NGHIÊN CỨU THIẾT KẾ MẠCH TẠO MÃ CHO BỘ ĐIỀU HỢP BUS MÁY CHỦ BẢO MẬT VÀ CÁC THIẾT BỊ LƯU TRỮ

Trần Cảnh Dương
Trường Đại học Tài nguyên và Môi trường Hà Nội

Tóm tắt

SAN là một mạng lưu trữ tốc độ cao dùng cho việc truyền dữ liệu giữa các máy chủ tham gia vào hệ thống lưu trữ, cũng như giữa các hệ thống lưu trữ với nhau. Điều cần thiết đó là mã hóa dữ liệu tại bộ điều hợp bus chủ, trên toàn bộ kết nối của mạng SAN và trên các thiết bị lưu trữ. Mã hóa có thể giúp ngăn chặn việc rò rỉ ngẫu nhiên hoặc cố ý tại nơi có được quyền truy cập dữ liệu và trên đường truyền. Thiết bị bảo mật phần cứng được sử dụng để tăng cường các mô-đun bảo mật phần cứng truyền thống trong vấn đề kiểm soát cách sử dụng khóa và cung cấp môi trường an toàn cho các chức năng mã hóa. Bài báo đề xuất thiết kế mạch tạo mã cho bộ điều hợp máy chủ bảo mật và các thiết bị lưu trữ, hỗ trợ khả năng mật mã cho mô-đun nền tảng đáng tin cậy mà nó bao gồm việc tạo số ngẫu nhiên, tạo khóa bất đối xứng, mã hóa/giải mã bất đối xứng.

Từ khóa: Mạng lưu trữ; Bộ điều hợp bus máy chủ; Tạo số ngẫu nhiên; Tạo khóa bất đối xứng; Mã hóa/giải mã bất đối xứng; Thanh ghi dịch hồi tiếp tuyến tính.

Abstract

Study on the design of a code generation circuit for a secure server bus adapter and storage devices

SAN is a high-speed storage network used for data transmission between servers participating in storage systems, as well as between storage systems. It is essential to encrypt data at the host bus adapter, across the entire SAN connection and across the storage devices. Encryption can help prevent accidental or intentional leaks where data access is acquired and along the way. Hardware security appliances are used to augment traditional hardware security modules in terms of controlling key usage and providing a secure environment for cryptographic functions. The paper proposes the design of a code generator circuit for secure server adapters and storage devices, supporting cryptographic capabilities for the trusted platform module which includes random number generation; asymmetric key generation; Asymmetric encryption/decryption.

Keywords: Storage area network; Secure Host Bus Adapter (SHBA); Random number generation; Asymmetric key generation; Asymmetric encryption/decryption; Linear Feedback Shift registers.

1. Mở đầu

Có nhiều nghiên cứu về an toàn thông tin trên thế giới cũng như Việt Nam, các lỗi bảo mật phổ biến của ứng dụng web và cách phòng chống. Các nghiên cứu bao gồm xác định cấu trúc ứng dụng web, triển khai hệ thống phòng thủ, tổ chức mô hình mạng, thiết lập tường lửa, sử dụng công cụ phát hiện và ngăn chặn xâm nhập, ứng dụng phòng chống vi rút và bảo vệ máy tính cá nhân, thiết lập và cấu hình hệ thống máy chủ an toàn gồm máy chủ ứng

dụng web và máy chủ cơ sở dữ liệu, thiết lập cơ chế sao lưu phục hồi, vận hành an toàn. Có một số nghiên cứu về tấn công từ chối dịch vụ phân tán gồm các giai đoạn của cuộc tấn công, kiến trúc tổng quan của mạng tấn công, biện pháp phòng chống tấn công từ chối dịch vụ. Tấn công từ chối dịch vụ phân tán được phân loại gồm tấn công làm cạn kiệt băng thông hệ thống, tấn công làm cạn kiệt tài nguyên. Trên thực tế có một số mô hình thử nghiệm, cấu hình hệ thống gồm cấu hình Apache, cấu hình MySQL hoặc cài đặt tường lửa ứng dụng web ModSecurity, thiết lập hệ thống Snort để phát hiện và ngăn chặn xâm nhập.

Quản trị công nghệ thông tin (CNTT) cung cấp khả năng quản lý và kiểm soát CNTT bao gồm sắp xếp chiến lược, cung cấp giá trị, quản lý tài nguyên, quản lý hiệu suất và quản lý rủi ro. Chức năng quản lý rủi ro nhằm xác định các thủ tục để đảm bảo các rủi ro được quản lý đầy đủ đồng thời đánh giá các yếu tố rủi ro của các khoản đầu tư CNTT. Ngày càng nhiều các giải pháp mạng được sử dụng để tăng cường chức năng quản lý rủi ro của quản trị CNTT bao gồm quản lý thông tin và an ninh mạng. Internet đã phát triển để trở thành nền tảng chung để kết nối các doanh nghiệp và cộng đồng trên toàn thế giới. Truyền thông tin qua internet giữa các hệ thống và ứng dụng được nối mạng tinh vi là một tiêu chuẩn. Một số nghiên cứu trước đây đã xác định sự cần thiết của các biện pháp bảo vệ trong việc vận hành các hệ thống nối mạng, quản lý an ninh thông tin và hệ thống nối mạng là điều cần thiết.

SAN (Storage Area Network) là một mạng lưu trữ tốc độ cao. Các máy chủ được kết nối trên SAN để lưu trữ và truyền dữ liệu. Một giải pháp bảo mật SAN dựa trên việc sử dụng thiết bị bảo mật phần cứng (Hardware Security Appliance - HSA) như một giải pháp bổ sung nhằm tăng cường các mô-đun bảo mật phần cứng (Hardware Security Module - HSM) truyền thống trong vấn đề kiểm soát cách sử dụng khóa và cung cấp môi trường an toàn cho các chức năng mã hóa. Nhóm nghiên cứu gồm Adrian Baldwin và Simon Shiu từ phòng thí nghiệm Hewlett Packard, tại Bristol, Vương quốc Anh đã công bố giải pháp mã hóa và trao đổi khóa trong hệ thống mạng lưu trữ SAN.

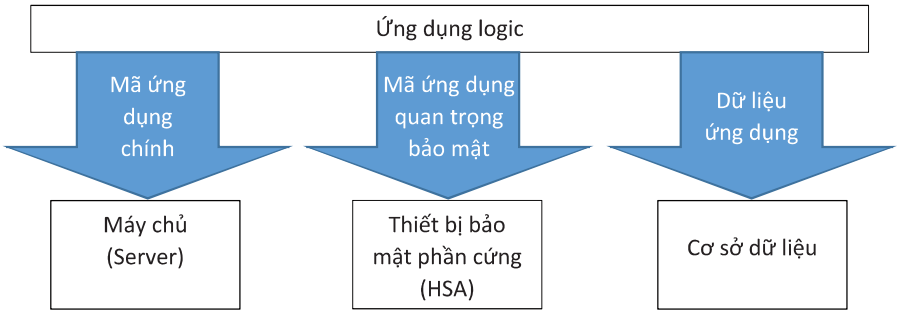
Đối với bảo mật mức cấu trúc, đĩa được phân chia đĩa thành các vùng. Sau đó các vùng này được phân tách trên cơ sở cấu trúc chuyển mạch SAN. Phân vùng cứng được thực hiện trong các thiết bị chuyển mạch, phân vùng mềm được thực hiện trên máy chủ. Các kỹ thuật bảo mật trên cơ sở phân tách dữ liệu tại thiết bị có thể chặn truy cập trái phép dữ liệu [2, 3]. Tuy nhiên, hệ thống vẫn còn nhược điểm, đó là quản trị viên có thể cấu hình lại hệ thống SAN từ đó kẻ đột nhập có thể thêm một máy phụ có quyền truy cập dữ liệu trái phép. Mặt khác, dữ liệu không được mã qua đường truyền cáp quang giữa các hệ thống lưu trữ và máy chủ do đó có thể thất thoát, sai lệch. Hơn nữa, hệ thống lưu trữ trong trung tâm dữ liệu và trên các bản sao lưu có liên quan không được mã hóa dẫn đến khả năng bị rò rỉ.

2. Thiết bị bảo mật phần cứng

Mô-đun bảo mật phần cứng (HSM) hỗ trợ việc bảo vệ các khóa tránh tiếp xúc với hệ thống bên ngoài, bảo vệ việc tạo, lưu trữ và sử dụng khóa. HSM thường

thực hiện các hoạt động mã hóa mà chưa chú trọng việc bảo đảm việc khi sử dụng các khóa [5].

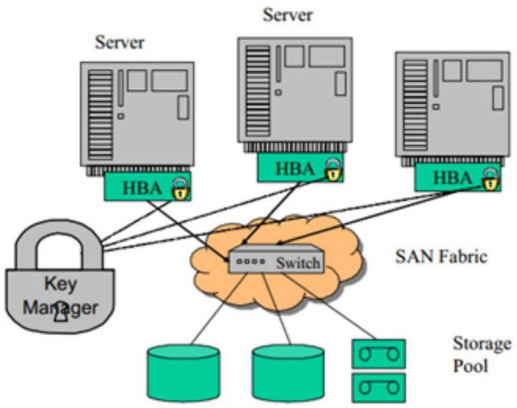
Thiết bị bảo mật phần cứng (HSA) có thể đảm bảo việc quản lý các khóa và mã hóa. HSA có chức năng mã hóa, bao gồm bộ xử lý chung, bộ nhớ và đồng hồ (clock). Hình 1 thể hiện sơ đồ mô tả ứng dụng bảo mật của thiết bị bảo mật phần cứng.



Hình 1: Sơ đồ mô tả ứng dụng bảo mật của thiết bị bảo mật phần cứng

Các dịch vụ có thể hoạt động trên nền tảng HSA với ít khả năng bị lỗi và rò rỉ cấu hình. Thiết kế phần cứng bao gồm các bộ xử lý mật mã, giải mã các khóa trong các thanh ghi.

Hiệu suất thực thi được tối ưu khi việc mã hóa và giải mã được thực thi tại bộ điều hợp bus máy chủ (HBA). Trong khi đó việc quản lý các khóa, quản lý quyền truy cập vào dữ liệu, có thể được thực thi (tách rời các máy chủ, thiết bị chuyển mạch và dữ liệu tại điểm thực thi (điểm quản lý), là một cổng thông tin lý tưởng để thay đổi chính sách và kiểm tra chặt chẽ các yêu cầu. Hình 2 biểu thị sơ đồ hệ thống SAN với các điểm kiểm soát mã hóa bổ sung.



Hình 2: Sơ đồ hệ thống SAN với các điểm kiểm soát mã hóa bổ sung

Bộ điều hợp bus máy chủ bảo mật (SHBA) đảm bảo tin cậy cho tất cả dữ liệu được định tuyến qua nó. Thành phần đáng tin cậy này cần phải có khả năng mã hóa nhanh đảm bảo thông lượng dữ liệu cao cũng như tạo khóa và lưu trữ khóa. Đơn vị cơ bản của dữ liệu sẽ phụ thuộc vào thuật toán mã hóa cụ thể. Dữ liệu được đọc trong các khối 128 bit [1]. Các khóa mã hóa được sử dụng không phải là khóa phiên và dữ liệu được mã hóa có khả năng vẫn còn trên đĩa trong những khoảng thời gian đáng kể. Do đó, các khóa này phải được kiểm soát cẩn thận và giảm thiểu tối đa việc rò rỉ thông tin khóa. Lưu trữ một số khóa xác định cho mỗi khối đĩa sẽ tạo ra số lượng lớn các khóa và việc xác định khóa thích hợp cho khối đó trở nên khó khăn hơn. Ngược lại, khi sử dụng một khóa duy nhất cho toàn bộ phân đoạn các bit dữ liệu chung có thể được phát hiện khi phân tích. Thay vào đó, khóa lịch trình sử dụng được tạo dựa trên việc sử dụng địa chỉ khối đĩa Block address để biến đổi tham số bí mật phân đoạn Segment_secret. Việc biến đổi dựa trên hàm băm nên khó có thể truy ngược

lại tham số bí mật ban đầu ngay cả khi khóa cho một số khối đĩa bị hỏng.

Theo cơ chế của HSA, cả quá trình ánh xạ và mã hóa/ giải mã được thực hiện bên trong phần cứng do đó tham số bí mật không bao giờ bị lộ ra ngoài khi phần cứng được bảo vệ. Việc quản lý phân phối các tham số bí được kiểm soát chặt chẽ. Nếu quản trị viên định cấu hình lại hệ thống lưu trữ để có quyền truy cập vào dữ liệu thì hành động đó sẽ được ghi lại.

3. Mã hóa dữ liệu

Một trong những vấn đề quan trọng trong bảo mật cho một mạng đó là tách biệt quyền truy cập vào dữ liệu. Do đó người ta cần mã hóa dữ liệu tại bộ điều hợp bus chủ (HBA) và trên các thiết bị lưu trữ. Mã hóa có thể giúp ngăn chặn việc rò rỉ ngẫu nhiên hoặc cố ý tại nơi có quyền truy cập dữ liệu và trên đường truyền. Các khóa giải mã chỉ có thể truy cập được trong một bối cảnh được ủy quyền. Các file mã hóa không thể đọc được. Quản lý an toàn việc phân phối và sử dụng các khóa mã hóa cho HBA là một vấn đề cần quan tâm đúng mực.

SAN (Storage Area Network) là một mạng lưu trữ tốc độ cao dùng cho việc truyền dữ liệu giữa các máy chủ tham gia vào hệ thống lưu trữ, cũng như giữa các hệ thống lưu trữ với nhau. Điều cần thiết đó là mã hóa dữ liệu tại bộ điều hợp bus chủ (HBA), trên toàn bộ kết nối của mạng SAN và trên các thiết bị lưu trữ. Mã hóa có thể giúp ngăn chặn việc rò rỉ ngẫu nhiên hoặc cố ý tại nơi có được quyền truy cập dữ liệu và trên đường truyền.

Liên kết nền tảng điện toán tin cậy (TCPA - The Trusted Computing Platform Alliance) áp dụng phạm vi rộng rãi của nền tảng máy tính bao gồm các máy chủ, các ứng dụng và điện thoại di động. Ví dụ một máy tính cá nhân có thể sử dụng 24 giờ trong ngày được nối mạng cục bộ, mạng intranet, internet.

Mục đích của TCPA nhằm bảo vệ việc tấn công phần mềm từ nền tảng (platform). Đối với người dùng cục bộ và người dùng từ xa việc bảo vệ tấn công phần mềm là cần thiết. Nền tảng có thể kiểm tra chữ ký trên một ổ đĩa mới hoặc ứng dụng không thuộc danh sách được phê duyệt và ghi sự kiện chỉ khi chữ ký không xuất hiện trong danh sách được phê duyệt [7].

Một mô-đun nền tảng đáng tin cậy (TPM - The Trusted Platform Module) có các khả năng mật mã sau đây:

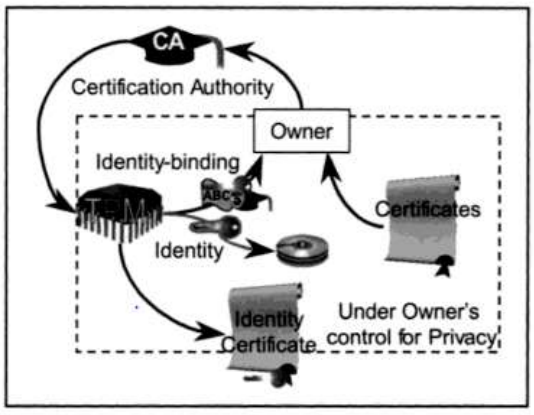
- Băm (HSA1 - Hashing)

- Tạo số ngẫu nhiên (RNG - Random Number Generation)

- Tạo khóa bất đối xứng (Asymmetric key generation)

- Mã hóa/giải mã bất đối xứng (Asymmetric encryption/decryption)

Hình 3 là sơ đồ mô tả nền tảng đảm bảo tin cậy.



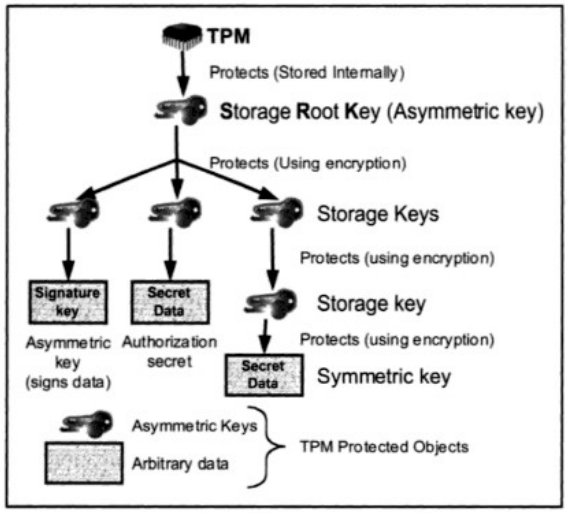
Hình 3: Sơ đồ mô tả nền tảng đảm bảo tin cậy

Cổng được dự định cho các khóa để mã hóa file và bản tin mã, các khóa để ký dữ liệu và cho bí mật được ủy quyền. Một CPU có thể chứa khóa đối xứng từ

một mô-đun nền tảng tin cậy (TPM - The Trusted Platform Module) và sử dụng nó để xây dựng mã chuyển dữ liệu đến một TPM và yêu cầu TPM ký dữ liệu. Cổng hoạt động như một chuỗi của các thao tác phân biệt trên những bí mật riêng.

Một đặc điểm quan trọng của nền tảng tin cậy đó là một đối tượng được bảo vệ TPM có thể bị niêm phong đến trạng thái phần mềm đặc biệt trong nền tảng. Khi đối tượng được bảo vệ TPM được tạo ra thì phần mềm phải tồn tại nếu bí mật được phát hành. Khi TPM mở một đối tượng được bảo vệ TPM (trong TPM và ẩn khỏi chế độ xem) thì TPM sẽ kiểm tra sự phù hợp của trạng thái phần mềm hiện tại so với trạng thái phần mềm đã nêu. Nếu đúng như vậy thì TPM cho phép truy cập đến bí mật. Nếu chúng không phù hợp thì TPM từ chối truy cập đến bí mật [7].

Hình 4 là Sơ đồ mô tả hệ thống phân cấp lưu trữ.



Hình 4: Sơ đồ mô tả hệ thống phân cấp lưu trữ

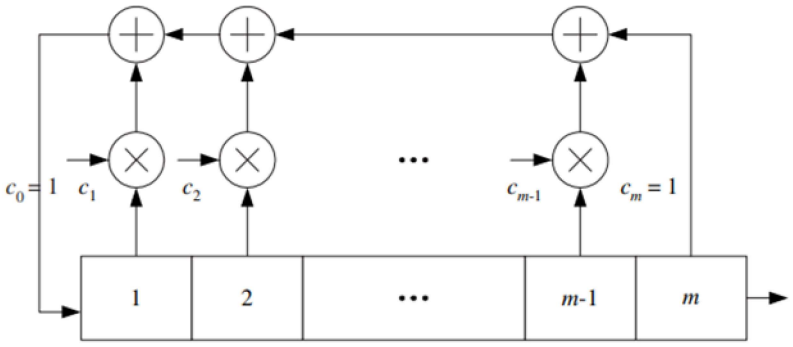
4. Thực hiện mã hóa bằng chuỗi giả ngẫu nhiên

Chuỗi giả ngẫu nhiên được tạo bởi thanh ghi dịch hồi tiếp tuyến tính (LFSR - Linear Feedback Shift Registers) [6]. Một thanh ghi dịch hồi tiếp tuyến tính m tầng được mô tả bằng đa thức m bậc có thể tạo chuỗi m tuần hoàn với chu kỳ 2^m - 1. Các đa thức này được biểu diễn bằng một vectơ nhị phân c = [cm, cm-1, ..., c1, c0] hoặc ký hiệu với vectơ bát phân. Ví dụ $f(x) = x^5+x^3+x^2+1$ là một vectơ nhị phân 101101 hoặc bát phân là 2D. Chuỗi m thỏa mãn đặc tính cân bằng và đặc tính độ dài chạy, khiến chúng có vẻ ngoài ngẫu nhiên. Đặc tính cân bằng thể hiện xác suất xuất hiện bit '0' và bit '1' là gần bằng nhau. Một bước chạy được định nghĩa là một nhóm bit cùng loại ('1' hoặc '0') liên tiếp tồn tại trong dãy. Độ dài bước chạy là số bit trong mỗi bước chạy. Đặc tính chạy trong dãy giả ngẫu nhiên phải thỏa mãn là trong một chu kỳ của dãy số tổng quát có $1/2^n$ số bước chạy có độ dài là n. Từ một dãy giả ngẫu nhiên đã có, nếu ta dịch chuyển theo cách dịch đi lần lượt từng vị trí bit sang phải hoặc sang trái, ta sẽ thu được dãy m mới có số phần tử trùng hợp và không trùng hợp với dãy ban đầu. Hàm tự tương quan của dãy giả ngẫu nhiên có dạng gần như là 2 mức, với giá trị đỉnh tại trễ là 0 là đỉnh và tại các vị trí khác là rất thấp. Đây là thước đo quan trọng nhất để đánh giá độ giống nhau của dãy với các bước dịch của nó, với hàm tự tương quan được xác định như sau:

$$R(\tau) = \sum_{n=0}^{N-1} \hat{a}_n \hat{a}_{n+\tau} = \begin{cases} N, & \tau \equiv 0 \\ c, & \tau \neq 0 \end{cases}$$

Trong đó $\hat{a}_n=(-1)^{a_n} \in \{+1, -1\}$, $a_n \in \{1,0\}$, c là một giá trị nhỏ.

Hình 5 mô tả mạch tạo chuỗi m sử dụng cấu hình Fibonacci.



Hình 5: Sơ đồ mô tả mạch tạo chuỗi m sử dụng cấu hình Fibonacci

Tự tương quan là thước đo mức độ giống nhau giữa một trình tự và các trình tự thay đổi theo thời gian của nó. Nó có thể được sử dụng để dự đoán điểm bắt đầu của chuỗi PN bằng cách phát hiện đỉnh. Để đảm bảo hàm tự tương quan (ACF - AutoCorrelation Function) tốt của phép xen kẽ, trình tự PN được ánh xạ trực tiếp vào bộ xen kẽ [3].

Các bước mã hóa bằng Matlab như sau [8]:

- Chọn một đa thức nguyên thủy

- Tạo dãy PN tương ứng với đa thức nguyên thủy đã chọn. Lưu trữ tất cả S - 1 dãy dịch chuyển của chuỗi này. Tạo một chuỗi PN có độ dài S =2^m - 1 cho một số nguyên m bằng cách sử dụng một thanh ghi dịch chuyển phản hồi tuyến tính với các kết nối phản hồi được xác định bởi một đa thức nguyên thủy bậc m trên trường Galois GF(2).

- Nối thêm bit "0" tại cuối mỗi dãy dịch chuyển từ dãy ban đầu nhằm thỏa mãn tính cân bằng giữa số lượng bit "1" và số lượng bit "0" trong chuỗi này.

- Tìm các cụm (lần chạy) có ít nhất hai bit "1" liên tiếp.

- Lưu trữ vị trí của các bit "1" của các cụm.

- Giữa hai bit "1" liên tiếp chèn một bit "0" từ vị trí gần nhất.

- Lưu vị trí hoán đổi.

- Tiếp tục các bước từ 6 đến hết trình tự.

- Lưu trữ các vị trí hoán đổi, chúng ta có một dãy hoán vị trực giao.

5. Kết quả và thảo luận

Bài viết này trình bày giải pháp tăng cường bảo mật trong hệ thống SAN trên cơ sở xây dựng cách thức mã hóa và sơ đồ quản lý khóa hiệu quả đồng thời sử dụng HSA nhằm bảo vệ khóa và lưu các quy trình kiểm soát việc sử dụng khóa trên cơ sở thực thi các chính sách tương ứng [4]. Giải pháp đảm bảo các dịch vụ chính thực thi trong phần cứng an toàn. Tuy giải pháp này phải thêm hệ thống phần cứng, thêm chi phí nhưng cho phép việc mã hóa dữ liệu được thực hiện tự động.

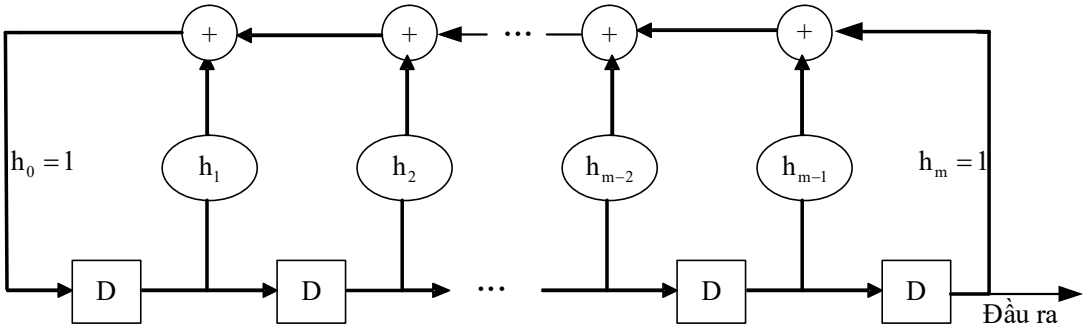
Trong quá trình tạo mã, tác giả lựa chọn dãy phi tuyến có độ dài lớn, độ phức tạp cao và hàm tương quan tốt. Độ phức tạp của một số dãy được thực hiện bằng phương pháp lồng ghép phi tuyến các dãy tuyến tính được tạo bởi bộ thanh ghi dịch phản hồi tuyến tính. Từ đó đưa ra lựa chọn dãy có độ phức tạp cao nhất, thực hiện tính toán các giá trị lồng ghép, đánh giá dãy đã tạo.

Để thực hiện mã hóa, trong bài báo này tác giả phân tích, đề xuất và mô phỏng ứng dụng cấu trúc xen kẽ bằng thanh ghi dịch chuyển phản hồi tuyến tính.

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

$$h(d)=h_0+h_1d+h_2d^2+\ldots+h_{m-1}d^{m-1}+h_md^m=\sum_{i=0}^{m}h_id^i$$

Đa thức này đưa ra một thanh ghi dịch phản hồi tuyến tính (LFSR) như biểu diễn trong Hình 6 gồm m khối biểu diễn cho các phần tử nhớ hay các thành phần flip-flops (các phần tử tạo trễ 1 chu kì xung nhịp), một phần tử nhớ có thể nhớ giá trị '0' hoặc '1'. Tại mỗi thời điểm truyền, giá trị trong các phần tử nhớ được dịch sang phần tử bên phải và các phần tử nhớ phản hồi theo dạng của đa thức h(d) là cộng và phản hồi đến phần tử bên trái. Phép tính tổng là được tính mô-đun 2, tương đương với phép tính XOR trong mạch điện tử.



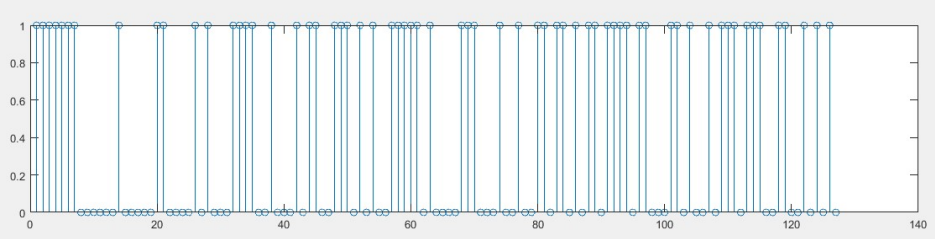
Hình 6: Thanh ghi dịch phản hồi tương đương h(d)

Thống kê số lượng đa thức nguyên tố có bậc m được thể hiện theo bảng sau.

Bậc (m)	**Độ dài chuỗi ($N = 2^m - 1$)**	**Số lượng đa thức**
3	7	2
4	15	2
5	31	6
6	63	6
7	127	18
8	255	16
9	511	48
10	1023	60
11	2047	176
12	4095	144
13	8191	630
14	16383	756
15	32767	1800
16	65535	2048
17	131071	7710
18	262143	7776

Mô phỏng chuỗi PN với m = 7 *(đa thức x^7+x^6+1)*

clear all; close all; x1=[1 1 1 1 1 1 1]; n1=length(x1); len1=2^n1-1; p1(1,1) = x1(1,1); z1 = x1; for y1 = 2 : len1 x1=z1; for i = 1 : n1 if (i==1) z1(1,i) = xor (x1(1,6),x1(1,7)); else z1(1,i) = x1(1,i-1); end end p1(1,y1)=z1(1,7); end subplot 211; stem (p1);



Thanh ghi dịch chuyển phản hồi tuyến tính có bậc m = 7 tương ứng với chuỗi PN có chu kỳ 127 bit.

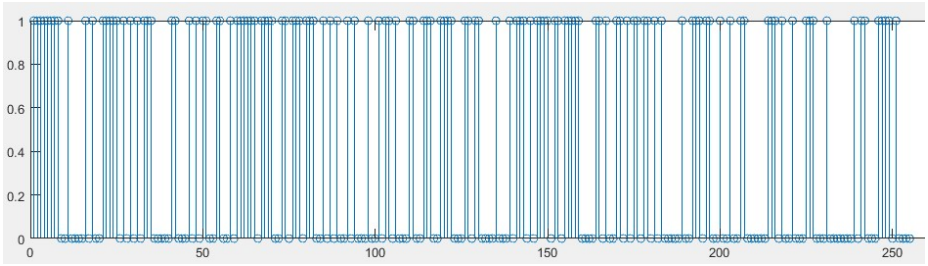
a) Simulate PN series with m = 8 (polynomial $x^8+x^4+x^3+x^2+1$)

Mô phỏng chuỗi PN với m = 8 *(đa thức $x^8+x^4+x^3+x^2+1$)*

clear all; close all; x1=[1 1 1 1 1 1 1 1]; n1 = length(x1); len1 = 2^n1-1; p1(1,1) = x1(1,1); z1 = x1; for y1 = 2 : len1 x1 = z1; for i = 1 : n1 if (i==1) z1(1,i) = xor (x1(1,2), xor (x1(1,3), xor (x1(1,4), x1(1,8)))); else z1(1,i) = x1(1,i-1); end end p1(1,y1) = z1(1,8); end subplot 211; stem (p1);

Thanh ghi dịch chuyển phản hồi tuyến tính có bậc m = 8 tương ứng với chuỗi PN có chu kỳ 255 bit. Tùy theo nhu cầu thực tế ta có thể mở rộng với giá trị m lớn hơn sẽ có dòng PN có chu kỳ lớn (2^m - 1).

Sau khi chạy chương trình mô phỏng, ta có kết quả như sau.



1 1 1 1 1 1 1 1 0 0 1 0 0
0 0 1 0 1 0 0 1 1 1 1 1
0 1 0 1 0 1 0 1 1 1 0 0
0 0 0 1 1 0 0 0 1 0 1 0
1 1 0 0 1 1 0 0 1 0 1 1
1 1 1 1 0 1 1 1 1 0 0 1
1 0 1 1 1 0 1 1 1 0 0 1
0 1 0 1 0 0 1 0 1 0 0 0
1 0 0 1 0 1 1 0 1 0 0 0
1 1 0 0 1 1 1 0 0 1 1 1
1 0 0 0 1 1 0 1 1 0 0 0
0 1 0 0 0 1 0 1 1 1 0 1
0 1 1 1 1 0 1 1 0 1 1 1
1 1 0 0 0 0 1 1 0 1 0 0
1 1 0 1 0 1 1 0 1 1 0 1
0 1 0 0 0 0 0 1 0 0 1 1
1 0 1 1 0 0 1 0 0 1 0 0
1 1 0 0 0 0 0 0 1 1 1 0
1 0 0 1 0 0 0 1 1 1 0 0
0 1 0 0 0 0 0 0 0 1 0 1
1 0 0 0 1 1 1 1 0 1 0 0
0 0

Dãy hoán vị trực giao được mô tả theo bảng sau:

Vị trí bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Giá trị bit	1	1	1	1	1	1	1	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	1
Vị trí bit mới	1	3	5	7	9	11	13	15	2	4	17	6	8	10	12	19	14	21	16	18	23	25	27

Vị trí bit	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44
Giá trị bit	1	1	0	1	0	1	0	1	0	1	1	1	0	0	0	0	0	1	1	0	0
Vị trí bit mới	29	31	20	33	22	35	24	37	26	39	41	43	28	30	32	34	36	45	47	38	40

……

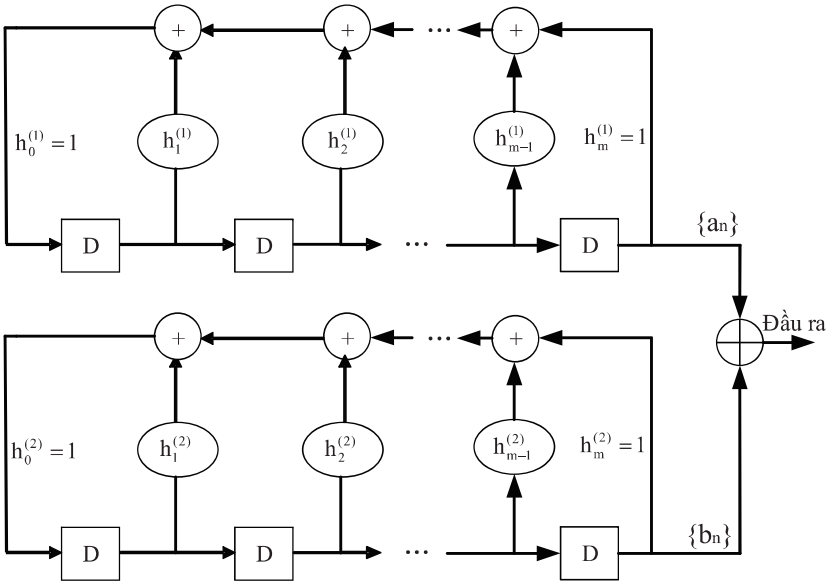
Vị trí bit	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256
Giá trị bit	1	0	1	1	0	0	0	1	1	1	1	0	1	0	0	0	0	0
Vị trí bit mới	241	238	243	245	240	242	244	247	249	251	253	246	255	248	250	252	254	256

Dãy Gold có thể được cấu tạo từ bất kì cặp dãy m nào. Gọi $a = \{a_n\}$, $b = \{b_n\}$ là một cặp dãy m có chu kì $N = 2^m - 1$ được sinh ra từ các đa thức nguyên tố $h_1(d)$ và $h_2(d)$ có bậc m. Tập hợp Gold kí hiệu là G(a,b) được cấu tạo như sau:

$$G(a,b) = \{a, b, a \oplus b, a \oplus Tb, a \oplus T^2b, ..., a \oplus T^{N-1}b\}$$

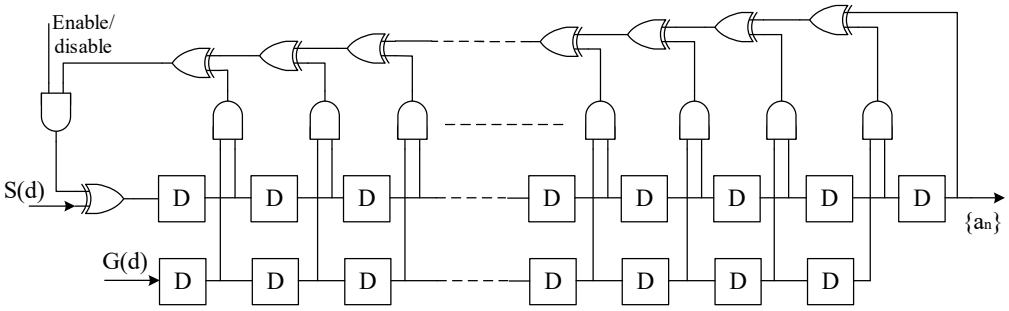
Trong đó, T là phép dịch dãy, G(a,b) chứa $N + 2 = 2^m + 1$ dãy có chu kì $N = 2^m - 1$.

Hình 7 hiển thị sơ đồ mạch tạo dãy Gold.



Hình 7: Sơ đồ mạch tạo dãy Gold

Phần cứng có thể được thực hiện để tạo dãy phi tuyến theo phương pháp lồng ghép. Sơ đồ mạch tạo dãy lồng ghép phi tuyến được biểu diễn trong Hình 8. Với sơ đồ lồng ghép này, việc thực hiện tạo dãy phi tuyến có thể được thực hiện trên các phần cứng như FPGA hay các chip xử lý.



Hình 8: Sơ đồ mạch tạo dãy lồng ghép phi tuyến

An toàn của thông tin phụ thuộc hai yếu tố đó là khóa mã và thuật toán mã hóa. Trong thương mại điện tử các thuật toán mã hóa thường được công khai, do đó độ an toàn của thông tin chỉ phụ thuộc vào độ an toàn của khóa mã. Trong hệ mật dùng khóa giả ngẫu nhiên, hệ thống sẽ cung cấp một số ngẫu nhiên ban đầu (key seed - mầm khóa) cho thuật toán sinh khóa để tạo ra khóa mã cho mỗi phiên liên lạc. Trong quá trình mã hóa thuật toán mã hóa sẽ tạo ra khóa mã dịch cho phiên liên lạc đó. Nói một cách khác, độ an toàn của hệ thống sẽ phụ thuộc vào mầm khóa và thuật toán sinh khóa. Để chống lại các tấn công vét cạn nhằm tìm khóa đúng, không gian mầm khóa phải đủ lớn và việc chọn mầm khóa để sinh khóa phải hoàn toàn ngẫu nhiên. Giả sử độ dài mầm là n thì lực lượng không gian mầm sẽ là 2^n khóa mầm. Các mã giả ngẫu nhiên trong bài báo này đáp ứng được yêu cầu về độ dài của mầm khóa bằng cách tăng bậc của đa thức sinh khóa.

6. Kết luận

Thiết bị bảo mật phần cứng có thể đảm bảo việc quản lý các khóa và mã hóa. Hiệu suất thực thi được tối ưu khi việc mã hóa và giải mã được thực thi tại bộ điều hợp bus máy chủ. Bộ điều hợp bus máy chủ bảo mật (SHBA) đảm bảo tin cậy cho tất cả dữ liệu được định tuyến qua nó. Thành phần đáng tin cậy này cần phải có khả năng mã hóa nhanh đảm bảo thông lượng dữ liệu cao cũng như tạo khóa và lưu trữ khóa. Đơn vị cơ bản của dữ liệu sẽ phụ thuộc vào thuật toán mã hóa cụ thể. Một trong những vấn đề quan trọng trong bảo mật cho một mạng đó là tách biệt quyền truy cập vào dữ liệu. Do đó người ta cần mã hóa dữ liệu tại bộ điều hợp bus chủ và trên các thiết bị lưu trữ. Mã hóa có thể giúp ngăn chặn việc rò rỉ ngẫu nhiên hoặc cố ý tại nơi có quyền truy cập dữ liệu và trên đường truyền. Các khóa giải mã chỉ có thể truy cập được trong một bối cảnh được ủy quyền. Các file mã hóa không thể đọc được. Bài báo đề xuất thực hiện mã hóa bằng chuỗi giả ngẫu nhiên cho bộ điều hợp bus máy chủ đồng thời lập phần mềm mô phỏng xây dựng một số mạch tạo chuỗi giả ngẫu nhiên bậc m. Như vậy trên cơ sở các chuỗi giả ngẫu nhiên bậc m ta có thể nâng cao độ phức tạp của mã bằng cách tăng bậc m, mặt khác có thể tạo các tổ hợp tạo nên dãy Gold từ đó tăng số lượng mã theo nhu cầu thực tế.

TÀI LIỆU THAM KHẢO

[1]. A.Baldwin, Y.Beres, M.Casassa Mont and S.Shiu (2001). *Trust services: A trust infrastructure for e-commerce*. HP Labs TR HPL-2001-198. http://www.hpl.hp.com/techreports/2001/HPL-2001-198.html.

[2]. DataLink (2002). *SAN data security and fabric management.* DataLink White paper http://www.storagesearch.com/datalink-sansecurity- art-1.pdf.

[3]. H. Yoshida (1999). *LUN security considerations for storage area networks*. Hitachi data systems.

[4]. M. Sloman, J. Lobo, E.C. Lupu (eds) (2001). *Policies for distributed systems and networks.* Proceedings of the 2nd International Policy Workshop. Lecture notes in computer science, vol 1995 Springer Verlag.

[5]. Rsa Laboratoris (2001). *PKCS#11 v2.11: Cryptographic token interface standard.* ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v211/pkcs- 11v2-11r1.pdf.

[6]. Santit Traithavil (2006). *Simulation of PN code sequences for cellular systems*. Department of Engineering, The Australian National University - February 17, 2006.

[7]. S. Pearson, B. Balacheff, L. Chen, D. Plaquin and G. Proudler (2002). *Trusted Computing Platforms: TCPA technology in comtext*. HP Books, Prentice Hall.

[8]. Tran Canh Duong et al (2021). *Generating the interleave division multiple access (IDMA) used in 5G mobile communication system.* Journal of Xidian University - ISSN No:1001-2400- Volume-15-Issue-12-December-2021, p. 546 - 534.

[9]. Yang Hu et al (2018). *Low-cost implementation techniques for interleave division multiple access.* IEEE wireless communications letters, Vol.7, No. 6, December 2018, p. 1026 - 1029 (combi).

BBT nhận bài: 13/4/2023; Phản biện xong: 28/4/2023; Chấp nhận đăng: 29/6/2023