Voice Encryption in GSM Network Using RC4 Algorithm

تشفير الصوت في شبكات الهاتف السيار باستخدام خوارزمية RC4

Sudan University of Science & Technology

College of Graduate of Studies

Supplementary Research submitted In Partial Fulfillment of

The Requirements

For the Degree of Master in Computer Science

By:

Nuha Hussein Abd Alrazig Ali

Supervisor:

Dr. Faisal Mohammed Abdallaha

JUNE 2015

Approval Page

Name of Candidate: Nuha Hussein Abd Alrazig Ali

Thesis title: Encryption of Voice in Global System Networks using RC4 Algorithm

Approved by:

1. External Examiner

Name: Ali Ahmed Alfakialdalla

Signature: ..... Date: 02/06/2015

2. Internal Examiner

Name: Dr. Abuagla Babiker Mohammed Babiker

Signature: ..... Date: 2/6/2015

3. Supervisor

Name: Faisal Mohammed Abdalla

Signature: ..... Date: 2-6-2015

Sudan University of Science and Technology
College of Graduate Studies

Declaration

I, the signing here-under, declare that I'm the sole author of the (M.Sc.) thesis entitled

Voice Encryption In GSM Network Using RC4 Algorithm

which is an original intellectual work. Willingly, I assign the copy-right of this work to the College of Graduate Studies (CGS), Sudan University of Science & Technology (SUST). Accordingly, SUST has all the rights to publish this work for scientific purposes.

Candidate's name: Nuha Hussein Abd ALrazig ALi

Candidate's signature: ..... **Date:** 7-9-2015

إقرار

أنا الموقع أدناه أُقر بأننى المؤلف الوحيد لرسالة الماجستير المعنونة

تشفير الصوت في شبكات الهاتف السيار
باستخدام خوارزمية RC4

وهى منتج فكري أصيل . وباختياري أعطى حقوق طبع ونشر هذا العمل لكلية الدراسات العليا - جامعه السودان للعلوم والتكنولوجيا، عليه يحق للجامعه نشر هذا العمل للأغراض العلمية .

اسم الدارس : نهى حسين عبد الرازق علي

توقيع الدارس : ..... التاريخ : 7/9/2015

الايـــة

﴿وَقُل رَّبِّ أَدْخِلْنِي مُدْخَلَ صِدْقٍ وَأَخْرِجْنِي مُخْرَجَ صِدْقٍ وَاجْعَل لِّي مِن لَّدُنكَ سُلْطَانًا نَّصِيرًا ﴾

سورة الإسراء الاية ﴿80﴾

﴿**Say: 'Lord, grant me an entrance of sincerity and an exit of sincerity, and give me from Yours a victorious power**﴾

Al-'Isra' ﴿80﴾

Dedication

I dedicate this project to my parents and all the students , teachers of

Sudan University of Science & Technology

May this project be a source of inspiration for all of them

شكر وتقدير

بسم الله الرحمن الرحيم والحمد لله رب العالمين ، سبحان الذي بيده ملكوت كل شئ وهو على كل شئ قدير وما توفيقي الا بيده سبحانه والصلاة والسلام على امام المرسلين نبينا محمد صلى الله عليه وسلم .

انجاز هذا البحث كان بالمعنى الحقيقي فرصة لنا لتجربة واتقان مهارات جديدة والتعرف على اشخاص مختلفين والتعاون معهم في مختلف مراحل البحث . كما انه ليس نتيجة جهدنا الخاص فقط ولكن بمساعدتهم وتوجيهم لنا في مراحل ومواضيع البحث المختلفة لذا اود ان اشكرهم جميعاً . واخص بالشكر **د. فيصل محمد عبد الله** والذي بذل كل ما في وسعه باشرافه وتوجيه لنا في كل مراحل البحث .

وكل الحب والاحترام لوالدي الحبيبين اللذان قدما لي كل الحب والدعم والتوجيه في مراحل الحياة المختلفة .

Acknowledgements

In the name of Almighty Allah, The most Beneficent, The most Merciful. Completing the project was in the true sense a great learning opportunity which provided us a chance to experience and master new skills, meet different people and collaborate with them. Though this project was the result of our own effort but we could not have reached this far, if it would not have been the guidance of various persons who helped us in different aspects.

We would like to thank all those people who guided and helped us in completion of this project. Starting with our project supervisor **Dr. Faisal Mohammed Abd allaha** who was always with us throughout the project and helped us in every way he could ,and different people who helped us in understanding the various issues regarding modulation, synchronization and demodulation of the GSM waveform.

We are grateful to our beloved parents who provided their complete support, help and advice in every part of our lives.

Abstract

Mobile telecommunications such as Global System for Mobile Communication (GSM) are now well established globally and users rely heavily on the convenient communications it provides. The level of security provided by GSM is superior to its predecessors and is more than adequate for the majority of users. However, some users in the areas of government, defense or business require more security over and above that provided by the GSM standards and by standard GSM equipment. In a GSM network, only the radio channels between the mobile station (MS) and the base transceiver station (BTS) are encrypted. This research presents methodology for implementation of end-to-end security over the available GSM infrastructure by adding encryption algorithm (RC4 algorithm) to standard GSM. The communications between parties is encrypted in GSM environments and simulation is carried using MATLAB software as simulation tool the results show that's the proposed method can be applied and without any modification to GSM standard and optimum result can be obtained.

الخلاصة

يلعب التشفير الصوتي دورا كبيرا في العديد من أنظمة الاتصالات الهامة، مثل أنظمة الاتصالات العسكرية، ونظام الاتصالات والبنوك والاعمال والافراد . يقدم هذا البحث نظاما مقترحا لتطبيق تشفير الصوت من النهاية (موبايل) للنهاية (موبايل) على شبكة الهاتف الخليوي (GSM) . في معيار (GSM) يتم استخدام خوارزمية التشفير (A5) فقط ما بين الهاتف ومحطة الارسال والاستقبال اما في بقية مكونات الشكبة فلا يوجد تشفير ترسل البيانات كما هي ، لذا قمنا في هذا البحث باقتراح تطبيق التشفير من النهاية للنهاية باضافة خوارزمية (RC4) لضمان التشفير الكامل للبيانات على كل الشبكة .

تم استخدام برمجية الماتلاب (MATLAB) كاداة محاكاة (GSM) وتم الحصول على أفضل النتائج في سياق امن الصوت والجودة.

Table of Contents

List of Figures

Chapter “1”

Introduction

1.1 Background :

Wireless Networks share many common characteristics with traditional wire-line networks such as public switch telephone/data networks, and hence many security issues with the wire-line networks also apply to the wireless environment. The GSM system doesn't provide end-to-end security and lacks in provision of traffic confidentiality to its subscribers. Anonymity, authentication, and confidentiality are the security services which are offered by the world's largest mobile telephony system. Still this system is defenseless against many attacks and fails to ensure taut safety of the user's telephone conversations and data transfer sessions. Confidentiality of transmitted data is achieved by encrypting the information flow between the communicating parties. In GSM networks, only the radio link between the mobile terminal and the base station is encrypted whereas the rest of the network transmits data in clear-text. Radio link confidentiality in GSM is not sufficient for attaining end-to-end security. As a result, a need for investigating mechanisms for implementing absolute confidentiality of traffic arises.

In this research, a new method for securing GSM mobile networks is proposed, using MATLAB software as simulator in GSM environments . MATLAB (Matrix Laboratory) becomes the de facto tool in digital signal processing. MATLAB is a well-known tool for numerical calculations, this research employs its features as simulation of GSM environment. This makes MATLAB a perfect tool for the application this research deals with.

1.2 Problem Statement :

GSM is one of the most commonly used cellular technologies in the world, used by governments, banks, companies, business and individuals. GSM as many wireless technologies suffer from interception and eavesdropping of the transmission speech. GSM employs many cryptographic algorithms for security like A5/1, A5/2 and A5/3. Even so, these algorithms do not provide sufficient level of security such as confidentiality in GSM environment. Therefore, it is desirable to increase security by providing end-to-end voice encryption to solve this problem.

1.3 Scope of Research:

GSM, like many other widely used systems, security is crucial. The security involves mechanisms used to protect the different shareholders, like subscribers and service providers. The aspects of security that this thesis covers are mainly authentication and confidentiality. The important aspects of the system that need protection are described, along with the implementation of mechanisms used for the protection. It appears that many of the very valuable aspects of GSM can be attacked.

The anonymity of a GSM user is compromised resulting in the attacker being able to observe the time, rate, length, sources or destinations of calls. Even tracking a subscriber's movements becomes possible. However, a passive attack is not sufficient to perform these attacks. The attacker needs to mount an active attack using equipment offering base station functionality.

Authentication is a crucial aspect of a wireless communication system due to the nature of the medium used, i e the radio link that is available to everyone and not only the legitimate entities. Even the authentication mechanisms are attacked. It is possible to clone a subscription either by having physical access to the smart card

or over the air interface. Cloning a subscription over the air requires base station functionality.

The most obvious threat against communication systems is eavesdropping on conversations. The privacy of GSM conversations is protected using some version of the A5 algorithm. There are several impressive crypt analytical attacks against these algorithms, that break the encryption and make it possible to eavesdrop in real-time. Most of these algorithms require, however, extensive computation power and unrealistic quantities of known plaintext, which make it difficult to use them in practice. Difficulties using crypt analytical attacks to break the confidentiality of GSM calls do not mean that conversations are well protected. In this research RC4 algorithm is used in GSM network in order to provide confidentiality by encrypting speech inside network, encryption is a well-established technology for protecting sensitive data. Anyone having access to the encrypted data cannot learn anything about the sensitive data without the encryption key. A method for authentication to user at different sides of communication channel also provided.

1.4 Research objectives :

The primary goal of this research was to achieve end –to – end calls security in GSM by adding simple, fast and strong algorithm in GSM handset standard at end point (mobile station). This will done by design a MATLAB module simulate GSM environment, Also to avoid using the same keystream in more than one session.

1.5 Thesis Structure

This Research is divided into 5 chapters. Chapter 1 introduces the background, Scope of research, problem definition and Objectives. Chapter 2 provides a GSM foundation, making the reader capable of understanding the Chapter 1 and related studies. Chapter 3 contains the methodology. Chapter 4 contains the implementation of proposed method using MATLAB software. This is followed by a conclusion and future work in chapter 5. The research also provides 3 appendices, as well as a list of acronyms, output and definitions at the end.

Chapter “2”

Literature & Related Studies

2.1 GSM

GSM (Global System for Mobile Communications) is a digital cellular technology used for transmitting voice and data services. GSM allows users to roam seamlessly from one network to another, while also providing personal mobility. In addition, both speech and signaling channels are digitalized, which essentially labeled GSM as the second-generation (2G) mobile system. Since its first launch in 1991, GSM rapidly became the most popular mobile phone system in the world. In June 2010, an estimated 4.4 billion subscribers across more than 219 countries were using GSM or 3GSM.

2.1.1 GSM Generations :

a. **1st Generation:** (NMT, C-Nets, AMPS, TACS) are considered to be the first analog cellular systems, which started early 1980s. There were radio telephone systems even before that. 1G networks were conceived and designed purely for voice calls with almost no consideration of data services (with the possible exception of built-in modems in some headsets)[3].

b. **2nd Generation:** (GSM, CDMA One, D-AMPS) are the first digital cellular systems launched early 1990s, offering improved sound quality, better security and higher total capacity. GSM supports circuit-switched data (CSD), allowing users to place dial-up data calls digitally, so that the network's switching station receives actual ones and zeroes rather than the screech of an analog modem[3].

c. **2.5G Generation:** (GPRS, CDMA2000 1x) are the enhanced versions of 2G networks with theoretical data rates up to about 144kbit/s. GPRS offered the first always-on data service[3].

d. **3rd Generation:** (UMTS FDD and TDD, CDMA2000 1x EVDO, CDMA2000 3x, TD-SCDMA, Arib WCDMA, EDGE, IMT-

2000 DECT) are newer cellular networks that have data rates of 384kbit/s and more.

The UN's International Telecommunications Union IMT-2000 standard requires stationary speeds of 2Mbps and mobile speeds of 384kbps for a "true"3G[3].

e. 4th Generation: technology refers to the fourth generation of mobile phone communication standards. LTE and WiMAX are marketed as parts of this generation, even though they fall short of the actual standard. The ITI has taken ownership of 4G, bundling into a specification known as IMT-Advanced. The document calls for 4G technologies to deliver downlink speeds of 1Gbps when stationary and 100Mbps when mobile, roughly 500-fold and 250-fold increase over IMT-2000 respectively. Unfortunately, those specs are so aggressive that no commercialized standard currently meets them[3].

Historically, WiMAX and Long-Term Evolution (LTE), the standard generally accepted to succeed both CDMA2000 and GSM, have been marketed and labeled as "4G technologies," but that's only partially true: they both make use of a newer, extremely efficient multiplexing scheme (OFDMA, as opposed to the older CDMA or TDMA) however, WiMAX tops at around 40Mbps and LTE at around 100Mbps theoretical speed. Practical, real-world commercial networks using WiMAX and LTE range between 4Mbps and 30Mbps. Even though the speed of WiMAX and LTE is well short of IMT-Advanced standard, they're very different than 3G networks and carriers around the world refer to them as "4G". Updates to these standards -- WiMAX 2 and LTE-Advanced, respectively -- will increase throughput further, but neither has been finalized yet.

2.1.2 GSM Architecture :

Cellular communication means that there are a lot of different areas, looks like cell, contain communication system devices, such as antennas, base stations[1][2][7].

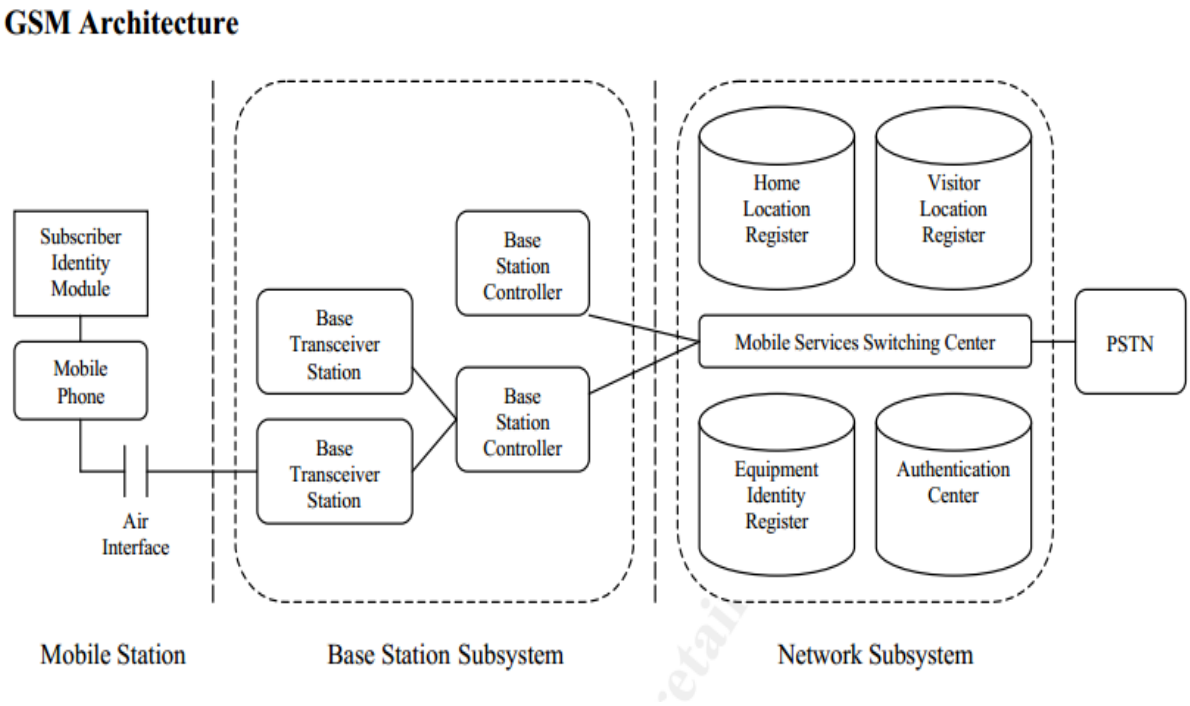


Figure (2-1) GSM architecture

According to above Figure (2-1) the architecture of GSM [2] as follows :

2.1.2.1 Mobile Station :

Every GSM mobile phone has :

a- Subscriber Identity Module (SIM)

- Smart Card containing keys IMSI and Ki , identifiers .
- Contain A3/A8 algorithms.

b- Mobile Equipment (ME)

- Physical mobile device
- International Mobile Equipment Identities (IMEI) reveals the serial number of the mobile station, manufacturer, type approval and country of production.
- It contain A5 algorithm.

2.1.2.2 Base Station Subsystem (BSS) :

The role of the Base Station Subsystem (BSS) is to connect the user on a mobile phone with other landline or mobile users. The Base Transceiver Station (BTS) is in direct contact with the mobile phones via the air interface and can be thought of as a complex radio modem. The Base Station Controller (BSC) is responsible for the control of the several BTS. It monitors each call and decides when to handover the call from one BTS to another, as well as manage radio frequencies allocated for the calls through the BTS.

a. Base Transceiver Station (BTS) :

- The Base Transceiver Station belonging to a PLMN serving the MS. Base stations form a patchwork of radio cells over a given geographic coverage area. Base Stations are connected to base station controllers (BSC).

b. Base Station Controller (BSC) :

- It is a node controlling a number of BTS, coordinating handovers and performing BS co-ordination not related to switching. The BSC to BTS link is in many cases a point to point microwave link. BSC are also connected to mobile switching centers (MSC) via fixed or microware links.

2.1.2.3 Network Subsystem (NSS) :

It is a complete exchange, capable of routing calls from a fixed network via the BSC and BTS to an individual mobile station. The Mobile Services Switching Center (MSC) interconnects the cellular network with the Public Switched Telephone Network (PSTN). The MSC also serves to co-ordinate setting up calls to and from GSM users.

2.1.2.4 Home Location Register (HLR):

A database which stores data about GSM subscribers, including the Individual Subscriber Authentication Key (Ki) for each Subscriber Identity Module (SIM).

2.1.2.5 Visitor Location Register (VLR):

contains relevant information for all mobiles currently served by a MSC. The permanent data stored in the VLR is also stored in the HLR. In addition, it also stores the Temporary Mobile Subscriber Identity (TMSI), which is used for limited intervals to prevent the transmission of the IMSI via the air interface.

2.1.2.6 Equipment Identity Register (EIR) :

stores all the International Mobile Equipment Identities (IMEI) of mobile equipment and their rights on the network.

2.1.2.7 The Authentication Center (AuC) :

is a protective database that houses the KI, the A3 authentication algorithm, the A5 ciphering algorithm and the A8 ciphering key generating algorithm. It is responsible for creating the sets of random numbers (RAND), Signed Response (SRES) and the Cipher key (KC), though the created sets are stored in the HLR and VLR.

2.1.3 GSM Features

The GSM distingue by[6] [15][25]:

- Total Mobility.
- High Capacity and Optimal Spectrum Allocation.
- Security.
- Services:

The list of services available to GSM subscribers typically includes the following[6][15][25]:

- Tele Services: Includes mobile phones, emergency calling etc.
- Data services: Includes SMS (Short message service), fax, voicemail, electronic mail.
- Supplemental services: such as call forwarding, call hold, call waiting, conference, etc

2.1.4 GSM Security

The security methods standardized for the GSM System make it the most secure cellular telecommunications standard currently available. Although the confidentiality of a call and anonymity of the GSM subscriber is only guaranteed on the radio channel, this is a major step in achieving end-to- end security. The subscriber's anonymity is ensured through the use of temporary identification numbers(TMSI). The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling [4][5][6].

2.1.5 Algorithms to Secure voice in GSM:

There are three algorithms which are used in the GSM security A3 acts as the authentication algorithm , A8 algorithm acts the session key algorithm and A5, the stream-ciphering algorithm and among this A5 algorithm, there are many other versions too, each having its separate functionality. These are: A5, A5/1, A5/2, A5/3 and so on. Among these algorithms some operators do not use any encryption for voice / data traffic at all and some which works on these algorithms, works on 3G technology so they use A5/3 algorithm.

2.1.5.1 A5/1 Algorithm:

An A5/1 algorithm is the strong over the air privacy algorithm. it's only in practice by members of European Conference of Postal and Telecommunication Administrations (CEPT) countries but the key for encryption of this algorithm is 64 bits which is standard used. The A5/1algorithm does network based encryption i.e. it is used at the corner of the GSM network for encrypting the links between the Mobile Station (MS) &Base transceiver system (BTS) and vice versa.

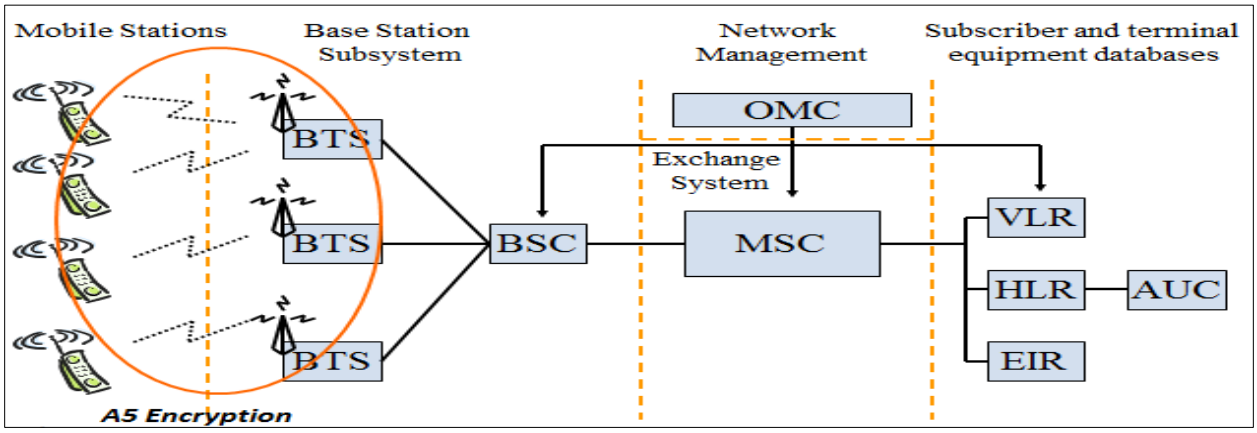
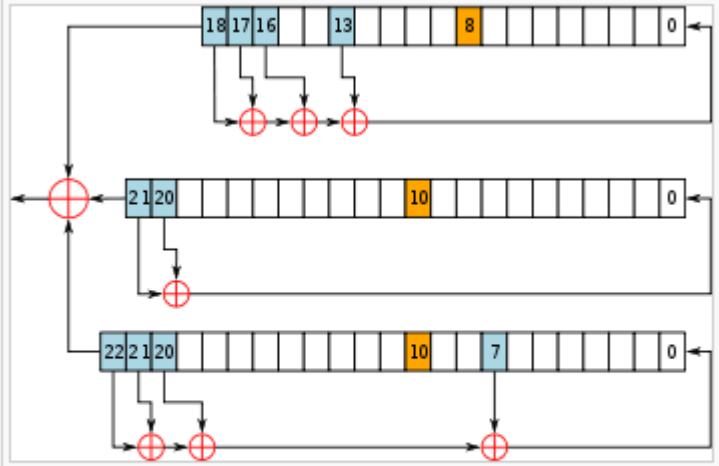


Figure (2-2) A5 Encryption

Description : A GSM transmission is organized as sequences of bursts. In a typical channel and in one direction, one burst is sent every 4.615 milliseconds and contains 114 bits available for information. A5/1 is used to produce for each burst a 114 bit sequence of keystream which is XORed with the 114 bits prior to modulation. A5/1 is initialized using a 64-bit key together with a publicly known 22-bit frame number. Older fielded GSM implementations using Comp128v1 for key generation, had 10 of the key bits fixed at zero, resulting in an effective key length of 54 bits. This weakness was rectified with the introduction of Comp128v2 which yields proper 64 bits keys. When operating in GPRS / EDGE

mode, higher bandwidth radio modulation allows for larger 348 bits frames, and A5/3 is then used in a stream cipher mode to maintain confidentiality.



The A5/1 stream cipher uses three LFSRs. A register is clocked if its clocking bit (orange) agrees with one or both of the clocking bits of the other two registers.

Figure (2-3) A5 works

A5/1 is based around a combination of three linear feedback shift registers (LFSRs) with irregular clocking. The three shift registers are specified as follows Table (1):

Table (1) Registers used in A5

LFSR No.	Length in bits	Feedback polynomial	Clocking bit
1	19	X19+X18+X17+X14+1	8
2	22	X22+X21+1	10
3	23	X23+X22+X21+X8+1	10

The bits are indexed with the least significant bit (LSB) as 0.

The registers are clocked in a stop/go fashion using a majority rule. Each register has an associated clocking bit. At each cycle, the clocking bit of all three registers

is examined and the majority bit is determined. A register is clocked if the clocking bit agrees with the majority bit. Hence at each step at least two or three registers are clocked, and each register steps with probability 3/4.

Initially, the registers are set to zero. Then for 64 cycles, the 64-bit secret key is mixed in according to the following scheme: in cycle $0 \le i \le 64$, the ith key bit is added to the least significant bit of each register using :

$$XOR - R[0] = R[0] \oplus K[i]$$

Each register is then clocked.

Similarly, the 22-bits of the frame number are added in 22 cycles. Then the entire system is clocked using the normal majority clocking mechanism for 100 cycles, with the output discarded. After this is completed, the cipher is ready to produce two 114 bit sequences of output keystream, first 114 for downlink, last 114 for uplink.

Security : A number of attacks on A5/1 have been published, and the American National Security Agency is able to routinely decrypt A5/1 messages according to released internal documents.

Some attacks require an expensive preprocessing stage after which the cipher can be broken in minutes or seconds. Until recently, the weaknesses have been passive attacks using the known plaintext assumption.

2.1.6 GSM Speech Coding :

Speech coding is an application of data compression of digital audio signals containing speech. Speech coding uses speech-specific parameter estimation using audio signal processing techniques to model the speech signal, combined with generic data compression algorithms to represent the resulting modeled parameters in a compact bit stream. The two most important applications of speech coding are mobile calls and Voice over IP .

There is three speech coding algorithms are part of GSM standard. The purpose of these coders is to compress the speech signal before its transmission, reducing the number of bits needed in its digital representation, while keeping an acceptable quality of the decoded output see figure (5). As GSM transcoding (the process of coding and decoding) modifies the speech signal, it is likely to have an influence on speaker recognition performance, together with other perturbations introduced by the mobile cellular network (channel errors, background noise)[16].

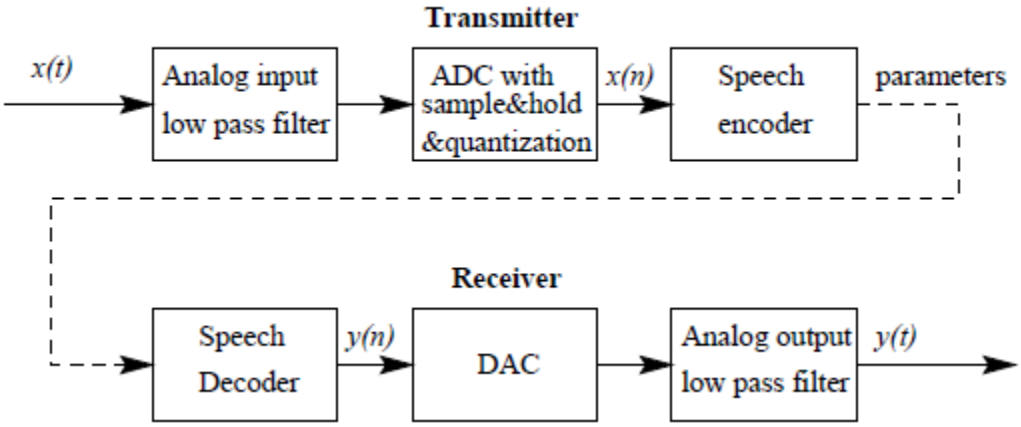


Figure (2-4): Basic structure of all digital speech coders

2.1.6.1 GSM Speech Coders :

There exist three different GSM speech coders, which are referred to as the full rate, half rate and enhanced full rate GSM coders. These coders work on a 13 bit uniform PCM speech input signal, sampled at 8 kHz. The input is processed on a frame-by-frame basis, with a frame size of 20 ms (160 samples). A brief description of these coders follows.

- **Full Rate (FR)** :

  The FR coder was standardized in 1987. This coder belongs to the class of Regular Pulse Excitation - Long Term Prediction - linear predictive (RPE-LTP) coders. In the encoder part, a frame of 160 speech samples is encoded as a block of 260 bits, leading to a bit rate of 13 kbps. The decoder maps the encoded blocks of 260 bits to output blocks of 160

reconstructed speech samples. The GSM full rate channel supports 22.8 kbps. Thus, the remaining 9.8 kbps are used for error protection .

- **Half Rate (HR)** :

  The HR coder standard was established to cope with the increasing number of subscribers. This coder is a 5.6 kbps VSELP (Vector Sum Excited Linear Prediction) coder from Motorola . In order to double the capacity of the GSM cellular system, the half rate channel supports 11.4 kbps. Therefore, 5.8 kbps are used for error protection. The measured output speech quality for the HR coder is comparable to the quality of the FR coder in all tested conditions , except for tandem and background noise conditions.

- **Enhanced Full Rate (EFR)** :

  The EFR coder was the latest to be standardized. This coder is intended for utilization in the full rate channel, and it provides a substantial improvement in quality compared to the FR coder . The EFR coder uses 12.2 kbps for speech coding and 10.6 kbps for error protection. The speech coding scheme is based on Algebraic Code Excited Linear Prediction (ACELP).

2.2 RC4 Algorithm :

This stream cipher was invented in 1987 by Ron Rivest, one of the inventors of the RSA public key cryptography algorithm and co-founders of RSA security. Even though the RC4 cipher is officially named "Rivest Cipher 4", it is also known as "Ron's Code 4".. It is a widely used stream cipher. RC4 had a really large success thanks to its simplicity and efficiency. The primary advantage of a stream cipher is that stream ciphers are almost always faster and use far less code than do block ciphers. RC4

can be implemented in just a few lines of code. Table (1), compares execution times of RC4 with three well-known symmetric block ciphers[19]. RC4 was used in many popular standards and protocols such as WEP, WPA, SSL or TLS.

There are three major components to the RC4 encryption process:

1. The secret key
2. The key-scheduling algorithm (KSA)
3. The pseudo-random generation algorithm (PRGA).

The RC4 algorithm can be implemented in the four :

Step 1: Secret key is created, which at simplest term is a password.

Step 2: The secret key is used to generate the state table using the KSA algorithm.

Step 3: The state table is used to generate a random pseudo bit stream using the PRGA algorithm.

Step 4: The random pseudo bit stream is XOR'd with the plaintext to create the cipher text.

Table (1) Speed Comparisons of Symmetric Ciphers on a Pentium II

Cipher	Key Length	Speed (Mbps)
DES	56	9
3DES	168	3
RC2	variable	0.9
RC4	variable	45

2.3 Related Studies:

2.3.1 Khaled Merit and Abdelazziz Ouamri [11] in their paper were proposed a method to fulfill the end-to-end secure communication in the GSM voice channel. They used Data Encryption Standard algorithm (DES with random permutation and Inverse) with proposed method to solves the problem of adjustable of that traditional encryption algorithms with RPE-LTP vocoder requirements and constrains in GSM system figure [6]. In addition, this encryption method has the advantages of suiting the RPE-LTP compression module requirements, good compatibility to GSM networks, and suitable implementation without any adjustment in current GSM signaling system.

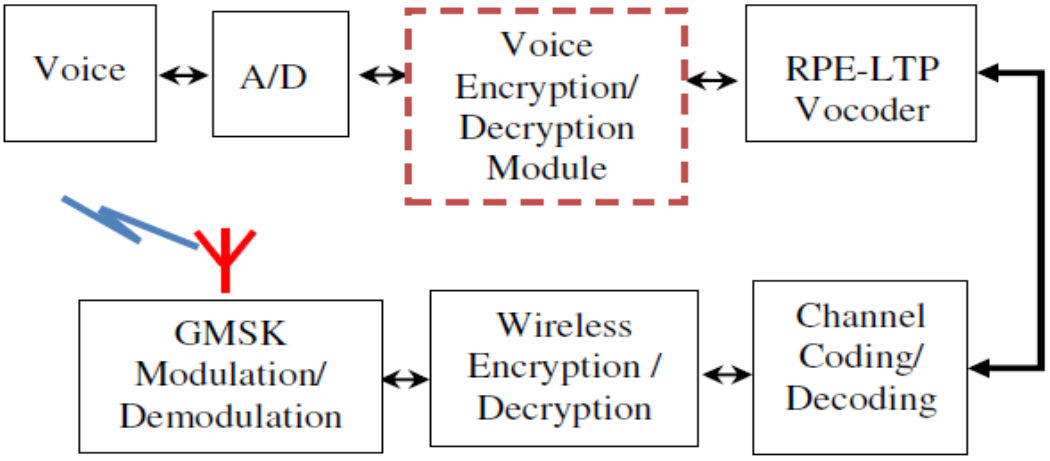


Figure (2-5): proposed system

2.3.2 Himanshu Gupta and Dr. Vinod Kumar Sharma [12] in their paper explore the role of multiple encryption in secure voice communication over the insecure network figure (2-6). It provides high level security for voice communication. Multiple encryption of voice data can uproot the problem of information theft during the communication through telephone, mobile phone, etc.

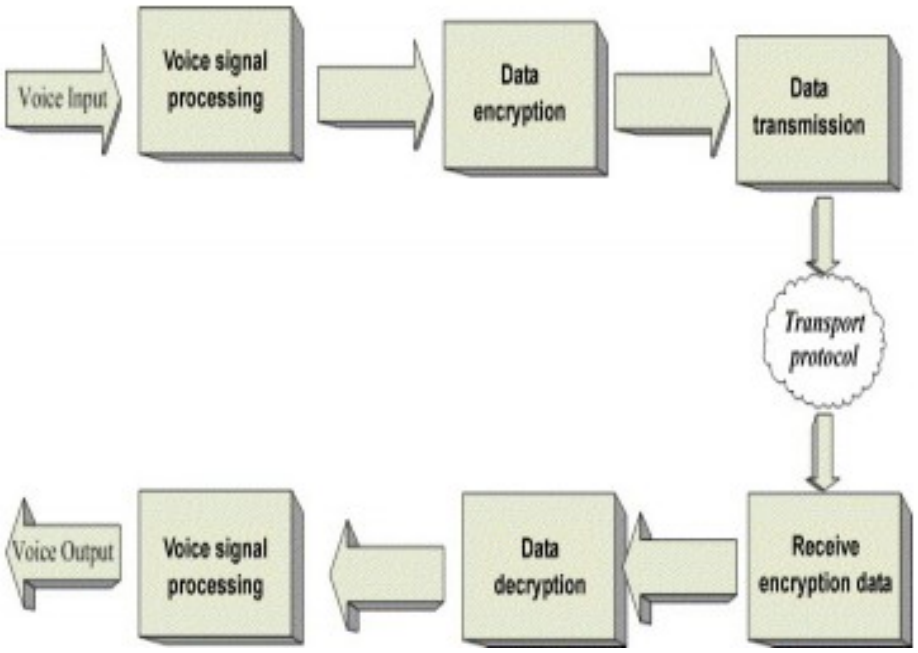


Figure (2-6): proposed system

Chapter “3”

Methodology

3.1 Overview of the Project :

The GSM standard is extracted voice coefficient and performs all operations on it. Figure (3-1) explain summarized of proposed method.

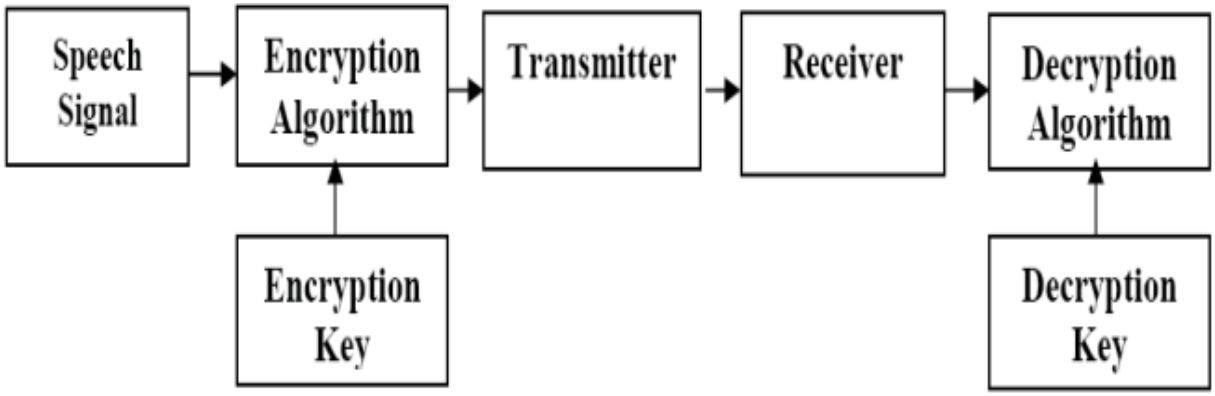


Figure (3-1) Proposed System

In more details see figure (3-2) the proposed method as follows : -

- Proposed system simulate GSM handset standard using MATLAB software .
- When run the basic function (include all function simulate GSM standard) it call first function that recording the voice by microphone, determine the frequency rate (Fs) and time of recording (n) then the voice will converted by default from analog to digital converter using Pulse Code Modulation(PCM) . here we write the original voice in (*.wav) file.
- Divided the stream of bits to frame each of it has 160 sample /20 ms each sample has 13 bits (104 kbps) .
- Fed frames to RPE-LTP functions , that functions extract all coefficients and compressed voice (13 kbps) .
- Pass output (coefficient) to channel coding to done error detection and error correction here the convolution distributed randomly error on data at this step we obtain 456 bit/20 ms .

- Fed 456 bit to Interleaver module , It divided data to 8 blocks each has 57 bits and shuffled them even block in first and odd at end. In addition to rearrange group of bits it improve the perform of error correction mechanism and decrease the possibility of whole bursts during transmission .
- Encrypted above blocks by XORed them with keystream produced by RC4 algorithm the keystream derivate from secret key changed at any session that is fed to transmitter and receiver, key stream change during call at any frame of data.
- Modulated encrypted data to transmit it over air at this phase first convert data by applying NRZ , shaped the signal to be as analog signal . at the receiver demodulated operation will done and reverse above steps respectively to recover the voice from their coefficient . see this step in more details in chapter 4 .

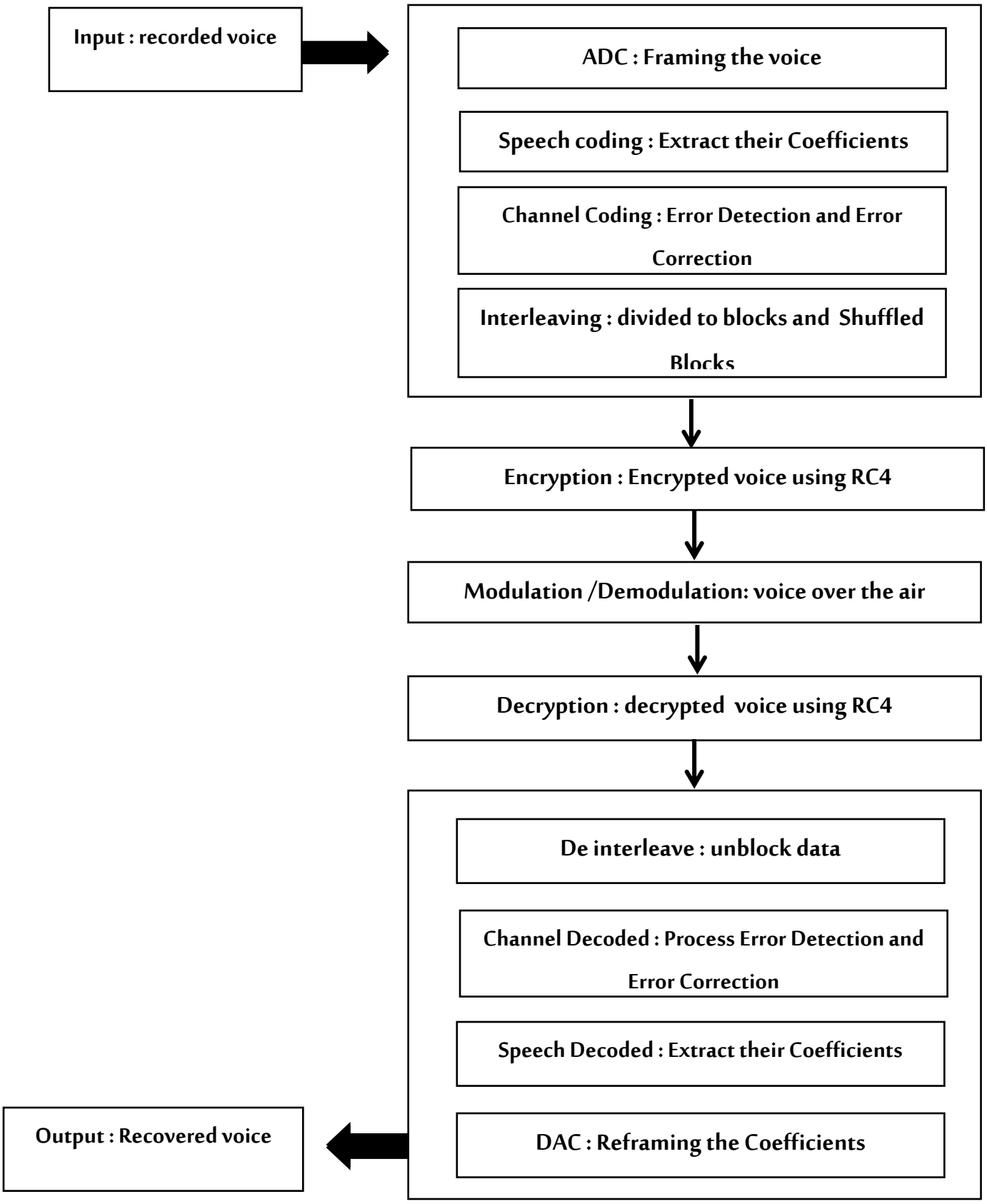


Figure (3-2) Flow Chart of proposed system

Chapter “4”

Implementation

4.1 GSM Module :

The features in GSM which enable its quality of communication over the channel involve its physical layer which corresponds to the following order [7]:

4.1.1 Transmitter components

1- RPE-LTP Speech Coding
2- Convolution Coder
3- Interleaving
4- Encryption
5- Modulation

4.1.2 Receiver components

1- De Modulation
2- Decryption
3- De Interleaving
4- Viterbi Decoding
5- RPE-LTP Speech Decoding

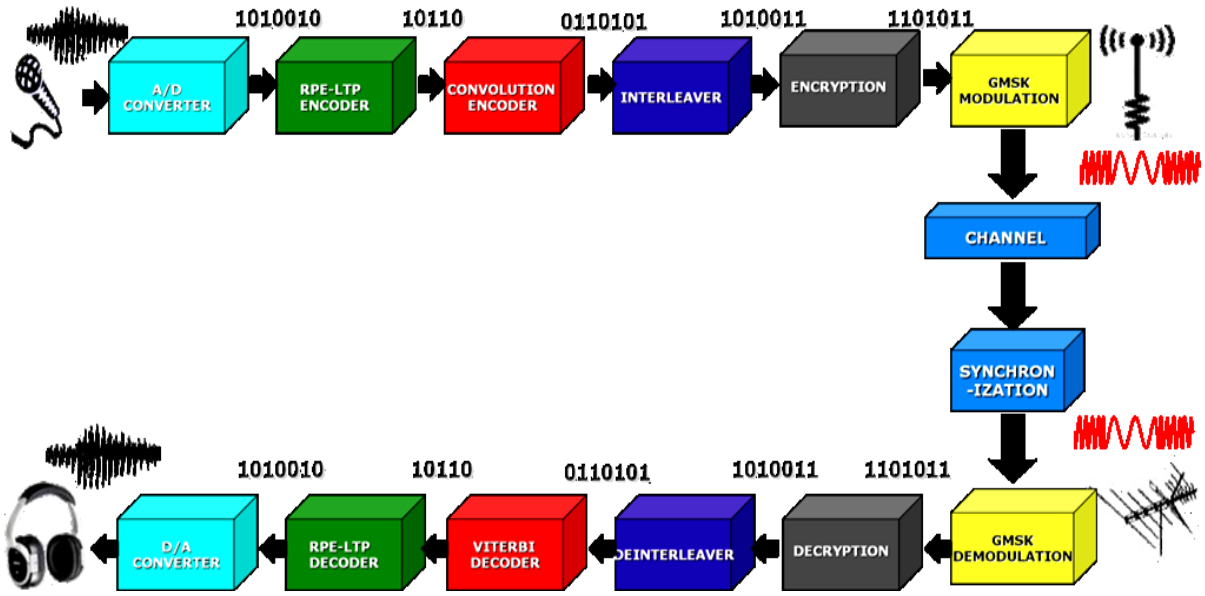


Figure (4-1): GSM Modem

4.1.1.1 RPE-LTP Speech Coding :

Regular Pulse Excitation Long Term Prediction (RPE-LTP) codec the data. the analog input speech coming from the microphone is digitized by passing it through the ADC (Analog to Digital Converter) which samples at sampling frequency of 8K with 13 bit resolution to achieve the ADC output data rate of **104kbps**.According to GSM specifications the input speech is split up into frames with 160 samples/frame out of 8000 samples per second (50 frame/s) to make the frame time equal to 20 ms.

The output of RPE-LTP codec is 260 bits for 160 samples (2080 bits) . That makes the output data rate 260 bits/20 ms =**13kbps** see figure (4-2) .

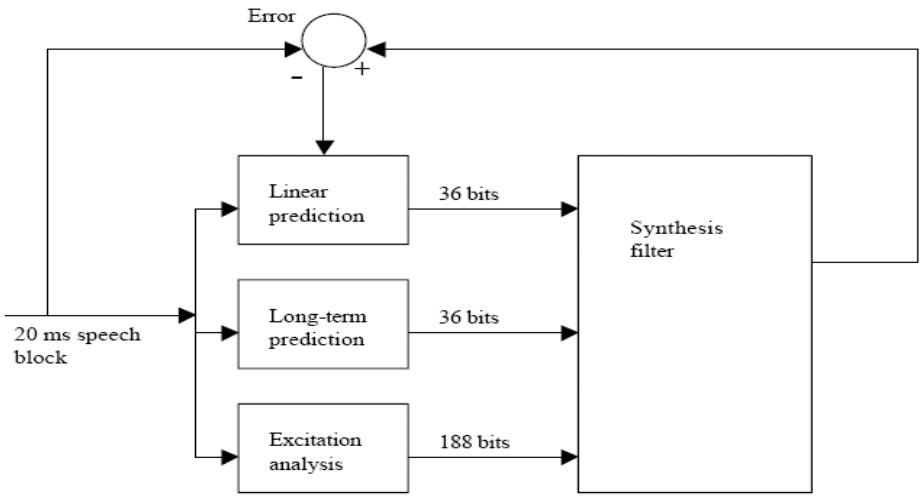


Figure (4-2): Speech Encoder RPE-LTP

Stages of RPE-LTP Encoder

1- Linear Prediction analysis (short-term prediction) :

Linear prediction can be understood in two ways. The first concept is to use LPC for removing short term redundancy from the speech signal. This is already a good property, because the residual signal after LPC filtering has lower amplitude and thus it is already easier to code e.g. with Pulse Code Modulation (PCM). The other concept

is that linear prediction gives us a very good model of the vocal tract. The inverse LP filter (the LP synthesis filter H(z)) models the vocal tract, and its transfer function describes the spectrum envelope of a short segment of speech signal . The idea of LPC filtering and inverse filtering can be seen in figure (4-3), where the actual excitation e(t) is estimated from the (radiated) speech (x(t)) with a time varying LPC-filter (A(z)) resulting estimated $\tilde{e}(n)$. Inversely, computer generated $\tilde{e}(n)$ can be filtered with time varying LPC-synthesis filter 1/ A(z) and understandable speech is generated $\tilde{e}(n)$. This kind of approach is often used in speech synthesis applications.[11]

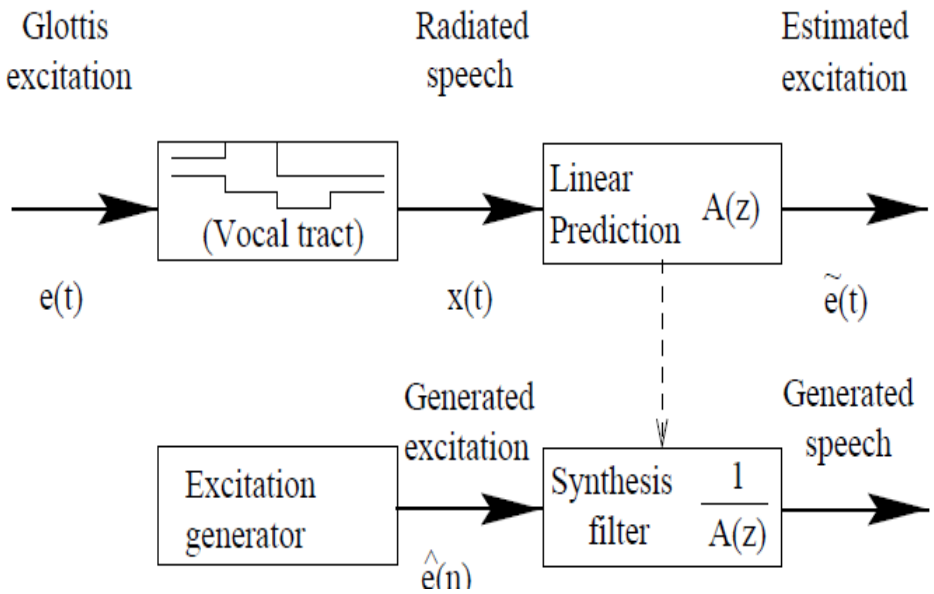


Figure (4-3): Block diagram of the speech production modeling and LP

The LPC (Linear Prediction Coding) stage involves the autocorrelation (using Levinson-Durbin recursion)[11] of the 160 samples to find the strength of the signal with its time separated version. After doing some formulation and According to GSM specifications we get (8) lattice filter coefficients for 160 auto correlated samples. At the end calculation of Log Area Ratios

(LAR). The LAR's are calculated from the lattice filter coefficients then we get (8) LAR's for 8 lattice filter coefficients. final the output is 8 parameters coded in **36 bits**.

2- Long-Term Prediction (LTP) :

At this stage estimate (4) lag coefficients coded to (4*7) bits and (4) gain coefficients coded (4*2) bit then output is (8) parameters coded in **36 bits**.

The **lag** is determined as the peak of the cross-correlation between the current frame and the last two frames, and the **gain** is the found by normalizing the cross correlation coefficients.

3- Excitation analysis :

involves the sections of RPE decimation, RPE Interpolation and grid position. It coded 160 sample in **188 bits** and we get (60) parameters .

Now on we have got the (76) parameters comprised in **260 bits** which are summarized as Table (4-1):

Table (4-1) : Speech Codec Summary

		Bits per 20ms block
LPC Filter	8 parameters	36
LTP Filter	Delay parameters	28
	Gain parameters	8
Excitation signal	Subsampling phase	8
	Maximum amplitude	24
	13 samples	156
Total	**76 parameters**	**260 bits**

4.1.1.2 Channel Coding :

Every transmitted waveform has to go through a channel or medium for its transmission. The channel is always non-ideal and imparts various kinds of impairments to the waveform like noise, interference, fading etc depending upon the channel characteristics. In order to make the waveform withstand these effects Channel Coding is employed so that the transmitted symbols can be accurately recovered at the receiver.

Figure (4-4) explain Channel coding with previous and next phase .

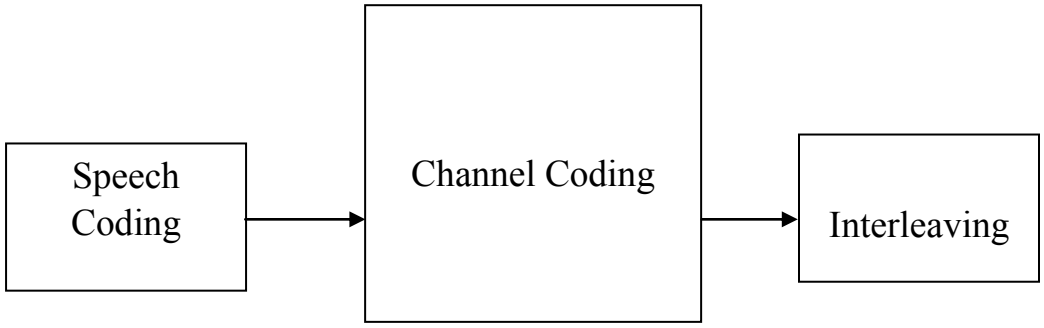


Figure (4-4): channel coding block diagram

In GSM the Channel Coding figure (4-5) used is a combination of Error Detection Coding and Error Correction Coding.

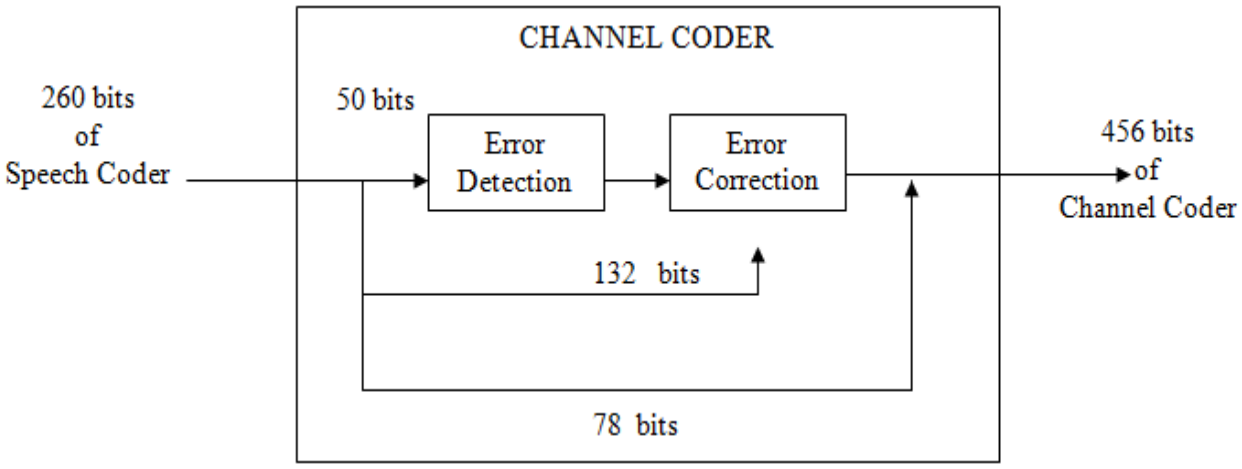


Figure (4-5): Channel Coding in GSM

- **Error Detection Coding :** The Error Detection Coding employed is Cyclic Redundancy Check (CRC) or polynomial codes figure(4-6).

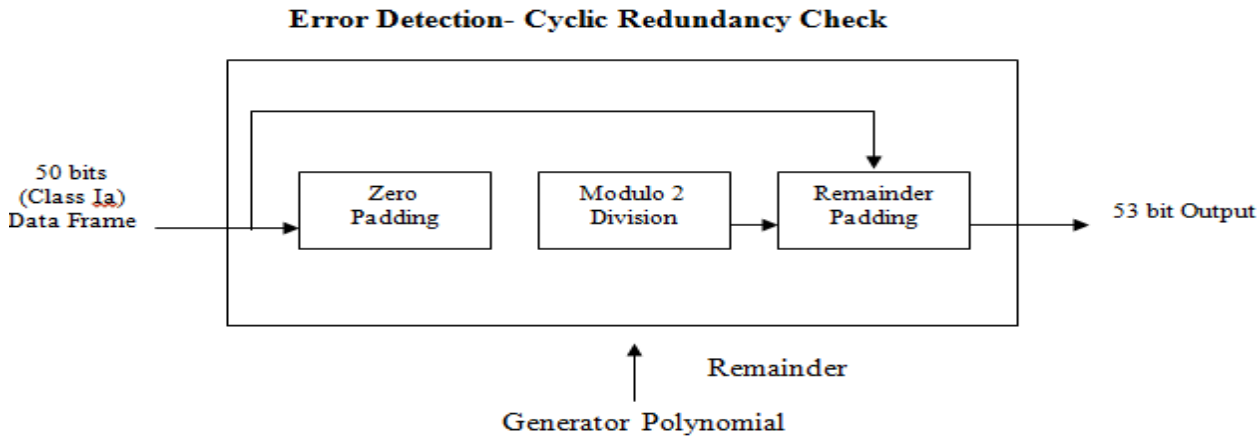


Figure (4-6): Error Detection Coding

- **Error Correction Coding :**In GSM error correction is of much more significance than error detection for accuracy . As data has to be communicated in real time and without errors In addition to the error detection process, error correction is ensured by using the Error Correction coding called the Convolution Coding.

4.1.1.3 Convolution Coder :

Convolution code is a very powerful type of error-correcting code used in channel coding to counter the random errors that occur during the signal transmission. The idea of channel coding is to improve the capacity of a channel by adding some carefully designed redundant information to the data being transmitted through the channel figure (4-7). In the process the data can be recovered with more certainty at the receiver.

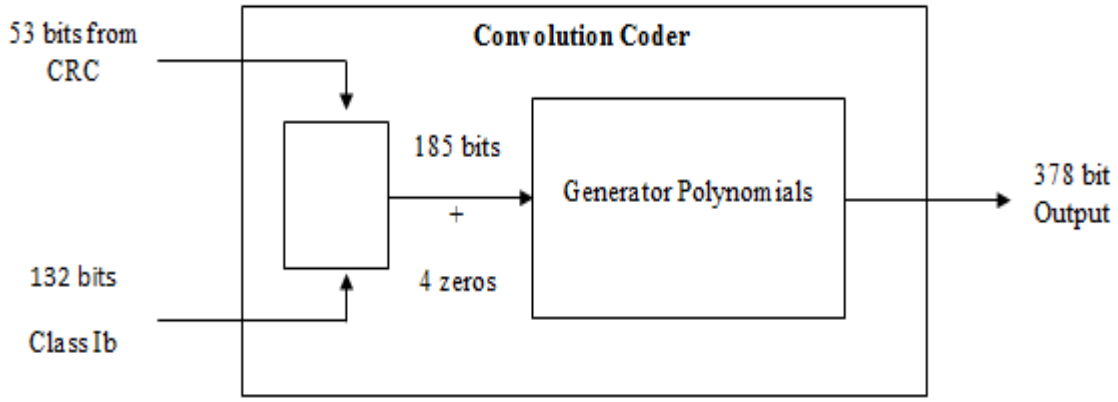


Figure (4-7): Error Correction- Convolution Coder

4.1.1.4 Interleaving :

Interleaving is used to cater for burst errors by shuffling the bits. In GSM the interleaving is done in the following manner. The 456 bits by the convolution encoder are divided into 57 bit blocks by selecting the 0th, 8th, 16th through 448th bits in the first block, the 1st, 9th 17th through 448th bits in the 2nd block and so on to have 8 blocks.. Then the bits in the first 4 blocks are placed in the even bit positions for the total block of 456 bits, and the bits in the second set of 4 blocks are placed in the odd positions. These 57 bit blocks are the sent for the encryption.

Figure (4-8) explain the operations of Interleaver module.

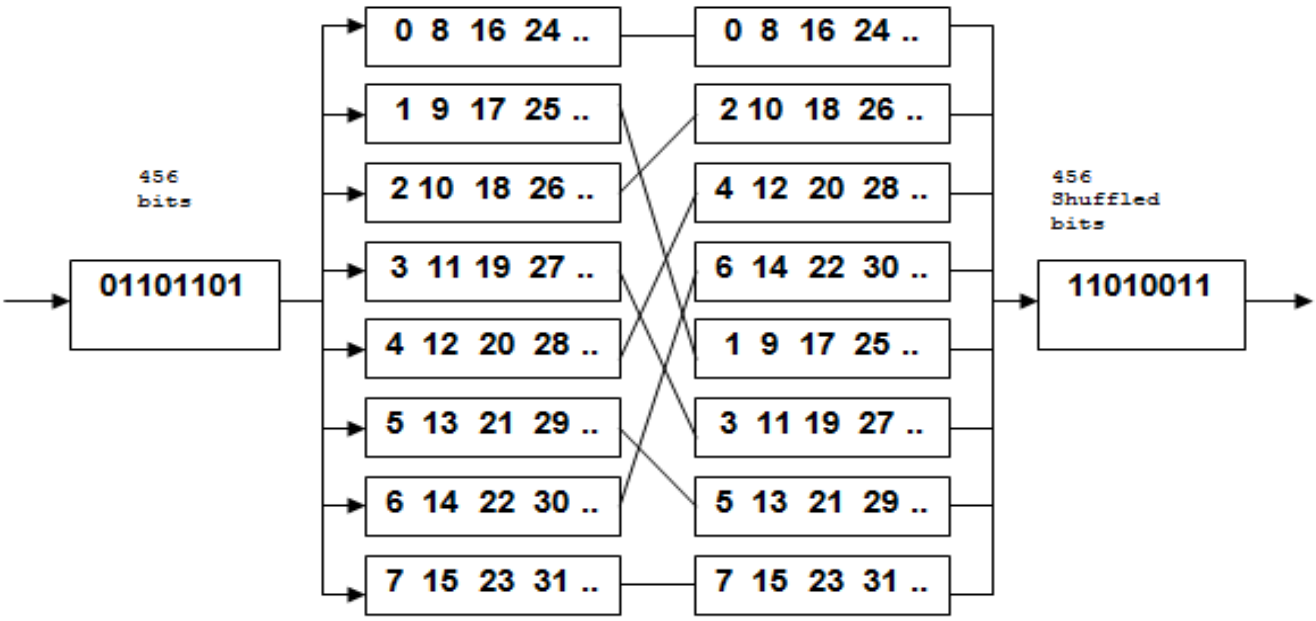


Figure (4-8): Interleaver

4.1.1.5 Encryption (RC4 Algorithm) :

A protection has been introduced in GSM by means of ciphering the transmission. Ciphering is achieved by performing an exclusive or" operation between a pseudo-random bit sequence produced by RC4 algorithm and a 456 bit received from Interleave function then it divided it to blocks each one has 8 bits. after encryption process completed data is sent to Modulation function . the pseudo-random sequence is derived from the pseudo-random generation algorithm (PRGA) and a key established previously. Deciphering follows exactly the same operation of encryption figure (4-9).

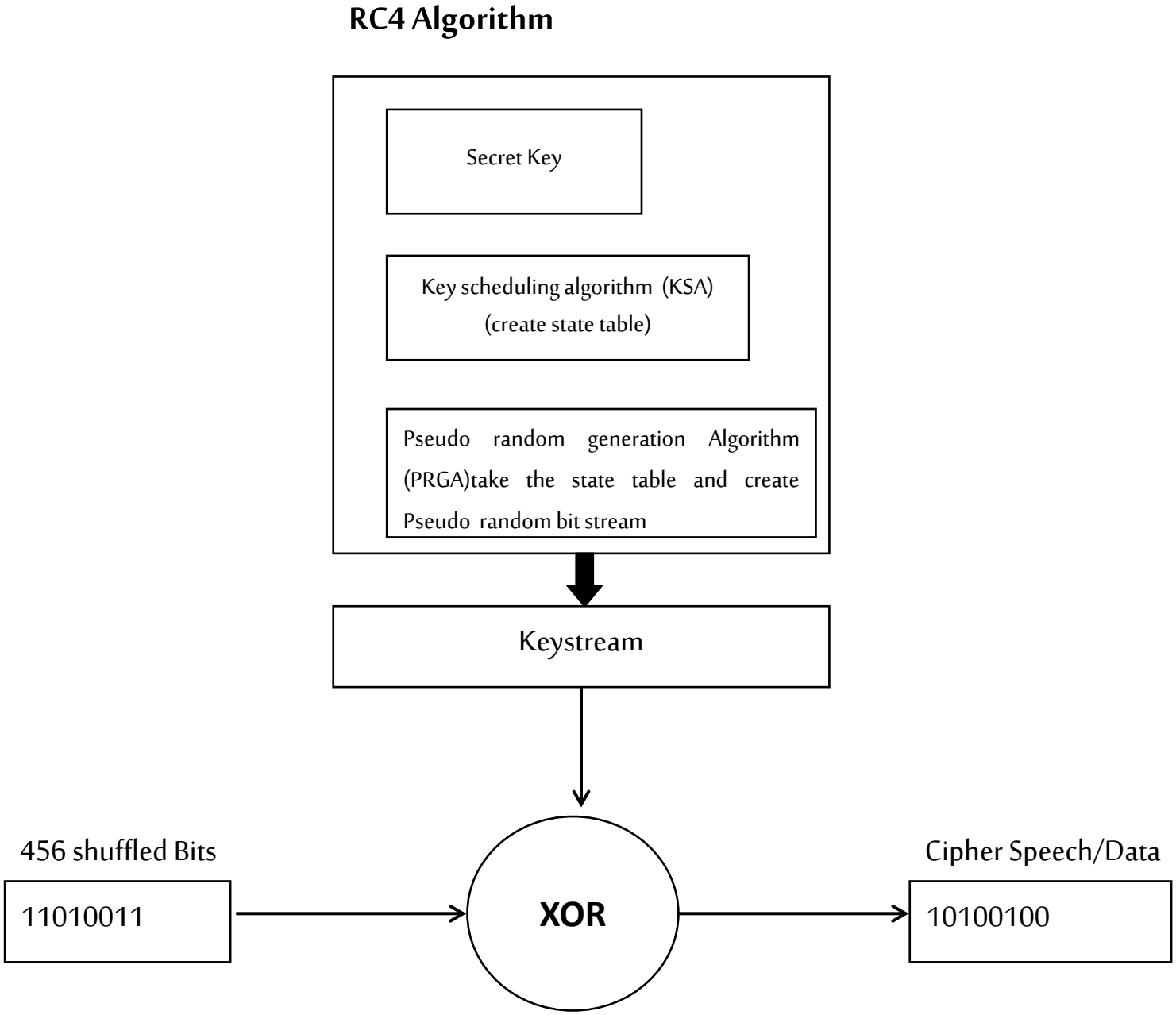


Figure (4-9): RC4 Encryption

4.1.1.6 Modulation:

GSM uses Gaussian Minimum Shift Keying (GMSK) as its modulation scheme. In digital communication, GMSK is a Continuous-Phase Frequency-Shift Keying modulation (CPFSK) scheme.

CPFSK is a commonly-used variation of frequency-shift keying (FSK), which is itself a special case of analog frequency modulation.

GMSK is a form of MSK which is Minimum Shift Keying. MSK uses changes in phase to represent 0's and 1's. the pulse sent to represent a 0 or a 1, not only depends on what information is being sent, but what was previously sent.

GSM specific GMSK is similar to standard minimum-shift keying (MSK), however the digital data stream is first shaped with a Gaussian filter before being applied to a frequency modulator. This has the advantage of reducing sideband power, which in turn reduces out-of-band interference between signal carriers in adjacent frequency channels.

In GMSK modulation the incoming sequence of bits is converted to NRZ sequence with 4 samples per symbol corresponding to four 1's for bit '1' and four -1's for '0'. Then this NRZ sequence is filtered with a Guassian filter which provides spectral efficiency figure (4-11).

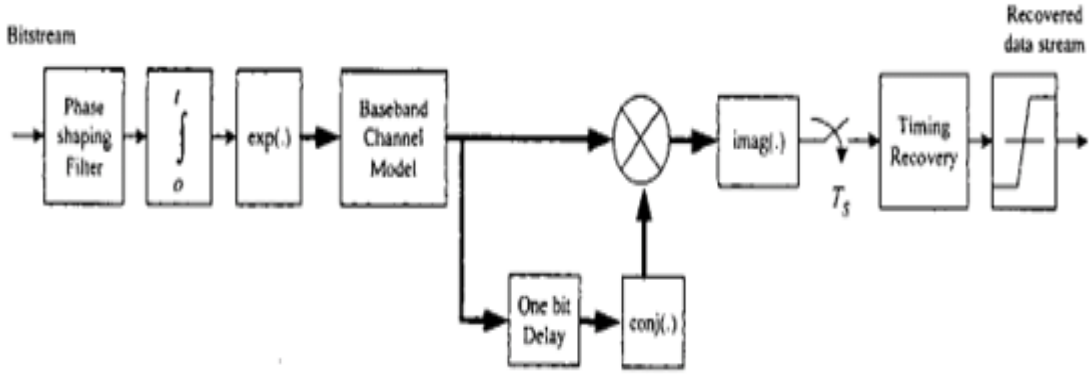


Figure (4-10): GMSK Modulator and De Modulator

NRZ refers to a form of digital data transmission in which the binary low and high states, represented by numerals 0 and 1, are transmitted by specific and constant DC (direct-current) voltage s.

The filtered NRZ sequence is integrated to produce the phase information that is the inherent characteristic of a FM modulation. The phase is scaled for pi/2 change for every bit. The sine and cosine of this phase are taken to

produce I and Q channel information. The GMSK complex signal consists of I as the real part and Q as the imaginary part.

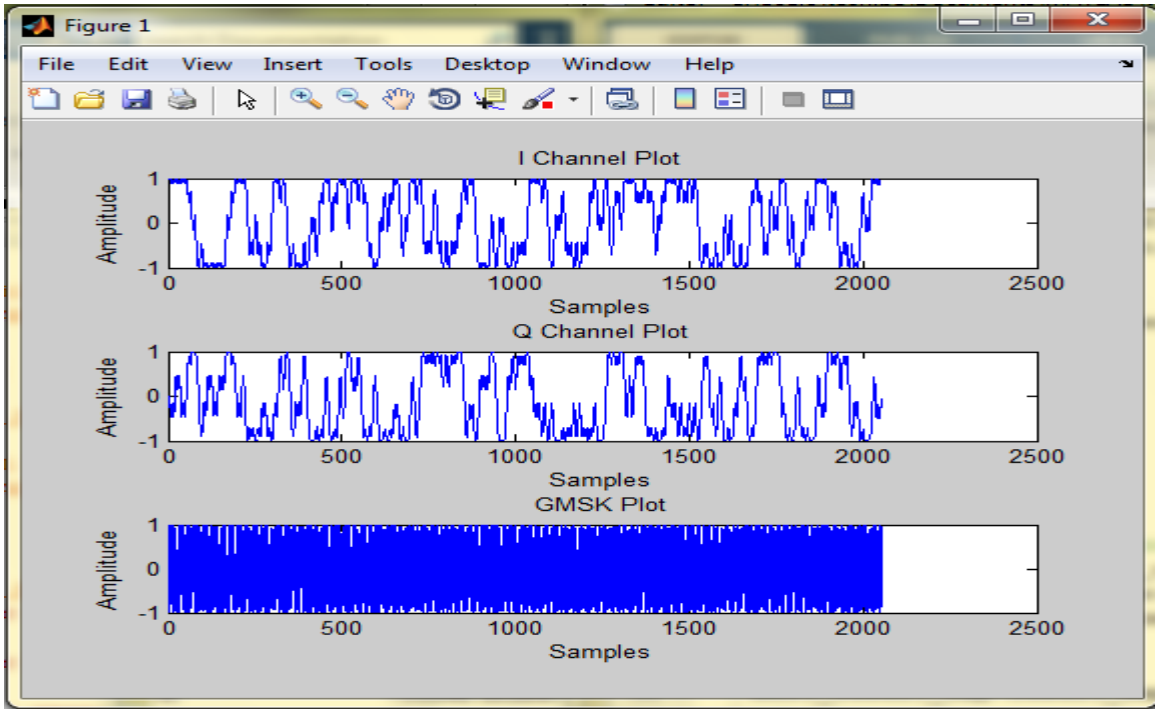


Figure (4-11) : In phase, Quadrature phase and GMSK signal

4.1.2.1 GMSK Demodulation: we have adopted non coherent detection. We have employed one bit differential detector which delays the incoming sequence of GMSK complex signal by one bit that is 4 to 5 samples delay. The resulting complex signal is multiplied with the original GMSK signal to produce the phase information that is stored in the imaginary part of the complex signal figure (4-12). The imaginary part is given to the symbol timing recovery which efficiently decides the symbols that were sent from the transmitter side.

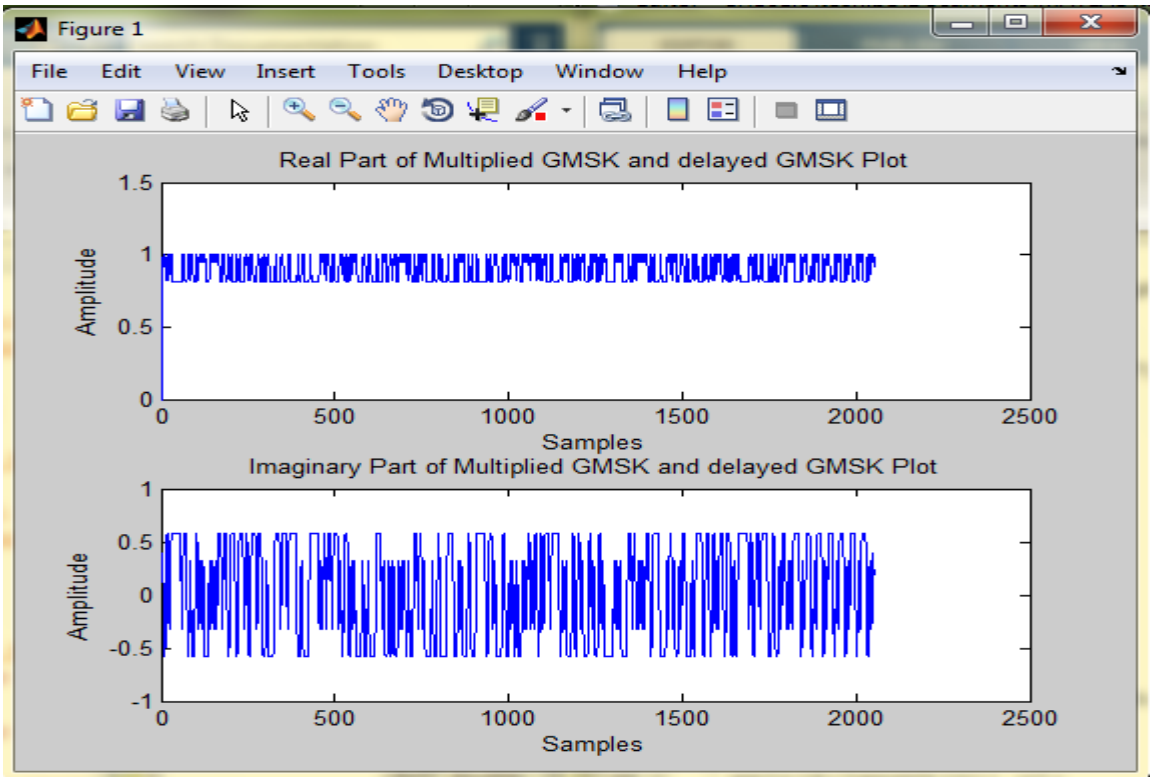


Figure (4-12) : Real and Imaginary part of Multiplied GMSK Signal and Bit Delayed GMSK Signal

1- Synchronization :

plays the most crucial role in correct data reception at the receiver. In our model of GSM we have used synchronization for detecting the timing phase errors. Since we have used non-coherent detection for demodulation

so we did not face the issue of carrier frequency synchronization in our implementation.

2- Symbol Timing Recovery :

The Symbol Timing Recovery is used to approximate the best instant at which if the symbol is sampled will result in a correct decision regarding the symbol. The symbol in case of GMSK is defined as bit 1 or bit 0. We have represented one symbol by 4 samples at transmitter end. Symbol Timing is required because the clocks of any two devices are running at different speeds. Though roughly they can be at the same frequency but in reality there is always some minute difference in the phase of the clock signals they generate. One solution to this problem is to transmit a special sequence after every frame but it consumes bandwidth because additional data has to be transmitted along with the original data. Second method is a digital timing recovery loop the main advantage of this loop is that the sampling is allowed to be unsynchronized and timing adjustment is done after the unsynchronized sampling. The sampling rate at A/D is kept at two times or more of the maximum frequency component in the incoming signal.

3- Interpolator:

The purpose of the interpolator is to compute the intermediate best sample which would have occurred if the signal was continuous. This interpolated value is then used to make the decision for detection. The interpolator filter we have employed is the first order linear filter. This linear filter serves the purpose well and is computationally efficient.

4.1.2.2 Decryption (RC4) :

We use the RC4 algorithm and the same streamkey Xoring it with ciphered signal to obtain original data figure (4-9) then data fed to De-Interleaver .

4.1.2.3 De Interleaving :

De-interleaving consists in performing the reverse operation. The major drawback of interleaving is the corresponding delay: transmission time from the first burst to the last one in a block .

4.1.2.4 Viterbi Decoding :

To retrieve data back without errors the decoding process is done at the receiver so pure data stream can be obtained back. This process is called Channel Decoding. In GSM, like channel coding both Error Detection and Error Correction Decoding is performed but this time, the Error Correction takes precedence.

- **Error Correction Decoding:**

  The error correction decoding employs the Maximum Likelihood Estimation method for recovering back the original data stream. Maximum likelihood decoding means finding the sequence of code branch in the code trellis that was most likely transmitted.

- **Trellis diagram :**

  A convolutional encoder is a finite state machine. An encoder with n binary cells will have 2^n states. These states keep on changing with the advent of new bits. The states are important because they play a key role in decoding the bit stream. These states alter themselves like the formation of a tree. As a result of which they form a tree-like diagram called “Trellis”.

- **Error Detection Decoding :**

The first 53 bits of Viterbi decoded sequence are fed into Error Detection block.

4.1.2.5 RPE-LTP Decoder :

The RPE LTP decoder works in the sense that the incoming 260 bits are separated on the basis of the 76 parameters. The bits are decoded back to the parameters and the speech is synthesized using the decoder scheme figure (4-13) .

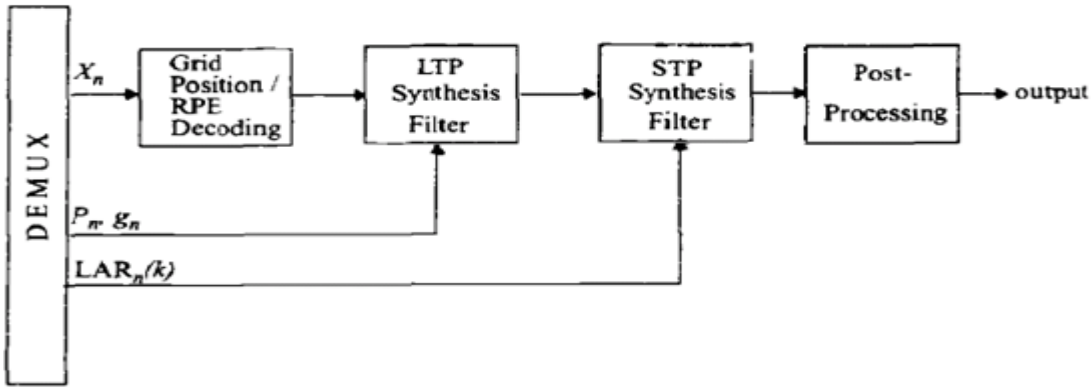
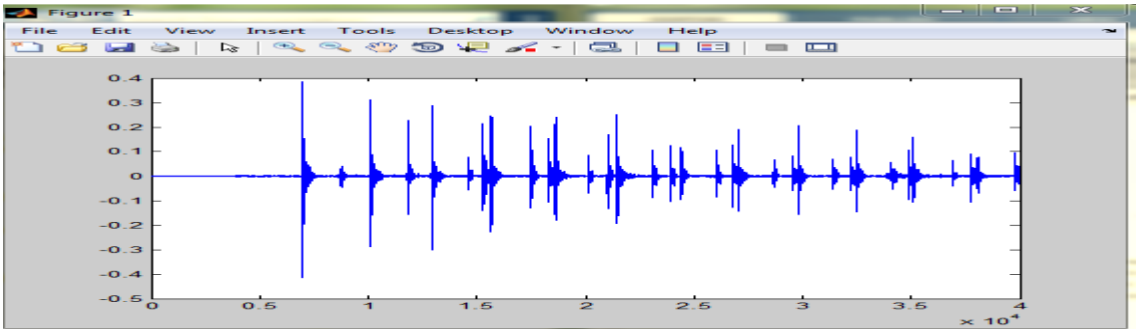


Figure (4-13) : RPE LTP Decoder

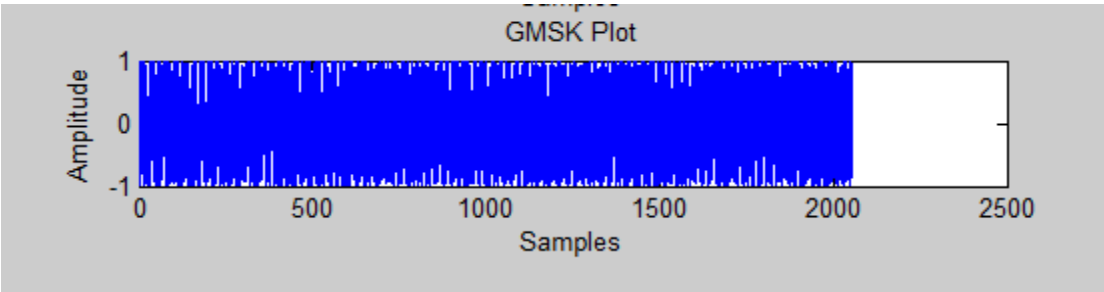
Using the scheme shown above, we proceed by decoding the bits and obtaining the speech parameters. Then we obtain the long term residual from the quantized residual sequences and then estimate the short term residual from the long term residual. Finally the speech is synthesized from the filtering of the short term residual with the recovered prediction coefficients. The recovered speech is processed to improve its quality and then it is passed to the D/A converter to be played back via speaker.

4.1.3 Results and discussion :

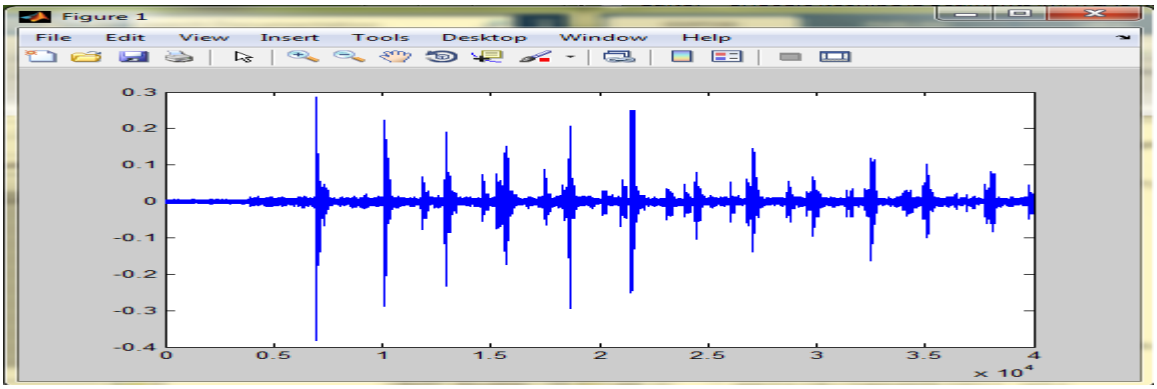
To evaluate the encryption performance of the proposed method, it is employed to encrypt the voice data. An original voice signal having 40,000 samples, sampled at rate of 8 KHz is encrypted using the keystream generated out of the RC4 algorithm. The voice signal is preprocessed, compressed and do some operation (mentioned in this chapter) on it to get the corresponding voice bitstream. The voice bitstream is then XORed with the keystream. The simulation result of voice encryption is shown in Figure(4-14) . As it can be seen that the encrypted voice signal shown in Figure(4-14)(b) is totally distinct from the original voice signal shown in Figure(4-14)(a) and it is randomly distributed like a noise signal. The signal distribution in Figure(4-14) (b) is completely flat/uniform at two extreme ends. This shows the effectiveness and suitability of the proposed scheme for voice data encryption. Figure(4-14)(c) explain the recovered voice with considered that the delay is 1symbol (4 samples).



(a)



(b)



(c)

Figure (4-14) Voice Encryption (a) Original voice (b) Encrypted voice (c) Recovered voice

The experiment also show the closed values between original voice values in table (4-2) and their Corresponding recovered voice values in table(4-3).

Table (4-2): first 24 values of original speech

1	0.0000000000	2	0.0000305176	3	0.0000305176	4	0.0000000000
5	0.0000305176	6	0.0000000000	7	0.0000000000	8	0.0000000000
9	0.0000000000	10	0.0000000000	11	0.0000000000	12	0.0000305176
13	0.0000000000	14	0.0000000000	15	0.0000000000	16	0.0000000000
17	0.0000000000	18	-0.0000305176	19	0.0000000000	20	0.0000000000
21	0.0000305176	22	0.0000305176	23	0.0000000000	24	0.0000000000

Table (4-3): first 24 values of recovered speech

1	0.0015563965	2	0.0048522949	3	0.0047607422	4	0.0002136230
5	0.0000000000	6	-0.0000305176	7	0.0000000000	8	0.0000305176
9	0.0001525879	10	0.0005493164	11	0.0001831055	12	-0.0000610352
13	0.0016479492	14	-0.0043334961	15	-0.0015869141	16	0.0014648438
17	0.0000000000	18	0.0000915527	19	0.0000000000	20	0.0000000000
21	0.0002441406	22	-0.0000305176	23	0.0001525879	24	0.0001525879

table (4-4) show that no change appears on two signals before encryption and after decryption this result prove that RC4 algorithm add more confidentiality and protect speech/data without any modification in GSM modules.

Table (4-4): compare encrypt/decrypt data

Data before pass to RC4 algorithm
10111111101110000101101110101110101011111100000110111101110010010111001100010010110110100111000110011000110111100110001100000010011011101110110101101010100000110011010100111011110110101011010000111100011100010110011010100101010011010001100011101100011100001111100011110001011001101010010101001101000110001110110001110000111011001010100111111100010000111011111000100101100100000000110011011110110000010101101010100011010001011101101101100100100100101101110000110101011010100111111100000101010001000110001101101001101110101100000000000000000000000000000000000000000000000000000000000000000000000000
Encrypted Data
01011010010111011011111001001011010010100010010001011000001011001001011011110111001111111001010001111101001110111000011011100111100010110000100010001111011001101101000011011110001111110101000111011001100101001000001101000000101010001111110100001001100101010000100100101001100000111010110001010011001101011101100010111111100010110000110011101010000101000110111011100101001100101100110000000101110110001111001100010001101111011100101000011010000100001100001110111001011110010111100101111001011110010111100101111001011110010111100101111001011110010111100101111001
decrypted Data
10111111101110000101101110101110101011111100000110111101110010010111001100010010110110100111000110011000110111100110001100000010011011101110110101101010100000110011010100111011110110101011010000111100011100010110011010100101010011010001100011101100011100001111100011110001011001101010010101001101000110001110110001110000111011001010100111111100010000111011111000100101100100000000110011011110110000010101101010100011010001011101101101100100100100101101110000110101011010100111111100000101010001000110001101101001101110101100000000000000000000000000000000000000000000000000000000000000000000000000

Chapter “5”

Conclusion

5.1 Conclusion

In this research we proposed encryption method to fulfill the end–to-end secured communication in the GSM voice. We use RC4 algorithm to add more confidentiality to GSM conversation and data. The proposed method was implemented without any modification on GSM standard .

The advantage of this method it was depended on GSM specification and without any adjustment in current GSM signaling system . the simulation is carried up using MATLAB software and the results obtained show that RC4 algorithm in GSM add more confidentiality and protect speech without any modification to GSM modules with reasonable speed compared with other ciphers such as DES, AES .

5.2 Future Work :

To presents high speed and area efficient hardware implementation of the RC4 algorithm with changing key at any session to avoid attack as possible.

The proposed architecture of the RC4 to be apply in future it consist of a control and storage unit . the storage unit is responsible for the key set-up and keystream generation phases . the operation of storage unit synchronized by control unit . control unit generates the appropriate clock and control signals.

design uses only one 256 bytes simple dual port RAM for key stream generation and it takes 3 clock cycles per byte. It supports a variable key length of from 1 byte to 256 bytes and achieves 54.8MB/s throughput at 164.6MHz operating frequency.

References

Books and papers :

[1] Data Communication and Networking By Behrouz A.Forouzan 4th Edition.

[2] Mobile-Communications 4th Edition by Dr-Jochen-Schiller .

[3] http://www.speedguide.net/faq/what-are-1g-2g-3g-and-4g-networks-365.

[4] GSM and Personal Communications Handbook (Mobile Communications Library) by Siegmund Redl , Matthias Weber , Malcolm W. Oliphant .

[5] Brand/GSM_vokoder.pdf

[6] Security in the GSM Network Ammar Yasir Korkusuz Bogazici University, Electrical-Electronics Engineering Department, MSc. Student.

[7] Wireless Communication by V. S. Bagad .

[8] Software Communication Architecture Compliant Software Radio For GSM Transmission And Reception Submitted to the Faculty of EE Dept. National University of Sciences and Technology, Rawalpindi in partial fulfillment of B.E. degree in Telecommunication Engineering March 2008

[9] An Investigation Into Authentication Security of GSM Algorithm for Mobile banking By Ali Raheem .

[10] Proceedings of the International Conference on Information Systems Design and Intelligent Application 2012 edited by Suresh Chandra Satapathy, P S Avadhani, Ajith Abraham.

[11] Securing Speech in GSM Networks using DES with Random Permutation and Inversion Algorithm (International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.4, July 2012)

[12] Role of Multiple Encryption in Secure Voice Communication (International Journal of Computer Science and Electronics Engineering (IJCSEE) Volume 1, Issue 2 (2013) ISSN 2320–4028 (Online))

[13] Pitch Modification and Quantization for Offline Speech Coding Anssi_Ramo TAMPERE UNIVERSITY OF TECHNOLOGY 1999

[14] MATLAB® Software for the Code Excited Linear Prediction Algorithm by Karthikeyan N. Ramamurthy and Andreas S. Spanias

[15] SPEECH CODING ALGORITHMS Foundation and Evolution of Standardized Coders by WAI C. CHU

[16] Decoding GSM by Magnus Glendrange, Kristian Hove and Espen Hvideberg .

[17] GSM Full Rate Speech Transcoding – Recommendation GSM 06.10 by ETSI SMG February 1992 .

[18] Rescorla, E. SSL and TLS: Designing and Building Secure Systems. Reading, MA: Addison-Wesley, 2001.

[19] Cryptography and network security by William Stallings.

[20] http://www.info.biz.hr/Typo3/typo3_01/dummy-3.8.0/fileadmin/Mirko_

[21] http://www.sans.org/reading-room/whitepapers/telephone/gsm-standard-an-overview-security-317

[22] http://www.ijcem.org/papers012012/ijcem_012012_13.pdf

[23] http://www.researchgate.net/publication/254053165_A_simple_and_cheap_end-to-end_voice_encryption_framework_over_GSM-based_networks

[24] http://www.teletopix.org/gsm/how-voice-signal-processing-in-gsm

[25] http://www.scribd.com/doc/19708640/9-GSM-Speech-Channel-Coding#scribd

[26] http://www.washingtonpost.com/business/technology/by-cracking-cellphone-code-nsa-has-capacity-for-decoding-private-conversations/2013/12/13/e119b598-612f-11e3-bf45-61f69f54fc5f_story.html.

[27] http://yro.slashdot.org/story/13/12/14/0148251/nsa-able-to-crack-a51-cellphone-crypto.

[28] http://www.mobileworld.org/gsm_about_04.html

[29] http://cryptome.org/a51-bsw.htm

APPENDIX - A

Outputs of Experiment :

INPUT SAMPLES (partial of 40000 values)
03.0518e-050003.0518e-053.0518e-05000-3.0518e-053.0518e-053.0518e-0500000003.0518e-050003.0518e-0500000-3.0518e-050000000000-3.0518e-05-3.0518e-05-3.0518e-050000-3.0518e-050000000003.0518e-0503.0518e-050000003.0518e-05-3.0518e-0503.0518e-05-3.0518e-050000000-3.0518e-05000-3.0518e-050-3.0518e-0500000-3.0518e-05000000-3.0518e-0500000000-3.0518e-05-3.0518e-05000003.0518e-0500000-3.0518e-050000000003.0518e-0503.0518e-05003.0518e-05-3.0518e-053.0518e-05000-3.0518e-05-3.0518e-05000-3.0518e-050-3.0518e-05000-3.0518e-0500003.0518e-050000003.0518e-0503.0518e-050000003.0518e-050003.0518e-053.0518e-0500000000-3.0518e-053.0518e-0500000003.0518e-0500-3.0518e-05000-3.0518e-05-3.0518e-05003.0518e-050-3.0518e-05000000-3.0518e-05-3.0518e-0500-3.0518e-053.0518e-0503.0518e-050000003.0518e-05000-3.0518e-05000003.0518e-05-3.0518e-050000000003.0518e-05000000-3.0518e-0500-3.0518e-0500-3.0518e-05000000003.0518e-0500-3.0518e-053.0518e-0500-3.0518e-05-3.0518e-050003.0518e-05-3.0518e-05000-3.0518e-053.0518e-050003.0518e-05-3.0518e-0500000000000-3.0518e-0500000000003.0518e-05-3.0518e-0500-3.0518e-053.0518e-05000000000000000-3.0518e-050000000-3.0518e-05000-3.0518e-0500-3.0518e-05-3.0518e-05000003.0518e-053.0518e-05-3.0518e-050-3.0518e-05000000003.0518e-050000-3.0518e-053.0518e-05003.0518e-05000003.0518e-053.0518e-0500000-3.0518e-050-3.0518e-053.0518e-0503.0518e-05003.0518e-05003.0518e-050003.0518e-05-3.0518e-05-3.0518e-053.0518e-05000-3.0518e-05003.0518e-05000000-3.0518e-05000-3.0518e-05003.0518e-053.0518e-05-3.0518e-05000000000-3.0518e-053.0518e-05003.0518e-0500003.0518e-05-3.0518e-050000-3.0518e-053.0518e-0500-3.0518e-0500000-3.0518e-050-3.0518e-053.0518e-05003.0518e-0500000000-3.0518e-050003.0518e-0503.0518e-050000-3.0518e-05003.0518e-053.0518e-05000-3.0518e-05-3.0518e-05000-3.0518e-05003.0518e-0503.0518e-05003.0518e-05003.0518e-0500000000000-3.0518e-053.0518e-050000000000-3.0518e-050-3.0518e-0500000-3.0518e-050003.0518e-05000000000-3.0518e-053.0518e-053.0518e-05-3.0518e-050000000000000-3.0518e-0500000000-3.0518e-050000-3.0518e-050-3.0518e-0500000-3.0518e-0500-3.0518e-050003.0518e-050000003.0518e-05000003.0518e-050003.0518e-053.0518e-05000000003.0518e-053.0518e-053.0518e-0500-3.0518e-05000-3.0518e-05-3.0518e-0500000000000000000003.0518e-053.0518e-053.0518e-050-3.0518e-050000003.0518e-05-3.0518e-05-3.0518e-05000003.0518e-050-3.0518e-0500000000-3.0518e-0500003.0518e-0500000-3.0518e-053.0518e-053.0518e-0500003.0518e-050000000000003.0518e-050000003.0518e-0500000000003.0518e-050-3.0518e-050000-3.0518e-05000000-3.0518e-0500-3.0518e-05000-3.0518e-053.0518e-050000000000000-3.0518e-050-3.0518e-050000000003.0518e-05000000000003.0518e-05000000000-3.0518e-05003.0518e-0500000003.0518e-05000000-3.0518e-0503.0518e-0500000000-3.0518e-05000000003.0518e-050-3.0518e-0503.0518e-0500-3.0518e-050000-3.0518e-0500003.0518e-0500000000-3.0518e-050000000003.0518e-05000003.0518e-

05003.0518e-0503.0518e-05-3.0518e-0500000000-3.0518e-050-3.0518e-05-3.0518e-
050000000000-3.0518e-050-3.0518e-05000000-3.0518e-0500000000000000003.0518e-
053.0518e-050-3.0518e-0500000000000000003.0518e-05000003.0518e-050000000-
3.0518e-05-3.0518e-0500000-3.0518e-05-3.0518e-05000-3.0518e-053.0518e-0500-
3.0518e-0500000000000000003.0518e-0500-3.0518e-050000003.0518e-0500-3.0518e-05-
3.0518e-050000-3.0518e-05000003.0518e-05003.0518e-0503.0518e-05000000-3.0518e-
050000003.0518e-05000000-3.0518e-05-3.0518e-050-3.0518e-0500000000000000-
3.0518e-0500003.0518e-050000000000-3.0518e-053.0518e-05-3.0518e-
05000000003.0518e-0503.0518e-050003.0518e-05-3.0518e-050000000000-3.0518e-
0500003.0518e-053.0518e-0503.0518e-050000000000-3.0518e-05-3.0518e-05-3.0518e-
05-3.0518e-0500000-3.0518e-0500000-3.0518e-050-3.0518e-0503.0518e-05003.0518e-
0500-3.0518e-050-3.0518e-05000-3.0518e-0503.0518e-05-3.0518e-050000-3.0518e-
0503.0518e-050-3.0518e-053.0518e-053.0518e-0503.0518e-05-3.0518e-05003.0518e-
0500-3.0518e-053.0518e-05003.0518e-0500003.0518e-0500003.0518e-050-3.0518e-050-
3.0518e-0503.0518e-0503.0518e-05-3.0518e-0503.0518e-0500000-3.0518e-
050000000000-3.0518e-0503.0518e-0503.0518e-050-3.0518e-05003.0518e-05000000-
3.0518e-050-3.0518e-0500000003.0518e-0503.0518e-0500000-3.0518e-0500000-3.0518e-
050000003.0518e-0500003.0518e-05000000000-3.0518e-0503.0518e-
05000000000000000-3.0518e-053.0518e-05000-3.0518e-050003.0518e-05000-3.0518e-
0500003.0518e-053.0518e-0503.0518e-0500-3.0518e-050-3.0518e-
0500000000000003.0518e-05000000000000000003.0518e-050003.0518e-
05000000003.0518e-053.0518e-05003.0518e-05000003.0518e-0500-3.0518e-053.0518e-
050-3.0518e-05-3.0518e-05000003.0518e-0503.0518e-050003.0518e-050-3.0518e-050-
3.0518e-0500-3.0518e-05000-3.0518e-05000000003.0518e-05-3.0518e-050000-3.0518e-
05000003.0518e-05000000003.0518e-053.0518e-050000000003.0518e-050-3.0518e-
0500000000003.0518e-0503.0518e-053.0518e-053.0518e-05000000000000-3.0518e-
05000-3.0518e-050-3.0518e-050000000-3.0518e-053.0518e-0503.0518e-0500003.0518e-
053.0518e-050-3.0518e-0503.0518e-05-3.0518e-0500000000000003.0518e-05-3.0518e-
050000000-3.0518e-050-3.0518e-0500000-3.0518e-0503.0518e-050003.0518e-
05000000000000003.0518e-0503.0518e-050-3.0518e-05-3.0518e-05-3.0518e-050000000-
3.0518e-05003.0518e-05-3.0518e-0503.0518e-050000000-3.0518e-
05000000000000000000000003.0518e-0503.0518e-050003.0518e-0500-3.0518e-
053.0518e-050-3.0518e-0500-3.0518e-050000-3.0518e-0500003.0518e-050003.0518e-
05003.0518e-05-3.0518e-05000000-3.0518e-0503.0518e-050003.0518e-05-3.0518e-
05000-3.0518e-05000-3.0518e-0503.0518e-050-3.0518e-0500-3.0518e-05-3.0518e-
050000-3.0518e-05-3.0518e-05-3.0518e-050000000003.0518e-050-3.0518e-0503.0518e-
0503.0518e-05000-3.0518e-05000000-3.0518e-053.0518e-0500003.0518e-05000-3.0518e-
0503.0518e-050000000000-3.0518e-053.0518e-05-3.0518e-0503.0518e-
05000000000000003.0518e-050000-3.0518e-053.0518e-05000000000000-3.0518e-
05000-3.0518e-05003.0518e-053.0518e-050000-3.0518e-0503.0518e-050-3.0518e-
050000-3.0518e-0500000-3.0518e-05-3.0518e-0500003.0518e-050000-3.0518e-
05000000003.0518e-050-3.0518e-0500-3.0518e-05000000000003.0518e-050000-3.0518e-
05-3.0518e-050-3.0518e-05000-3.0518e-0500003.0518e-053.0518e-05-3.0518e-0500-
3.0518e-05-3.0518e-0500-3.0518e-0500-3.0518e-0500-3.0518e-053.0518e-05-3.0518e-
0500-3.0518e-0500000003.0518e-0500-3.0518e-053.0518e-053.0518e-

050000000003.0518e-05000000-3.0518e-0500-3.0518e-05003.0518e-05003.0518e-
050003.0518e-050000003.0518e-05-3.0518e-050003.0518e-050-3.0518e-0500000-
3.0518e-0500003.0518e-05003.0518e-050003.0518e-05000003.0518e-0500000003.0518e-
050000-3.0518e-0500-3.0518e-05-3.0518e-050-3.0518e-050003.0518e-053.0518e-05000-
3.0518e-053.0518e-0500003.0518e-0503.0518e-05003.0518e-053.0518e-0500000-
3.0518e-05000-3.0518e-05003.0518e-0500003.0518e-0503.0518e-050000-3.0518e-
0500000-3.0518e-050003.0518e-053.0518e-0500-3.0518e-05003.0518e-0500-3.0518e-
053.0518e-050000-3.0518e-05000000000003.0518e-05000-3.0518e-0503.0518e-
05003.0518e-05-3.0518e-050 3.0518e-05-3.0518e-0500000000-3.0518e-050-3.0518e-
053.0518e-0503.0518e-053.0518e-050000000000000003.0518e-050-3.0518e-05000000-
3.0518e-0500-3.0518e-0500000003.0518e-053.0518e-050000000-3.0518e-05000000-
3.0518e-05-3.0518e-05000003.0518e-0503.0518e-05-3.0518e-0500-3.0518e-
050003.0518e-0500000003.0518e-0503.0518e-05000-3.0518e-05-3.0518e-
0500003.0518e-050-3.0518e-0500003.0518e-050-3.0518e-05000003.0518e-
0500000000003.0518e-050000000000000-3.0518e-05-3.0518e-05000000-3.0518e-0500-
3.0518e-0500000000000000000-3.0518e-05003.0518e-0500-3.0518e-053.0518e-
050000000000-3.0518e-053.0518e-0500-3.0518e-050003.0518e-050-3.0518e-
0500000003.0518e-05-3.0518e-050-3.0518e-050-3.0518e-05-3.0518e-050003.0518e-
05000003.0518e-050-3.0518e-05-3.0518e-050000000-3.0518e-050-3.0518e-0503.0518e-
0500003.0518e-0500000-3.0518e-05-3.0518e-050000-3.0518e-0503.0518e-0503.0518e-
050000-3.0518e-05000-3.0518e-0500000000-3.0518e-050003.0518e-0503.0518e-050-
3.0518e-0503.0518e-0500-3.0518e-050000003.0518e-0503.0518e-05000003.0518e-
0503.0518e-050003.0518e-0500000-3.0518e-05000000000-3.0518e-
0500000000003.0518e-0503.0518e-05003.0518e-05003.0518e-05003.0518e-05003.0518e-
05000000000003.0518e-0500-3.0518e-0500-3.0518e-050-3.0518e-05003.0518e-
053.0518e-05000-3.0518e-050000003.0518e-0500-3.0518e-050000-3.0518e-0503.0518e-
0500000-3.0518e-0500000003.0518e-0500000-3.0518e-05000003.0518e-
0500000003.0518e-050-3.0518e-050-3.0518e-053.0518e-050000-3.0518e-050-3.0518e-
050000-3.0518e-053.0518e-050003.0518e-050-3.0518e-0503.0518e-053.0518e-050-
3.0518e-0500000000-3.0518e-0500003.0518e-05-3.0518e-0500-3.0518e-05000003.0518e-
053.0518e-05000-3.0518e-05-3.0518e-050003.0518e-050000003.0518e-0500-3.0518e-
05003.0518e-05000003.0518e-0500-3.0518e-05000000003.0518e-05000000003.0518e-
05000000-3.0518e-0500003.0518e-05003.0518e-050003.0518e-05-3.0518e-050-3.0518e-
050003.0518e-050000003.0518e-05000000000-3.0518e-050003.0518e-050003.0518e-
0500000000003.0518e-0503.0518e-050-3.0518e-0500-3.0518e-05000-3.0518e-05000-
3.0518e-050-3.0518e-053.0518e-05-3.0518e-053.0518e-05000003.0518e-0503.0518e-
05000000000003.0518e-0500-3.0518e-050000000000-3.0518e-05003.0518e-0500-
3.0518e-0500000000-3.0518e-0503.0518e-0500003.0518e-0500000-3.0518e-0500-
3.0518e-05000000000003.0518e-053.0518e-053.0518e-053.0518e-0500-3.0518e-
053.0518e-050000000000003.0518e-05003.0518e-0503.0518e-05003.0518e-
0500003.0518e-0500-3.0518e-05003.0518e-053.0518e-0500-3.0518e-050-3.0518e-05-
3.0518e-050003.0518e-053.0518e-050-3.0518e-0503.0518e-0500003.0518e-0503.0518e-
05-3.0518e-0503.0518e-05000-3.0518e-050003.0518e-050-3.0518e-050-3.0518e-05-
3.0518e-05003.0518e-050003.0518e-053.0518e-05003.0518e-053.0518e-05-3.0518e-050-
3.0518e-050003.0518e-050000-3.0518e-0500-3.0518e-0500-3.0518e-05-3.0518e-

053.0518e-050000-3.0518e-0503.0518e-05000-3.0518e-053.0518e-0503.0518e-
0503.0518e-05-3.0518e-05000-3.0518e-0500000000000000003.0518e-0500003.0518e-
0500000000000000000003.0518e-050000-3.0518e-05003.0518e-0500000-3.0518e-
05000000-3.0518e-0500-3.0518e-05000-3.0518e-050000-3.0518e-05000000000000000-
3.0518e-05000-3.0518e-050-3.0518e-050-3.0518e-0500003.0518e-050000-3.0518e-
053.0518e-05000003.0518e-050000003.0518e-050000-3.0518e-050-3.0518e-
0500000000000000003.0518e-0503.0518e-053.0518e-0503.0518e-05000003.0518e-
0503.0518e-050003.0518e-0500-3.0518e-05003.0518e-050-3.0518e-050000-3.0518e-05-
3.0518e-053.0518e-05003.0518e-05003.0518e-05000-3.0518e-053.0518e-05000000-
3.0518e-0500000000000000000000-3.0518e-050-3.0518e-050-3.0518e-0500000-3.0518e-
050-3.0518e-053.0518e-0500000-3.0518e-050-3.0518e-050-3.0518e-050000-3.0518e-050-
3.0518e-0503.0518e-050000003.0518e-05000000-3.0518e-05000000003.0518e-
0503.0518e-053.0518e-0500000000003.0518e-0503.0518e-0500000003.0518e-
050003.0518e-0503.0518e-053.0518e-050000-3.0518e-05003.0518e-0500000000000000-
3.0518e-05000000000-3.0518e-0503.0518e-050000000-3.0518e-053.0518e-
050003.0518e-0503.0518e-050000000-3.0518e-0503.0518e-050003.0518e-050000-
3.0518e-053.0518e-053.0518e-05003.0518e-0500000000-3.0518e-0500003.0518e-
05000000-3.0518e-05-3.0518e-053.0518e-05003.0518e-0500-3.0518e-050-3.0518e-
053.0518e-0503.0518e-0500003.0518e-05-3.0518e-0500000000000000-3.0518e-
0500003.0518e-0500000000-3.0518e-05000-3.0518e-05003.0518e-050-3.0518e-
0500003.0518e-053.0518e-053.0518e-0500-3.0518e-0500-3.0518e-050000-3.0518e-
050000003.0518e-05000003.0518e-050000000-3.0518e-053.0518e-05-3.0518e-050-
3.0518e-050000-3.0518e-050000000003.0518e-0500000000000000-3.0518e-
050003.0518e-050000-3.0518e-050-3.0518e-0503.0518e-05003.0518e-
0500000000003.0518e-05-3.0518e-050-3.0518e-0500-3.0518e-050000-3.0518e-
05000003.0518e-050000000-3.0518e-05000000-3.0518e-05000000-3.0518e-050-3.0518e-
0500003.0518e-050000000000003.0518e-0500003.0518e-050-3.0518e-0503.0518e-
050000000-3.0518e-05-3.0518e-050003.0518e-050-3.0518e-0500-3.0518e-05000-
3.0518e-05003.0518e-050000003.0518e-0500003.0518e-050003.0518e-053.0518e-
050000003.0518e-0503.0518e-050003.0518e-05000-3.0518e-053.0518e-053.0518e-050-
3.0518e-05000000000003.0518e-0503.0518e-0500000-3.0518e-0503.0518e-0500-
3.0518e-050-3.0518e-0500-3.0518e-05000000000000000000000000000000000-3.0518e-
050000000-3.0518e-0500000000000000000000003.0518e-05-3.0518e-
0500000003.0518e-0500000-3.0518e-050000000000-3.0518e-05-3.0518e-05-3.0518e-05-
3.0518e-050-3.0518e-05000000-3.0518e-05-3.0518e-050-3.0518e-05000-3.0518e-
0500000003.0518e-0500000000003.0518e-053.0518e-05000000000003.0518e-
05000003.0518e-053.0518e-0500000-3.0518e-050000003.0518e-05003.0518e-
050003.0518e-05003.0518e-0503.0518e-053.0518e-0500000000003.0518e-0503.0518e-
053.0518e-05-3.0518e-05000000000003.0518e-05003.0518e-050003.0518e-05000-
3.0518e-05003.0518e-05000000-3.0518e-053.0518e-050000-3.0518e-05-3.0518e-
053.0518e-050.000915530.000915530.000152590.00012207-0.00027466-0.00036621-
0.0014038-0.0019836-0.0007019-0.00033569-0.00082397-0.0011597-
0.000976560.000274660.000762940.000854490.000915530.000305180.000213620.00149
540.00308230.00314330.0013123-0.00048828-0.000732420.000427250.00067139-
0.00048828-0.000427250.00051880.00073242-0.00073242-0.0032654-0.0030212-

0.0007019-0.00036621-0.0011292-0.000427250.000854490.00057983-0.0011292-
0.002533-
0.00189210.000152590.00125120.00195310.0034790.00457760.00326540.00109860.000
39673-3.0518e-05-0.00085449-0.0020142-0.001709-0.00048828-0.0018311-0.0039978-
0.0043335-0.0024719-0.0013123-
0.000976560.000335690.00149540.00152590.00219730.00225830.00167850.00186160.0
0167850.00109860.000610350.000366210.000274660.00051880.000854490.00073242-
0.00045776-0.0018311-0.0025024-0.0022888-0.0011597-
0.000335690.000305180.00051889.1553e-05-0.00061035-0.00057983-
0.000305180.000305180.00222780.00305180.0011902-0.00042725-6.1035e-059.1553e-
05-0.0007019-0.0015564-0.0018616-
0.00140380.000122070.00122070.00128170.0005188-0.00015259-0.00076294-
0.0018005-0.00177-0.00051880.00109860.00207520.00149540.00027466-
0.000152590.000823970.00076294-0.0011902-0.0017395-

OUTPUT OF CONVOLUTION CODER

1110111001110011001110001100101101111100011011001111100000101011111010111
1010000100110010101100000111110110100101001001101110100010001110010101111
1001010000110000001101101100110000111011011111110011010101000011001101100
0010100011010100011100110101101100100110111101001001110101100001000000100
1111001110001111111011101001001110100001100111100001111100100000011101000
1110001001111011010100011100011010011011000101111011100101110111100011000
010001100010111101

OUTPUT OF INTERLEAVER

1111110000011111100001011101101010110101101101001101010110001110110111100
1010001110000111001000110101101010110010100101100110101001110101000111001
1101101010000010100010010011111010100011111011111100100001000111110010011
0001010001001111010001001111000110100111110010100101111100100000001001011
1010100001011111110111010110100011011000001101010110010111010010101000111
0100000101111011001111010000100101110100011110011111011010111001010001011
101000000111100111

OUTPUT OF DEMODULATION

0101101001011101101111100100101101001010001001000101100000101100100101101
1110111001111111001010001111101001110111000011011100111100010110000100010
0011110110011011010000110111100011111101010001110110011001010010000011010
0000010101000111111010000100110010101000010010100110000011101011000101001
1001101011101100010111111100010110000110011101010000101000110110111001010
0110010110011000000010111011000111100110001000110111110111011101000110100
0001000011000011101110010111100101111001011110010111100101111001011110010
1

OUTPUT OF DEINTERLEAVER

1110111001110011001110001100101101111100011011001111100000101011111010111
1010000100110010101100000111110110100101001001101110100010001110010101111
1001010000110000001101101100110000111011011111110011010101000011001101100

00101000110101000111001101011011001001101111010010011101011000010000001001111100111000111111101110100100111010000110011110000111110010000001110100011100010011110110101000111000110100110110001011110111001011101111000110000100001100010111101

VITERBI DECODING

11101110011100110011100011001011011111000110110011111100000101011111101011110100001001100101011000001111101101001010010011011101000100011100101011111001010000100110010101100000111110110100101001001101110100010001110010101111100101000001100000011011011001100001110110111111100110101010000110011011000010100011010100011100110101100100110111101001001110101101000010000001001111001110001111111011101001001110100001100111100001111100100000011101000111100010011111

RECOVERED SPEECH

0.001556400.000152590.001647900.000244140.0048523-3.0518e-050.00054932-0.00433359.1553e-05-3.0518e-050.004760700.00018311-0.001586900.000152590.000213623.0518e-05-6.1035e-050.001464800.000152590.0032043-3.0518e-050.00039673-0.00131233.0518e-050.00012207-0.0061349.1553e-05-0.00061035-0.000396730-0.00045776-0.00039673-6.1035e-05-0.00012207-6.1035e-05-3.0518e-05-9.1553e-05-0.0061346.1035e-05-3.0518e-050.000244140.00018311-3.0518e-05-0.00411990.000366219.1553e-05-0.00158690.0001220700.00018311-6.1035e-0500.00329590.000274663.0518e-050.0046387-9.1553e-050-0.00296029.1553e-05-3.0518e-050.000396730.000274663.0518e-05-0.00302120.000152599.1553e-05-0.0037231-0.0003967300.0011292-0.00045776-6.1035e-05-0.0048218-6.1035e-05-3.0518e-05-0.00164790.000122076.1035e-05-0.00320430.000244140.00018311-3.0518e-050.000549320.00033569-0.0015259-3.0518e-059.1553e-0500.000183110-0.00155640.000152590.00021362-0.0030518-6.1035e-05-9.1553e-05-0.00152590.000152599.1553e-05-0.00161740.000396730.00024414-0.00622560.000122070.000122070.0016174-0.00061035-0.000396730.0046387-0.00045776-0.00039673-0.0016174-0.00012207-6.1035e-05-9.1553e-05-9.1553e-050.000122076.1035e-05-3.0518e-050.000244140.001709-3.0518e-050.000549320.00344859.1553e-05-3.0518e-050.004760700.000183113.0518e-0500.00015259-0.00131233.0518e-05-6.1035e-05-0.006378200.00015259-0.0030212-3.0518e-050.00039673-0.00445563.0518e-050.000122079.1553e-059.1553e-05-0.00061035-0.00350950-0.000457760.0042419-6.1035e-05-0.000122070.00149540000.0015564-0.0001525900.0045776-0.00039673-6.1035e-05-0.00173950.00012207-0.000488280.0020447-0.00024414-0.000396730.0014038-6.1035e-059.1553e-050.0047302-0.00036621-0.00033569-0.0017090.00018311-0.00045776-0.00109863.0518e-05-0.00045776-0.00152590.000244140.0002746609.1553e-050.00018311-0.000122079.1553e-050.000183110.0030823-0.000305183.0518e-05-0.00491330.00042725-0.00329590.0005188-6.1035e-05-0.0064392-0.00024414-6.1035e-050.0048828-6.1035e-05-0.00018311-0.0045471-0.000488280.00048828-0.00024414-0.00039673-0.00015259-0.00631719.1553e-053.0518e-05-0.0066223-0.00030518-0.000152590.0048523-0.000488280.000488280.0015869-0.000457766.1035e-05-0.00131230.0002746600.00164790.00021362-0.00012207-0.00616460.00015259-

6.1035e-05-0.00189210-0.000244140.00354-0.000213620.0005188-0.0016479-
0.00021362-0.000244140.00302120.00021362-6.1035e-05-0.0017090.00012207-
0.000488280.005127-0.00024414-0.00039673-0.001709-6.1035e-059.1553e-05-
0.0047302-0.00036621-0.00033569-0.00491330.00018311-0.00045776-
0.00573733.0518e-05-0.00045776-0.00149540.000244140.00027466-3.0518e-059.1553e-
050.000183110.00457769.1553e-050.00018311-0.00012207-0.000305183.0518e-05-
0.000244140.00042725-0.00640870.0005188-6.1035e-050.0029297-0.00024414-6.1035e-
05-0.0044861-3.0518e-05-0.00018311-0.0029907-0.00051880.000488280.0043945-
0.00039673-0.000152590.00143439.1553e-053.0518e-05-0.0034485-0.00033569-
0.000152590.0016785-0.000457760.00048828-0.0015259-0.000457766.1035e-05-
0.0060730.0002746600.00158690.00018311-0.00012207-0.00299070.00018311-6.1035e-
05-0.000305183.0518e-05-0.000244140-0.00625610.00106810.000213620.0046997-
0.00036621-0.000213620.000488280.000396730.00045776-0.00067139-0.00064087-
0.000396730.000122070-9.1553e-0509.1553e-050.00018311-
0.00616460.00106810.00021362-0.00155640.0007019-3.0518e-05-
0.00579830.00186160.00064087-0.00640870.00158690.00018311-
0.00592040.00210570.00042725-0.0061340.00210570.0005188-
0.0061340.00204470.000396736.1035e-050.00103760.00454710.000366210.00064087-
0.0046692-0.00051880.00042725-0.00112920.00045776-0.00067139-0.0021973-
0.000396730.000122070.0031128-9.1553e-050-0.00146480.000183119.1553e-
050.00106810.000213623.0518e-050.0037537-3.0518e-
050.000457760.00183110.00064087-
0.000152590.00619510.000183110.000335690.00360110.000427259.1553e-
050.000488280.00051880.000122070.000427250.000396730.00317380.00103760.001434
30.0034790.000640876.1035e-050.00415040.000427250.000396730.0020142-
0.00067139-0.00064087-0.003546.1035e-0500.001464809.1553e-05-0.00604253.0518e-
050.00106810.0048828-3.0518e- 0.00137330.000274660.0021057-0.00271619.1553e-
050.00210570.0052490.000122070.00204470.000335696.1035e-050.00103760.0014648-
0.00122070.000640876.1035e-05-0.00521850.000427250.000396730.0051575-
0.00067139-0.000640870.00427250.0001220700.003021203.0518e-05-
0.00137339.1553e-050.0010376-0.00292973.0518e-
050.000640870.00155640.000457760.0018005-0.0040588-
0.000152590.00152590.001770.000335690.0020447-0.00582899.1553e-
050.00204470.00521850.000122070.00204470.0050659000000-0.00311280-
0.000152593.0518e-050.000396730.000183110.00454710.000427250.00018311-6.1035e-
05-0.00054932-0.00033569-0.0045166-0.00057983-
0.000213620.00476070.000579830.00061035-0.00177-6.1035e-05-0.00036621-0.006012-
0.00039673-0.00024414-
0.00476070.000976560.000122070.00140380.00134280.000244140.00283810.00048828-
0.000213620.0030823-0.000457760.00448610.00012207-0.0007019-
0.000244140.00021362-0.00039673-0.0015869-0.000152593.0518e-05-
0.00115970.00018311-0.00015259-0.00582890.00018311-6.1035e-050.0041199-
0.000335690.00018311-0.0021362-0.000213626.1035e-050.00210570.00061035-
0.00021362-0.0062866-0.000366210.00021362-0.0066223-0.00024414-9.1553e-05-
0.000579830.00012207-0.00015259-0.00494380.00024414-0.000274660.0052185-

0.00021362-3.0518e-05-0.00051880.00137330.00012207-0.0007019-
0.00180050.00021362-0.00036621-0.0062561-0.000152596.1035e-
050.00506590.00021362-0.00015259-0.00582890.00018311-6.1035e-05-0.0021362-
0.000366210.00018311-0.00057983-0.000213626.1035e-050.000579830.00054932-
0.00021362-0.0062866-0.000335690.00021362-0.0019836-0.00027466-9.1553e-
050.000976560.00012207-0.00015259-0.00491330.00018311-0.000274660.0020447-
0.00027466-3.0518e-05-0.00045776-0.00491330.00012207-0.0007019-
0.00180050.00021362-0.00039673-0.0032043-0.000152593.0518e-05-
0.00122070.00018311-0.000152590.00350950.00018311-6.1035e-050.00094604-
0.000335690.00018311-0.0020752-0.000213626.1035e-050.00213620.00064087-
0.00021362-6.1035e-05-0.000396730.000213620.0027161-0.00030518-9.1553e-
050.00567630.00015259-0.000152590.00134280.00018311-0.000274660.00048828-
0.00021362-3.0518e-0500.00469970.00039673-0.000427250.00115976.1035e-05-
0.00039673-0.0019531-0.00070196.1035e-05-0.0044861-0.000427250.00054932-
0.000946040.000213620.00045776-0.00122070.000396730.000213623.0518e-053.0518e-
053.0518e-05-3.0518e-050.00012207-6.1035e-05-3.0518e-0500-0.0015564-
0.000122070.000122070.000152593.0518e-059.1553e-050.00476070.00057983-
0.00042725-0.0036011-0.0003662100-0.000549320.00057983-0.000152596.1035e-
050.00012207-0.0050964-0.00039673-0.00070196.1035e-050.00021362-
0.000427250.00210570.000610350.00021362-
0.0026550.000335690.000396730.000213623.0518e-053.0518e-05-0.0015564-3.0518e-
050.00012207-0.0031738-3.0518e-0506.1035e-050-0.00012207-
0.00140380.000152593.0518e-05-0.00149549.1553e-050.000579830.0042114-
0.00045776-0.0003662100-0.000549320.000579830.00140386.1035e-050.00012207-
0.00039673-0.00039673-0.00073242-0.00152590.00021362-
0.000427250.000549320.000610350.000244140.000457760.000335690.000366210.00021
3623.0518e-053.0518e-050.0046997-3.0518e-050.00012207-6.1035e-05-3.0518e-05-
6.1035e-050.00155640-0.000122070.000122070.000152593.0518e-05-0.00146489.1553e-
050.00054932-0.0019836-0.00045776-0.00036621-0.00622560-
0.000549320.000549320.00451666.1035e-050.00012207-0.0066528-0.00039673-
0.00073242-0.00619510.00021362-0.00045776-0.00570680.000610350.00024414-
0.00109860.000335690.00039673-0.00292973.0518e-053.0518e-05-0.0062256-3.0518e-
050.000122070.0015259-3.0518e-050-0.00625610-0.00012207-
0.00610350.000152593.0518e-05-0.00616469.1553e-050.00057983-0.0066833-
0.00045776-0.00036621-0.00619510.0046997-3.0518e-05-0.00015259-0.0018616-
3.0518e-050.00033569-0.0017395-0.00057983-6.1035e-050.000274660.00030518-
0.000122070.00469970.00021362-6.1035e-05-0.0018616-9.1553e-050.00030518-
0.00015259-0.00057983-0.00012207-0.00454710.000335690.000152590.001776.1035e-
05-0.000244140.001770.00051880-0.0018311-0.000274660.000183110.0047607-
0.00024414-0.00033569-0.001770.000244140.00036621-0.00021362-0.0068665-9.1553e-
0500.0030518-6.1035e-050.00030518-0.001709-0.00057983-6.1035e-05-
0.00286870.00030518-0.00012207-0.00625610.00021362-6.1035e-05-0.0018616-
6.1035e-050.000305180.0014038-0.00061035-0.00012207-
0.00140380.000335690.000152590.00491330-0.00024414-0.00604250.000549320-
0.0033875-0.000274660.00018311-0.0061646-0.00027466-

0.000335690.00292970.000305180.00036621-0.00021362-0.00061035-0.00164790-
6.1035e-05- 0.00164790.00030518-0.00021362-0.0036926-6.1035e-050.00030518-
0.0012512-0.0001220700.00021362-6.1035e-05-0.000335690.00457760.00030518-
0.00021362-0.00057983-
0.000122070.000122070.00500490.000152590.000244140.0047302-
0.000244140.00018311-0.0025940-0.00021362-0.00183110.0001831100.0013123-
0.00033569-0.00021362-0.0060120.00036621-0.00030518-0.00061035-9.1553e-05-
3.0518e-05-6.1035e-05-9.1553e-050.0018005-0.00015259-0.00057983-
0.00158690.000274660.00030518-0.006378200.00018311-0.0047607-0.00030518-
0.000122070.00030518-0.00015259-0.00061035-
0.00482180.000152590.000305180.000152590.000213626.1035e-05-
0.000244140.000213620.00057983-0.0031128-0.00024414-0.00027466-
0.00140386.1035e-05-0.00021362-0.003479-0.000183110.000305180.0050659-
0.00021362000-0.00155640-0.000152599.1553e-0500-0.00155640.00018311-
0.000152590.00012207-3.0518e-05000.00018311-3.0518e-050.004730200.00045776-
0.00186160-0.000183110.0047913-0.000549320.00042725-0.00195310.00024414-
0.00015259-0.0029602-0.00061035-0.00021362-0.00616460.00024414-
0.000610350.000427250.000335699.1553e-05-

APPENDIX - B

Notes :

a) The switch represents the possibility to have different modes for modeling voiced/unvoiced/combined frames. There are two excitations (e(n)):filtered impulse train (U_v), or white noise (U_n). Excitations are scaled with some scalar g_v and g_n respectively. The switch between the different excitations selects whether speech is voiced, unvoiced

or in some cases a scaled combination of both (transitions).

$$H(z) = \frac{1}{1 + \sum_{i=1}^{p} a_i z^{-i}} = \frac{1}{A(z)},$$

modulates the excitation and output speech is produced. This LPC-synthesis filter has the form of an all-pole IIR-filter (the output depends only on previous outputs and current input).

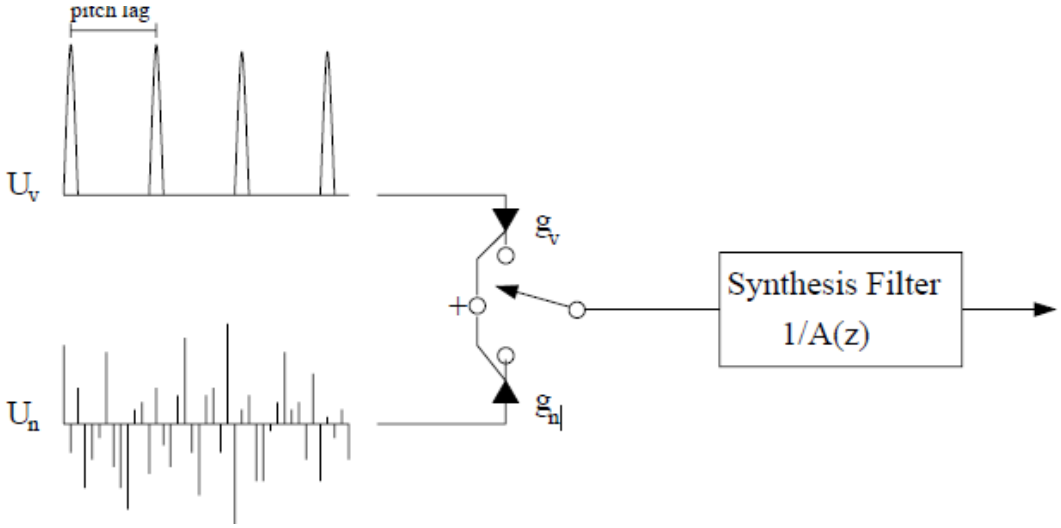


Figure (26): Speech production model featuring dual excitation and synthesis filtering

Excitation is ideally either a regular pulse train U_v or white noise U_n like presented in Figure (24). Gains g_v and g_n decide by what amount the current time instant is considered to be voiced or unvoiced. If the current time frame

is considered to be totally unvoiced like the consonant /s/, the excitation is pure white noise and gv = 0. Noise is generated with some pseudo-random algorithm. However, if the time frame is considered more or less voiced, the pitch lag and both gains also have to be estimated.

Formally pitch is the auditory percept of tone. Usually pitch is the same as the shortest period of the signal when it starts to repeat itself, but auditory perception may differ from this smallest _true_ pitch period (f0), which is estimated with a different method e.g. visually or through listening tests.

b) Because the LPC is quite heavy to calculate directly with matrix inversion when the number of predictor coefficients increases. The most used method, the Levinson-Durbin recursion, uses the autocorrelation function

Levinson-Durbin recursion :

is a procedure in linear algebra to recursively calculate the solution to an equation involving a Toeplitz matrix The algorithm runs in Θ(n2) time, which is a strong improvement over Gauss–Jordan elimination, which runs in Θ(n3).

Toeplitz matrix :

diagonal-constant matrix, named after Otto Toeplitz, is a matrix in which each descending diagonal from left to right is constant. Any n×n matrix A of the form

$$A = \begin{bmatrix} a_0 & a_{-1} & a_{-2} & \dots & \dots & a_{-n+1} \\ a_1 & a_0 & a_{-1} & \ddots & & \vdots \\ a_2 & a_1 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & a_{-1} & a_{-2} \\ \vdots & & \ddots & a_1 & a_0 & a_{-1} \\ a_{n-1} & \dots & \dots & a_2 & a_1 & a_0 \end{bmatrix}$$

is a Toeplitz matrix. If the i,j element of A is denoted Ai,j, then we have

$A_{i,j} = A_{i+1,j+1} = a_{i-j}$.