HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

NGUYỄN THANH BÌNH

XÂY DỰNG GIẢI PHÁP TRUYỀN DỮ LIỆU QUA KÊNH THOẠI CỦA MẠNG GSM VÀ ỨNG DỤNG THUẬT TOÁN SINH SỐ GIẢ NGẪU NHIÊN DỰA TRÊN CÁC DÃY PHI TUYẾN LỒNG GHÉP ĐỂ BẢO MẬT DỮ LIỆU

Chuyên ngành: Kỹ thuật điện tử

Mã số: 9.52.02.03

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – 2022

Công trình được hoàn thành tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Người hướng dẫn khoa học:

GS. TSKH Nguyễn Xuân Quỳnh

Phản biện 1:

Phản biện 2:

Luận án được bảo vệ trước Hội đồng chấm luận án cấp Học viện họp tại:

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

Vào hồi giờ ngày tháng năm 2022

Có thể tìm hiểu luận án tại thư viện:

1. Thư viện Quốc gia

2. Thư viện Học viện Công nghệ Bưu chính Viễn thông

PHẦN MỞ ĐẦU

Trong mạng viễn thông di động GSM đã có bảo mật và an toàn thông tin bằng các thuật toán sinh khóa, xác thực và mã hóa (A8, A3, A5). Tuy nhiên, thuật toán xác thực, bảo mật trên là không bảo đảm cho mục đích bảo mật thông tin trong các giao dịch quan trọng, đặc biệt là trong quốc phòng, an ninh. Đây chính là mục tiêu và là tính cấp thiết của Luận án đặt ra.

Trong lĩnh vực quốc phòng, an ninh truyền dẫn liên mạng IP – GSM/3G/LTE – PSTN – Satellite – HF/VHF/UHF là yêu cầu thực tế. Từ thực tiễn này, đòi hỏi cần phải có giải pháp và kỹ thuật để dễ dàng kết nối liên thông – bảo mật thông tin thoại và dữ liệu cho đa môi trường truyền dẫn trên, đây chính là mục tiêu, giải pháp Luận án cần nghiên cứu giải quyết.

Ngoài ra, việc sinh khóa, xác thực và mã hóa cần có các thuật toán đủ mạnh để bảo mật thông tin quốc phòng an ninh. Từ đó đặt ra là cần nghiên cứu, xây dựng thuật toán mạnh, nhưng thuật toán đó độ phức tạp thực thi tương đối để phù hợp với ứng dụng cài đặt, chạy trên thiết kế có tài nguyên hạn chế.

Mục tiêu nghiên cứu: Có 03 mục tiêu chính

- Nghiên cứu, đề xuất giải pháp truyền dữ liệu thoại đã mã hóa hiệu quả trên các thiết bị đầu cuối đi qua các kênh thoại trên các liên mạng truyền dẫn viễn thông khác nhau; thực hiện mã hóa bảo mật thông tin thoại **Số** thông suốt từ thiết bị thoại đầu cuối đến đầu cuối trong các dịch vụ thoại, dữ liệu mạng di động các thế hệ 2G/3G/LTE và mạng PSTN đảm bảo chất lượng tiếng nói ở mức chấp nhận được sau giải mã, và phổ tần tín hiệu tiếng nói sau mã hóa tựa nhiễu trắng.

- Lựa chọn và xây dựng thuật toán đảm bảo độ tin cậy, tính khả thi về khả năng thực hiện thời gian thực thuật toán trên các thiết bị có tài nguyên tính toán hạn chế, nhưng phải bảo đảm độ phức tạp tính toán để đạt được Độ mật ở mức cao nhất.

- Thực thi thuật toán mã hóa, thuật toán nén tín hiệu tiếng nói và điều chế để truyền dữ liệu đã được bảo mật truyền qua kênh tiếng nói mạng GSM,

không yêu cầu thay đổi cấu hình thiết bị đầu cuối đang dùng, không yêu cầu thay đổi dịch vụ mạng viễn thông đang dùng, đảm bảo tính dịch vụ liên mạng.

Phạm vi nghiên cứu

(i) Nghiên cứu các phương pháp nén và các bộ mã tín hiệu tiếng nói; nghiên cứu về đặc điểm cơ bản mạng truyền dẫn thoại (tập trung vào mạng PSTN và GSM);

(ii) Nghiên cứu về phương pháp điều chế/giải điều chế dữ liệu;

(iii) Nghiên cứu mô hình toán học, xây dựng và đánh giá dãy PN phi tuyến có cấu trúc lồng ghép hai chiều.

Ý nghĩa khoa học và thực tiễn:

Về mặt lý thuyết, luận án đã đề xuất thuật toán và xây dựng một kỹ thuật về điều chế dữ liệu tựa ngẫu nhiên (dữ liệu thoại sau nén đã được sử dụng dãy phi tuyến lồng ghép 2 chiều mã hóa) thành dạng tín hiệu tương tự có cấu trúc phổ tần gần giống với phổ tần của tiếng nói để tránh được các bộ phân tích và nhận dạng tiếng nói trên các thiết bị đầu cuối và trên các thiết bị trong hệ thống mạng viễn thông.

Về ý nghĩa thực tiễn, kết quả nghiên cứu đã đưa ra một phương pháp, một sản phẩm hoàn chỉnh để bảo mật thông tin thoại bằng kỹ thuật số. Hướng phát triển tiếp có thể xây dựng giải pháp truyền dữ liệu mật được dấu dưới dạng tín hiệu giả thoại truyền trên các môi trường khác kênh GSM như PSTN, HF, Satellite, các mạng IP,..

Các đóng góp khoa học của luận án bao gồm:

(i) Đề xuất một kiến trúc lồng ghép mới cho m-dãy lồng ghép (một phương pháp mới sinh dãy lồng ghép và lồng ghép phi tuyến, được công bố chi tiết trong bài báo [1b]) và xây dựng giải pháp bảo mật dữ liệu thoại sử dụng thuật toán sinh số giả ngẫu nhiên dựa trên dãy phi tuyến lồng ghép kiểu mới;

(ii) Đề xuất thuật toán cải tiến tốc độ nén, nâng cao chất lượng mã thoại MELPe (có công bố các nội dung liên quan trong bài báo [2b]);

(iii) Đề xuất thực hiện kỹ thuật điều chế và giải điều chế để truyền dữ liệu thoại đã được mã hóa bảo mật qua các thiết bị đầu cuối và mạng (liên mạng) truyền dẫn và đề xuất giải pháp truyền dữ liệu thoại bảo mật qua kênh thoại GSM, các kênh hữu tuyến và vô tuyến bang hẹp khác (được trình bày cụ thể trong bài báo [3b]).

(iiii) Tùy biến rút gòn để đưa được các chương trình thực thi nén, điều chế biến đổi tín hiệu số viết mô phỏng trên máy tính vào Vi xử lý STM32 chạy đáp ứng xử lý thời gian thực (đã đóng gói được thành sản phẩm).

Bố cục của luận án:

Luận án gồm có ba chương: Chương 1. Tổng quan về vấn đề nghiên cứu; Chương 2. Đề xuất thuật toán nén, thuật toán bảo mật và truyền dữ liệu qua kênh thoại mạng GSM;

Chương 3. trình bày về m-dãy, tạo và đánh giá dãy lồng ghép phi tuyễn, thực thi bảo mật dữ liệu sử dụng thuật toán sinh số giả ngẫu nhiên dựa trên dãy phi tuyến hai chiều lồng ghép;

Chương 1: Tổng quan về vấn đề nghiên cứu

Trình bày những thông tin cơ bản liên quan đến hệ thống thông tin di động; về vấn đề an toàn và bảo mật trong mạng GSM; các phương pháp mã thoại nói chung và trong hệ thống GSM;

1.1 Tổng quan về mạng viễn thông di động GSM

Cấu trúc mạng di động GSM được chia thành 3 khối chính gồm: Khối MS, Khối trạm gốc BSS, Khối mạng lõi NSS; ngoài ra còn có 3 lớp giao diện: Um, Abit và A.

1.2. Bảo mật và một số điểm yếu vấn đề này trong hệ thống mạng GSM

Mạng GSM sử dụng thuật toán A5 để mã hóa bảo mật thoại trên kênh vô tuyến, tín hiệu tiếng nói được truyền ở dạng rõ dạng PCM và ADPCM qua mạng lõi. A5 có một số hạn chế về mật mã, không an toàn. Do đó, A5 không thể bảo đảm bảo mật cuộc gọi thoại hoàn toàn cho khách hàng. Hơn nữa,

người dùng không có quyền kiểm soát chính sách bảo mật, mã hóa của nhà cung cấp dịch vụ mạng và nhà sản xuất điện thoại di động

1.2.1. Một số tấn công bảo mật trong mạng di động GSM:

- Tấn công giả mạo thiết bị di động đầu cuối, giả mạo trạm BTS
- Nghe lén cuộc gọi
- Tấn công xen giữa (man in the middle attack).

1.2.2 Một số phương pháp bảo mật thông tin thoại di động

- Về công nghệ, chia thành 3 loại: Bảo mật hoàn toàn bằng kỹ thuật phần cứng. Kết hợp giữa sử dụng phần cứng và phần mềm. Sử dụng hoàn toàn giải pháp bảo mật bằng phần mềm (giải pháp phần mềm đơn giản, nhưng có độ an toàn, bảo mật rất kém).
- Về kỹ thuật, có thể chia thành 2 nhóm: tương tự (Scramblers) và số (Digital Voice Protection).

Bảo mật tín hiệu thoại bằng phương pháp tương tự ít được sử dụng trong các ứng dụng cần độ bảo mật cao. Để giải quyết triệt để vấn đề này, cần thực hiện mã hóa dữ liệu thoại số bằng thuật toán trao đổi khóa phiên và mã hóa đủ mạnh.

1.3 Một số đặc điểm tín hiệu tiếng nói cơ bản của mạng GSM.

Kênh thoại mạng GSM với băng tần 300-3400Hz được thiết kế để truyền tín hiệu tiếng nói, băng hẹp dẫn đến bị hạn chế tốc độ. Những bộ mã (codec) sử dụng trong GSM khai thác triệt để những thuộc tính của tín hiệu tiếng nói để thu được hiệu suất nén cao, trong khi vẫn giữ lại chất lượng tiếng nói nghe hiểu của người nghe (Điều này dẫn đến tín hiệu không phải tiếng nói bị lọc bỏ bớt bởi các bộ lọc được lập trong mã LPC), trong hầu hết các mô hình nén thoại, tín hiệu được tái tạo sẽ sai khác so với tín hiệu ban đầu. Để đảm bảo âm lượng tiếng nói trong cuộc đàm thoại, mạng GSM sử dụng bộ AGC (Automatic Gain Control) để điều khiển độ lớn biên độ đầu ra. Điều này dẫn đến biên độ của tín hiệu ra có thể khác so với tín hiệu vào; thông thường xen lẫn tín hiệu tiếng nói là những khoảng lặng, bộ phát hiện tiếng nói (VAD -

Voice Activity Detectors) có chức năng phát hiện tín hiệu tiếng nói và loại bỏ những khoảng lặng để tiết kiệm băng thông và năng lượng, vì vậy việc truyền dữ liệu có thể bỏ qua khoảng lặng.

1.4 Một số phương pháp mã hoá tiếng nói cơ bản: Mã hoá tiếng nói được chia ra thành ba loại chính là mã hoá dạng sóng, mã hoá nguồn và mã hoá lai.

Kết luận chương 1

Chương 1 trình bày tổng quan mạng viễn thông do động GSM; các lỗ hổng an toàn và bảo mật trong hệ thống mạng GSM; một số đặc điểm kênh thoại mạng GSM; cấu trúc, mô hình hóa phương thức tạo tiếng nói; một số phương pháp nén thoại trong mạng GSM; phương pháp bảo mật tốt nhất cho người sử dụng là End to End.

Chương 2: Đề xuất thuật toán nén, thuật toán bảo mật và truyền dữ liệu qua kênh thoại mạng GSM

2.1 Giải pháp mã hóa mật cuộc gọi thoại di động trên kênh GSM

Để mã hóa cuộc gọi thoại trên kênh voice GSM, có một giải pháp đơn giản là phương pháp mã hóa ở mức tương tự (trước khi tín hiệu được số hóa). Phương pháp này dễ áp dụng, song giải pháp có độ mật thấp.

Có thể sử dụng một giải pháp trung gian, đó là sử dụng chế độ truyền dữ liệu trên băng tần GSM (kênh CSD). Đây là một chuẩn truyền số liệu có sẵn trên kênh GSM được sử dụng để truyền tín hiệu Fax. Tuy nhiên việc hỗ trợ chế độ CSD hiện nay có nhiều hạn chế. Ta cũng không bàn tới việc truyền dữ liệu qua kênh IP (GPRS hoặc 3G/4G) vì lý do tính không thời gian thực, độ ưu tiên thấp.

Đề xuất phương án bảo đảm tốt nhất để mã hóa và truyền dữ liệu mật qua kênh GSM là *xây dựng module thực hiện các công đoạn: tự thực hiện Vocoder với bitrate thấp; mã hóa dữ liệu thoại thu được sử dụng một thuật toán mã đủ mạnh, có thể sử dụng mã hóa khóa đối đối xứng; điều chế dữ liệu mã thành tín hiệu trong phổ tiếng nói, đưa tín hiệu đã điều chế này (dạng*

*tương tự) vào đầu vào của thiết bị đầu cuối (ME) thuộc hệ thống GSM truyền qua kênh GSM thông thườn*g, việc này như là phát triển một Modem làm việc trên kênh thoại 2G/3G, *nếu làm được Modem có tính năng này, thì Modem này không chỉ cho phép truyền dữ liệu qua kênh Voice GSM 2G/3G, mà nó còn có thể truyền dữ liệu qua tất cả các giao thức, các mạng cho phép truyền thông tin thoại như các mạng điện thoại chuyển mạch gói, mạng vô tuyến công nghệ SDR, OTT,..* Ở bên máy thu, ta sẽ thực hiện các bước theo thứ tự ngược lại để thu được tín hiệu tiếng nói ban đầu.

Có hai vấn đề cần quan tâm khi thực hiện phương án này: cần xử lý điều chế ở mức thời gian thực; sử dụng một giải pháp Vocoder có Bitrate đủ thấp để có thể điều chế lại thành tín hiệu trong phổ tần và giống tín hiệu tiếng nói (Chú ý là tín hiệu này lại thông qua tầng Vocoder của GSM một lần nữa, do đó bị ảnh hưởng bởi bộ phát hiện tiếng nói tích cực VAD), cần chỉnh sửa bộ điều chế để truyền dữ liệu đủ hiệu quả và tránh việc bị VAD xác định là không phải tiếng nói.

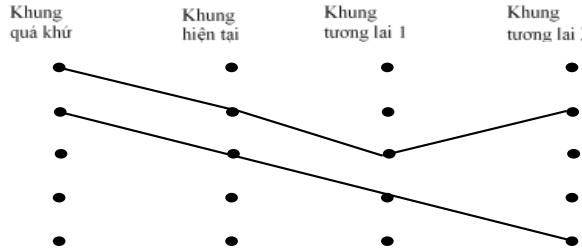
2.2 Đề xuất bộ mã hoá dự đoán tuyến tính kích thích hỗn hợp MELP tốc độ thấp cải tiến

Điểm mấu chốt trong thỏa hiệp giữa chất lượng và tốc độ của bộ mã thoại là độ chính xác của xác định Pitch vì Pitch không chỉ xác định chính xác tần số cơ bản mà còn ảnh hưởng đến việc nội suy tất cả các tham số khác [*19*].

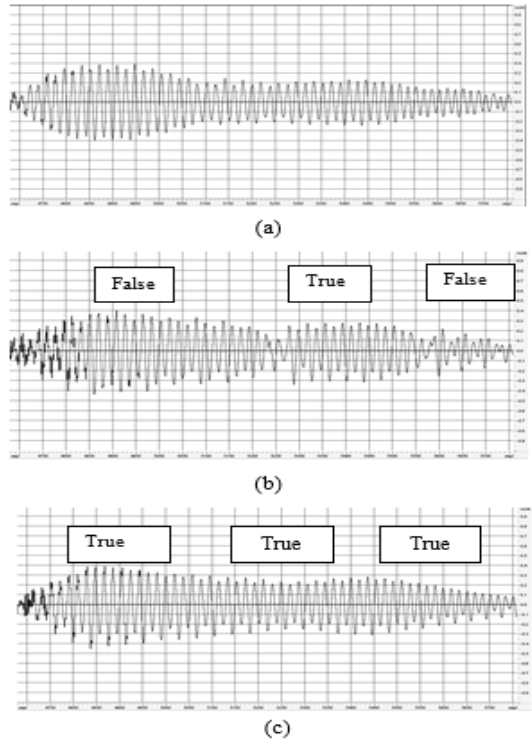
Một vấn đề khác, là hiện tượng thay đổi Pitch đột ngột do ảnh hưởng của cấu trúc hài hay nhiễu. Để giải quyết vấn đề này, phương pháp bám pitch được thực hiện theo quy hoạch động, khắc phục được hiện tượng trên nhưng không làm mất độ chính xác của pitch như các phương pháp làm trơn thông thường khác.

Để thực hiện, các tham số pitch và sai số phổ tương ứng của bốn khung được sử dụng bao gồm: khung quá khứ, khung hiện tại, và hai khung tương lai. Trong mỗi khung, chọn ra 5 Pitch $P_j[i]$ ($i = 0 \div 4$) có sai số phổ tương ứng nhỏ nhất $V_j[i]$. Mục đích cuối cùng là tìm là pitch thực sự của khung hiện tại. Theo phương pháp quy hoạch động, pitch cần tìm trong khung hiện tại sẽ

nằm trong đường pitch có trọng số nhỏ nhất. Lưu ý là do chỉ bám pitch trên các khung voice liên tục nên nếu đường pitch gặp một khung unvoice thì sẽ kết thúc ngay ở đó.



Hình 2.1. Bám pitch theo phương pháp quy hoạch động



Hình 2.2. So sánh chất lượng MELP chuẩn và iMELP cải tiến; (a) Tín hiệu gốc; (b)Tín hiệu MELP chuẩn; (c) Tín hiệu iMELP cải tiến ở tốc độ 1200bps

Hình 2.2 thể hiện ưu điểm của MELP cải tiến so với MELP. Các âm đột biến khó chịu do xác định sai pitch (thể hiện rõ nhất tại vùng cạnh đường chấm, tức là các vùng mà MELP bắt đầu xác định sai pitch) trong MELP đã được loại trừ trong MELP cải tiến.

Bước tìm pitch nguyên không yêu cầu tìm ngay được pitch thực sự, giá trị pitch tìm được trong bước này là bội hay chỉ gần pitch thực sự cũng là đạt yêu cầu. Thủ tục tìm pitch phân và tìm pitch cuối cùng sẽ xác định làm tinh và xác định pitch thực sự.

Đánh giá chất lượng thoại theo PESQ của ITU với bộ nén thoại iMELP cùng với LPC10 (trong bộ Matlab) được như bảng sau:

Bảng 2.1 Đánh giá bộ nén

Thoại gốc	Đã nén	MOS
ORG_nguyen_hue.wav	iMelp_nguyen_hue.wav	2.066
org_nh.wav	iMelp_nh.wav	2.545
sample_vinh8.wav	iMelp_1200_vinh.wav	2.614
ORG_nguyen_hue.wav	LPC_nguyen_hue.wav	1.437
org_nh.wav	LPC_org_nh.wav	1.459

2.4 Giải pháp điều chế để truyền dữ liệu qua kênh thoại GSM

2.4.1 Phương pháp điều chế tín hiệu tựa tiếng nói (speech-like waveform)

speech-like waveform là phương pháp truyền dữ liệu dưới dạng tổng hợp thành tiếng nói và cơ bản sử dụng 3 đặc tính chính:

1) Đường bao của phổ tiếng nói được biểu diễn bởi các tần số phổ vạch.

2) Tần số cơ bản hoặc cao độ của giọng nói (pitch)

3) Hình dạng và năng lượng kích thích (ACELP hoặc CELP)

Các thông số nêu trên được bảo tồn khi truyền qua kênh thoại GSM và PSTN.

Dữ liệu đầu vào được ánh xạ tới các thông số trên bằng 3 bảng mã - codebook và sau đó được nhập vào bộ tổng hợp (Hình 2.9 trong Luận án). Tín hiệu tổng hợp này không phải là một ngôn ngữ nào mà nó chỉ có cùng tính chất của tiếng nói.

Có hai nhiệm vụ chính cần thực hiện trong phương pháp này: Một là chọn loại mã hóa tiếng nói nào sẽ được sử dụng và Hai là lập các bảng mã. Do hệ

thống GSM dùng mã nén tiếng nói theo thuật toán CELP – ACELP nên loại mã hóa cùng loại sẽ được chọn. Lập bảng mã là công việc phức tạp và tốn nhiều thời gian nhất. Bảng mã thực hiện ánh xạ dữ liệu vào các thông số và sau đó nhập chúng vào bộ tổng hợp tiếng nói.

Có hai phương pháp được sử dụng để điền vào các bảng mã:

Phương pháp biểu đồ.

Phương pháp Giải thuật di truyền GA.

2.4.2 Đề xuất phương pháp điều chế tín hiệu kiểu viễn thông truyền thống có cấu trúc phổ gần giống phổ của tiếng nói

2.4.2.1 Điều chế tín hiệu kiểu viễn thông truyền thống

Thực nghiệm cho thấy điều chế dịch pha (PSK) tốt hơn so với điều chế dịch biên (ASK) và điều chế dịch tần (FSK), tại sao lại như vậy: được trình bày trong báo cáo luận án. Điều chế dịch pha vi sai DPSK thường được chọn vì tính đơn giản khi thực hiện và không cần bộ thu kết hợp.

Hạn chế của phương pháp điều chế tín hiệu kiểu viễn thông truyền thống là tốc độ truyền thấp và hiện tượng mất tín hiệu do VAD. Với GSM thời gian đáp ứng của bộ lọc dự đoán thời gian ngắn STP là 5 ms, bộ lọc dự đoán thời gian dài LTP là 20 ms. Như thế thời gian truyền một ký hiệu – symbol không dưới 5 ms. Tần số truyền ký hiệu cực đại sẽ là 200 Hz (1/5ms). Nếu dùng điều chế DPSK thì tốc độ truyền chỉ là 200 bps. Để tăng tốc độ truyền phải tăng mức điều chế và khi đó sai số BER sẽ tăng. Tác động của VAD cũng cần phải được xem xét, với yêu cầu truyền dữ liệu thời gian thực không thể chấp nhận có dữ liệu các khoảng lặng, để khắc phục người ta thường chèn những đoạn tín hiệu có tính xung để "đánh lừa" bộ VAD. Khi đó phải trả giá bằng tốc độ truyền dữ liệu giảm.

Để tín hiệu modem truyền qua kênh GSM không bị gián đoạn (mất) do VAD tác động, thì tín hiệu modem phải có đặc tính sao cho VAD nhận diện như tín hiệu voice. Có 2 phương pháp: thứ nhất là điều chế tín hiệu tựa tiếng nói speech-like waveform; thứ hai là điều chế theo phương thức viễn thông

truyền thống có chèn những đoạn tín hiệu có tính xung để "đánh lừa" bộ VAD. Dựa trên phương pháp thứ hai, đề xuất kỹ thuật mới là điều chế tín hiệu kiểu viễn thông truyền thống có cấu trúc phổ gần giống phổ của tiếng nói, cụ thể là OFDM. Phổ của OFDM giống phổ của âm hữu thanh nên không cần chèn tín hiệu để đánh lừa bộ VAD. Hơn nữa, nếu lựa chọn số vạch phổ, khoảng cách giữa các vạch phổ nằm trong dải của âm hữu thanh thì dữ liệu sau khi điều chế thành tín hiệu điều chế truyền qua kênh GSM đến máy thu, được máy thu giải điều chế sẽ bảo toàn ít bị sai lệch.

2.4.2.2 Điều chế tín hiệu kiểu viễn thông truyền thống có cấu trúc phổ gần giống phổ của tiếng nói

OFDM là phương pháp điều chế đa sóng mang trực giao. Sự chồng lấn phổ tín hiệu làm cho hệ thống OFDM có hiệu suất sử dụng phổ lớn hơn nhiều so với kỹ thuật điều chế thông thường. Từ phân tích ở trên, công trình này lựa chọn phương pháp điều chế OFDM để truyền dữ liệu qua kênh GSM.

Những vấn đề mới được đề xuất là:

1) Lựa chọn các thông số

Để tín hiệu truyền qua kênh thoại GSM được bảo toàn thì tín hiệu phải có cấu trúc phổ giống phổ của tiếng nói và cần phải xem xét các đặc điểm xử lý tiếng nói của hệ thống GSM.

Thứ nhất dải phổ của OFDM phải nằm trong dải thoại 300 – 3400 Hz.

Thứ hai số vạch phổ không nên nhiều quá. Mỗi sóng mang con được điều chế số về pha hoặc biên độ với số mức là 2 (4). *Ở đây số sóng mang con được chọn là 16.*

Thứ ba khoảng thời gian truyền một symbol không được ngắn hơn thời gian giữa 2 superframe (4 frame) trong GSM là 20ms, tương ứng với tốc độ truyền symbol là 50Hz. Như vậy khoảng cách ngắn nhất giữa các vạch phổ sóng mang phụ của OFDM là 50Hz. *Trong trường hợp này chọn là 75Hz và như vậy dư 25Hz làm khoảng bảo vệ.*

Dải tần của OFDM sẽ là : 75Hz x 16 = 1200Hz ta chọn tần số trung tâm là 1500 Hz như vậy dải phổ của OFDM từ 900Hz đến 2100Hz thỏa mãn điều kiện thứ nhất là dải phổ nằm trong dải phổ của thoại từ 300 đến 3400 Hz.

Thứ tư chọn phương thức điều chế: *Ở đây điều pha QPSK được chọn cho điều chế OFDM truyền qua kênh thoại GSM*.

2) *Thực hiện điều chế OFDM với QPSK :*

Về mặt lý thuyết mà nói thì phương pháp điều chế tín hiệu tựa tiếng nói sẽ cho kết quả tốt nhất. Tuy nhiên trong thực tế rất khó thực hiện và có thực hiện được thì chất lượng cũng không cao như đã phân tích ở trên. *Thực nghiệm cho thấy điều chế tín hiệu OFDM có cấu trúc phổ gần giống phổ của tiếng nói có ưu điểm không bị VAD chặn, dễ thực hiện, kết quả khá tốt. Trường hợp kênh truyền có băng thông tối đa BER < 0.05%, trường hợp kênh truyền xấu BER không quá vài %.*

Kết luận chương 2

Chương này đã nêu ra một số phương pháp có thể mã hóa tín hiệu thoại dựa trên các đặc tính kênh để truyền qua kênh thoại GSM, như mã hóa xáo trộn phổ tín hiệu, can thiệp vào mã nguồn phần điều chế Modem GSM, sử dụng chế độ truyền dữ liệu trên băng tần GSM (kênh CSD) và đề xuất phương án nghiên cứu của Luận án để mã hóa và truyền dữ liệu cuộc gọi thoại mật qua kênh GSM. Cũng đã chỉ ra được kết quả của phương pháp này không chỉ để truyền dữ liệu qua kênh thoại GSM mà nó còn có thể được ứng dụng để truyền dữ liệu qua các kênh truyền thoại khác, như các kênh thoại vệ tinh, thoại VoIP, PSTN.

Chương này cũng đã làm rõ them về những trở ngại của đặc kỹ thuật của mạng GSM và kênh Voice GSM, đó là vấn đề tính thời gian thực, phương pháp nén tín hiệu thoại, điều chế và truyền trên bang tần hẹp, đặc tính cấu trúc khung truyền dữ liệu, chức năng nhận diện tín hiệu thoại (VAD) và phân tích, lựa chọn thuật toán nén MELP, đề xuất và thực hiện *cải tiến thuật toán MELP thành iMELP* để phù hợp với các tính chất kênh truyền (*băng tần hẹp,*

trên kênh hay lỗi bít, mất gói, mất đồng bộ và phải hiệu quả trong việc cân đối giữa băng thông và chất lượng tín hiệu thoại, đặc biệt độ phức tạp tính toán có thể thực hiện trên các Chíp ARM hay DSP) mà đề tài hướng đến.

Trong chương 2 trình bày một số phương pháp điều chế dữ liệu tựa ngẫu nhiên thành tín hiệu tựa tiếng nói mà một số nghiên cứu trên thế giới đã làm, từ đó đề xuất phương pháp điều chế, kỹ thuật lựa chọn các thông số và thực hiện điều chế OFDM với QPSK. *Đây là hướng nghiên cứu, mục tiêu chính và kết quả thực nghiệm đạt được của Luận án nghiên cứu*.

Chương 3: Bảo mật dữ liệu sử dụng thuật toán sinh số giả ngẫu nhiên dựa trên dãy phi tuyến hai chiều lồng ghép

3.1. Giới thiệu m-dãy

3.1.1. Thanh ghi dịch và đa thức nguyên thủy

Để dựng một m-dãy có độ dài $N = 2^m - 1$, ta biểu diễn đa thức nguyên thủy (prime polynomial) h(d) bậc m có dạng như sau:

$$h(d) = h_0 + h_1 d + h_2 d^2 + \ldots + h_{m-1} d^{m-1} + h_m d^m = \sum_{i=0}^{m} h_i d^i \qquad (3.1)$$

Trong đó $h_0 = h_m = 1$. Đa thức này được sử dụng để xây dựng thanh ghi dịch phản hồi tuyến tính (LFSR) như biểu diễn trong Hình 3.1 (của Luận án).

3.1.2. Dãy có độ dài cực đại

Chu kì cực đại có thể là 2^m-1. Trong tài liệu [20] đã chứng minh rằng, nếu h(d) là một đa thức nguyên thủy bậc m, thanh ghi dịch sinh bởi đa thức h(d) sẽ sinh ra dãy đầu ra có chu kỳ kì 2^m-1. Ta gọi dãy đó là m-dãy.

3.1.3. Các thuộc tính của m-dãy

Theo [*20*] một m-dãy $\{a_n\}$ với đa thức sinh h(d) có các thuộc tính:

1) Dãy có bậc m thì chu kì của dãy là $N = 2^m - 1$.

2) Có chính xác $N = 2^m - 1$ dãy không toàn '0' được tạo bởi h(d).

3) Trong số N dãy được tạo bởi h(x) có chính xác một dãy $\{a_n\}$ có tính chất: $a_n = a_{2n}$ cho tất cả n = 0,1,2,…

4) Bước chạy có độ dài m:

5) Thuộc tính cộng và dịch:

6) Số giá trị 1 trong mỗi chu kỳ là 2^{m-1}; số giá trị 0 là $2^{m-1} – 1$.

7) Hàm tự tương quan (ACF) có hai mức:

8) Nếu dãy nhị phân m được lấy mẫu với f bằng mũ 2, thì cùng dãy trả về.

9) Lấy mẫu một m-dãy với mỗi phép quay f, gcd(f,N) = 1, $1 \leq f \leq N-1$, $N = 2^m – 1$, sẽ đưa ra $\Phi(2^m-1)/m$ m-dãy có chu kì $2^m – 1$.

10) Khoảng tuyến tính bằng bậc m.

3.2 Dãy có cấu trúc lồng ghép

3.2.1 Xây dựng dãy lồng ghép và dãy phi tuyến lồng ghép

Ý tưởng cơ bản của kỹ thuật lồng ghép là dựa vào các m-dãy có độ dài có thể phân tích được thành tích và có ít nhất một nhân tử dạng $2^m – 1$. Thứ tự lồng ghép và các dãy con sẽ được xác định và quyết định cấu trúc của mã. Sau đó, chuyển đổi cấu trúc đó thành phi tuyến để tăng tổ hợp mã và độ phức tạp, có thể theo các phương pháp sau:

- Phương pháp 1: Giữ nguyên thứ tự lồng ghép nhưng thay m-dãy con thành phần bằng m-dãy khác có cùng độ dài.

- Phương pháp 2: Giữ nguyên thứ tự lồng ghép nhưng thay m-dãy con thành phần bằng dãy phân bố tựa ngẫu nhiên cùng độ dài.

- Phương pháp 3: Dùng dãy tích của T m-dãy con thành phần tạo dãy lớn.

- Phương pháp 4: Dùng dãy tích của T dãy con thành phần là các m-dãy khác nhau tạo dãy lớn.

Các phương pháp trên có thể được chia làm hai nhóm phương pháp chính là: nhóm thứ nhất là nhóm sử dụng cấu trúc lồng ghép đa cấp (thứ tự lồng ghép I_p^T) và lồng dãy con có đặc tính ngẫu nhiên được tạo từ m-dãy khác thay thế để tạo dãy phi tuyến (phương pháp 1 và 2) và nhóm thứ 2 là nhóm trực tiếp tạo dãy phi tuyến bằng cách tạo dãy tích T bậc và thực hiện nhiều cấp (phương pháp 3 và 4). Khi tạo dãy tích thông thường ta sẽ tạo được dãy có độ dài k.L (k nguyên dương tùy ý, $L = 2^m – 1$), còn khi tạo dãy lồng ghép đa

cấp phi tuyến được trình bày trong luận án này có giá trị độ dài của dãy là T.L = $2^n - 1$ (T là chu kì lồng ghép, L là độ dài m-dãy L = $2^m - 1$).

Về mặt toán học, có thể biểu diễn và phân tích dãy có cấu trúc lồng ghép bằng hai công cụ trên trường hữu hạn là hàm Vết hoặc biến đổi D. Hai công cụ toán học này là tương đương và đều là cách biểu diễn các phần tử trong trường hữu hạn. Đánh giá về 2 phương pháp này như sau:

Phương pháp dùng hàm Vết là rất thích hợp cho việc nghiên cứu tạo và lồng ghép dãy m, tuy nhiên hàm Vết chỉ có thể thực hiện được với dãy có độ dài L = $p^m - 1$, nên nó không thể được dùng cho cấu trúc lồng ghép dãy có độ dài tùy ý (L ≠ $p^m - 1$), hơn nữa nó không thể cho biết thông tin về trạng thái LFSR.

Phép biến đổi D là ngắn và dễ dàng thực hiện được, hơn nữa nó còn chứa đầy đủ thông tin về trạng thái LFSR. Phép biến đổi D có thể được áp dụng cho bất kì dãy tuần hoàn nào có độ dài có thể phân tích thành dạng L = T.N. Phép biến đổi D là phương pháp gần với phần cứng nhất, phương pháp này có thể được dùng để tính độ phức tạp (ELS) và hàm tương quan (ACF) của dãy. Do đó phép biến đổi D sẽ được để thực hiện phân tích, đánh giá và tạo dãy.

Kiến trúc dãy lồng ghép [1b]

Ta quan tâm tới m-dãy tam phân $\{b_n\}$ có độ dài L = q^n-l với q là một số nguyên tố nhận các giá trị trong tập {2, 3, 5, 7…} sao cho n=m.l.

Gọi: N = p^m-1; S = L/N

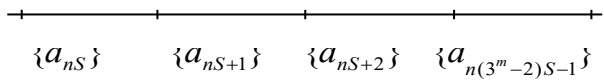
Trong bài báo [1b] đã chỉ ra rằng trong trường hợp này, ta có thể xây dựng nên dãy $\{b_n\}$ bằng cách lồng ghép (S-1) dãy con thành phần, mỗi dãy có độ dài N. Các dãy con có được bằng cách áp dụng phép nhảy bước (decimation) trên dãy $\{b_n\}$ với bước nhảy bằng S

Khi phép nhảy bước bắt đầu từ bit đầu tiên của $\{b_n\}$, ta thu được dãy con:

$$\{a_0, a_S, \ldots, a_{(3^m-2)S}\}$$

Tương tự như vậy, với vị trí bắt đầu nhảy bước là t, ta thu được dãy con $\{a_t, a_{S+t}, \ldots, a_{(3^m-2)S+t}\}$

Do đó, xét trên miền thời gian, các dãy con này (sắp xếp theo cột) có thể được coi là ghép kênh theo bước thời gian S $\{a_{nS}\}\{a_{nS+1}\}\ldots\{a_{n(3^m-2)S-1}\}$ để đặt vào S khe thời gian như trong sơ đồ dưới đây



***Sơ đồ I**: Ghép các dãy con theo thời gian.*

Thứ tự mà các chuỗi con được ghép vào trong thực tế là thứ tự lồng ghép I_P^S đã xét ở trên.

Bây giờ ta chỉ cần tìm kiếm trong Bảng 3.4 (trong Luận án) để tìm ra biển diễn theo biến đổi d $S_i(d^S)$ của dãy con (theo cột) và từ đó có được I_P^S chính là thứ tự của $S_i(d^S)$ trong Bảng 3.1 (trong Luận án). Riêng trường hợp dãy con chứa toàn giá trị con, ta coi thứ tự lồng ghép là ∞.

Trong bài báo [1b] cũng chỉ ra một tính chất quan trọng của dãy lồng ghép, đó là mỗi dãy con của dãy lồng ghép là một m-dãy với bậc m, nhưng lệch pha với nhau một khoảng xác định bằng phần tử tương ứng trong I_P^S. *Nhiệm vụ chính để xây dựng dãy lồng ghép là tìm cách tính toán trước các giá trị của* I_P^S, từ đó có thể xác định ngay được các dãy con để ghép thành dãy đầu ra

Xây dựng dãy lồng ghép phi tuyến

Có rất nhiều cách thức để tạo dãy phi tuyến, ở đây sẽ thực hiện theo cách thức lồng ghép phi tuyến dựa vào các giá trị pha tìm được và chỉ thay đổi dãy con để tạo dãy mới có khoảng tuyến tính lớn hơn. Để tạo dãy phi tuyến ta thực hiện theo những bước như sau, theo bài báo [1b]:

Ta sẽ sử dụng hai m-dãy đầu vào $\{a_n\}$ và $\{b_n\}$ với cùng bậc n và bộ tham số n, m, S giống nhau. Sử dụng kiến trúc lồng ghép, ta xây dựng nên các dãy lồng ghép với thứ tự lồng ghép I_P^S và I'^S_P tương ứng.

Trong bước này, bằng cách giữ nguyên các giá trị pha lồng ghép I_p^T và thay đổi các dãy con (dãy lồng ghép) bằng các dãy con tương ưng với dãy đầu vào thứ hai. Ở đây, thực hiện chọn m-dãy với các tính chất được tạo từ hai đa thức nguyên tố khác nhau để lồng ghép với các giá trị pha lồng ghép I_p^T khác nhau được tính từ các đa thức tạo m-dãy có bậc là bội của đa thức tạo dãy lồng ghép.

Trong phần 3.2.2.3 sau đây có các đánh giá chi tiết về độ phức tạp tuyến tính của một dãy lồng ghép phi tuyến cụ thể (sử dụng khoảng tương đương tuyến tính – ELS), từ đó kết luận rằng dãy lồng ghép phi tuyến có độ phức tạp cao hơn so với dãy lồng ghép thông thường

3.2.2. Các tính chất của dãy lồng ghép

3.2.2.1. Tính ngẫu nhiên

1) Thuộc tính cân bằng;

2) Thuộc tính chạy;

3) Thuộc tính tự tương quan;

3.2.2.2. Hàm tự tương quan

Để đánh giá đặc tính tự tương quan của dãy phi tuyến ta dựa vào dãy lồng ghép pha I_p^T của dãy phi tuyến được cho trong [22].

3.2.2.3. Độ phức tạp

Độ phức tạp tuyến tính là thông số để đánh giá độ phức tạp của dãy, được đưa ra trong [23] để đánh giá độ phức tạp của dãy phi tuyến được tạo bằng phương thức lồng ghép.

3.2.3. Các phương pháp sinh dãy lồng ghép và lồng ghép phi tuyến

Trong bài báo [1b] đã giới thiệu 3 phương pháp sinh dãy lồng ghép, trong đó phương pháp sinh dãy lồng ghép sử dụng biến đổi d và phương pháp sinh dãy lồng ghép sử dụng hàm vết là kế thừa các kết quả nghiên cứu trước đó [22][40]. *Phương pháp thứ ba tính toán trực tiếp giá trị I_P^S là một phương pháp mới, được tác giả luận án đề xuất trong công bố này*.

*** *Phương pháp tính toán trực tiếp giá trị thứ tự lồng ghép*

Thực tế khi lập chương trình trên máy vi tính để cài đặt hai phương pháp phân rã m-dãy nêu trên, việc thực hiện cả hai phương pháp trên dường như không hiệu quả, đặc biệt là khi độ dài dãy tăng lên đáng kể. Ta chỉ có thể lập được Bảng 3.1 (trong Luận án) nếu tổng kích thước của bảng có thể lưu hiệu quả trong bô nhớ máy tính hoặc thiết bị tính toán. Đồng thời ta cần phải thực hiện đầy đủ S bước để xây dựng bậc lồng ghép gồm S phần tử. Vì thế tác giả luận án sẽ giới thiệu một phương pháp hiệu quả hơn để tìm ra những phần tử đầu tiên của bậc lồng ghép.

Trước hết ta sinh ra phần đầu của chuỗi $\{b_n\}$ từ trạng thái ban đầu được cho trước, nhưng thay vì tạo chuỗi toàn chu kỳ (p^n-1 phần tử), ta chỉ cần tạo ra m.S giá trị đầu tiên.

Tiếp đó ta sẽ sắp xếp lại các giá trị này bằng cấu trúc lồng ghép theo định nghĩa của dãy lồng ghép, từ đó ta có thể nhận được trực tiếp các trạng thái ban đầu của dãy con $F_i(d)$.

Từ vị trí của trạng thái này (liên quan đến thứ tự xen kẽ), Ta chỉ cần sao chép N giá trị liên tiếp của $F_i(d)$ thành chuỗi đầu ra của dãy lồng ghép. Nếu dãy con $F_i(d)$ có kích thước quá lớn, ta có thể xây dựng lên dãy con này từ trạng thái ban đầu vừa được chỉ ra mà không cần quan tâm tới giá trị vị trí trong tập thứ tự lồng ghép.

Lợi thế của phương pháp tính trực tiếp thứ tự lồng ghép

Phương pháp tính trực tiếp thứ tự lồng ghép không yêu cầu các tính toán đa thức trên trường hữu hạn như hai phương pháp trước đó, chỉ cần sử dụng phương pháp sinh m-dãy song cũng tạo ra kết quả tương ứng. Trong trường hợp dãy con $F_i(d)$ có kích thước rất lớn, phương pháp tính trực tiếp thứ tự lồng ghép cũng cho phép sinh ra dãy lồng ghép mà không cần xây dựng toàn bộ dãy con $F_i(d)$.

Hiệu quả của phương pháp tính trực tiếp thứ tự lồng ghép: nếu sử dụng phương pháp d-Transform (phương pháp 1) ta cần tính toán toàn bộ chu kỳ

của dãy ban đầu với số lượng 2^m-1 phần tử để lập Bảng 3.1 (trong Luận án); nếu sử dụng phương pháp tính trực tiếp ta chỉ cần tính toán cho m.S giá trị đầu tiên của dãy ban đầu. Với các tham số cụ thể, hiệu quả đạt được như trong **Bảng 3.3**

Lượng bộ nhớ cần thiết cho phương pháp tính trực tiếp thứ tự lồng ghép là m.S ô nhớ. Lượng bộ nhớ này thường nhỏ hơn so với việc xây dựng toàn bộ dãy con $F_i(d)$.

Bảng 3.3 Bảng tính hiệu quả cải tiến số phép tính

STT	n	m	N	S	m.S	Tỷ lệ rút gọn
1	18	6	262143	4161	24966	9.52%
2	18	9	262143	513	4617	1.76%
3	24	8	16777215	65793	526344	3.14%
4	26	13	67108863	8193	106509	0.16%

Thực nghiệm đánh giá các dãy lồng ghép cụ thể

Tác giả đã sử dụng công cụ Matlab để mô phỏng, tính toán và thực hiện thuật toán tạo m-dãy và dãy lồng ghép:

Luận án sẽ thực hiện tạo dãy phi tuyến có độ dài $(2^{18} – 1) = 262143$ bit. Để tạo dãy phi tuyến có độ dài 262143 bit, ta thực hiện lồng ghép các m-dãy con với các đa thức nguyên thủy thuộc trường hữu hạn $GF(2^9)$ có độ dài dãy tương ứng là 511 bit theo các pha lồng ghép I_p^T được tạo dựa trên hàm Vết với các cặp phép ánh xạ $\{GF(2^{18}) \rightarrow GF(2^9)\}$.

3.3. Ứng dụng dãy lồng ghép phi tuyến trong kỹ thuật mật mã

Các nghiên cứu về kiến trúc dãy lồng ghép phi tuyến ở trên đã cung cấp một bộ tạo dãy có tính chất giả ngẫu nhiên tốt, có khả năng ứng dụng trong kỹ thuật mật mã. Để có thể áp dụng dãy lồng ghép phi tuyến vào việc mã hóa luồng dữ liệu thoại số, tác giả luận án đề xuất quy trình thực hiện như sau

Bước 1: Lựa chọn tham số

Trường Galois sẽ sử dụng là trường GF(2^n) để có thể dễ dàng khai thác các ưu thế của các hệ vi xử lý cũng như FPGA khi tính toán nhị phân.

Chọn bậc dãy ban đầu là n = 26 với m=13. Giá trị các tham số khác như sau:

S = (2^{26}-1) / (2^{13}-1) = 8193

Bộ tham số được lựa chọn như trên có một lý do khác là do với giá trị tham số này, toàn bộ tập tập thứ tự lồng ghép IPS (8193 x 16 bit) có thể lưu trữ gọn trong một Block RAM 18Kbit của FPGA.

Bước 2: Lựa chọn đa thức sinh và tính toán đa thức con

Để tạo dãy lồng ghép phi tuyến ta cần hai dãy ban đầu với hai đa thức sinh nguyên thủy được lựa chọn là:

$f(d) = d^{26} + d^{22} + d^{21} + d^{18} + d^{13} + d^{12} + d^{10} + d^8 + d^6 + d^5 + d^2 + d + 1$

$g(d) = d^{26} + d^{20} + d^{19} + d^{18} + d^{16} + d^{15} + d^{14} + d^{13} + d^9 + d^8 + d^4 + d + 1$

Với các tham số trên, ta sử dụng công thức sinh m-dãy để sinh ra hai bộ m*S bit tương ứng với hai dãy, sau đó sử dụng thuật toán Belekamp – Massey để tính được các đa thức con của hai dãy con là:

$f_1(d) = d^{13} + d^{12} + d^{11} + d^9 + d^7 + d^5 + d^4 + d^3 + 1$

$g_1(d) = d^{13} + d^{11} + d^{10} + d^8 + d^5 + d^3 + d^2 + d + 1$

Trong thực tế ta không cân sử dụng tới $f_1(d)$, chỉ cần tìm $g_1(d)$ là đủ

Bước 3: Tìm tập thứ tự lồng ghép IPS cho dãy lồng ghép thứ nhất (với đa thức sinh f(d) và đa thức con $f_1(d)$)

Tạo bảng lồng ghép từ bộ m*S phần tử của m-dãy thứ nhất theo đa thức sinh f(d)

Ta sinh ra toàn bộ chu kỳ 2^m-1 phần tử của dãy con 1 theo đa thức sinh $f_1(d)$

So sánh các cột của bảng lồng ghép với từng đoạn con m-bit lệch pha trong dãy con để xác định từng phần tử của tập thứ tự lồng ghép I_k. Nếu cột thứ k của bảng lồng ghép trung với m phần tử của dãy con bắt đầu từ vị trí j thì I_k

= j. Nếu cột thứ k của bảng lồng ghép chứa m bit toàn 0 thì ta gán $I_k = -1$ (trường hợp này theo mô tả lý thuyết ở trên thì cần đặt $I_k = \infty$, song để biểu diễn trong mảng số nguyên ta sử dụng giá trị -1).

Bước 4: Thực thi sinh dãy lồng ghép phi tuyến trong thực tế

Toàn bộ 3 bước trên là các bước tiền xử lý, thực hiện trong quá trình chuẩn bị. Dữ liệu được lưu trữ để thực thi sinh dãy lồng ghép phi tuyến bao gồm tham số n, m, S, đa thức $g_1(d)$ và tập thứ tự lồng ghép IPS.

Để sinh một phần dãy lồng ghép phi tuyến sử dụng cho việc mã hóa một buffer dữ liệu, ta thực hiện các bước sau

Sử dụng công thức sinh m-dãy để sinh đầy đủ chu kỳ của dãy con với đa thức sinh $g_1(d)$ bậc m, lưu kết quả trong mảng dữ liệu kích thước 2^m-1 phần tử. Để tránh thao tác quay vòng dữ liệu, ta copy nhân đôi mảng dữ liệu thành $2(2^m-1)$ phần tử.

Để sinh chuỗi khóa lồng ghép phi tuyến từ giá trị khởi đầu n phần tử, ta sẽ tách riêng (n-m) bit đầu tiên của giá trị khởi đầu, chuyển thành một số nguyên k để xác định thứ tự cột trong ma trận lồng ghép. Ta cũng chuyển m bit còn lại thành số nguyên t để xác định vị trí bắt đầu lấy khóa trong cột.

Như vậy chuỗi khóa lấy ra sẽ được bắt đầu từ vị trị $I_k + t$, lấy liên tục tới vị trí I_k+2^m-2. Nếu chưa đủ lượng bit khóa đầu ra cần thiết, ta sẽ tiếp tục chuyển sang các cột tiếp theo với chuỗi khóa lấy từ I_{k+1} tới $I_{k+1}+2^m-2$. Quá trình cứ tiếp tục như vậy tới khi lấy được đủ lượng bit khóa đầu ra theo yêu cầu. Nếu giá trị cột khóa vượt quá S-1 ta lại quay lại cột đầu tiên. Nếu $I_k = -1$ thì chuỗi khóa đầu ra là lấy từ một chuỗi toàn 0 kích thước 2^m-1 phần tử.

Để có thể sử dụng chuỗi khóa đầu ra trong môi trường vi xử lý, ta cần chuyển từ dãy bit thành dãy các byte nhị phân bằng cách ghép 8 bit liên tục thành một byte dữ liệu.

Quá trình mã hóa và giải mã dữ liệu thực hiện theo phương pháp mã dòng (Stream Cipher) thông thường: khi mã hóa thì bản mã là kết quả cộng module

2 từng bit (XOR) giữa bản rõ và khóa, ngược lại khi giải mã thì bản mã là kết quả cộng module 2 từng bit (XOR) giữa bản mã và khóa.

3.4. Phân tích kết quả thực nghiệm

Nền tảng thử nghiệm được xây dựng dựa trên hệ thống ARM Cortex M4. Quá trình mã hóa và giải mã được thực hiện bởi vi điều khiển STM32F437 của hãng ST dựa trên lõi ARM Cortex M4:

+ Core: Arm® 32-bit Cortex®-M4 CPU với bộ tính toán số thực FPU, hoạt động với tần số 180 MHz, tỷ suất DMIPS/MHZ cao 1.25 giúp cho hệ thống có thể đạt được hiệu năng 225 DMIPS.

+ Bộ nhớ: dung lượng bộ nhớ Flash 2 MByte, dung lượng SRAM 256Kbyte.

Bảng 3.6 dưới đưa ra độ trễ của hai chuỗi lời kiểm tra trước và sau khi tối ưu hóa. Thời gian của hai bài kiểm tra là 16,75 s và 3 s. Sau khi tối ưu hóa, độ trễ mã hóa mỗi khung hình giảm 63,6% và độ trễ giải mã mỗi khung hình giảm 41,6%. Tổng độ trễ của thuật toán MELPe trên mỗi khung hình là khoảng 55,4 ms, đáp ứng nhu cầu giao tiếp thời gian thực. Chất lượng giọng nói được kiểm tra bởi PESQ (Đánh giá cảm nhận về chất lượng giọng nói). Kết quả PESQ của giọng nói được mã hóa sau khi tối ưu hóa là 3.201, rất gần với kết quả PESQ trước khi tối ưu hóa, 3.158. PESQ cho thấy rằng việc tối ưu hóa không làm giảm chất lượng giọng nói.

Bảng 3.3 So sánh độ trễ tính toán

Thời gian thoại (giây)	Frame	Enc/Dec	Delay khi chưa tối ưu (ms)	Delay sau khi tối ưu (ms)
16.75	248	Encode	127.1	46.2
16.75	249	Decode	16.6	9.6
3	44	Encode	111.2	45.5
3	45	Decode	14.8	8.7

*** Với ba tính năng bổ sung, MELPe có hiệu suất tốt hơn ở tốc độ bit thấp hơn. Để đáp ứng nhu cầu ứng dụng kỹ thuật dựa trên ARM Cortex M4, việc tối ưu hóa được thực hiện theo hai cách, bao gồm tối ưu hóa thuật toán và tối ưu hóa mã. Sau khi tối ưu hóa, độ trễ của mỗi frame được giảm từ 135.1 mili giây xuống 55.4 mili giây mà chất lượng không giảm. Các thí nghiệm chỉ ra rằng hiệu quả của việc tối ưu hóa, đáp ứng nhu cầu thực hiện theo thời gian thực.

Kết luận chương 3

Chương 3 đã giới thiệu tổng quan về m-dãy, các đa thức các thuộc tính của m-dãy, tính chất các dãy lồng ghép; giới thiệu về cấu trúc dãy lồng ghép (bao gồm cả dãy phi tuyến lồng ghép), trong đó kiến trúc dãy lồng ghép có kế thừa nội dung các bài báo của chính nghiên cứu sinh là tác giả và đồng tác giả (bài báo số [40]); về các phương pháp sinh dãy lồng ghép và lồng ghép phi tuyến, từ Luận án nghiên cứu này nghiên cứu sinh đã đóng góp một phương pháp mới (ngoài phương pháp biến đổi -d và hàm Vết đã kế thừa từ các bài báo trước của các đồng tác giả) đó là *phương pháp thứ ba tính toán trực tiếp giá trị* I_P^S *là một phương pháp mới, được tác giả luận án đề xuất trong công bố [1b] này.*

Chương này cũng đưa ra phương pháp là lợi thế của phương pháp tính toán trực tiếp giá trị thứ tự lồng ghép; *xây dựng được bảng so sánh hiệu quả rút gọn tính toán khi ứng dụng phương pháp này*; *Ứng dụng dãy lồng ghép phi tuyến trong kỹ thuật mật mã;* Thực nghiêm đánh giá các dãy lồng ghép cụ thể**,** phương pháp thực thi dãy lồng ghép bằng phần cứng; Tối ưu và thực thi thuật toán nén/giải nén Melpe, phân tích đánh giá hiệu năng sau tối ưu và các thủ tục mã mật/giải mã bằng Vi xử lý ARM STM32F.

KẾT LUẬN

Trong quá trình thực hiện luận án, tác giả đã có một số đóng góp khoa học mới, cụ thể như sau:

(i) Đề xuất giải pháp bảo mật dữ liệu thoại sử dụng thuật toán sinh số giả ngẫu nhiên dựa trên dãy phi tuyến lồng ghép;

(ii) Đề xuất thuật toán cải tiến, nâng cao chất lượng mã thoại MELPe và giải pháp truyền dữ liệu thoại bảo mật qua kênh thoại GSM;

(iii) Đề xuất thực hiện kỹ thuật điều chế và giải điều chế để truyền dữ liệu thoại đã được mã hóa bảo mật qua các thiết bị đầu cuối và mạng (liên mạng) truyền dẫn.

Với những đóng góp khoa học nêu trên, luận án là cơ sở để nghiên cứu, phát triển cho các hệ thống truyền dẫn bảo mật tín hiệu thoại qua kênh thoại GSM và qua các nền tảng khác nhau dựa trên kênh thoại. Các thuật toán, giải pháp được chứng minh và mô phỏng, đánh giá rõ ràng, thực hiện cài đặt thuật toán trên chip ARM tạo ra Module được kiểm tra an toàn, thẩm định tính thực thi đúng đắn với lý thuyết để có thể ứng dụng trong thực tế.

Các vấn đề cần nghiên cứu tiếp

Việc phát triển thuật toán nâng cao chất lượng tiếng nói cho phép thiết kế, chế tạo phần cứng thiết bị điện thoại di động, cài đặt các thư viện, các chương trình điều khiển, các thuật toán và hoàn thiện thành một thiết bị điện thoại di động có bảo mật dùng kênh 2G của mạng viễn thông di động GSM đảm bảo tính an toàn trong cài đặt thuật toán vào thiết bị.

Hướng tiếp theo là nghiên cứu lý thuyết lấy mẫu theo Nyquist đa băng con để tăng tốc độ điều chế / giải điều chế Modem OFDM, thực thi tích hợp toàn bộ Modem này vào Chip ARM để có thể lắp vào điện thoại di động. Lập trình trên chip với không gian chật hẹp, tài nguyên hạn chế nên yêu cầu phải tối ưu hóa về tốc độ, về kích thước mã chương trình, về không gian vùng nhớ dữ liệu và vùng nhớ phục vụ thao tác tính toán. Hướng khác là tích hợp chức năng modem vào phần mềm của điện thoại di động thông minh.

DANH MỤC CÁC CÔNG TRÌNH ĐÃ CÔNG BỐ CỦA LUẬN ÁN

[1b] Hieu Le Minh, Truong Dang Van, **Binh Nguyen Thanh** and Quynh Le Chi, "Construction of Nonlinear q-ary m-sequences with Interleaved Structure by d-Transform", IEEE ICCE 2018, pp.389-392, 2018.

[2b] **Nguyễn Thanh Bình**, Nguyễn Thành Vinh, Nguyễn Xuân Liêm. "Phân tích, thiết kế tích hợp hệ mã thoại Vocoder dựa trên chuẩn MELP cải tiến phục vụ bảo mật thoại và dữ liệu qua kênh vô tuyến HF chuyên dụng", Tạp chí Khoa học và Công nghệ (Journal of Science and Technology), Số 115, bài số 10, 11/2016,

[3b] **Nguyễn Thanh Bình**, Đặng Vân Trường, Trần Văn Liên, "Một phương án truyền dữ liệu qua kênh thoại GSM", Tạp chí Khoa học Công nghệ Thông tin và Truyền thông (Journal of Science and Technology on Information and Communications), Số 03&04, trang 80 – 86, năm 2019,

[4b] Đặng Vũ Sơn, **Nguyễn Thanh Bình**, Nguyễn Hữu Trung, "Về vấn đề đảm bảo an ninh mạng thông tin vô tuyến theo tiếp cận xử lý tín hiệu nhiều chiều", Tạp chí An Toàn Thông Tin, Số 1, bài số 6, năm 2015,