# KHẢO SÁT BÀI TOÁN MÃ HÓA THÔNG TIN TRONG MẠNG CỤC BỘ KHÔNG DÂY

## ON SECURITY IN WIRELESS LOCAL AREA NETWORK

**Trần Ngọc Bảo,**
*Khoa CNTT, Trường Đại học Sư phạm Tp.HCM.*
**Nguyễn Đình Thúc, Trần Đan Thư,**
*Khoa CNTT, Trường Đại học Khoa học Tự nhiên Tp.HCM.*

***TÓM TẮT:***

*Bảo mật thông tin là một trong các dịch vụ an ninh quan trọng cho mạng cục bộ không dây (WLAN – Wireless Local Area Network), nhằm bảo đảm thông tin được giữ bí mật. Bài toán này ít được quan tâm trong các nghiên cứu lý thuyết đề xuất mà chủ yếu tập trung ở các giải pháp công nghệ, ứng dụng các hệ mã phổ biến như RC4 trong WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) hay AES (Advanced Encryption Standard) trong WPA2. Giải pháp mạng riêng ảo (VPN -Virtual Private Network) cũng được nhiều nhà cung cấp dịch vụ quan tâm. Theo hướng tiếp cận giải pháp VPN, chúng tôi tập trung nghiên cứu về khả năng mở rộng của các hệ mã khối phổ biến hiện nay như hệ mã ma trận Hill, hệ mã AES, XAES,...Từ phân tích các thuật toán mã tuyến tính, các hệ mã khối và các mở rộng đã được nghiên cứu phân tích, chúng tôi đã đề xuất hệ mã khối SSM (Scalable Substitution Matrix Cipher) theo hướng tiếp cận kiến trúc SPN (Substitution-Permutation Network) kết hợp khả năng mở rộng kích thước khóa của hệ mã ma trận và thành phần phi tuyến S-Box. Kết quả S-Box đề xuất không chỉ sử dụng trong thuật toán mã khối SSM mà còn có thể sử dụng thay thế cho thành phần S-Box trong các hệ mã AES, XAES.*

*Từ khóa: WLAN, Hill Cipher, Matrix Cipher, AES, S-Box.*

***ABSTRACT:***

*Confidentiality is one of the important security services for wireless local area network (WLAN), to ensure the information is confidential and integrity. This problem mainly focus on commercial solutions that apply popular encryption algorithms such as: RC4 in WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access); AES (Advanced Encryption Standard) in WPA2. Virtual private network (VPN) solution also uses in products of Wi-Fi vendor. According to VPN solution approach, we focused on the scalability of block cipher systems such as Hill cipher, matrix cipher and AES. In these crypto systems, S-box is significant non-linear component. In this paper, we propose a new approach to represent general S-Box based on a given non-linear function to increases the complexity of algebraic expression and size of S-Box. In experiment with size of 8, proposed S-Box can archive the maximum number of terms (255 terms) and therefore it can be used to replace the classical S-Box component in the original AES. Furthermore, proposed S-Box inherits all good cryptographic characteristics of the original AES S-Box, such as nonlinearity, differential uniformity, and strict avalanche.*

*Keyword: WLAN Security, Hill Cipher, Matrix Cipher, AES, S-Box.*

## 1. GIỚI THIỆU

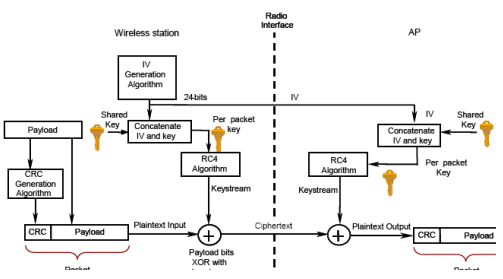
Mạng cục bộ không dây (WLAN-Wireless Local Area Network) là hệ thống mạng máy tính cho phép người dùng kết nối với hệ thống mạng dây truyền thống thông qua một kết nối không dây. Mạng cục bộ không dây linh động và dễ di chuyển hơn mạng dây truyền thống, các máy tính, các thành phần mạng kết nối với nhau thông qua một thiết bị gọi là điểm truy cập (Access Point). Access Point bao gồm angten dùng để truyền nhận các tín hiệu thông tin (ở dạng sóng vô tuyến) đến các thiết bị không dây (như Laptop, PDA, …) và cổng RJ-45 để giao tiếp với mạng dây truyền thống. Phạm vi phủ sóng trung bình của một Access Point là 300 feet (gần 100m). Phạm vi phủ sóng này được gọi là một ô-Cell hay Range. Người dùng có thể di chuyển tự do trong cell mà vẫn không mất kết nối với hệ thống mạng thông qua Access Point. Công nghệ không dây được thiết kế phù hợp với nhiều chuẩn và hỗ trợ nhiều mức độ an toàn bảo mật khác nhau. Thuận lợi chính của các chuẩn là được hầu hết các công ty áp dụng vào các dòng sản phẩm của họ, và cho phép dễ dàng kết hợp với các sản phẩm của các công ty khác nhau. Hai chuẩn hiện tại được công nhận phổ biến là IEEE 802.11 và Bluetooth. Trong đó, mạng cục bộ không dây sử dụng chuẩn 802.11. Chuẩn 802.11 được Viện Kỹ thuật Điện - Điện tử Hoa Kỳ (IEEE) phát triển năm 1997. Chuẩn này hỗ trợ kết nối trong phạm vi trung bình, và có các ứng dụng truyền nhận dữ liệu với tốc độ cao.

Việc bảo vệ hệ thống mạng cục bộ không dây thường dựa trên các giải pháp và đã trở thành tiêu chí chính sau: kiểm soát truy cập (Access Control) – xác nhận quyền truy cập của người dùng, bảo mật thông tin (Confidentiality) - đảm bảo thông tin được giữ bí mật, bảo toàn thông tin (Integrity) - đảm bảo thông tin đến người nhận không bị sửa đổi, và tính sẵn sàng (Availability) - đảm bảo hệ thống luôn sẵn sàng đáp ứng những dịch vụ mà nó cung cấp.

Các bài toán này đã và đang được rất nhiều viện nghiên cứu, các cơ quan, công ty về bảo mật trên thế giới cũng như những nhà sản xuất thiết bị không dây quan tâm. Đây là một hướng nghiên cứu mở cho những những người muốn nghiên cứu vấn đề an toàn trong hệ thống mạng không dây, đặc biệt là mạng cục bộ không dây. Do đó, chúng tôi nghiên cứu và giải quyết vấn đề này.

Như đã biết, IEEE 802.11 là chuẩn được sử dụng đầu tiên cho WLAN. Chuẩn này sử dụng giao thức WEP để bảo vệ thông tin trong quá trình truyền nhận dữ liệu giữa Client và Access Point. Từ năm 2000 nhiều nghiên cứu về an toàn thông tin mạng không dây khẳng định giao thức WEP có nhiều yếu điểm và không đảm bảo được tính an toàn của hệ thống trước nguy cơ tấn công của tin tặc:

- Do khóa WEP ở dạng khóa chia sẻ quy ước trước giữa máy trạm và Access Point, nghĩa là tĩnh trong một khoảng thời gian (trừ trường hợp bị thay đổi do người quản trị cấu hình lại) nên các gói tin đều dùng chung 1 khóa để tạo keystream dùng mã hóa dữ liệu. Việc tạo ra keystream khác nhau cho mỗi gói tin tùy thuộc vào giá trị IV. Vì vậy, nếu biết nội dung thông điệp và giá trị IV, tin tặc có khả năng biết được keystream, từ đó xây dựng từ điển các cặp (IV, keystream) để giải mã các thông điệp khác cũng như tìm ra khóa bí mật. Theo (Cisco 2003) và (Tom và các cộng sự 2002), tin tặc có thể thực hiện các tấn công WEP qua các hình thức phổ biến như: nghe lén thông tin (Eavesdropping), tấn công replay, phân tích đường truyền (Traffic Analysis), giả mạo (Masquerade), thay đổi thông điệp (Message Modification), từ chối dịch vụ (Denial-of-Service – DoS).




*Hình 1.1. Qui trình mã hóa và giải mã trong WEP (Tom và các cộng sự 2002)*

- WEP sử dụng thuật toán RC4 cho mục đích mã hóa và CRC-32 cho mục đích đảm bảo tính toàn vẹn dữ liệu (Binoy 2004), (William 2004). Tin tặc đánh vào yếu điểm của RC4 và CRC-32 để tấn công vào WEP (Scott và các cộng sự 2001), (Scott và các cộng sự 2002).
- Giữa Access Point và các máy trạm sử dụng duy nhất một khóa để thực hiện xác nhận quyền truy cập, mã hóa và giải mã thông tin. Khoá này có thể bị đánh cắp rất dễ dàng thông qua một số công cụ có sẵn trên internet (http://www.wi-foo.com/index-3.html).

Trước nguy cơ tấn công từ các yếu điểm của WEP, năm 2003 tổ chức Wi-Fi Alliance giới thiệu giao thức Wi-Fi Protected Access gọi tắt là WPA như là giải pháp tạm thời khắc phục một số yếu điểm của WEP. Giao thức WPA được trích từ một phần trong chuẩn IEEE 802.11i (Wi-Fi Alliance 2004a), (Wi-Fi Alliance 2004b) sử dụng TKIP-Temporal Key Integrity Protocol và MIC-Message Integrity Code (N. Ferguson 2002) để mở rộng miền giá trị của IV từ 24 bit lên 48 bit nhằm chống tấn công replay và MIC được gọi là Michael thay cho CRC-32 trong WEP.

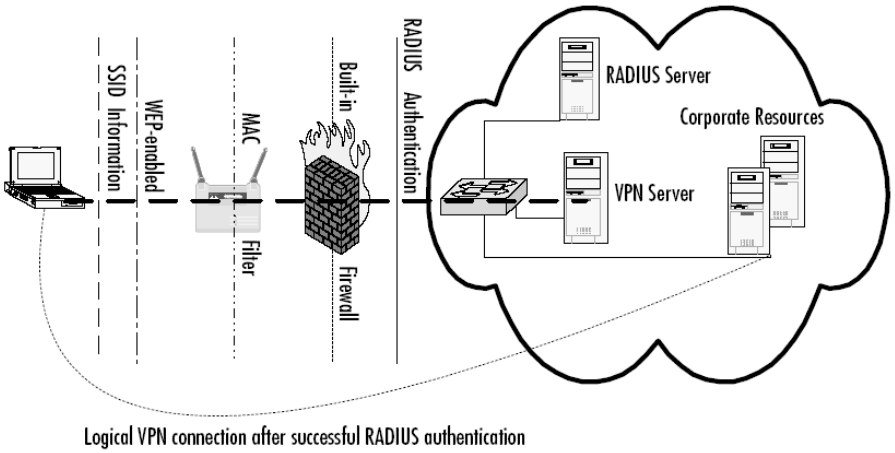
WPA chỉ được xem là giải pháp tạm thời vá những lỗ hổng của WEP nên WPA chỉ mang tính nhất thời. Giao thức này vẫn dùng thuật toán RC4 để mã hóa dữ liệu, chỉ bổ sung thêm TKIP và Michael để tăng độ an toàn, và hạn chế khả năng tấn công của tin tặc. Tuy nhiên, nhiều nghiên cứu cũng đã chỉ ra những hạn chế và khả năng tấn công WPA (Takehiro).

Tháng 3 năm 2006, giao thức WPA2 (IEEE 802.11i) đã chính thức trở thành tiêu chuẩn an toàn đối với thiết bị mạng cục bộ không dây; chuẩn này sử dụng thuật toán mã hóa AES thay cho RC4 trong WEP và WPA.

*Bảng 1.1 Bảng so sánh các đặc điểm mã hóa của WEP, WPA và WPA2*

| **Đặc điểm** | **WEP** | **WPA** | **WPA2** |
|---|---|---|---|
| Kích thước khóa (Key size) | 40 bits | - 128 bit dùng cho mã hóa<br>- 64 bit dùng cho chứng thực | 128 bit |
| Chu kỳ khóa (Key life) | 24 bit IV | 48 bit IV | 48 bit IV |
| Khóa cho mỗi gói tin (Packet key) | Concatenated | Mixing Function | Không yêu cầu |
| Toàn vẹn dữ liệu | CRC -32 | Michael | CCM |
| Chống tấn công Replay | Không có | IV Sequence | IV Sequence |
| Quản lý khóa (Key Management) | Không có | EAP – based | EAP – based |
| Mã hóa | RC4 | RC4 | AES |

Đối với các hệ thống mạng không dây công cộng (Hotspot) như khách sạn, sân bay, dịch vụ internet café…thường không cài đặt cơ chế kiểm soát truy cập, cũng như bảo mật cho Access Point để người dùng dễ dàng truy cập internet, ngay cả khi sử dụng thiết bị có hỗ trợ các giao thức bảo vệ thông tin theo WEP, WPA hoặc cao hơn. Do đó, vấn đề đặt ra là làm thế nào để bảo vệ được hệ thống mạng nội bộ đồng thời bảo vệ được người dùng khi truy xuất mạng qua thiết bị không dây. Để giải quyết bài toán này, nhiều giải pháp về phần cứng lẫn phần mềm được triển khai, trong đó nổi bật nhất là giải pháp mạng riêng ảo VPN-Virtual Private Network (Microsoft) một dạng mở rộng của mạng riêng (Private Network). Hiện trên thị trường có rất nhiều công ty cung cấp giải pháp tích hợp VPN vào hệ thống mạng không dây nhằm tăng độ an toàn dữ liệu cũng như khả năng bảo mật trên mạng không dây.




*Hình 1.2. Kiến trúc VPN*

Theo hướng tiếp cận giải pháp VPN, chúng tôi tập trung nghiên cứu về khả năng mở rộng của các hệ mã khối phổ biến hiện nay như hệ mã ma trận Hill, hệ mã AES, XAES (Trần Minh Triết 2008),…Trong lý thuyết mật mã, độ an toàn của các hệ mã khối phụ thuộc rất nhiều vào kích thước khóa và thành phần phi tuyến của hệ mã. Với các hệ mã khối phổ biến hiện nay (AES, Hill,..) khả năng mở rộng kích thước khóa cũng như kích thước khối là rất khó khăn do những thay đổi sẽ ảnh hưởng trực tiếp đến kiến trúc thuật toán. Chúng tôi đã đề xuất một hệ mã khối SMGI (Scalable Matrix Cipher based on Graph Isomorphism) theo hướng tiếp cận kiến trúc SPN kết hợp khả năng mở rộng kích thước khóa của hệ mã ma trận và thành phần phi tuyến S-Box sử dụng phép biến đổi tuyến tính. Bên cạnh đó, chúng tôi cũng đề xuất kiến trúc thành phần phi tuyến S-Box sử dụng đẳng cấu đồ thị, S-Box đề xuất không chỉ sử dụng trong thuật toán mã khối đề xuất SMGI mà còn có thể sử dụng thay thế cho thành phần S-Box trong các hệ mã AES và XAES.

## 2. HỆ MÃ KHỐI

Trong lý thuyết mật mã, độ an toàn của các hệ mã khối phụ thuộc rất nhiều vào kích thước khóa và thành phần phi tuyến của hệ mã. Hầu hết các hệ mã khối đối xứng không hỗ trợ khả năng mở rộng tự do khóa như các hệ mã công khai. Các hệ mã AES mặc dù hỗ trợ khả năng này nhưng các ràng buộc là tương đối nghiêm ngặt. Cụ thể, với Rijndael, kích thước của khóa luôn phải chia hết cho $2^2$: 128 bit, 192 bit, 256 bit,...Điều đó đồng nghĩa với các ràng buộc phải tuân thủ nghiêm ngặt khi tiến hành mở rộng kích thước khóa.

Ngược lại, với hệ mã tuyến tính, việc thay đổi kích thước khóa là rất dễ dàng: chỉ cần thay đổi kích thước của ma trận khóa. Như vậy hoàn toàn không bị ràng buộc về cách thức kích thước khóa có thể thay đổi. Tuy nhiên, điểm yếu cơ bản của

hệ mã này là tính tuyến tính. Bên cạnh đó, việc tăng kích thước khóa kéo theo một loạt vấn đề liên quan đến phát sinh và lưu trữ khóa cần giải quyết.

Câu hỏi đặt ra là: "Liệu có thể xây dựng một thuật toán mã hóa có tính chất phi tuyến như AES và khả năng mở rộng tự do kích thước khóa như mã ma trận"?

Câu trả lời là có thể. Cụ thể, giữ lại kiến trúc tương tự như AES nhưng thay phép trộn tuyến tính $\lambda\lambda$ bằng phép nhân ma trận như trong mã tuyến tính ta có hệ mã mới, thỏa các ràng buộc đặt ra. Chẳng hạn, SSM là một tiếp cận dạng này.

SSM được xây dựng theo kiến trúc mã hóa khối SPN, mỗi khối dữ liệu $PP$ (Plaintext) gồm $nn$ bytes sẽ được mã hóa thành bản mã $CC$ có cùng kích thước. Quy trình mã hóa được chia thành $N_{r-1}N_{r-1}$ giai đoạn

$$N_{r-1} = 2\left\lceil\frac{2n}{3\beta}\right\rceil + 2 \quad (1.1)$$

Trong đó $\beta\beta$ là branch number tối thiểu (Dang Hai Van và các cộng sự 2008); và mỗi giai đoạn gồm 2 chu kì thực hiện lần lượt 2 phép biến đổi sau:

- Phép thay thế phi tuyến (S-Box được ký hiệu là $\varphi\varphi$): mỗi byte trong khối $PP$ sẽ được thay thế bằng một byte tương ứng sử dụng Gray S-Box (Tran Minh Triet 2008). Phép thay thế phi tuyến được thực hiện trên trường $GF(2^8)GF(2^8)$.
- Phép mã hóa ma trận (MC-Matrix Cipher được ký hiệu là $\lambda\lambda$): khối dữ liệu gồm $nn$ byte sẽ được mã hóa theo phương pháp mã hóa ma trận với khóa $K = M_{n\times n}$ $K = M_{n\times n}$. Phép mã hóa ma trận được thực hiện trên $\mathbb{Z}_{2^8}^n\mathbb{Z}_{2^8}^n$.

Có thể tóm lược quy trình mã hóa hệ mã SSM như sau:

Gọi $\xi^r[K]\xi^r[K]$ là giai đoạn mã hóa thứ $rr$ trong quy trình mã hóa gồm $N_{r-1}N_{r-1}$ giai đoạn

$$\xi^r[K] = \lambda[K]o\varphi \quad (1.2)$$

khi đó

$$SSM[K] = \xi^{N_r-1}[K]o\ldots o\xi^1[K]o\xi^0[K] \quad (1.3)$$

Các tính chất về an toàn của SSM đối với phương pháp phân tích mã sai phân và phân tích mã tuyến tính đã được trình bày chi tiết trong bài báo của nhóm tác giả Dang Hai Van và các cộng sự 2008. Xét về phương diện mở rộng thì hệ mã SSM chưa thực sự linh động vì hai lý do sau: thứ nhất, đơn vị dữ liệu mã hóa là byte, mỗi khối dữ liệu mã hóa là một chuỗi $nn$ byte; thứ hai, thành phần phi tuyến luôn sử dụng cố định Gray S-Box. Chúng tôi phát triển hệ mã SMGI khắc phục những nhược điểm này thông qua việc tham số hóa hai thành phần: (i) đơn vị dữ liệu mã hóa là $bitbit$, mỗi khối dữ liệu mã hóa là một chuỗi $n \times m - bitn \times m - bit$, và (ii) thành phần phi tuyến S-Box cũng được xây dựng từ phép biến đổi tuyến tính theo kiến trúc đề xuất trong phần 3 nên dễ dàng mở rộng và số lượng S-Box được lựa chọn cũng phong phú hơn.

## 3. THÀNH PHẦN PHI TUYẾN S-BOX

### 3.1 Cơ sở toán học

Trên cơ sở đề xuất kiến trúc S-box, chúng tôi phát biểu và đã chứng minh một số kết quả sau:

Định nghĩa 1.1: Cho ma trận khả nghịch cấp m, $A = (a_{ij})_{m\times m}A = (a_{ij})_{m\times m}$ trên

$\mathbb{Z}_2\mathbb{Z}_2$. Song ánh $f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$ được gọi là một phép biến đổi tuyến tính,

$\forall x, y \in \mathbb{Z}_2^m \forall x, y \in \mathbb{Z}_2^m$ nếu

$$\begin{cases} y = (y_{m-1}y_{m-2}\dots y_i \dots y_1 y_0) = f(x) \\ \quad = f(x_{m-1}x_{m-2}\dots x_i \dots x_1 x_0) \\ \quad (y_{m-1}y_{m-2}\dots y_i \dots y_1 y_0)^T \\ \quad = A(x_{m-1}x_{m-2}\dots x_i \dots x_1 x_0)^T \end{cases} \quad (1.4)$$

Trong đó $x_i x_i$, $y_i = f_i(x) \in \mathbb{Z}_2\ (\forall i \in \{0,1,\dots,m-1\})$

$y_i = f_i(x) \in \mathbb{Z}_2\ (\forall i \in \{0,1,\dots,m-1\})$ là bit thứ $ii$ của $xx$ và $yy$.

**Định lý 1.4**: Cho $f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$ là phép biến đổi tuyến tính như trong định nghĩa 1.1 và $A = (a_{ij})_{m\times m} A = (a_{ij})_{m\times m}$ là ma trận khả nghịch cấp $m$ trên $\mathbb{Z}_2$ $\mathbb{Z}_2$, khi đó ta có:

$$\forall i, j \in \{0,1,\dots,m-1\}, a_{(i+1)(j+1)} = f_i(2^j) \quad (1.5)$$

**Bổ đề 1.1 (Jeffrey 2005-Định lý 2.1.1):** $GL(m, \mathbb{Z}_2)\ GL(m, \mathbb{Z}_2)$ là số lượng ma trận khả nghịch cấp $m$ trên $\mathbb{Z}_2\mathbb{Z}_2$, khi đó:

$$|GL(m, \mathbb{Z}_2)| = 2^{m^2}\left(1-\frac{1}{2}\right)\left(1-\frac{1}{2^2}\right)(\dots)\left(1-\frac{1}{2^m}\right) = 2^{m^2}\prod_{i=1}^{m}\left(1-\frac{1}{2^i}\right) \quad (1.6)$$

**Hệ quả 1.1:** Từ công thức 1.6, với $m = 8\, m = 8$ ta có:

$$|GL(8, \mathbb{Z}_2)| = 2^{8^2}\prod_{i=1}^{8}\left(1-\frac{1}{2^i}\right) \cong 5.34 \times 10^{18} \quad (1.7)$$

**Định lý 1.5**: Cho song ánh $f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$ trong đó

$f(2^t) \in \{2^t, 2^t+1, \dots, 2^{t+1}-1\}, \forall t \in \{0,1,\dots,m-1\}.$

$f(2^t) \in \{2^t, 2^t+1, \dots, 2^{t+1}-1\}, \forall t \in \{0,1,\dots,m-1\}.$

Gọi $A = (a_{ij})_{m\times m} A = (a_{ij})_{m\times m}$ là ma trận vuông cấp $m$ trên $\mathbb{Z}_2\mathbb{Z}_2$, sao cho $\forall i, j \in \{0,1,\dots,m-1\}, a_{(i+1)(j+1)} = f_i(2^j) \forall i, j \in \{0,1,\dots,m-1\}, a_{(i+1)(j+1)} = f_i(2^j)$ thì A khả nghịch và $ff$ là một phép biến đổi tuyến tính.

**Bổ đề 1.2:** Gọi $\wp(m) = \{A = (a_{ij})_{m\times m} \wp(m) = \{A = (a_{ij})_{m\times m}$ là ma trận tam giác trên trên $\mathbb{Z}_2\}\mathbb{Z}_2\}$, khi đó:

$$|\wp(m)| = 2^{\frac{(m-1)m}{2}} \quad (1.8)$$

**Mệnh đề 1.2**: Số ma trận được tạo theo định lý 1.5 là $\wp(m)\wp(m)$

Hệ quả 1.2: Gọi $\wp(m)\wp(m)$ là tập hợp các ma trận $A = (a_{ij})_{m\times m}\, A = (a_{ij})_{m\times m}$

cấp m trên $\mathbb{Z}_2\mathbb{Z}_2$ được tạo theo định lý 1.6, và $PP$ là một ma trận hoán vị. Gọi $\mathbb{P} = P\wp(m) = \{PX/X \in \wp(m)\}\mathbb{P} = P\wp(m) = \{PX/X \in \wp(m)\}$, khi đó:

$$|\mathbb{P}| = (m!) \times 2^{\left(\frac{m(m-1)}{2}\right)} \quad (1.9)$$

### 3.2 Kiến trúc S-Box sử dụng phép biến đổi tuyến tính

#### 3.2.1. Kiến trúc S-Box đề xuất

Trong phần này chúng tôi đề xuất kiến trúc S-Box kết hợp phép biến đổi tuyến tính $ff$ và hàm phi tuyến $\mathcal{P}.\mathcal{P}$. Kiến trúc S-Box đề xuất trong phần này cũng sẽ được sử dụng thay cho thành phần S-Box trong hệ mã SSM, AES, XAES, và SMGI.

Định nghĩa 1.2: Cho phép biến đổi $f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$, $\mathcal{A}\mathcal{A}$ là phép biến đổi Affine, $\mathcal{P}\,\mathcal{P}$ là hàm phi tuyến trên trường $GF(2^m)GF(2^m)$, $\mathcal{P}(x) = \begin{cases} x^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases}$ $\mathcal{P}(x) = \begin{cases} x^{-1}, & x \neq 0 \\ 0, & x = 0 \end{cases}$, S-Box $S_m(x): GF(2^m) \longrightarrow GF(2^m) S_m(x): GF(2^m) \longrightarrow GF(2^m)$ là một ánh xạ được định nghĩa như sau:

$$S_m(x) = \mathcal{A} \circ \mathcal{P} \circ f = \mathcal{A}[\mathcal{P}[f(x)]] \quad (1.10)$$

**Hệ quả 1.3:** Theo bổ đề 1.1, số lượng S-Box $S_m(x)S_m(x)$ đề xuất như định nghĩa 1.2 là:

$$|GL(m, \mathbb{Z}_2)| = 2^{m^2} \prod_{i=1}^{m} \left(1 - \frac{1}{2^i}\right) \quad (1.11)$$

**Hệ quả 1.4**: Với phép biến đổi $f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m f: \mathbb{Z}_2^m \longrightarrow \mathbb{Z}_2^m$ được xây dựng theo định lý 1.5 thì số lượng S-Box $S_m(x)S_m(x)$ đề xuất như định nghĩa 1.2 là:

$$|\wp(m)| = 2^{\frac{(m-1)m}{2}} \quad (1.12)$$

#### *3.2.2. Thực nghiệm thống kê khả năng phát sinh S-box có biểu diễn đại số đạt ngưỡng tối ưu.*

Chúng tôi cài đặt thử nghiệm với $mm$=8, phát sinh ngẫu nhiên một số S-box trong số $2^{28}$ S-box theo kiến trúc đề xuất (như mô tả trong mệnh đề 1.3); xác định biểu diễn đại số của các S-box này và thống kê theo số lượng hệ số khác không trong biểu diễn đại số. Kết quả chi tiết được mô tả trong bảng 1.2.

*Bảng 1.2 Thống kê số lượng S-box (theo số hệ số khác không trong biểu diễn đại số)*

| Số S-Box phát sinh ngẫu nhiên | 100 | 200 | 300 | 500 | 1000 |
|---|---|---|---|---|---|
| Số hệ số khác không | Số S-box kết quả | | | | |
| 250 | 0 | 0 | 1 | 2 | 5 |
| 251 | 0 | 0 | 1 | 3 | 15 |

| | | | | | |
|---|---|---|---|---|---|
| 252 | 10 | 17 | 24 | 36 | 72 |
| 253 | 20 | 34 | 44 | 80 | 167 |
| 254 | 41 | 85 | 131 | 215 | 388 |
| 255 | 29 | 64 | 99 | 164 | 352 |

Quá trình thử nghiệm cũng cho thấy khả năng phát sinh thành công S-box có số hệ số đạt ngưỡng tối đa vào khoảng 30%. Kết quả được mô tả chi tiết trong bảng 1.3.

*Bảng 1.3 Thống kê khả năng phát sinh S-box có biểu diễn đại số với số hệ số khác không đạt ngưỡng tối đa.*

| Số hệ số | Số lượng S-Box phát sinh | | | | |
|---|---|---|---|---|---|
| | 100 | 200 | 300 | 500 | 1000 |
| 251 Hệ số | 0% | 0% | 0% | 1% | 2% |
| 252 Hệ số | 10% | 9% | 8% | 7% | 7% |
| 253 Hệ số | 20% | 17% | 15% | 16% | 17% |
| 254 Hệ số | 41% | 43% | 44% | 43% | 39% |
| 255 Hệ số | 29% | 32% | 33% | 33% | 35% |

### *3.2.3. So sánh S-Box trong AES với S-Box đề xuất*

*Bảng 1.4 Bảng so sánh S-Box đề xuất với AES, Gray S-Box,...*

| S-Box | f $(f(2^0), f(2^1), f(2^2), \ldots, f(2^7)$ $(f(2^0), f(2^1), f(2^2), \ldots, f($ | SAC | Tính phi tuyến | Tính đồng nhất sai phân | Biểu diễn đại số | Tái sử dụng |
|---|---|---|---|---|---|---|
| AES (J. Rosenthal 2003) | (1, 2, 4, 8, 16, 32, 64, 128) | ~1/2 | 112 | 4 | 9 đơn thức | |
| Cui L S-Box (L. Cui 2007) | (31, 62, 124, 248, 241, 227, 199, 143) | ~1/2 | 112 | 4 | 253 đơn thức | Toàn bộ |
| Gray S-Box (Tran Minh Triet và các cộng sự 2008) | (1, 3, 6, 12, 24, 48, 96, 192) | ~1/2 | 112 | 4 | 255 đơn thức | Toàn bộ |
| Giá trị tối ưu | | 1/2 | 120 | 4 | 255 đơn thức | Toàn bộ |
| S-Box đề xuất | | | | | | |
| Ví dụ 1 | (1, 3, 5, 9, 17, 33, 65, 129) | ~1/2 | 112 | 4 | 254 đơn thức | Toàn bộ |
| Ví dụ 2 | (1, 3, 7, 14, 28, 56, 112, 224) | ~1/2 | 112 | 4 | 255 đơn thức | Toàn bộ |

| | | | | | | |
|---|---|---|---|---|---|---|
| Ví dụ 3 | (1, 3, 5, 14, 18, 33, 82, 172) | ~1/2 | 112 | 4 | 254 đơn thức | Toàn bộ |
| Ví dụ 4 | (1, 3, 7, 15, 30, 60, 120, 240) | ~1/2 | 112 | 4 | 253 đơn thức | Toàn bộ |

Từ bảng 1.3, ta thấy S-Box đề xuất có biểu diễn đại số tốt hơn S-Box gốc (trong đó có một số đạt kết quả tối ưu 255 đơn thức) mà vẫn kế thừa được các đặc tính an toàn khác như: SAC, tính phi tuyến, ….

## 4. KẾT LUẬN

**Bảo mật thông tin** là một trong các dịch vụ chính quan trọng trong an ninh hệ thống mạng cục bộ, nhằm đảm bảo thông tin được giữ bí mật. Với các thiết bị không dây (thường đa dạng và không đồng nhất về năng lực tính toán, lưu trữ cũng như năng lượng), bên cạnh tiêu chí về tính bảo mật, chi phí tính toán là tiêu chí quan trọng khi thiết kế thuật toán mã hóa. Trên cơ sở phân tích các thuật toán mã tuyến tính, các hệ mã khối và các mở rộng đã được nghiên cứu phân tích, từ đó đề xuất kiến trúc hệ thành phần phi tuyến S-Box cho các hệ mã SSM và SMGI kết hợp tính dễ mở rộng của mã tuyến tính và tính an toàn của thành phần phi tuyến S-Box của các hệ mã khối.

## TÀI LIỆU THAM KHẢO

Cisco system (October, 2003), "A Comprehensive Review of 802.11 Wireless LAN Security and the Cisco Wireless Security Suite".

Tom Karygiannis, Les Owens (2002), "Wireless Network Security – 802.11, Bluetooth and Handheld Devices", Special Publication 800-48, National Institute of Standard and Technologies

Binoy A. George (2004), Securing IEEE 802.11 Protocol Wireless Networks Using Java Secure Proxy Server, Master thesis of Science, Department of Computer Sicence, University of Cape Town.

WilliamC.Barker(2004),"Specifications for the Triple Data Encryption Algorithm (TDEA) block cipher", Special Publication 800-67, National Institute of Standard and Technologies

Scott Fluhrer, Itsik Mantin, Adi Shamir (2001), "Weaknesses in the Key Scheduling Algorithm of RC4", The 8th International Workshop on Selected Areas in Cryptography, Springer LNCS, Vol. 2259.

Scott Fluhrer, Itsik Mantin, Adi Shamir (2002), "Attacks on RC4 and WEP", RSA Laboratories, Vol 5, No.2.

Wi-Fi Alliance (2004a), "Wi-Fi Protectd Access: Strong, standards-based, interoperable security for today's Wi-Fi networks".

Wi-Fi Alliance (2004b), "WPA™ Deployment Guidelines for Public Access Wi-Fi® Networks".

N. Ferguson (2002), "Michael: An Improved MIC for 802.11 WEP".

[Online].Available: http://grouper.ieee.org/groups/802/11/documents/DocumentHoder/2-020.zip TakehiroTakahashi, "WPA Passive Dictionary Attack Overview", http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf

Microsoft VPN Overview White Paper, "Virtual Private Networking in Windows 2000: An Overview".

Trần Minh Triết (2008), Nghiên cứu và phát triển các phương pháp bảo vệ thông tin dựa trên AES, Luận án Tiến sĩ, Đại học Khoa học Tự nhiên Tp.HCM.

Dang Hai Van, Nguyen Thanh Binh,

Tran Minh Triet, Tran Ngoc Bao, Nguyen Ho Minh Duc, "SSM: Scalable Substitution Matrix Cipher", Journal of Science and Technology, Vol 46, Number 5A, Special Issue on Theories and Applications of Computer Science (ICTACS 2009), Nha Trang, Vietnam, pp. 165-178.

Jeffrey Overbey, William Traves, and Jerzy Wojdylo, "On the Keyspace of the Hill Cipher", Cryptologia. 29:1 (2005): 59-72.

J. Rosenthal (2003). "A polynomial description of the Rijndael Advanced Encryption Standard. Journal of Algebra and its Applications", 2(2):223–236.

L. Cui and Y. Cao (2007). A new S-box structure named Affine-Power-Affine. International Journal of Innovative Computing, Information and Control, 3(3), pp.751-759.

Tran Minh Triet, Bui Doan Khanh, Duong Anh Duc (2008), "Gray S-box for Advanced Encryption Standard" , Proceedings of 2008 IEEE International Conference on Computational Intelligence and Security (CIS 08), Suzhou-SIP, China, Dec. 13-17, 2008, ISBN 978-0-7695-3508-1, pp. 253-258.