Giải pháp bảo mật đầu cuối cho điện thoại di động

Trần Văn Khánh, Nguyễn Thành Vinh

***Tóm tắt*— Trong bài báo này, trên cơ sở nghiên cứu về các giải pháp công nghệ trong việc thiết kế chế tạo điện thoại di động có bảo mật trên thế giới, nhóm tác giả đã tổng hợp và đưa ra xu hướng phát triển công nghệ bảo mật cho các thiết bị di động đồng thời luận giải về các thách thức đặt ra đối với việc nghiên cứu thiết kế chế tạo điện thoại di động có bảo mật, đề xuất mô hình thiết kế chế tạo đảm bảo tính tối ưu dựa trên giải pháp bảo mật đầu cuối. Mô hình đề xuất đã được ứng dụng trong việc thiết kế, chế tạo 01 dòng điện thoại di động phổ thông có bảo mật.**

***Abstract*— In this paper, on the background of researching technological solutions to design and manufacture security mobile phones in the world, the authors synthesized and introduced the trend of developing security technologies for mobile devices, simultaneously explain the challenges posed in the design and manufacture of mobile phones security, propose design and manufacturing models to ensure optimization based on End-To-End Encryption solution. The proposed model has been applied in designing and manufacturing 01 type of security feature phone.**

***Từ khóa*— Điện thoại di động có bảo mật; mã hóa đầu cuối; Mạng thông tin di động.**

***Keywords*— Security mobile phone; End-To-End Encryption; Mobile communication network.**

I. GIỚI THIỆU

Sự phát triển của công nghệ viễn thông trong nước và trên thế giới nhìn chung đang phát triển theo con đường hướng đến hội tụ IP [1]. Mặc dù trong nước hạ tầng cơ sở viễn thông mạng GSM 2G hiện tại vẫn là ổn định và rộng lớn nhất, tuy nhiên sự phát triển của mạng viễn thông 3G, 4G-LTE thậm trí 5G sẽ là một xu thế tất yếu bởi sự phù hợp của nó với xu thế phát triển công nghệ viễn thông trên thế giới trong tương lai [2]. Xu hướng phát triển công nghệ viễn thông này đã và đang đặt ra những thách thức đối với bài toán bảo mật đầu cuối trên các thiết bị di động. Một mặt các thiết bị di động có bảo mật trong nước cần phải đáp ứng được nhu cầu cơ sở hạ tầng viễn thông thời điểm hiện tại, mặt khác phải có sự mềm dẻo, thích nghi với xu thế phát triển công nghệ viễn thông. Chính vì vậy mà giải pháp thiết kế hệ thống điện thoại di động có bảo mật nhất là tài nguyên phần cứng cho hệ thống, lựa chọn chipset GSM cần có tính mở đảm bảo khả năng nâng cấp phát triển sản phẩm phù hợp với xu hướng phát triển mạng viễn thông.

Bố cục của bài báo như sau, sau Mục giới thiệu, Mục II của bài báo sẽ phân tích các giải pháp bảo mật thoại trên mạng thông tin di động. Nhóm tác giả sẽ khái quát về công nghệ thiết kế bảo mật dựa trên nền tảng phần cứng, phần mềm, nền tảng số tương tự và tập trung ở các giải pháp công nghệ hiện đại trên thế giới như giải pháp bảo mật của Secfone, Motorola, Rohde & Schwarz, GO-Trust, GSMK... từ đó tổng hợp và đưa ra được xu hướng phát triển giải pháp bảo mật cho các thiết bị di động. Mục III trình bày về mô hình giải pháp thiết kế tổng quan dựa trên nền tảng mã hóa đầu cuối End-To-End Encryption với module mật mã được thiết kế độc lập. Mục IV mô tả tham số cấu hình thiết bị thử nghiệm, môi trường thử nghiệm, hệ thống thiết bị thử nghiệm và kết quả thử nghiệm giải pháp bảo mật đề xuất. Cuối cùng là Mục V kết luận và hướng phát triển.

II. GIẢI PHÁP BẢO MẬT THOẠI TRONG MẠNG THÔNG TIN DI ĐỘNG

Trên thị trường thế giới hiện có khá nhiều sản phẩm, giải pháp bảo mật thông tin thoại qua mạng điện thoại di động. Nhìn chung, có thể phân làm hai dạng giải pháp:

Dạng 1: Nhà sản xuất cung cấp điện thoại di động có bảo mật cho người dùng cuối theo dạng trọn gói (nghĩa là điện thoại được đưa đến tay

Bài báo được nhận ngày 29/7/2019. Bài báo được gửi phản biện thứ nhất vào ngày 02/9/2019 và được chấp nhận đăng vào ngày16/9 /2019. Bài báo được gửi phản biện thứ hai vào ngày 5/9/2019 và được chấp nhận đăng vào ngày 17/9/2019.

người dùng ở dạng một sản phẩm hoàn chỉnh gồm cả phần cứng và phần mềm ứng dụng, trong đó đã tích hợp sẵn tính năng bảo mật);

Dạng 2: Nhà sản xuất hoặc nhà cung cấp dịch vụ bảo mật chuyển giao cho người dùng cuối một gói phần mềm hoặc thiết bị bảo mật để cài đặt, tích hợp vào điện thoại di động mà người dùng cuối đang sử dụng trước đó.

Xét về mặt công nghệ bảo mật cho điện thoại di động cũng tương đối đa dạng. Tuy nhiên có thể phân thành ba nhóm:

Nhóm 1: Bảo mật hoàn toàn bằng kỹ thuật phần cứng, nghĩa là tính năng bảo mật được tích hợp sẵn như là một thành phần phần cứng của máy điện thoại (chẳng hạn như các dòng điện thoại thương mại có bảo mật của Motorola, Crypto AG; các dòng điện thoại di động sử dụng trong quân sự của nhiều nước như Liên Bang Nga, khối NATO) hoặc ở dạng một thiết bị bảo mật đường truyền, bảo mật dữ liệu âm thanh sử dụng kết hợp với điện thoại di động. Về cơ bản, các dòng điện thoại dạng này là điện thoại phổ thông (fearture-phone), chủ yếu chỉ gồm tính năng nghe gọi, nhắn tin thông qua hệ thống mạng GSM.

Nhóm 2: Kết hợp giữa sử dụng phần cứng và phần mềm trong giải pháp bảo mật. Trong đó, phần cứng Smart Card được dùng để lưu trữ các tham số bí mật và xử lý mật mã; phần mềm thực hiện các tính năng khác như quản lý cuộc gọi, giao tiếp với các tầng truyền thông hoặc ứng dụng khác trong điện thoại.

Nhóm 3: Sử dụng hoàn toàn giải pháp bảo mật bằng phần mềm.

Nhóm 2 và nhóm 3 chủ yếu áp dụng trong bảo mật điện thoại di động dạng thông minh (smart-phone), phương thức truyền dữ liệu mật (đã mã hóa) chủ yếu dựa trên nền tảng IP thông qua mạng 3G/4G.

Có một điều đáng chú ý và đã được nhiều chuyên gia nghiên cứu lâu năm trong lĩnh vực bảo mật và an toàn thông tin, các nhà mật mã học trên thế giới thừa nhận là việc sử dụng các giải pháp bảo mật điện thoại cung cấp bởi một bên không tin cậy vìkhông đảm bảo được rằng thông tin trao đổi trong các hệ thống như vậy là không bị lộ lọt hoặc nghe lén. Đối với thông tin trao đổi trong khu vực an ninh - quốc phòng hoặc thông tin liên quan đến bí mật nhà nước thì sử dụng giải pháp, sản phẩm bảo mật do một cơ quan đủ thẩm quyền trong nước đảm bảo là điều phù hợp với quy định hiện nay.

Việc sử dụng hoàn toàn các giải pháp phần mềm xét về mặt ứng dụng cũng như thiết kế chế tạo là đơn giản hơn cả so với các giải pháp còn lại nhưng lại có độ an toàn nhỏ nhất do các phần mềm bảo mật được cài đặt trên thiết bị mà nền tảng phần hệ điều hành và cả phần cứng của nó đều không được kiểm soát. Một trong những ưu điểm nổi trội khi sử dụng hoàn toàn giải pháp phần cứng đó là khả năng bảo mật của điện thoại được đảm bảo tốt hơn do các module mã hóa đã được cứng hóa trên thiết bị.

Có hai hướng áp dụng các giải pháp bảo mật phần cứng cho điện thoại di động.

Hướng thứ nhất: Xây dựng, thiết kế các chipset bảo mật chuyên dụng dạng ASIC dành riêng cho điện thoại di động Module bảo mật và mã hóa được tính toán và thiết kế ngay trong chipset. Ưu điểm của giải pháp này chính là tính tối ưu về mặt thiết kế cả về tài nguyên phần cứng sử dụng cũng như năng lượng tiêu thụ. Tuy nhiên việc thiết kế và chế tạo chipset bảo mật chuyên dụng cho điện thoại là một thách thức không chỉ về mặt công nghệ mà cả về mặt nhân lực kỹ thuật và tài chính trong nước trong thời điểm hiện tại. Trong khi đó thời gian sản xuất cũng như kinh phí phát triển sản phẩm trong tương lai cũng là một trong những yếu tố làm giảm tính ưu việt của phương pháp.

Hướng thứ hai: Thiết kế các module bảo mật độc lập kết hợp chipset được thiết kế sẵn đã được tùy biến. Phương pháp này có thời gian thiết kế nhanh hơn và và tiết kiệm hơn về mặt kinh tế khi phát triển hay nâng cấp sản phẩm do không mất công thiết kế lại từ đầu chipset dành cho thiết bị di động.

Tuy nhiên, như đã nói ở trên việc sử dụng hoàn toàn các giải pháp phần cứng dù được áp dụng theo hướng nào cũng không thể giải quyết trọn vẹn bài toán bảo mật cho điện thoại di động, đặc biệt là dòng điện thoại thông minh đang được sử dụng phổ biến trên thị trường với nguy cơ lộ lọt thông tin lớn do sử dụng các phần mềm ứng dụng trên hệ điều hành không được kiểm soát. Bởi vậy việc kết hợp cả giải pháp phần cứng và phần mềm chính là một giải pháp thiết kế chế tạo toàn diện của các dòng điện thoại thông minh có bảo mật trên thế giới.

Đối với bài toán bảo mật cho kênh thoại trên thế giới có rất nhiều mô hình giải pháp và công nghệ khác nhau. Tuy vậy có thể chia thành hai nhóm giải pháp công nghệ lớn đó là nhóm giải pháp dựa trên nền tảng tương tự (Scramblers) sử dụng các thiết bị biến đổi tín hiệu thoại và sau đó mã hóa và nhóm giải pháp dựa trên nền tảng số (Digital Voice Protection – các tham số của tín hiệu thoại được lấy và biến đổi về dạng số thông qua thiết bị vocoder, sau đó tiến hành mã). Đối với các giải pháp bảo mật thoại trên nền tảng tương tự Scramblers thường sử dụng các phương pháp mã tín hiệu thoại cơ bản như:

Dạng (1): Xáo trộn theo miền thời gian (Time-Domain Scramblers (TDS)),

Dạng (2): Xáo trộn tần số (Frequency-Domain Scramblers (FDS)),

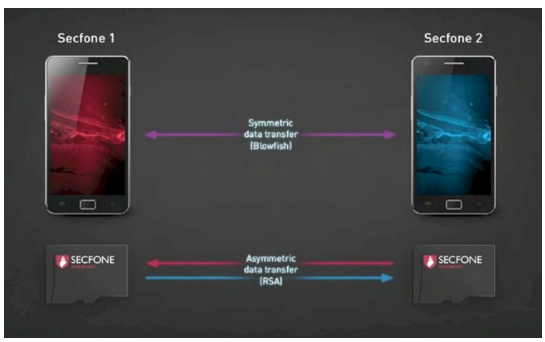
Dạng (3): Sự kết xáo trộn tần số và thời gian (Time-Frequency Scrambling (TFS)),

Dạng (4): Mã bằng phương pháp sử dụng các chuỗi Pseudo-Noise (Encryption by using Pseudo-Noise Sequences (ENS)).

Thông thường khi sử dụng các giải pháp bảo mật thoại trên nên tảng tương tự tín hiệu sau khi mã vẫn còn giữ lại một số dấu hiệu của tín hiệu thoại ban đầu khi chưa mã. Mặc dù các giải pháp bảo mật thoại dựa trên nền tảng tương tự thực thi đơn giản, giá thành rẻ và chất lượng thoại phục hồi sau mã cao tuy nhiên độ bảo mật không cao so với các giải pháp bảo mật trên nền tảng số chính vì vậy mà đối với các bài toán yêu cầu độ bảo mật cao phương pháp bảo mật trên nền tảng tương tự ít được sử dụng.

Dưới đây là một số các giải pháp bảo mật cho điện thoại di động trên nền tảng số của một số hãng bảo mật nổi tiếng.

A. Giải pháp bảo mật của Secfone



Hình 1. Giải pháp bảo mật của Secfone

Secfone cung cấp chế độ an toàn cao nhất ở mức độ quân sự cùng với ba lớp bảo vệ. Họ cung cấp dịch vụ mã hoá thoại dựa trên công nghệ VoIP cùng với giải pháp mạng đóng. Trong mạng Secfone chỉ có người nhận cuộc hội thoại mới có thể giải mã thông tin nhờ có một khoá giải mã tồn tại trong thẻ mã hoá dạng MicroSD Card. Với việc không có thông tin rõ được được lưu trên hệ thống máy chủ cũng như là khoá công khai trong hệ thống, Secfone mã hoá từng bit ở phía đầu cuối. Dữ liệu cuộc gọi cũng không đưa qua máy chủ, ngay cả dưới dạng mã hoá.

Thẻ mã hoá CryptoCard có khả năng bảo vệ khoá, cứng hoá an toàn. khả năng bảo vệ khoá cứng của Cryptochip được tích hợp trong CryptoCard có thể ngăn ngừa được việc giải mã cuộc liên lạc khi khoá giải mã bị sao chép hoặc đánh cắp. Quá trình bảo vệ được thực hiện bởi 3 mức bảo vệ riêng biệt. Cryptochip được tích hợp trong MicroSD giúp chúng có thể hoạt động với bất kỳ smartphone nào có khe cắm thẻ nhớ.

Mạng riêng mã hoá của Secfone không đơn thuần chỉ mã hoá thoại. Chúng còn mã hoá các dịch vụ dựa trên nên IP khác.

Đặc điểm:

(1) Kết nối VoIP có bảo mật thông qua mạng IP (3G/LTE).

(2) Sử dụng máy chủ MVCN™ server.

(3) 2048-bit RSA [3] để xác thực với server.

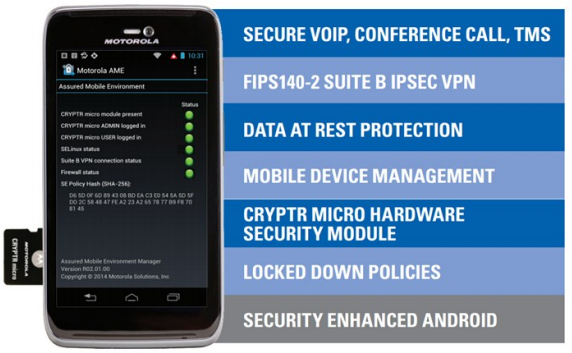
(4) 1024-bit RSA [4] để xác thực giữa các đầu cuối.

(5) 448-bit Blowfish CBC [5-7] để mã hóa dữ liệu voice giữa các đầu cuối.

(6) Tham số an toàn được lưu trên microSD card.

B. Giải pháp bảo mật của Motorola

Hãng Motorola cung cấp giải pháp bảo mật cho các cơ quan tình báo tại châu Âu, Trung Đông và Châu Phi gọi là AME 2000. AME 2000 viết tắt của từ Assured Mobile Eviroment, chúng được kết hợp giữa thiết bị phần cứng và giải pháp phần mềm để cung cấp dịch vụ mã hoá đầu cuối và trao đổi thông tin thông qua mạng riêng hoặc mạng không dây công cộng nhằm hỗ trợ các cơ quan tình báo. AME 2000 là một chiếc điện thoại thông minh cùng với hệ điều hành dựa trên Android, chúng được giới thiệu tại triển lãm Critical Communications World tại Paris từ 22/5/2013-24/5/2013.



Hình 2. Giải pháp bảo mật của Motorola

Đặc điểm chính của thiết bị:

Sử dụng điện thoại thông minh do hãng tự thiết kế (COTS-Commercial off the shelf) chạy hệ điều hành dựa trên Android.

Mã hoá đầu cuối thoại và tin nhắn giữa các thiết bị AME theo chuẩn AES 256/NSA Suite B [1-2].

Dịch vụ mạng riêng ảo (VPN) Suite B IPSec cung cấp kênh bảo mật dữ liệu giữa các thiết bị di động khi qua một mạng riêng hoặc mạng công cộng như là GSM, 3G, 4G LTE và Wi-Fi.

AME 2000 thực thi thêm các yêu cầu an toàn được chính phủ hỗ trợ từ Security Enhanced Android (SEAndroid) để cung cấp thêm việc điều khiển các chính sách an ninh tăng cường nhằm đảm bảo các luồng xử lý không thể bị can thiệp hay tấn công bởi các lỗ hổng và ứng dụng mang mã độc.

Thẻ nhớ Motorola CRYPTR, một dạng mô đun an toàn cứng trong dạng thẻ microSD đạt tiêu chuẩn FIPS 140-2 Level 3, chuẩn Suite B, cung cấp cho AME 2000 khoá, phiên và chứng thực, và cách các tổ chức mật mã cao cấp.

Ngoài ra, AME 2000 còn được hỗ trợ cập nhật và vá lỗ hổng thông qua OTA. Khoá mã có thể được xoá từ xa phòng trường hợp mất thiết bị hoặc bị thao túng.

C. Giải pháp bảo mật của Rohde & Schwarz

Hãng Rohde & Schwarz đưa ra giải pháp TopSec Mobile

TopSec Mobile là một thiết bị mã hoá di động sử dụng trong thực hiện cuộc gọi thoại cho điện thoại thông minh, PCs. Các cơ quan và chính phủ sử dụng điện thoại để chia sẻ những thông tin nhạy cảm. Tuy nhiên, các cuộc gọi thoại trên di động rất dễ bị nghe lén và ghi âm lại. Đó là lý do vì sao các thông tin bí mật và cần được bảo vệ của các công ty này phải sử dụng một bộ mã hoá mạnh mẽ. Và hơn thế nữa, người sử dụng cần một giải pháp bảo mật đơn giản và linh hoạt giúp cho họ có thể dễ dàng thực hiện cuộc gọi như bình thường mà không cần tới các cách thức liên lạc phức tạp.

Hình 3. Giải pháp bảo mật TopSec Mobile của Rohde & Schwarz

Tính năng chính của thiết bị:

- Sử dụng thiết bị mã hoá riêng biệt với điện thoại đảm bảo yêu cầu an toàn cao nhất.

- Điện thoại thông minh được sử dụng có thể có đầy đủ các tính năng như điện thoại thông minh thông thường.

- Dễ dàng kết nối đến điện thoại thông minh qua Bluetooth.

- Mã hoá đầu cuối cuộc gọi thoại dựa trên nền tảng IP (mã hoá VoIP).

- Sử dụng dễ dàng trên toàn cầu đối với mạng không dây, có dây và mạng IP.

- Mã hoá thoại sử dụng AES 256 bit.

D. Giải pháp bảo mật của CryptoAG

CryptoAG hãng bảo mật của Thuỵ Sĩ cung cấp giải pháp bảo mật cho điện thoại với tên gọi là CRYPTO MOBILE HC-9100. Giải pháp CRYPTO MOBILE HC-9100 là công nghệ tiên tiến nhất của CryptoAG, nền tảng công nghệ mã hoá được ứng dụng dưới dạng một thẻ microSD cùng với khả năng hoạt động đáng kinh ngạc. Là một phần của hệ thống kiến trúc Crypto, bộ mã hoá được tích hợp trong phần cứng vi xử lý của thẻ microSD. Bộ nhớ tích hợp bên trong cũng được điều khiển và bảo vệ bởi bộ vi xử lý này.

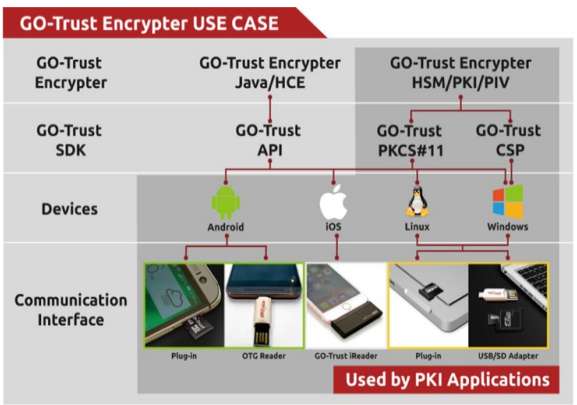
Thẻ Crypto Mobile HC-9100 phù hợp với các thiết bị điện thoại thông minh như là Samsung Galaxy S4 Mini và Samsung Galaxy A3 cũng như nhiều dòng điện thoại của Nokia.

Hình 4. Giải pháp bảo mật của CryptoAG-Thụy Sĩ

Tính năng:

- Độ an toàn cao, bộ mã hoá được cứng hoá.
- Nhỏ gọn, thẻ microSD có hiệu năng cao, có vi xử lý phát triển bởi CryptoAG.
- Kiến trúc an toàn Crypto cùng với thiết kế chống can thiệp.
- Bộ nhớ an toàn, phù hợp với dòng Samsung Galaxy S4 Mini cùng với các dòng điện thoại Nokia.
- Giải pháp mã hoá dời dạc trên điện thoại.

E. Giải pháp bảo mật GO-Trust của Mỹ



Hình 5. Giải pháp bảo mật của GO-Trust

Go-Trust đưa ra 5 phiên bản mã hoá trên thẻ microSD an toàn cùng bộ thuật toán mã hoá GO-Trust.

Các phiên bản được cung cấp như sau:

- HSM: Thẻ đạt chứng chỉ an toàn FIPS 140-2 Level 3 cùng với khối cứng hoá thuật toán mã hoá và hỗ trợ lên tới 200 khe khoá. Thông lượng mã hoá cứng AES đạt tới 550Kbps và có khả năng hỗ trợ mã hoá thoại thời gian thực.
- PKI: Thẻ đạt chứng chỉ an toàn FIPS 140-2 Level 3 cùng với PKI được nhúng và cung cấp toàn bộ SDK đối với môi trường PKI.
- PIV: Thẻ đạt được chứng chỉ FIPS 140-2 Level 3 và FIPS 201 đã được nhúng hệ xác thực người dùng PIV đạt theo hướng dẫn chất lượng cần đạt của PIV from NIST(SP800-157).
- Java: thẻ mã hoá microSD sử dụng chứng thực EMV JAVA 3.0 và Global platform 2.2.1 chip.
- HCE: thẻ mã hoá microSD bao gồm chứng thực BCTC Java cho tiếng Trung để hỗ trợ trao đổi NFC dựa trên công nghệ Android HCE.

F. Giải pháp bảo mật GSMK CryptoPhone 500i của Hãng GMSK.

Hình 6. Giải pháp bảo mật của CryptoPhone

GSMK CryptoPhone 500i là sản phẩn bảo mật di động dựa trên nền Android cùng với ứng dụng an ninh phục vụ việc mã hoá tin nhắn và thoại VoIP trên các mạng.

CryptoPhone 500i là một sản phẩm an toàn, tất cả mã nguồn của sản phẩm đều được cung cấp cho phép việc độc lập kiểm tra. Do đó người dùng có thể kiểm tra độc lập độ mạnh của bộ mã hóa và khả năng xuất hiện các lỗ hổng nào trong việc giao tiếp giữa các thiết bị đã được tin tưởng cùng với dữ liệu và thoại quan trọng. Chiếc điện thoại GSMK CryptoPhone 500i được đánh giá là một chiếc điện thoại bảo mật đáng tin cậy có thể sử dụng được trong bất kỳ trường hợp nào.

Công nghệ mã hoá của GSMK CryptoPhone dựa trên điểm mạnh và cấu trúc tốt của thuật toán kết hợp với độ dài khoá để cung cấp giải pháp bảo mật toàn diện.

G. Giải pháp bảo mật trong E-Crypto G10i Quad Band và E-Crypto 301 của hãng GMSK:

Một số đặc điểm mật mã của các sản phẩm E-Crypto G10i và E-Crypto 301:

- Trao đổi khóa Diffie-Hellman 4096-bit;
- Hàm băm SHA256;

- Xác thực khóa dựa trên Readout-hash;

- Mã hóa voice và SMS bằng mã khối AES256 và Twofish. Các khóa mã được hủy ngay khi kết thúc cuộc gọi;

- Mã hóa hệ thống lưu trữ cho: danh bạ, tin nhắn, ghi chú và các khóa được bảo vệ bởi thư mục thông minh chống lại sự truy cập trái phép;

- Audio codecs:

- Encrypted calls: CELP and ACELP VLBR4

- Decoding & playback: WAV, WMA, AMR-NB, AMR-WB, AAC, AAC+, eAAC+, QCP, MP3, polyphonic ring tones

- Hỗ trợ các kết nối GPRS, OBEX, WLAN, Bluetooth, IrDa, USB, SD-card [9-10];

- GSM quad-band 850/900 /1800/1900 MHz EDGE EGPRS class B, multi-slot class 10CSD;

Các giải pháp bảo mật cho điện thoại di động trên thế giới đã cho chúng ta một điểm nhìn khá phong phú về phương pháp giải quyết bài toán bảo mật dựa trên nền tảng công nghệ phần cứng và phần mềm.

Đối với phần cứng: Giải pháp thiết kế module bảo mật tách rời ở dạng phần cứng có tính độc lập tương đối đối chipset GSM dạng nhu thẻ nhớ là một giải pháp được nhiều hãng lớn áp dụng bởi tính bảo mật cũng như khả năng mềm dẻo trong việc thay đổi thiết kế hệ thống.

Đối với phần mềm: việc áp dụng thêm các dịch vụ bảo vệ kênh truyền mạng riêng ảo VPN cũng là một trong những giải pháp đảm bảo tính an toàn, tin cậy cho hệ thống. Có thể hệ thống lại một số điểm chung của các phương pháp bảo mật trên như sau:

(1) Tất cả các sản phẩm bảo mật trên sử dụng cùng một công nghệ thoại VoIP để bảo mật.

(2) Phần lớn các hãng cung cấp giải pháp bảo mật thông qua thiết bị giống thẻ nhớ microSD. Chiếc thẻ MicroSD này chứa bộ thuật toán mã hoá và tham số mật mã đã được cứng hoá trong bộ vi xử lý.

(3) Một vài hệ thống ứng dụng thêm các dịch vụ bảo vệ kênh truyền, mạng riêng ảo VPN.

(4) Các tham số mật mã đạt theo chuẩn chứng chỉ an toàn FIPS 140-2 level 3 hoặc sử dụng các gói đề xuất của NSA.

III. GIẢI PHÁP ĐỀ XUẤT

Trong phần này, nhóm tác giả sẽ trình bày về mô hình giải pháp thiết kế tổng quan dựa trên nền tảng mã hóa đầu cuối End-To-End Encryption, đưa ra mô hình thiết kế thiết bị điện thoại di động có bảo mật, liệt kê các khối xử lý chính trong mô hình thiết kế. Sau đó đi vào trình bày chi tiết mô hình, chức năng các khối xử lý chính, luồng xử lý tín hiệu ở ở kênh truyền và nhận. Cuối cùng là một số thông tin về giải pháp đảm bảo mật mã được thực thi.

A. Mô hình giải pháp thiết kế tổng quan

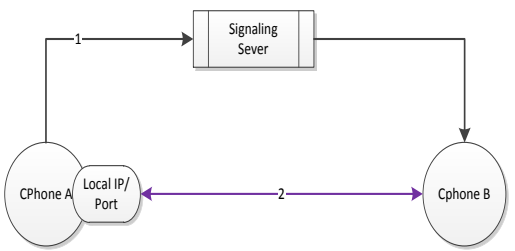
1. Giải pháp bảo mật đầu cuối

Giải pháp mã hóa đầu cuối End-To-End Encryption (E2EE) được đề xuất sử dụng trong công trình nghiên cứu nhằm tăng cường bảo mật thoại giữa hai người dùng đầu cuối. Theo đó, nội dung thoại sẽ được mã hóa ngay trên thiết bị của người gửi trước khi chuyển tới người nhận. Tương tự việc giải mã cũng vậy, nó chỉ được thực hiện trên thiết bị của người nhận và điều này đảm bảo dữ liệu không bị rò rỉ bởi bên thứ ba. Giải pháp bảo mật này đã được ứng dụng trong các hệ thống của Viber, Skype.

Các module mã hóa, giải mã trong thiết bị được thiết kế độc lập trong hệ thống đảm bảo tính làm chủ về khả năng tích hợp các tham số, thuật toán mật mã và thiết kế chế tạo phần cứng.

Việc truyền dữ liệu đã mã thoại giữa hai thiết bị được thực thi trên mạng thông tin di động 3G sử dụng 03 máy chủ Signaling, STUN và TURN.

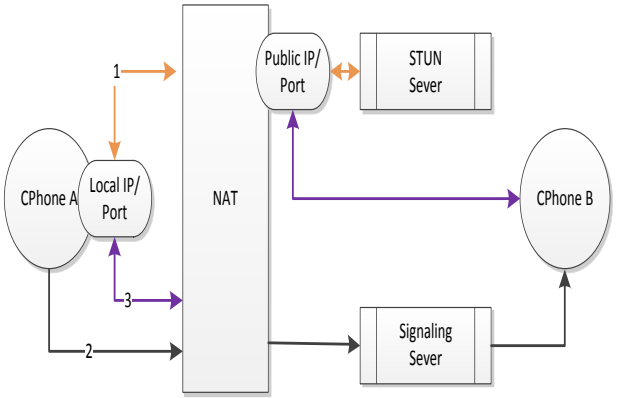
Để nhận luồng dữ liệu thoại đã mã từ điện thoại bảo mật CPhoneB, CPhoneA phải gửi thông tin liên hệ của mình (địa chỉ IP và cổng) đến CPhone B. Điều này thường được thực hiện thông qua một máy chủ báo hiệu Signaling Sever mà cả hai CPhone phải có kết nối.



Hình 7. Kết nối giữa hai CPhone trong cùng một mạng LAN

Nếu cả CPhoneA và CPhoneB ở trong các mạng LAN khác nhau và được phân tách bằng bộ định tuyến NAT, kịch bản ở trên sẽ thất bại. Vì CPhoneA không biết rằng nên sử dụng địa chỉ IP công cộng và cổng cho bộ định tuyến NAT để chuyển sang CPhoneB, CPhoneA sẽ

báo cho CPhoneB sử dụng địa chỉ IP và cổng cục bộ. Vì địa chỉ đó không thể truy cập được đối với CPhoneB, việc truyền luồng dữ liệu thoại sẽ thất bại trong Bước 2.

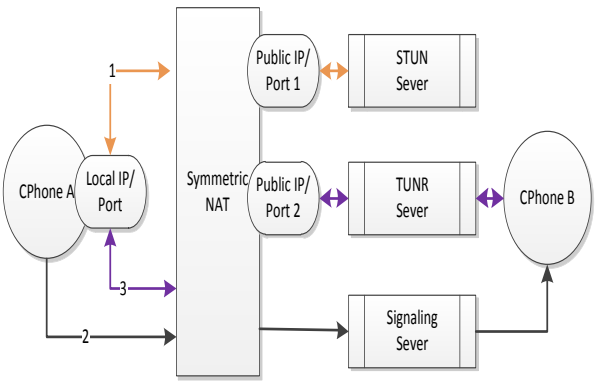


Hình 8. Kết nối giữa hai CPhone sử dụng máy chủ STUN

Vấn đề trên có thể được giải quyết bằng cách sử dụng máy chủ STUN như trong Hình 8. Với sự trợ giúp của máy chủ STUN, CPhoneA có thể xác định địa chỉ IP công cộng & cổng của mình trong Bước 1. Sau đó, nó có thể truyền thông tin chính xác đến CPhoneB, nhờ thông tin đã biết CPhoneB có thể gửi luồng dữ liệu của nó đến địa chỉ IP công cộng của bộ định tuyến NAT. Tiếp theo, bộ định tuyến NAT sẽ chuyển tiếp luồng dữ liệu nhận được tới CPhoneA.

Giải pháp được trình bày phía trên sẽ không hoạt động đối với tất cả các NAT được triển khai trên thực tế. Đối với các NAT đối xứng Symmetric NAT, việc tạo (mở) một cổng không chỉ phụ thuộc vào LAN CPhoneA, mà còn phụ thuộc vào mỗi kết nối cụ thể mà nó kết nối tới. Do đó, khi CPhoneA yêu cầu cổng & địa chỉ IP công cộng của mình từ máy chủ STUN, cổng và địa chỉ này sẽ không hợp lệ đối với các kết nối đối với CPhoneB. Vì cổng công cộng chính xác không thể được xác định từ máy chủ STUN, nên việc gửi dữ liệu từ CPhoneB sẽ thất bại.

Để giải quyết vấn đề với Symmetric NAT, cần có máy chủ TURN (xem Hình 9). Khi CPhoneA xác định rằng các kết nối trực tiếp và STUN là không thể (bước 1), anh ta có thể thông báo cho CPhone B thông qua Máy chủ báo hiệu về một máy chủ TURN đã biết (bước 2). Trong bước 3, cả hai máy được kết nối thông qua máy chủ TURN và có thể giao tiếp với nhau.



Hình 9. Kết nối giữa hai CPhone sử dụng máy chủ TURN

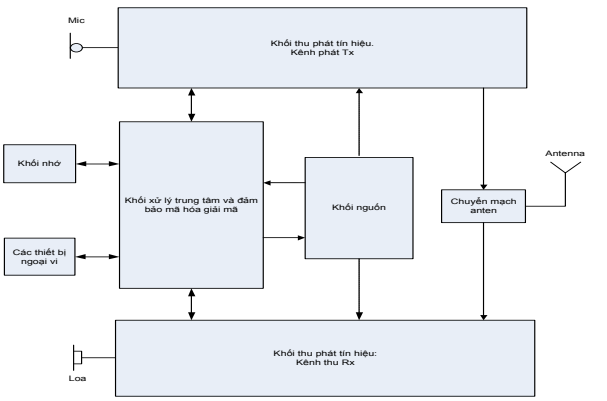
Sau khi 2 điện thoại tạo kết nối thành công quá trình trao đổi khóa được thực thi nhằm tạo một số thành phần mật mã đảm bảo quá trình mã hóa thoại. Giải pháp trao đổi khóa được thực thi theo tiêu chuẩn HMQV được mô tả trong công trình nghiên cứu "HMQV: A hight-Performance Secure Difie-Hellman protocol" của Hugo Krawczyk công bố tại hội thảo Advances in Cryptology – CRYPTO 2005.

Gói tin được xác thực thông qua giao thức HMAC-SHA256.

Quá trình mã hóa và giải mã được thực hiện ở thiết bị đầu cuối. Sử dụng thuật toán mã hóa mã khối với cấu trúc hệ mã là cấu trúc Feistel độ dài khối dữ liệu và khối mã là 128 bit, khóa 512 bit, 24 vòng lập.

2. Giải pháp thiết kế thiết bị bảo mật đầu cuối

Giải pháp thiết kế tổng quan điện thoại di động gồm ba khối cơ bản: Khối điều khiển trung tâm và bảo đảm mã hóa, giải mã, khối thu phát (gồm kênh thu Tx và kênh phát Rx) và khối nguồn.

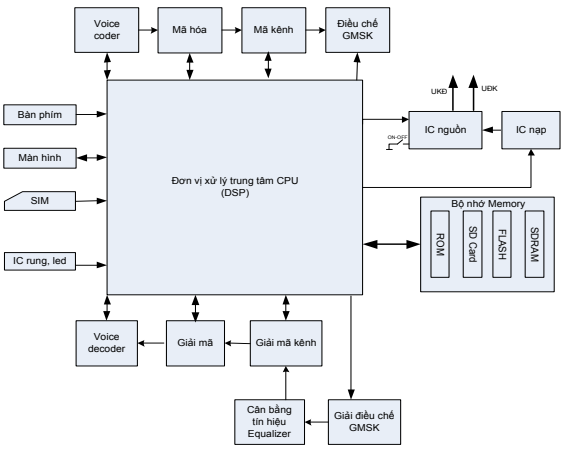


Hình 10. Giải pháp thiết kế tổng quan

B. Mô hình giải pháp thiết kế chi tiết hệ thống

1. Khối xử lý trung tâm và đảm bảo mã hóa, giải mã

Khối xử lý trung tâm và đảm bảo mã hóa, giải mã bao gồm đơn vị xử lý trung tâm CPU (Center Processor Unit) và bộ nhớ Memory.



Hình 11. Khối xử lý trung tâm

Đơn vị xử lý trung tâm thực hiện các chức năng chính như:

a. Điều khiển khối thu phát tín hiệu (các quá trình voice coder, voice decoder; mã hóa và giải mã dữ liệu, mã hóa và giải mã kênh; điều chế và giải điều chế GMSK)

b. Điều khiển khối nguồn bao gồm tắt mở nguồn chính và chuyển nguồn giữa các chế độ thu và phát, điều khiển quá trình nạp nguồn, quá trình tắt mở thiết bị, quá trình ngủ của thiết bị ở chế độ tiết kiệm pin.

c. Điều khiển quá trình đồng bộ giữa các IC

d. Quản lý các chương trình trong bộ nhớ

e. Điều khiển các thiết bị ngoại vi gồm màn hình, camera, SIM card, bàn phím, đèn led, rung chuông

Bộ nhớ Memory bao gồm bốn loại chính:

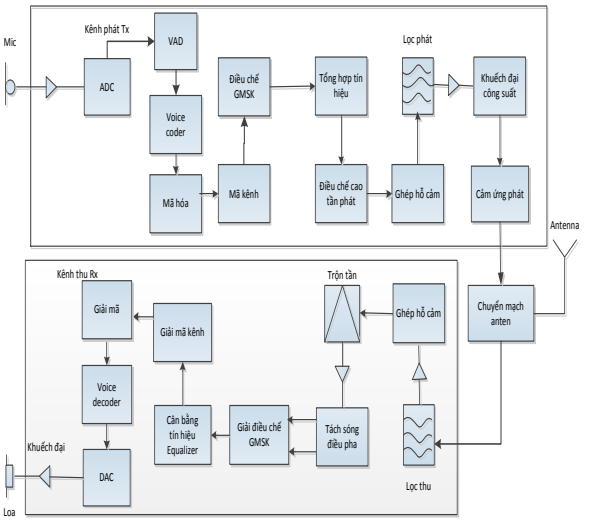
a. ROM: Là bộ nhớ do nhà sản xuất nạp vào trước khi xuất xưởng dùng để lưu các chương trình quản lý thiết bị, quản lý số nhận dạng thiết bị di động IMEI và các IC, đây là loại bộ nhớ chỉ đọc

b. SDRAM là RAM động có chức năng lưu trữ tạm thời các chương trình phục vụ trực tiếp cho quá trình xử lý của đơn vị xử lý trung tâm.

c. FLASH: Bộ nhớ dùng để nạp hệ điều hành và các chương trình ứng dụng trên hệ điều hành. Khi đơn vị xử lý trung tâm hoạt động CPU sẽ truy cập vào bộ nhớ FLASH để lấy các phần mềm điều khiển hoạt động của thiết bị.

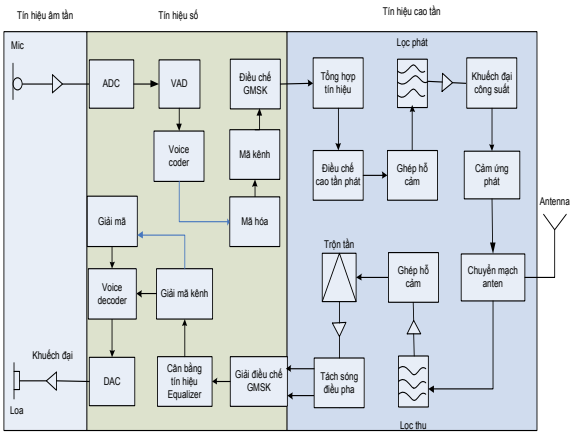
d. Thẻ nhớ SD card: lưu dữ liệu người dùng.

2. Khối thu phát tín hiệu



Hình 12. Khối thu phát tín hiệu

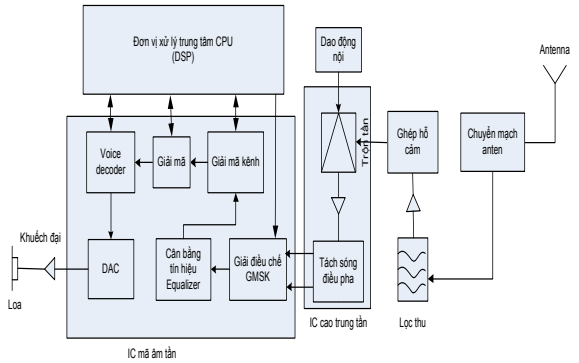
Khối thu phát tín hiệu của hệ thống gồm hai kênh là kênh thu Rx và kênh phát Tx. Tín hiệu qua hệ thống gồm tín hiệu số, tín hiệu cao tần và tín hiệu âm tần. Tín hiệu số là tín hiệu xử lý chính của CPU và bộ nhớ Memory là tín hiệu liên lạc giữa các IC cao tần và âm tần. Tín hiệu âm tần là tín hiệu thu được sau microphone hay tín hiệu ra tai nghe , tín hiệu âm tần sau khi biến đổi thành tín hiệu điện sẽ có tần số trong khoảng từ 20 Hz tới 20kHz. Tín hiệu cao tần có tần số từ 890MHz - 915MHz được điều chế từ tín hiệu số và sóng cao tần. Các tín hiệu cao tần phát sẽ được khuếch đại tăng công suất trước khi đưa ra anten phát về tổng đài qua các trạm thu phát tín hiệu.



Hình 13. Sự biến đổi các dạng tín hiệu trên kênh thu phát

a. Khối thu Rx

Kênh thu gồm hai đường riêng biệt dùng cho hai băng sóng là GSM 9000 MHz (tần số thu 935 MHz – 960 MHz) và DCS 1800 MHz (tần số thu 1805 MHz - 1880 MHz).

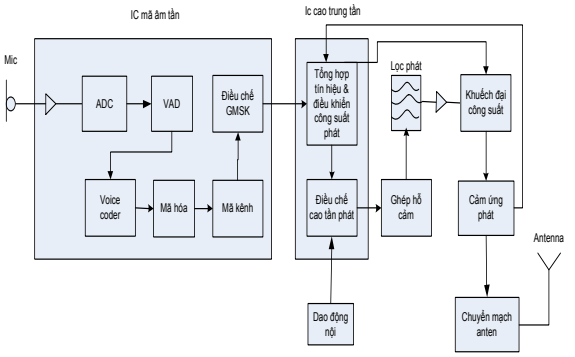


Hình 14. Kênh thu Rx

Tín hiệu thu khi vào anten sẽ được chuyển mạch nhờ bộ chuyển mạch vào băng tần tương ứng, đi qua bộ lọc để loại bỏ các tín hiệu nhiễu, bộ khuếch đại để nâng biên độ tín hiệu. Tín hiệu tiếp tục được chuyển qua bộ ghép hỗ cảm tạo tín hiệu cân bằng sau đó mạch trộn tần của IC cao trung tần sẽ trộn tín hiệu cao tần với tần số dao động nội của bộ dao động để tạo tín hiệu trung tần. Tiếp theo sau khi tín hiệu được đẩy qua mạch khuếch đại, khuếch đại lên biên độ đủ lớn sẽ được cung cấp cho mạch tách sóng điều pha. Các tín hiệu này được đưa sang IC mã âm tần để xử lý. Tại đây diễn ra quá trình giải điều chế GMSK, quá trình cần bằng tín hiệu âm thanh Equalizer nhằm thay đổi chất âm, quá trình giải mã kênh, voice decoder tại đây tín hiệu được giải nén và tách làm hai loại: tín hiệu thoại được đưa đến bộ chuyển đổi DA lấy ra tín hiệu âm tần sau đó khuếch đại và đưa ra loa, các tín hiệu khác được đưa xuống vi xử lý theo để lấy ra tín hiệu điều khiển báo rung chuông và tin nhắn.

b. Khối phát Tx:

Đối với kênh phát Tín hiệu thoại sau khi đi qua Micro sẽ được biến đổi thành tín hiệu điện ở dạng tương tự, thông thường tín hiệu điện sẽ được đưa qua bộ lọc thông dải tần số từ 300 Hz đến 3.4 kHz để giảm lượng dữ liệu cần thiết tương đương với sóng âm. Tín hiệu này tiếp tục được đưa vào IC mã âm tần tại đây được biến đổi thành tín hiệu số nhờ bộ biến đổi ADC dùng kỹ thuật điều xung mã PCM. Theo định lý Nyquist tần số lấy mẫu phải gấp ít nhất hai lần băng thông dữ liệu giá trị này đối với tín hiệu thoại thường là 8kHz và mỗi mẫu được mã hóa bằng bằng 8-16 bit thường là 13 bit. Tín hiệu ra khỏi ADC có tốc độ 104bps và được xử lý tiếp trong bộ Voice coder tuy nhiên trước đó tín hiệu được đưa qua khối VAD Voice Activity Detection khối sẽ nhận dạng tín hiệu thoại. Các tín hiệu không nằm trong dải tần tín hiệu thoại, thậm chí là các khoảng im lặng sẽ bị loại ra khỏi quá trình tiếp theo trong IC mã âm tần như quá trình voice coder, mã kênh (cung cấp khả năng chống sai cho dòng bit trước khi chuyển lên kênh tải) và quá trình điều chế GMSK. Chức năng cơ bản của khối Voice coder là giảm tốc độ của kênh truyền thoại nói một cách khác là nén tín hiệu thoại ở dạng số.



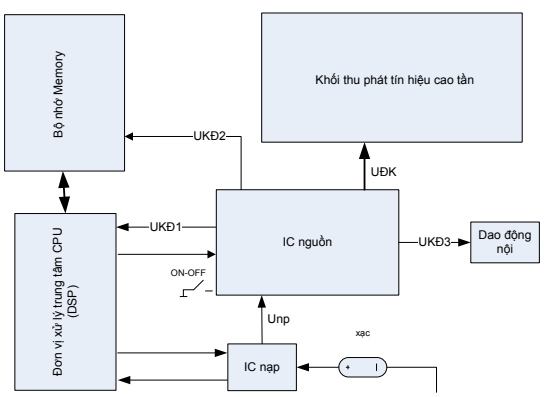
Hình 15. Khối phát Tx

Yêu cầu cơ bản của khối mã hóa tiếng nói chính là phải đảm bảo thời gian thực và chất lượng âm thoại có thể chấp nhận được. Trong chuẩn GSM thường sử dụng phương pháp mã hóa dự đoán tuyến tính nguồn tin LPC (Linear Predictive Coding). LPC vocoder có cấu trúc giống một bộ vocoder thông thường gồm một bộ phân tích (analyser), bộ kích thích (exciter) và bộ lọc ống phát thanh (vocal tract filter) mô phỏng cơ chế phát âm của con người. Vocoder chia tiếng nói thành các khung đều nhau, các khung này được đưa vào bộ phân tích và tìm ra các tham số tương ứng cho bộ kích thích và bộ lọc ống phát thanh. Sau đó thay vì làm tương tự như một vocoder thông thường là mã hóa các tham số này và gửi đi. Khi đó do giải biến đổi các thông số của bộ lọc ống phát thanh lớn cần rất nhiều bit để mã các thông số này. LPC vocoder dựa trên đặc tính là tín hiệu tiếng nói biến thiên chậm, do đó có thể dự đoán gần đúng bộ thông số hiện tại khi biết một số lượng nhất định các bộ thông số trước đó, nhờ vậy mà LPC vocoder sẽ chỉ truyền đi sai lệch dự đoán, giảm số bit cần mã, giảm đi tốc độ bit để truyền tiếng

nói. Cấu trúc của LPC Voice decoder bên nhận cũng tương tự sau khi thu được bộ các tham số này sẽ giải mã và đặt vào bộ kích thích và bộ lọc âm thanh.

Nhờ lọc tín hiệu thoại qua khối VAD mà hiệu năng của quá trình xử lý và truyền tín hiệu được tối ưu. Việc xử dụng khối VAD cũng có một nhược là khi người sử dụng nói với âm vực nhỏ khối VAD có thể cho đó là các khoảng im lặng trong cuộc trò chuyện, và đầu dây bên kia sẽ không thể nghe được các tín hiệu thoại này. Tuy nhiên các khối VAD hiện đại được thiết kế ngày một tối ưu hơn với độ nhạy cao hơn đã khắc phục được phần lớn nhược điểm kể trên. Chuỗi các tín hiệu sau điều chế GMSK sẽ được tổng hợp trong IC cao trung tần khi đi qua khối tổng hợp tín hiệu và điều khiển công suất phát. Quá trình điều khiển công suất phát của khối được thực hiện bằng việc đưa ra tín hiệu điều khiển cho khối Khuếch đại công suất và xử lý tín hiệu từ khối cảm ứng phát truyền về. Tại IC cao trung tần tín hiệu sau khi tổng hợp được điều chế cao tần phát có tần số trong phạm vi 890MHz – 915 MHz theo phương pháp điều pha, nhờ mạch điều chế cao tần trong IC cao trung tần. Một tần số trộn từ khối dao động nội sẽ được IC cao trung tần chọn lựa để đưa vào quá trình trộn tần trong khối điều chế cao tần phát. Các tín hiệu ra khỏi IC cao trung tần sẽ được tập hợp thành một đường duy nhất nhờ bộ ghép hỗ cảm, đi qua bộ lọc phát, bộ tiền khuếch đại, bộ khuếch đại công suất. Tín hiệu ra khỏi bộ khếch đại công suất sẽ đi qua bộ cảm ứng phát để đưa lên bộ chuyển mạch anten đi qua anten phát về các trạm BTS.

3. Khối nguồn



Hình 16. Sơ đồ khối nguồn điện thoại di động

Chức năng cơ bản của khối nguồn gồm có điều khiển tắt mở nguồn; chia nguồn thành nhiều mức khác nhau để cung cấp cho CPU, khối nhớ, khối giao động nội, khối thu phát tín hiệu cao tần, xử lý tín hiệu âm tần; ổn định nguồn cung cấp cho các tải tiêu thụ. Khi máy được lắp pin điện áp nạp Unp sẽ được cung cấp cho IC nguồn. Khi công tắc nguồn ON-OF được bật, IC nguồn hoạt động cung cấp các điện áp khởi động UKĐ cho các khối điều khiển như CPU (UKĐ1), Bộ nhớ Memory và IC mã âm tần (UKĐ2), mạch giao động nối (UKĐ3). Sau khi được cấp nguồn khối xử lý sẽ hoạt động, CPU trao đổi dữ liệu với Memory để lấy ra phần mềm điều khiển các hoạt động của máy, trong đó có các lệnh quay lại điều khiển khối nguồn để mở ra các điện áp điều khiển (UĐK) cấp cho bộ giao động tạo tạo ra xung nhịp đồng bộ các IC cao tần, IC mã âm tần, IC vi xử lý, khối thu và phát sóng cao tần hoạt động. Trong quá trình điều khiển nạp bổ xung một lệnh điều khiển từ đơn vị xử lý trung tâm CPU sẽ điều khiển nạp dòng điện từ bộ xạc đi vào IC nạp cho pin, và được CPU điều khiển thông qua tín hiệu điều khiển để nạp vào pin, khi pin đầy một tín hiệu báo hiệu pin đầy sẽ được truyền về CPU từ IC nạp cho CPU biết ngắt dòng nạp.

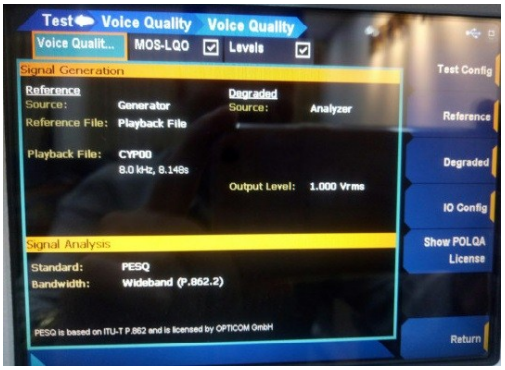
IV. THỰC NGHIỆM VÀ KẾT QUẢ

Phần này miêu tả tham số cấu hình thiết bị thực nghiệm, mô tả môi trường thiết bị thử nghiệm và kết quả thử nghiệm giải pháp bảo mật đề xuất.

Thiết bị được thiết kế với module xử lý mã hóa và điều khiển các thiết bị ngoại vi như màn hình bàn phím độc lập sử dụng chíp STM32F437UFBGA176, module xử lý nén sử dụng thuật toán Speex cũng được thiết kế độc lập trên cùng nền tảng chíp xử lý STM32F437UFBGA176. Thiết bị không sử dụng hệ điều hành có sẵn toàn bộ các phần mềm điều khiển, hiển thị được viết trên firmware, anten được thiết kế chế tạo bằng công nghệ mạch dẻo (flexible PCB) với 1 lớp FR4 dày khoảng 0,1 mm và lớp đồng (Cu) độ dày theo chuẩn 0,5oz (0.017 mm) hoạt động trên 2 dải tần số 900 MHz và 1800 MHz.

Để kiểm tra chất lượng thoại của thiết bị sau khi mã, nhóm tác giả sử dụng thiết bị phân tích âm thanh Audio Analyzer U8903B của Hãng Keysight được tích hợp bản quyền N3433A phần mềm đo kiểm chuẩn PESQ theo khuyến nghị trong ITU-T P.862 [11]. Thuật toán PESQ được thiết kế để dự đoán điểm ý kiến chủ quan của một mẫu âm thanh bị suy giảm. PESQ trả

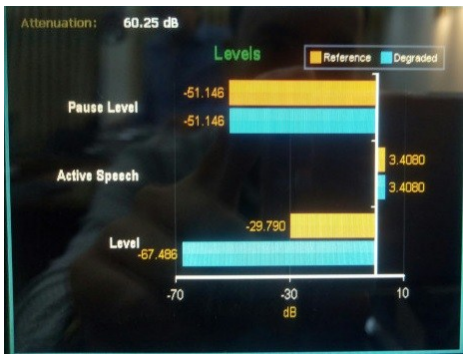
về điểm số từ 4,5 đến -0,5, với điểm số cao hơn cho thấy chất lượng tốt hơn. Cấu hình tham số của máy đo và file đầu vào được thiết lập như Hình 18.



Hình 18. Thiết lập cấu hình tham số máy đo và file đầu vào trên thiết bị U8903B

File test CYP00 có định dạng WAV kích thước 127,36 KB. Dải Bandwidth đo là dải hẹp Narowband (được định nghĩa theo khuyến nghị trong P.862.1).

Hình 19. Chất lượng thoại theo chuẩn PESQ được đo kiểm tự động trên thiết bị U8903B



Hình 20. Độ suy giảm tín của tín hiệu thoại gốc và tín hiệu thoại đã qua xử lý

Chất lượng thoại theo PESQ MOS Score đạt 3,1 điểm trên tổng thang điểm từ -0,5 đến 4,5 điểm. Độ suy giảm tín hiệu thoại đạt trung bình là 60,25 dB (Hình 19 và 20).

V. KẾT LUẬN

Trong bài báo này, trên cơ sở nghiên cứu về các giải pháp công nghệ trong việc thiết kế chế tạo điện thoại di động có bảo mật trên thế giới, nhóm tác giả đã tổng hợp và đưa ra xu hướng phát triển công nghệ bảo mật cho các thiết bị di động đồng thời luận giải về các thách thức đặt ra đối với bài toán nghiên cứu thiết kế chế tạo điện thoại di động có bảo mật, đề xuất mô hình thiết kế chế tạo đảm bảo tính tối ưu dựa trên giải pháp bảo mật đầu cuối. Bằng thực nghiệm, nhóm tác giả đã chứng minh tính hiệu quả của giải pháp bảo mật đề xuất, chất lượng thoại sau khi đã mã hóa đạt khoảng 3,1 điểm PESQ.

LỜI CẢM ƠN

Nhóm tác giả xin gửi lời cảm ơn đến những góp ý khoa học nghiêm túc, hỗ trợ chuyên môn nhiệt tình của nhóm nghiên cứu khoa học mật mã Viện Khoa học – Công nghệ mật mã, nhóm thiết kế chế tạo mạch in của Nhà máy M2. Đồng thời, xin gửi lời chân thành cảm ơn tới nhóm nghiên cứu phát triển anten Đại học Bách Khoa Hà Nội.

TÀI LIỆU THAM KHẢO

[1]. Tatsuro Murakami, “The NGN - a carrier-grade IP convergence network”, 2010 IEEE/IFIP Network Operations and Management Symposium Workshops, 2010.

[2]. Sklavos N, Koupopavlou O. Architectures and VLSI Implementations of the AES-Proposal Rijndael[J]. Computers, IEEE Transactions on, 2002, 51(12):1454-1459

[3]. R.L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM, Feb. 1978, 21(2): 120-126.

[4]. J.-H. Hong, RSA Public Key Crypto-Processor Core Design and Hierarchical System Test Using IEEE 1149 Family, Ph.D. dissertation, Dept. Elect. Eng., National Tsing Hua Univ., Hsinchu, Taiwan R.O.C., 2000: 322-334.

[5]. S.Bruce, "Description of a new variable-length key, 64-bit block cipher (Blowfish),"In Fast Software Encryption Second International Workshop, Leuven, Belgium, December 1993, Proceedings, Springer-Verlag, ISBN: 3-540-58108-1, pp.191-204, 1994.

[6]. K.Russell Meyers, and H.Ahmed Desoky, "An implementation of the Blowfish cryptosystem," Proceedings of the IEEE International Symposium on Signal Processing and Information Technology, Sarajevo, Bosnia and

Herzegovina, pp. 346-351, December 16-19, 2008.
[7]. M.Allam,"Data encryption performance based on Blowfish," 47th International Symposium ELMAR, Zadar, Croatia, 2005, pp. 131-134..
[8]. Diffie, Whitfield; Hellman, Martin E. (November 1976). "New Directions in Cryptography" (PDF). IEEE Transactions on Information Theory. 22 (6): 644–654.
[9]. S. Williams, "IrDA: past present and future", IEEE Pers. Commun., vol. 7, no. 1, pp. 11-19, Feb. 2000.
[10]. Yingying Yang; Qingxin Chu ; Chunxu Mao, " Multiband MIMO Antenna for GSM, DCS, and LTE Indoor Applications " IEEE Antennas and Wireless Propagation Letters, pp. 1573 - 1576, 12 January 2016.
[11]. ITU-T Recommendation P.862. Perceptual Evaluation of Speech Quality (PESQ), An Objective Method for End-to-end Speech Quality Assessment of Narrowband Telephone Networks and Speech Codecs.

SƠ LƯỢC VỀ TÁC GIẢ

TS. Trần Văn Khánh

Đơn vị công tác: Vụ Khoa học – Công nghệ.

Email: trankhanh.miptvn@gmail.com

Quá trình đào tạo: Nhận bằng Cử nhân năm 2009, thạc sĩ năm 2011; tiến sĩ năm 2015 tại trường Đại học Vật lý kỹ thuật Mátxcơva (Đại học tổng hợp quốc gia) Liên bang Nga.

Hướng nghiên cứu hiện nay: Kỹ thuật mật mã và an toàn nghiệp vụ mật mã. Nghiên cứu thiết kế chế tạo thiết bị bảo mật chuyên dụng trên nền tảng ASIC và FPGA.

KS. Nguyễn Thành Vinh

Đơn vị công tác: Vụ Khoa học – Công nghệ.

Email:nguyentvinh91@gmail.com

Quá trình đào tạo: Nhận bằng Kỹ sư năm 2014 tại trường Học viện Công nghệ bưu chính viễn thông

Hướng nghiên cứu hiện nay: Kỹ thuật mật mã và nghiệp vụ an toàn mật mã.