christinakyaw @ gmail.com).

II. Methodology

A. Linear Feedback Shift Register

Linear Feedback Shift Register (LFSR) is used to generate pseudo random numbers. LFSR has two main parts. These are shift register and feedback function.

A shift register's identifying function is shifting its contents into adjacent positions within the register or, in the case of the position on the end, out of the register. The position on the other end is left empty unless some new content is shifted into the register. The contents of a shift register are usually thought of as being binary, that is, ones and zeros. Two uses for shift register are

1. Convert between parallel and serial data
2. Delay a serial bit stream

Shift direction A shift register can shift its contents in either direction. (Some registers have extra inputs that dictate the direction of the shift.) The shift direction will always be from left to right.

Output During a shift, the bit on the far right end of the shift register is moved out of the register. This end bit position is often referred to as the output bit. To confuse matters a bit, the bits that are shifted out of the register are also often referred to as output bits. To really muddy the waters, every bit in the shift register is considered to be output during a serial to parallel conversion. Happily, the context in which the term "output" is used generally clears thing up.

Input After a shift, the bit on the left end of the shift register is left empty unless a new bit (one not contained in the original contents) is put into it. This bit is sometimes referred to as the input bit. As with the output bit, there are several different references to input.

In an LFSR, the bits contained in selected positions in the shift register are combined in some sort of function and the result is fed back into the register's input bit. By definition, the selected bit values are collected before the register is clocked and the result of the feedback function is inserted into the shift register during the shift, filling the position that is emptied as a result of the shift.

The feedback function in an LFSR has several names: XOR, odd parity, sum modulo 2. Whatever the name, the function is simple:

1. Add the selected bit values.
2. If the sum is odd, the output of the function is one; otherwise the output is zero.[4]

B. Voice over IP (VoIP)

Voice over Internet Protocol (VoIP) is a technology that allows making telephone calls using Internet connections. As telephone calls should face constraints in terms of latency, jitter and loss, networks must support some QoS. Also as a conversation is private, the use of a secured protocol to protect from loss of data integrity and identity spoofing is another important challenge.

For several years, VOIP was a technology prospect. Telecommunications companies and other organizations have already moving their telephony infrastructure to their data networks. The VOIP solution provides a cheaper and clearer alternative to traditional PSTN phone lines. Although its implementation is widespread, the technology is still developing. Before any voice can be sent, a call must be placed. In an ordinary phone system, this process involves dialing the digits of the called number, which are then processed by the telephone company's system to ring the called number.[1]

With VOIP, the user must enter the dialed number, which can take the form of a number dialed on a telephone keypad or the selection of a Universal Resource Indicator (URI), but after that a complex series of packet exchanges must occur, based on a VOIP signaling protocol.

The problem is that computer systems are addressed using their IP address, but the user enters an ordinary telephone number or URI to place the call. The telephone number or URI must be linked with an IP address to reach the called party, much as an alphabetic web address, such as "www.nist.gov" must be linked to the IP address of the NIST web server. A number of protocols are involved in determining the IP address that corresponds to the called party's telephone number.

Once the called party answers, voice must be transmitted by converting the voice into digitized form, then segmenting the voice signal into a stream of packets.

The first step in this process is converting analog voice signals to digital, using an analog-digital converter. Since digitized voice requires a large number of bits, a compression algorithm can be used to reduce the volume of data to be transmitted. Next, voice samples are inserted into data packets to be carried on the Internet. The protocol for the voice packets is typically the Real-time Transport Protocol, RTP (RFC 3550).

RTP packets have special header fields that hold data needed to correctly re-assemble the packets into a voice signal on the other end. But voice packets will be carried as payload by UDP protocols that are also used for ordinary data transmission. In other words, the RTP packets are carried as data by the UDP datagram, which can then be processed by ordinary network nodes throughout the Internet. At the other end, the process is reversed: the packets are disassembled and put into the proper order, digitized voice data extracted from the packets and uncompressed, then the digitized voice is processed by a digital-to-analog converter to render it into analog signals for the called party's handset speaker.

The feature of VOIP that has attracted the most attention is its cost-saving potential. By moving away from the public switched telephone networks, long distance phone calls become very inexpensive. Instead of being processed across conventional commercial telecommunications line configurations, voice traffic travels on the Internet or over private data network lines. VOIP is also cost effective because all of an organization's electronic traffic (phone and data) is condensed onto one physical network, bypassing the need for separate PBX tie lines.

Although there is a significant initial startup cost to such an enterprise, significant net savings can result from managing only one network and not needing to sustain a legacy telephony system in an increasingly digital/data centered world. Also, the network administrator's burden may be lessened as they can now focus on a single network. There is no longer a need for several teams to manage a data network and another to mange a voice network. The simplicity of VOIP systems is attractive, one organization / one network; but as we shall see, the integration of security measures into this architecture is very complex.

In theory, VOIP can provide reduced bandwidth use and quality superior to its predecessor, the conventional PSTN. That is, the use of high bandwidth media common to data communications, combined with the high quality of digitized voice, make VOIP a flexible alternative for speech transmission.

In practice, however, the situation is more complicated. Routing all of an organization's traffic over a single network causes congestion and sending this traffic over the Internet can cause a significant delay in the delivery of speech. Also, bandwidth usage is related to digitization of voice by codecs, circuits or software processes that code and decode data for transmission. That is, producing greater bandwidth savings may slow down encoding and transmission processes. Speed and voice quality improvements are being made as VOIP networks and phones are deployed in greater numbers, and many organizations that have recently switched to a VOIP scheme have noticed no significant degradation in speed or quality.[2]

With the introduction of VOIP, the need for security is compounded because now we must protect two invaluable assets, our data and our voice. Federal government agencies are required by law to protect a great deal of information, even if it is unclassified. Both privacy-sensitive and financial data must be protected, as well as other government information

that is categorized as sensitive but unclassified. Protecting the security of conversations is thus required.

In a conventional office telephone system, security is a more valid assumption. Intercepting conversations requires physical access to telephone lines or compromise of the office private branch exchange (PBX). Only particularly security-sensitive organizations bother to encrypt voice traffic over traditional telephone lines. The same cannot be said for Internet-based connections.

For example, When ordering merchandise over the phone, most people will read their credit card number to the person on the other end. The numbers are transmitted without encryption to the seller. In contrast, the risk of sending unencrypted data across the Internet is more significant. Packets sent from a user's home computer to an online retailer may pass through 15-20 systems that are not under the control of the user's ISP or the retailer. Because digits are transmitted using a standard for transmitting digits out of band as special messages, anyone with access to these systems could install software that scans packets for credit card information.

For this reason, online retailers use encryption software to protect a user's information and credit card number. So it stands to reason that if we are to transmit voice over the Internet Protocol, and specifically across the Internet, similar security measures must be applied. The current Internet architecture does not provide the same physical wire security as the phone lines. The key to securing VOIP is to use the security mechanisms like those deployed in data networks (firewalls, encryption, etc.) to emulate the security level currently enjoyed by PSTN network users.[3]

C. Gamma Distribution Function

Initial key is not simply collected by generated random number. First key which is got from Math.random, is calculated by Chi Square distribution function to get second key. This is another complicated function for attackers. Chi square is the special case of the gamma distribution function.

III. OVERALL SYSTEM DESIGN

Encryption side should initiate with decryption side before encryption and decryption take place. If the status is ready for the decryption side, encryption side will continue the encryption process. Before encryption, the Encryption System need to capture sound signals through sound card.

The final state is making cipher text by using key stream generated by key stream generator. Key stream generator needs to re-generate regularly after encryption of a block of a plain text. The decryption side will process the decryption by using synchronous random generator for key generation. And regenerate the sound signals.

This system firstly generate random key (first key) and send this key to the Client. Second key is calculated from first key by using Chi Square Distribution Function. The result is put into the LFSR. The captured sound is then encrypted using the key from LFSR. And then Encrypted sound is sent to Client.

Client is accepted Encrypted speech signals. These signals are put into the LFSR. Then the results from LFSR are decrypted. Finally, Client hears original sound. If speaking continues, sound will be captured. Unless speaking continues, the system will be stop.

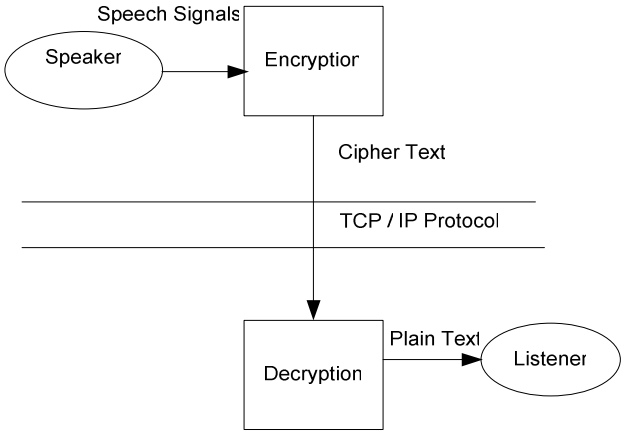

Fig.1 Block Diagram of the System

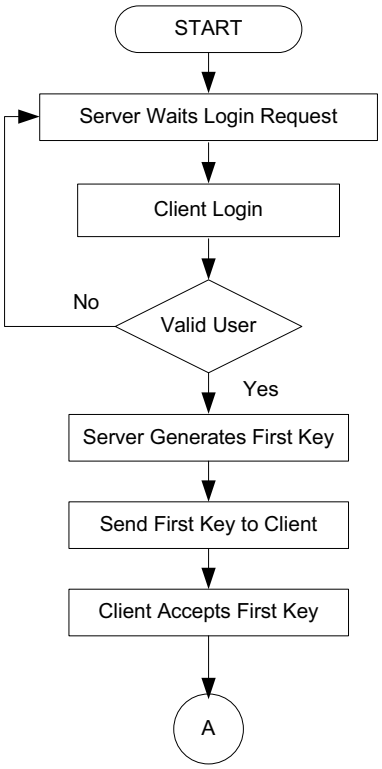

Fig.2 (a) Overall System Design

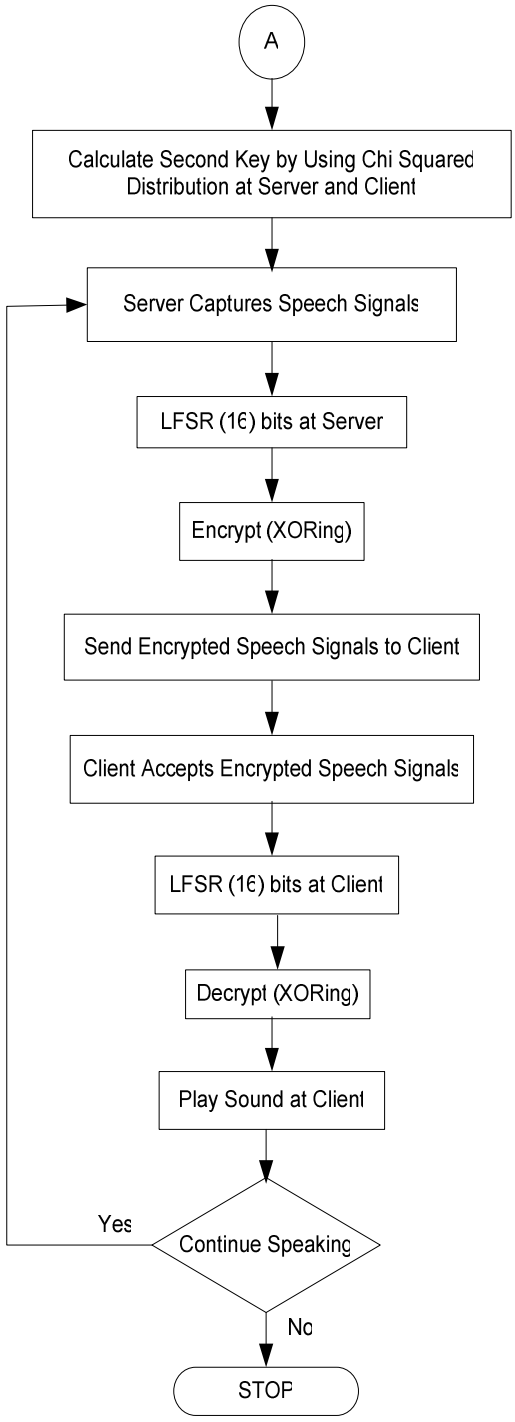

Fig.2(b) Overall System Design

IV. Test and Result

The whole system is the combination of LFSR Encryption of sound signals and LFSR Decryption of sound signals. The system is implemented by Java. This system involves two tests and results. They are

- Encrypted VoIP with Non-Decrypted VoIP
- Complete Encryption-Decryption VoIP.

First testing is LFSR Encryption Server with the Client which does not have decryption module. This testing can also be called attack.

At Encryption side, port number is assigned. And then user information must be entered. If Start button is clicked, Server will wait for the connection from the Client. This situation is shown in Fig 3.

At Decryption side, correct user name and password are entered. Server Address and Server Port are then assigned. If Connect button is clicked, Client will connect to Server. The connection become between Server and Client.

If user name or password is wrong, there will be a connection between Server and Client. But "invalid user" message is shown at Client.

If user information is true, the speech result cannot be decrypted and unclear speech can only be heard at client side. Fig 4 and 5 are tests and results of Encrypted VoIP with Non-Decrypted VoIP.

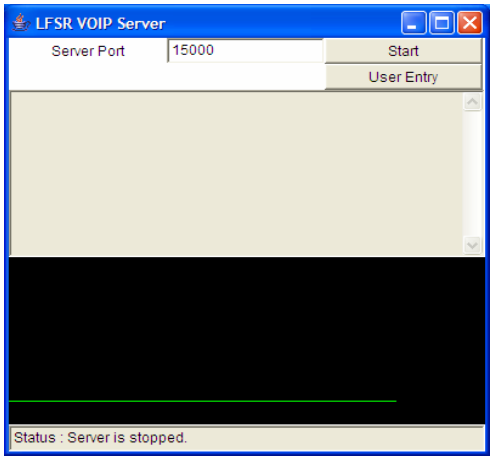

Fig.3 LFSR VOIP Server Waits for Connection

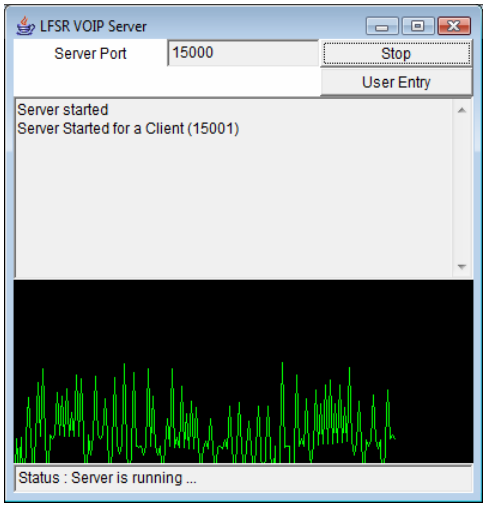

Fig.4 LFSR VoIP Server Encrypts Speech

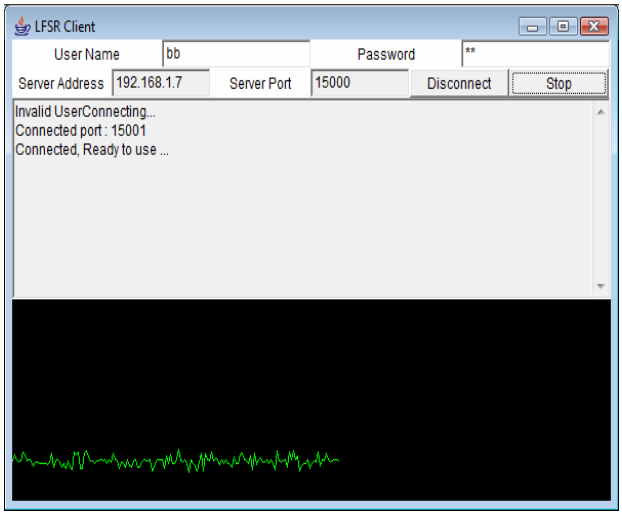

Fig.5 LFSR Client does not Decrypt Speech

Another one is complete LFSR encryption server and decryption client. This is the major testing of the system.

At Encryption side, port number is assigned. And then user information must be entered. If Start button is clicked, Server will wait for the connection from the Client.

At Decryption side, correct user name and password are entered. Server Address and Server Port are then assigned. If Connect button is clicked, Client will connect to Server. The connection become between Server and Client.

If user name or password is wrong, there will be a connection between Server and Client. But "invalid user" message is shown at Client.

If user information is true, the speech result can be decrypted and can be heard at client side.

Fig 6 and 7 are tests and results of Complete Encryption-Decryption VoIP.

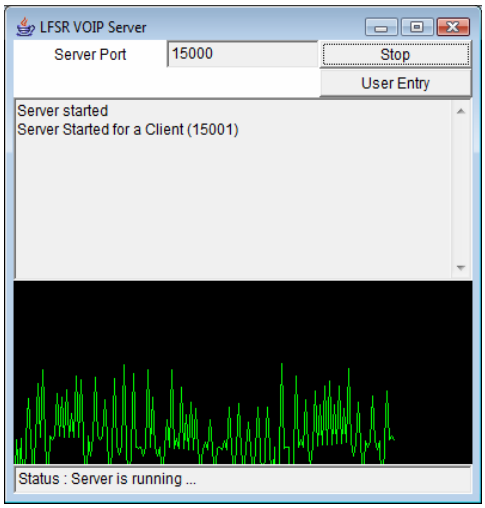

Fig.6 LFSR VOIP Server

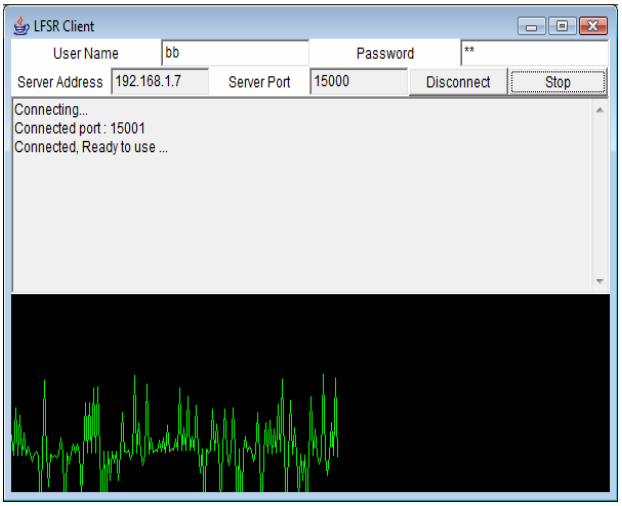

Fig.7 LFSR Client Decrypts Speech

V. Conclusion

Symmetric algorithms are those where the encryption key and the decryption key are the same or are calculated from each other. If the algorithm uses a single key for both encryption and decryption, then it is called as a single-key algorithm.

Stream ciphers are an important class of encryption algorithms. They encrypt individual characters (usually binary digits) of a plaintext message one at a time, using an encryption transformation which varies with time.

By contrast, numerous concrete block cipher proposals have been published, some of which have been standardized or placed in the public domain. Nevertheless, because of their significant advantages, stream ciphers are widely used today, and one can expect increasingly more concrete proposals in the coming years.

The limitation of this program is to communicate between two users. The algorithm for broadcasting of speech is not considered in this thesis. Java 2 and media frame work will need to run this program. Only TCP/IP network communication protocol can use for this program.

While there are a number of VoIP solutions available today, most of these have limitations of one kind or another. In some cases the solutions are built on early versions of standards and provide restricted interoperability with other vendors. In some cases the solutions do not provide the scalability, robustness, security or features required. The LFSR is committed to providing a next generation network that provides both full multi-vendor interoperability, and support for a full featured, secure service. The next step is to develop a coherent solution for scaleable next generation networks that support end-to-end VoIP. This will build on the proven methodology the LFSR. It will identify open interfaces and define Implementation Agreements for these interfaces. The LFSR will then produce test plans and conduct interoperability testing to accelerate the deployment of next generation networks. It is the aim of the LSFR to shorten the timescales in which end-to-end VoIP

solutions become available, and to accelerate the transition of carrier TDM voice networks to VoIP networks.

ACKNOWLEDGMENT

Firstly, the author is very grateful to U Thaung, Minister, Ministry of Science and Technology, for opening Master Degree program at West Yangon Technological University.

The author is very thankful to Dr. Khin Maung Aye, the Rector of West Yangon Technological University, for his motivation and support during the paper.

The author would like to express her heart-felt gratitude to Dr. Htun Htun, Lecturer and Head, Department of Information Technology, West Yangon Technological University, for editing her paper and accomplished guidance, for her willingness to share ideas and helpful suggestions throughout dissertation.

The author is especially grateful to her supervisor, Dr. Aye Aye Nyein, Deputy Professor and Head, Department of Electronic Engineering, West Yangon Technological University, for her valuable guidance, a lot of inspiration, motivation and encouragement during paper.

The author wishes to thank U Win Khaing Moe, Deputy Director General, Myanma Scientific and Technological Research Department, for his willingness to share his ideas during presentation.

The author wishes to thank the member of Examiners, Daw Aye Aye Tun, Lecturer, Department of Electronic Engineering, West Yangon Technological University, for her effective guidance, kind help and support during paper.

The author is also thankful to the member of Examiners, U Tin Maung Win, Assistant Lecturer, Department of Information Technology, West Yangon Technological University, for his valuable advice and correction on this paper.

The author would like to express her gratitude and appreciation to her dear parents and all her teachers who taught every thing since her childhood.

Finally, the author is very thankful to all her teachers, Department of Electronic Engineering and Information Technology, West Yangon Technological University, for their valuable guidance towards the successful completion of this paper.

REFERENCES

[1] Dao Q. Van, Anne Weiz and Benot Geller, Improving End to End Latency for Voice over IPSec Streams.

[2] D. Minoli and E. Minoli, Delivering Voice over IP Networks, New York: John Wiley & Sons, 1998.

[3] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, Security Considerations for voice Over IP Systems.

[4] P. Alfke, "Efficient Shift Registers, LFSR Counters, and Long Pseudo-Random Sequence Generators," Xilinx, Tech. Rep., 1996, [10] Qiu-Hua Lin, Fu-Liang Yin, Tie-Min Mei, and Hualou Liang, A Blind Source Separation Based Method for Speech Encryption.

Ms. Tin Lai Win (M'06) became a Member (M) of **MES (MYANMAR ENGINEERING SOCIETY)** in 2006. The author was born at Laputta Township, Ayeyarwadi Division, Myanmar in 1983. The author has got Bachelor of Engineering in information technology, Thanlyin Technological University, Yangon, Myanmar, 2006 and Master of Engineering in information technology, West Yangon Technological University, Yangon, Myanmar, 2008.

Now, She is a Ph.D student of Department of Technical and Vocational Education, Myanmar