Các ma trận MDS truy hồi hiệu quả cho thực thi từ mã Reed-Solomon và phép lũy thừa trực tiếp

Trần Thị Lượng, Nguyễn Ngọc Cương, Hoàng Đức Thọ, Hoàng Anh Công

***Tóm tắt*— Hiện nay, có nhiều mã khối sử dụng các ma trận của mã tách khoảng cách cực đại (MDS) như một phần quan trọng trong tầng khuếch tán của chúng. Tuy nhiên, các ma trận MDS luôn có một mô tả lớn, gây ra các thực thi phần cứng/phần mềm tốn chi phí. Các ma trận MDS truy hồi cho phép giải quyết bài toán này vì chúng có thể là lũy thừa của một ma trận Companion đơn giản, do đó chúng có thể phù hợp cho cả các môi trường bị ràng buộc, hạn chế. Trong bài báo này, phương pháp xây dựng các ma trận MDS truy hồi hiệu quả cho thực thi từ mã Reed-Solomon sẽ được trình bày. Sau đó, khả năng tạo ra các ma trận MDS truy hồi hiệu quả cho thực thi từ một ma trận MDS truy hồi hiệu quả ban đầu, nhờ phép biến đổi lũy thừa trực tiếp sẽ được chỉ ra. Các ma trận MDS truy hồi hiệu quả cho thực thi sẽ có ý nghĩa trong thực thi phần cứng. Chúng có thể được sử dụng cho tầng khuếch tán của nhiều mã khối và hàm băm, đặc biệt là các mã khối và hàm băm hạng nhẹ nhằm tiết kiệm tài nguyên và chi phí thực thi.**

***Abstract*— Nowaday, many block ciphers have used MDS matrices for their diffusion layer. However, the MDS matrices are always the components that cause large implementation cost for ciphers. Recursive MDS matrices will help to deal with this problem because they can be the power of a simple Companion matrix that is very sparse. In this paper, the ability to generate different efficient recursive MDS matrices for implementation from an original efficient recursive MDS matrix by direct exponential transformation is shown. These recursives MDS matrices are meaningful in hardware implementation. These matrices can be used in the diffusion layer of some block ciphers and hash functions ciphers and hash functions especially lightweight block ciphers and hash functions to save resources and implementation cost.**

Bài báo được nhận ngày 03/2/2022. Bài báo được nhận xét bởi phản biện thứ nhất ngày 22/2/2022 và được chấp nhận đăng ngày 21/3/2022. Bài báo được nhận xét bởi phản biện thứ hai ngày 25/2/2022 và được chấp nhận đăng ngày 18/3/2022.

Từ khóa— ma trận MDS; ma trận MDS truy hồi; mã RS.

Keywords— MDS matrix; recursive MDS matrices; RS codes.

I. GIỚI THIỆU

Trong FSE'94 [1], Vaudenay đã đề xuất sử dụng các ma trận MDS trong các nguyên thủy mật mã để tạo ra các đa hoán vị tuyến tính, các hàm tuyến tính với thuộc tính giống nhau. Vaudenay gọi các hàm này là các hàm có khả năng khuếch tán hoàn hảo: thay đổi t đầu vào thì làm thay đổi ít nhất $m - t + 1$ đầu ra. Ông đã chỉ ra làm thế nào để khai thác sự khuếch tán không hoàn hảo để phân tích mã các hàm không phải là các đa hoán vị tuyến tính. Hiện này có nhiều mã khối nổi tiếng như AES, SHARK, Anubis, Twofish, Square, Hierocrypt, Manta, Khazad, WHIRLPOOL, MUGI, hay mã dòng MUGI và hàm băm mật mã WHIRLPOOL sử dụng các ma trận MDS trong tầng khuếch tán của chúng.

Phương pháp phổ biến để xây dựng các ma trận MDS là trích rút chúng từ các mã MDS. Tuy nhiên, việc xây dựng các tầng khuếch tán MDS với chi phí thực thi thấp là một thách thức với các nhà thiết kế. Một vấn đề khác xuất hiện khi các tầng khuếch tán MDS được khai thác trong các mạng thay thế - hoán vị (SPN), trong đó ma trận MDS được sử dụng trong quá trình mã hóa và nghịch đảo của nó được sử dụng để thực hiện giải mã. Do đó, việc xây dựng các ma trận MDS với ma trận nghịch đảo của nó để có chi phí thấp là một vấn đề quan trọng khác.

Theo đó, các ma trận MDS truy hồi (lũy thừa của một ma trận Companion) đã được nghiên cứu bởi nhiều tác giả trên thế giới, do ứng dụng quan trọng của nó trong mật mã hạng nhẹ [3-7]. Tuy nhiên, theo các nghiên cứu này, để tìm

kiếm các ma trận MDS truy hồi như vậy đòi hỏi phải thực hiện một tìm kiếm vét cạn trên họ các ma trận Serial (điều này làm hạn chế kích cỡ các ma trận MDS tìm được) [5], hoặc là phải dùng một số phương pháp khác khá phức tạp, chẳng hạn xây dựng các ma trận MDS truy hồi từ các mã BCH [7]. Nhóm tác giả đã chỉ ra phương pháp xây dựng hiệu quả và đơn giản các ma trận MDS truy hồi từ các mã Reed-Solomon (RS) [8], tuy nhiên chưa đề cập đến việc tìm kiếm các ma trận MDS truy hồi hiệu quả từ phương pháp này. Trong tài liệu [9], nhóm tác giả đã chỉ ra một phương pháp xây dựng các ma trận MDS truy hồi hiệu quả cho thực thi từ mã RS, bằng cách tìm ra các ma trận MDS truy hồi đối xứng cỡ 4, 8 và 16 trên các trường $GF(2^4)$ và $GF(2^8)$. Tuy nhiên, nhóm tác giả chưa chỉ ra cách tìm các ma trận như vậy trong một trường tổng quát $GF(q)$ với $q = p^r$, p là số nguyên tố. Trong tài liệu [14], xét trên trường tổng quát $GF(q)$ và đưa ra phương pháp tìm các ma trận MDS truy hồi cỡ 4 hiệu quả cho thực thi (các ma trận MDS truy hồi đối xứng) từ mã RS.

Trong tài liệu [10], Ghulam Murtaza và Nassar Ikram lần đầu tiên giới thiệu về phép lũy thừa trực tiếp dùng cho ma trận MDS, nhưng các tác giả chưa chỉ ra sự bảo toàn một số thuộc tính mật mã tốt của các ma trận MDS qua phép biến đổi trên. Trong tài liệu [11], nhóm tác giả đã chỉ ra phép lũy thừa trực tiếp có khả năng bảo toàn tính truy hồi của ma trận MDS, tuy nhiên cũng chưa đề cập đến các ma trận MDS truy hồi hiệu quả cho thực thi.

Trong bài báo này, khả năng tạo ra các ma trận MDS truy hồi hiệu quả cho thực thi từ một ma trận MDS truy hồi hiệu quả ban đầu, nhờ phép biến đổi lũy thừa trực tiếp sẽ được trình bày. Các ma trận MDS truy hồi hiệu quả cho thực thi sẽ có ý nghĩa trong thực thi phần cứng. Chúng có thể được dùng cho tầng khuếch tán của nhiều mã khối và hàm băm, đặc biệt là các mã khối và hàm băm hạng nhẹ nhằm tiết kiệm tài nguyên và chi phí thực thi.

Bài báo được tổ chức như sau: Trong phần II, các kiến thức cơ sở và các công trình liên quan sẽ được trình bày. Phần III trình bày khả năng tạo ra các ma trận MDS truy hồi hiệu quả cho thực thi từ một ma trận MDS truy hồi hiệu quả ban đầu, nhờ phép biến đổi lũy thừa trực tiếp. Phần IV đưa ra so sánh giữa kết quả trong bài báo này với các kết quả trong tài liệu [7]. Phần V là kết luận.

Ký hiệu: Trong bài báo này, $A = [a_{i,j}]_{m\times m}$ ký hiệu một ma trận vuông cấp m, lcm ký hiệu bội số chung nhỏ nhất, $S_{d^{2^i}}$ hay $A_{d^{p^u}}$ ký hiệu các ma trận lũy thừa trực tiếp, $min\{\mathcal{L}\}$ là số nhỏ nhất trong tập $\mathcal{L}$.

II. KIẾN THỨC CƠ SỞ VÀ CÔNG TRÌNH LIÊN QUAN

A. Ma trận MDS truy hồi

Trong tài liệu [9], nhóm tác giả đã chỉ ra các ma trận MDS truy hồi đối xứng từ các mã RS trên các trường $GF(2^4)$ và $GF(2^8)$ như sau:

Mệnh đề 1: Khi xây dựng ma trận MDS truy hồi kích thước 4×4 trên trường $GF(2^4)$ hoặc $GF(2^8)$ từ mã *RS,* đa thức sinh $g(x)$ dạng (1) là đa thức đối xứng và có hệ số hằng bằng 1 khi và chỉ khi $b = 6$ hoặc $b = 126$ tương ứng.

Mệnh đề 2: Khi xây dựng ma trận MDS truy hồi kích thước $8\times 8, 16\times 16$ hoặc 32×32 trên trường $GF(2^8)$, đa thức sinh $g(x)$ dạng (1) là đa thức đối xứng và có hệ số hằng số bằng 1 khi và chỉ khi $b = 124$ hoặc $b = 120$ hoặc $b = 112$ tương ứng.

Trong tài liệu [9], nhóm tác giả tìm được 66 ma trận MDS truy hồi đối xứng cỡ 4, 8, 16 trên $GF(2^4)$ và $GF(2^8)$.

B. Phép lũy thừa trực tiếp

Khái niệm lũy thừa trực tiếp của một ma trận MDS đã được giới thiệu bởi Ghulam Murtaza và Nassar Ikram [10]. Các tác giả này đưa ra khái niệm ma trận lũy thừa trực tiếp như sau:

Định nghĩa 1: Cho *F* là trường *Galois.* Đối với ma trận cho trước $A = [a_{i,j}]_{m\times m}$, $a_{i,j} \in F$, xác định $A_{d^e} = [a_{i,j}^e]_{m\times m}$, $(e = 1,2,3,\ldots)$, nó được gọi là ma trận lũy thừa trực tiếp bậc *e* của *A*. Ma trận A_{d^2} còn được gọi là ma trận bình phương trực tiếp của *A*.

Trong tài liệu [11], nhóm tác giả đã chỉ ra phép lũy thừa trực tiếp có khả năng bảo toàn rất nhiều các thuộc tính mật mã tốt của ma trận MDS trong đó có tính truy hồi.

Trong tài liệu [12], nhóm tác giả đã chỉ ra phép lũy thừa trực tiếp bảo toàn tính MDS của ma trận MDS, và chỉ ra chu kỳ (τ) của phép lũy thừa trực tiếp một ma trận MDS qua Định lý dưới đây.

III. XÂY DỰNG CÁC MA TRẬN MDS TRUY HỒI HIỆU QUẢ CHO THỰC THI TỪ PHÉP LŨY THỪA TRỰC TIẾP

Trong phần này, khả năng tạo ra các ma trận MDS truy hồi hiệu quả cho thực thi từ một ma trận MDS truy hồi hiệu quả ban đầu, nhờ phép biến đổi lũy thừa trực tiếp sẽ được trình bày. Sau đó, các kết quả thực nghiệm nhờ phép lũy thừa trực tiếp để tìm thêm các ma trận MDS truy hồi hiệu quả sẽ được chỉ ra.

Trước hết, chu kỳ của phép lũy thừa trực tiếp của một ma trận MDS truy hồi là lũy thừa của một ma trận Companion sẽ được chỉ ra.

Xét ma trận MDS truy hồi $A = [a_{i,j}]_{m\times m}$, $a_{i,j} \in GF(p^r)$ là lũy thừa của một ma trận Companion S [13]. Ký hiệu $\dot{z}_1, \dots, \dot{z}_d$, với d $(d \le m)$ là phần tử khác nhau và khác 1 ở hàng cuối cùng của ma trận S. Ký hiệu $n_1, \dots, n_d$ là bậc tương ứng của các phần tử $\dot{z}_1, \dots, \dot{z}_d$ trong $GF(p^r)$. Ký hiệu $\mathbb{N}^+$ là tập các số nguyên dương và $lcm(n_1, \dots, n_d)$ là bội số chung nhỏ nhất của các số nguyên $n_1, \dots, n_d$.

Định lý sau đây được phát biểu như một trường hợp riêng của Định lý 1 [12]. Qua định lý này, nhóm tác giả muốn chỉ ra vai trò của ma trận Companion S: thứ nhất, nhóm tác giả muốn tận dụng khả năng bảo toàn tính truy hồi của phép lũy thừa trực tiếp, thứ hai thay vì phải xét $m \times m$ phần tử trong ma trận A, chỉ cần xét $d \le m$ phần tử ở hàng cuối cùng của S. Định lý 1 trong [12] xét trong trường hợp tổng quát khi A là một ma trận MDS bất kỳ.

Định lý 1: Cho ma trận MDS truy hồi $A = S^m$ trên $GF(p^r)$ với S là ma trận Companion. Khi đó, ta có $A_{d^{p^\tau}} = A$ với $\tau = min\{\mathcal{L}\}$, trong đó:

$$\mathcal{L} = \{\ell \in \mathbb{N}^+ : lcm(n_1, \dots, n_d) | (p^\ell - 1)\}$$

Hơn nữa, τ là giá trị nhỏ nhất có tính chất $A_{d^{p^\tau}} = A$.

Chứng minh:

Do A là ma trận MDS nên các phần tử $\dot{z}_1, \dots, \dot{z}_d$ đều khác 0 và do đó đều có bậc hữu hạn. Như vậy $lcm(n_1, \dots, n_d)$ tồn tại và là một số nguyên dương.

Rõ ràng $r \in \mathcal{L}$, vì bậc của phần tử khác 0 bất kỳ $a \in GF(p^r)$ đều là ước của $p^r - 1$, do đó $lcm(n_1, \dots, n_d)$ cũng là ước của $p^r - 1$. Vậy tồn tại $\tau = min\{\mathcal{L}\} \le r$. Từ đó, tồn tại số nguyên dương e sao cho:

$$p^\tau - 1 = e.lcm(n_1, \dots, n_d) \quad (1)$$

Theo giả thiết và theo Định lý 2 ([11]) - phép lũy thừa trực tiếp có khả năng bảo toàn tính truy hồi của ma trận MDS, nên ta có:

$$A_{d^{p^\tau}} = (S_{d^{p^\tau}})^m \quad (2)$$

Từ (1) ta có:

$$(\dot{z}_i)^{p^\tau - 1} = (\dot{z}_i)^{e.lcm(n_1,\dots,n_d)} = 1, (1 \le i \le d) \text{ hay:}$$

$$(\dot{z}_i)^{p^\tau} = (\dot{z}_i), (1 \le i \le d) \quad (3)$$

Suy ra $S_{d^{p^\tau}} = S$ hay:

$$(S_{d^{p^\tau}})^m = S^m \quad (4)$$

Từ (2) và (4), suy ra:

$$A_{d^{p^\tau}} = A \quad (5)$$

Giả sử tồn tại một số $u \in N^+$ sao cho:

$$A_{d^{p^u}} = A$$

Khi đó ta có:

$$(S_{d^{p^u}})^m = S^m \quad \Leftrightarrow \quad S_{d^{p^u}} = S$$
$$\Leftrightarrow (\dot{z}_i)^{p^u} = \dot{z}_i, \ 1 \le i \le d$$
$$\Leftrightarrow ord(\dot{z}_i) | (p^u - 1), 1 \le i \le d$$
$$\Leftrightarrow lcm(n_1, \dots, n_d) | (p^u - 1)$$
$$\Leftrightarrow u \in \mathcal{L}$$
$$\rightarrow \tau \le u \ \blacksquare$$

Gọi τ là chu kỳ của ma trận A qua phép biến đổi lũy thừa p trực tiếp.

Nhận xét 1: Nếu trong hàng cuối cùng của S chứa một phần tử sinh của trường, thì chu kỳ của phép lũy thừa trực tiếp của ma trận A là cực đại và bằng r.

Nhận xét 2: Nếu ma trận MDS ban đầu A là lũy thừa của một ma trận Serial S có hàng cuối

cùng đối xứng và có $z_0 = 1$. Thì với phép lũy thừa trực tiếp, có thể tạo ra $\tau - 1$ ma trận truy hồi khác cũng là lũy thừa của các ma trận Serial có hàng cuối cùng đối xứng và có $z_0 = 1$.

Như vậy, từ một ma trận MDS truy hồi hiệu quả cho thực thi ban đầu, nhờ phép biến đổi lũy thừa trực tiếp, ta có thể tạo ra các ma trận MDS truy hồi hiệu quả khác cho thực thi.

So sánh với Định lý 1 trong tài liệu [12]:

Đối với Định lý 1, để tìm chu kỳ của phép lũy thừa trực tiếp của ma trận A, ta phải tìm bội chung nhỏ nhất cho bậc của các phần tử khác nhau và khác 1 trong ma trận A. Tuy nhiên, trong trường hợp này thì chỉ cần tìm bội chung nhỏ nhất cho bậc của các phần tử khác nhau và khác 1 trong hàng cuối cùng của ma trận S. Như vậy sẽ thuận tiện và nhanh chóng hơn, đặc biệt trong trường hợp ma trận A có nhiều phần tử khác nhau trong ma trận (nhiều nhất là có m^2 phần tử khác nhau như vậy). Hơn nữa, khi ma trận S có hàng cuối cùng đối xứng và có $z_0 = 1$ thì số phần tử khác nhau và khác 1 trong hàng cuối cùng của ma trận S chỉ là $\frac{m}{2}$.

Ví dụ 1: Cho ma trận MDS truy hồi A trên $GF(2^8)$ với đa thức nguyên thủy là $x^8 + x^4 + x^3 + x^2 + 1$:

$$A = \begin{bmatrix} 1 & 38 & CF & 38 \\ 38 & 28 & BA & E6 \\ E6 & C & 82 & 8E \\ 8E & FA & E5 & 9E \end{bmatrix}$$

Đây là ma trận truy hồi được sinh ra từ ma trận Companion ứng với đa thức sinh đối xứng và có hệ số hằng số bằng 1 sau đây:

$$g_{126} = x^4 + a^{201}x^3 + a^{246}x^2 + a^{201}x + 1,$$

Ma trận Serial tương ứng với A (và gắn với đa thức g_{126}) là:

$$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & a^{201} & a^{246} & a^{201} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 38 & CF & 38 \end{bmatrix}$$

Ta có: $ord(38) = 85$, $ord(CF) = 85$, $lcm(ord(38), ord(CF)) = 85$.

Lần lượt thử các số $\ell = 1, 2, .., 7$ đến khi nào gặp số ℓ đầu tiên thỏa mãn:

$$2^\ell - 1 = 85d \text{ với } d \in \mathbb{N}^+.$$

Số đầu tiên thỏa mãn điều kiện trên là $\ell = 8$, do đó chu kỳ của phép lũy thừa 2 trực tiếp của ma trận A bằng 8.

Như vậy từ A, có thể tạo ra 7 ma trận truy hồi nữa tương ứng với 7 ma trận Serial có hàng cuối cùng đối xứng nhau và có $z_0 = 1$, đó là: $A_{d^{2^i}} = (S_{d^{2^i}})^4, 1 \le i \le 7$.

Trong đó: $S_{d^2} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & a^{147} & a^{237} & a^{147} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 29 & 8B & 29 \end{bmatrix}$,

$$S_{d^{2^2}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & a^{39} & a^{219} & a^{39} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 35 & 56 & 35 \end{bmatrix},$$

……

$$S_{d^{2^7}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & a^{228} & a^{123} & a^{228} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 3D & C5 & 3D \end{bmatrix}$$

Áp dụng Định lý 1, với mỗi đa thức đối xứng và có hệ số hằng số bằng 1 trong 66 đa thức ở Bảng 1 trong tài liệu [9], nhóm tác giả thực hiện tìm chu kỳ của phép lũy thừa 2 trực tiếp của mỗi đa thức đó, sau đó thực hiện chuỗi các lũy thừa 2 trực tiếp mỗi đa thức này theo chu kỳ của chúng, để tìm ra các đa thức đối xứng và có hệ số hằng số bằng 1 khác cùng chu kỳ. Từ những đa thức này có thể tìm được các ma trận MDS truy hồi đối xứng tương ứng.

Bằng phép lũy thừa trực tiếp, nhóm tác giả thu được chu kỳ của 66 ma trận MDS truy hồi

đối xứng. Với hai ma trận MDS truy hồi cỡ 4 trên $GF(2^4)$ thì chu kỳ đều bằng 4; với 64 ma trận MDS truy hồi cỡ 4, 8, 16, 32 trên $GF(2^8)$, các chu kỳ đều bằng 8. Do đó tổng đa thức đối xứng và có hệ số hằng số bằng 1 thu được không phải là 66 mà là 520, tương ứng với 520 ma trận truy hồi đối xứng hiệu quả cho thực thi.

Như vậy, nhờ cách xây dựng từ mã RS và khả năng bảo toàn tính truy hồi của phép lũy thừa trực tiếp, có thể tìm được rất nhiều những ma trận MDS truy hồi hiệu quả cho thực thi, những ma trận này sẽ là cẩm nang quan trọng cho các nhà thiết kế để lựa chọn cho các ứng dụng mật mã của họ.

Vì số lượng đa thức và ma trận truy hồi đối xứng quá lớn, nên không thể biểu diễn chi tiết tất cả, do đó nhóm tác giả đưa ra một vài ma trận MDS truy hồi ví dụ trong Bảng 1 với ma trận S và A từ ví dụ 1.

Đánh giá các ma trận kết quả

Tính hiệu quả của các ma trận MDS truy hồi được sinh ra này sẽ được đánh giá bằng số phép XOR và số phép Xtimes cần thiết để thực hiện phép nhân ma trận với một vectơ. Sau khi thu được 520 ma trận MDS truy hồi đối xứng ở trên, nhóm tác giả đánh giá tính hiệu quả của chúng bằng cách tính số phép XOR và Xtimes cho mỗi ma trận. Từ đó, đề xuất lựa chọn các ma trận MDS có số phép XOR và Xtimes ít nhất, chúng sẽ là các ma trận MDS truy hồi hiệu quả cho thực thi. Các ma trận MDS này được liệt kê trong Bảng 2 và các thuộc tính mật mã tương ứng của chúng được liệt kê trong Bảng 3.

BẢNG 1. MỘT SỐ MA TRẬN MDS TRUY HỒI ĐỐI XỨNG ĐƯỢC SINH TỪ PHÉP LŨY THỪA TRỰC TIẾP

STT	Ma trận lũy thừa trực tiếp của S	Ma trận MDS truy hồi tương ứng
1	$S_{d^2} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 29 & 8B & 29 \end{bmatrix}$	$A_1 = (S_{d^2})^4 = \begin{bmatrix} 1 & 29 & 8B & 29 \\ 29 & 34 & 3E & BE \\ BE & 50 & 17 & 47 \\ 47 & F3 & BB & 5A \end{bmatrix}$
2	$S_{d^{2^2}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 35 & 56 & 35 \end{bmatrix}$	$A_2 = (S_{d^{2^2}})^4 = \begin{bmatrix} 1 & 35 & 56 & 35 \\ 35 & 79 & 3D & 2E \\ 2E & D0 & 8 & D8 \\ D8 & B2 & 3F & 94 \end{bmatrix}$
3	$S_{d^{2^3}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 78 & C4 & 78 \end{bmatrix}$	$A_3 = (S_{d^{2^3}})^4 = \begin{bmatrix} 1 & 78 & C4 & 78 \\ 78 & E5 & 38 & 20 \\ 20 & C3 & 40 & 83 \\ 83 & 7E & 3C & 1E \end{bmatrix}$
4	$S_{d^{2^4}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & E4 & CE & E4 \end{bmatrix}$	$A_4 = (S_{d^{2^4}})^4 = \begin{bmatrix} 1 & E4 & CE & E4 \\ E4 & BB & 29 & 74 \\ 74 & DB & CD & 16 \\ 16 & F0 & 39 & 49 \end{bmatrix}$
5	$S_{d^{2^5}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & BA & 8A & BA \end{bmatrix}$	$A_5 = (S_{d^{2^5}})^4 = \begin{bmatrix} 1 & BA & 8A & BA \\ BA & 3F & 35 & B4 \\ B4 & 86 & 8F & 9 \\ 9 & B7 & 28 & 8C \end{bmatrix}$
6	$S_{d^{2^6}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 3E & 57 & 3E \end{bmatrix}$	$A_6 = (S_{d^{2^6}})^4 = \begin{bmatrix} 1 & 3E & 57 & 3E \\ 3E & 3C & 78 & 6A \\ 6A & 7 & 46 & 41 \\ 41 & 6F & 34 & 43 \end{bmatrix}$
7	$S_{d^{2^7}} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 3D & C5 & 3D \end{bmatrix}$	$A_7 = (S_{d^{2^7}})^4 = \begin{bmatrix} 1 & 3D & C5 & 3D \\ 3D & 39 & E4 & FD \\ FD & 15 & D9 & CC \\ CC & EC & 79 & C8 \end{bmatrix}$

BẢNG 2. DANH SÁCH CÁC ĐA THỨC VÀ MA TRẬN TRUY HỒI KẾT QUẢ TƯƠNG ỨNG

STT	Trường GF	Đa thức nguyên thủy	Kích thước ma trận	Ma trận MDS truy hồi và đa thức đối xứng tương ứng
1	$GF(2^8)$	$x^8+x^4+x^3+x^2+1$	4×4	$M_1 = \begin{matrix} 1 & 38 & CF & 38 \\ 38 & 28 & BA & E6 \\ E6 & C & 82 & 8E \\ 8E & FA & E5 & 9E \end{matrix}$ $g_{126} := x^4 + a^{201}x^3 + a^{246}x^2 + a^{201}x + 1$
2	$GF(2^8)$	$x^8+x^6+x^5+x^3+1$	8×8	$M_2 = \begin{matrix} 1 & 1B & 45 & F3 & 8E & F3 & 45 & 1B \\ 1B & 2D & B3 & 62 & A6 & A9 & 5B & 69 \\ 69 & DC & 67 & AB & 3B & BE & E3 & 9C \\ 9C & D3 & E3 & 47 & 77 & 1B & 81 & 59 \\ 59 & 59 & 57 & 4D & 2B & D9 & 9F & 44 \\ 44 & EA & 82 & 26 & EB & 5A & 2 & 2C \\ 2C & 2B & 3E & 18 & 57 & 71 & 8E & 6D \\ 6D & 87 & 1C & 51 & AB & 38 & 46 & 25 \end{matrix}$ $g_{124} := x^8 + a^{236}x^7 + a^{175}x^6 + a^{11}x^5 + a^{115}x^4 + a^{11}x^3 + a^{175}x^2 + a^{236}x + 1$
3	$GF(2^8)$	$x^8+x^5+x^3+x+1$	16×16	$M_3 = \begin{matrix} 01 & 33 & 75 & 1D & 03 & 84 & F9 & ED & 72 & ED & F9 & 84 & 03 & 1D & 75 & 33 \\ 33 & 83 & 04 & 74 & 48 & F1 & F2 & 0E & 43 & 85 & 9B & 0B & D1 & 02 & 2A & F7 \\ F7 & 5C & BD & E9 & 46 & 83 & 6D & 1D & A3 & AC & 19 & 50 & 39 & 3C & 3C & 45 \\ 45 & 17 & 84 & 45 & 26 & 48 & 2B & 06 & 35 & C8 & 04 & 17 & 9F & C1 & E4 & DC \\ DC & 56 & 4A & 7B & 0A & A0 & 89 & D3 & 19 & CD & 09 & 82 & 58 & 60 & 9C & F7 \\ F7 & B3 & 68 & A7 & 49 & C1 & 3C & 66 & 7E & F6 & 51 & C2 & B0 & B5 & 5E & F3 \\ F3 & 54 & 72 & F1 & 99 & C4 & C4 & 1A & 28 & 58 & F3 & DC & FC & 29 & 74 & FD \\ FD & 49 & 55 & 4D & DD & FD & 98 & 63 & BE & 8F & 04 & 97 & F0 & C3 & 28 & CE \\ CE & C5 & 7F & 6B & 34 & 4B & D7 & C8 & 69 & EE & A5 & 92 & EE & CE & F5 & 10 \\ 10 & 83 & 44 & 84 & 5B & 07 & 79 & 8E & 39 & 30 & DC & 96 & A2 & 15 & 4F & B8 \\ B8 & 4A & 5A & 83 & 67 & 31 & F3 & B5 & 02 & F5 & C4 & B6 & 75 & 65 & CC & 15 \\ 15 & 0A & 41 & C8 & BC & 96 & 63 & 8E & D5 & 7F & A7 & 35 & 89 & E7 & 6E & 7E \\ 7E & C4 & 30 & 50 & 4A & CC & 51 & 46 & E5 & F0 & B8 & D7 & B7 & 98 & DD & BF \\ BF & BD & 7D & A4 & BA & C1 & 81 & 48 & BF & FC & BD & 33 & 3D & 23 & 21 & 1E \\ 1E & EB & FC & 20 & 86 & 60 & AA & 59 & 53 & 67 & 97 & 67 & 11 & 60 & 62 & 75 \\ 75 & 29 & 9B & 22 & BF & DD & 9E & 2A & 49 & D3 & 99 & CC & F8 & CF & 10 & 55 \end{matrix}$ $g_{120} := x^{16} + a^{195}x^{15} + a^{169}x^{14} + a^{60}x^{13} + a^{243}x^{12} + a^{191}x^{11} + a^{17}x^{10} + a^{93}x^9 + a^{90}x^8 + a^{93}x^7 + a^{17}x^6 + a^{191}x^5 + a^{243}x^4 + a^{60}x^3 + a^{169}x^2 + a^{195}x + 1$

BẢNG 3. MỘT SỐ THUỘC TÍNH MẬT MÃ CỦA CÁC MA TRẬN MDS TRUY HỒI ĐƯỢC LỰA CHỌN

STT	Ma trận MDS truy hồi	Số nhánh	Số điểm bất động	Số phép XOR	Số phép Xtime
1	M_1	5	1	57	28
2	M_2	9	1	250	56
3	M_3	17	1	970	109

Có thể nhận thấy các hệ số điểm bất động của các ma trận ở bảng 2 đều rất nhỏ qua các vòng.

IV. SO SÁNH VỚI KẾT QUẢ TRONG [7]

Phương pháp tìm kiếm các ma trận MDS truy hồi dựa trên mã BCH được trình bày trong tài liệu [7]. Nhìn chung cách xây dựng này khá phức tạp, vì việc tìm đa thức sinh của mã BCH không đơn giản chút nào. Tuy nhiên, với mã *RS*, việc tính trực tiếp đa thức sinh của mã này rất đơn giản. Ngoài ra, trong tài liệu [7], các tác giả đã tìm được một số đa thức sinh dạng đối xứng tuy nhiên có trường hợp hệ số hằng số không bằng 1. Bảng 4 chỉ ra các đa thức này (ký hiệu α trong Bảng 4 là phần tử nguyên thủy của trường).

BẢNG 4. DANH SÁCH CÁC ĐA THỨC SINH ĐỐI XỨNG LÀ KẾT QUẢ CỦA TÀI LIỆU [7]

STT	Trường GF	Đa thức nguyên thủy	Kích thước ma trận	Đa thức sinh đối xứng	Ma trận Companion	Ma trận truy hồi tương ứng
1	$GF(2^4)$	x^4+x^3+1	4×4	$g_1 = x^4+\alpha^3x^3+\alpha x^2+\alpha^3x+1$	$S=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&\alpha^3&\alpha&\alpha^3\end{bmatrix}=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&8&2&8\end{bmatrix}$	$\begin{bmatrix}1&8&2&8\\8&E&1&D\\D&4&D&D\\D&1&7&1\end{bmatrix}$
2	$GF(2^4)$	x^4+x^3+1	4×4	$g_2 = x^4+\alpha^3x^3+\alpha x^2+x+\alpha^3+\alpha$	$S=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\\alpha^3+\alpha&1&\alpha&\alpha^3\end{bmatrix}=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\A&1&2&8\end{bmatrix}$	$\begin{bmatrix}A&1&2&8\\6&2&8&D\\F&B&1&4\\3&B&3&A\end{bmatrix}$
3	$GF(2^8)$	$x^8+x^4+x^3+x^2+1$	4×4	$g_3 = x^4+\alpha^3x^3+\alpha^{-3}x^2+\alpha^3x+1$	$S=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&\alpha^3&\alpha^{252}&\alpha^3\end{bmatrix}=\begin{bmatrix}0&1&0&0\\0&0&1&0\\0&0&0&1\\1&8&AD&8\end{bmatrix}$	$\begin{bmatrix}1&8&AD&8\\8&41&9&ED\\ED&33&7F&32\\32&60&72&F2\end{bmatrix}$

4	$GF(2^8)$	$x^8+x^4+x^3+x^2+1$	4×4	$g_4 = x^4+(\alpha^2+\alpha^3)x^3+\alpha^3x^2+(\alpha^3+\alpha^2)x+1$	$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & \alpha^3+\alpha^2 & \alpha^3 & \alpha^3+\alpha^2 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & C & 8 & C \end{bmatrix}$	$\begin{bmatrix} 1 & C & 8 & C \\ C & 51 & 6C & 58 \\ 58 & 8B & AB & EB \\ EB & D8 & 80 & 2B \end{bmatrix}$
5	$GF(2^8)$	$x^8+x^4+x^3+x^2+1$	4×4	$g_5 = x^4+\alpha^{202}x^3+(\alpha^{202}+1)x^2+x+\alpha+1$	$S = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ \alpha+1 & 1 & \alpha^{202}+1 & \alpha^{202} \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 3 & 1 & 71 & 70 \end{bmatrix}$	$\begin{bmatrix} 3 & 1 & 71 & 70 \\ 90 & 73 & D5 & D5 \\ 62 & 45 & AB & D8 \\ 75 & BA & 9A & AC \end{bmatrix}$

Các ma trận trong Bảng 4 được đánh giá và có kết quả trong Bảng 5 như sau:

BẢNG 5. MỘT SỐ THUỘC TÍNH MẬT MÃ CỦA CÁC MA TRẬN MDS TRUY HỒI TRONG [7]

STT	Số nhánh	Số điểm bất động	Số phép XORs	Số phép Xtimes
1	5	1, hệ số điểm bất động cao	22	12
2		1, hệ số điểm bất động cao	24	12
3	5	1, hệ số điểm bất động cao	49	27
4	5	1	46	27
5	5	1	56	28

Các ma trận trong Bảng 4 đều có kích thước 4, nhưng có các hệ số điểm bất động khá cao. Số lượng các phép XOR và Xtimes khá nhỏ. Do đó, cần cân nhắc để áp dụng các ma trận này vào thực tế. Các ma trận có ưu điểm là hệ số điểm bất động hầu hết rất nhỏ qua các vòng, và số lượng phép XOR và Xtimes cũng khá nhỏ. Mặt khác, kết quả của [7] chỉ bao gồm các ma trận kích thước 4, kết quả bao gồm ma trận kích thước 4, 8 và 16. Mặc dù số lượng phép XOR, Xtimes của các ma trận cao hơn một chút so với ma trận của [7], các ma trận này vẫn khá hiệu quả, hoàn toàn có thể áp dụng cho cả mật mã khối thường và mã khối hạng nhẹ.

Trong tài liệu [9], nhóm tác giả đã tìm thấy 66 ma trận MDS truy đối xứng nhưng không đưa ra bất kỳ đánh giá nào cho các ma trận thu được, nhưng trong bài báo này, nhóm tác giả đã tìm thấy 520 ma trận như vậy bằng cách sử dụng biến đổi lũy thừa trực tiếp, nhiều hơn nhiều so với [9]. Bên cạnh đó cũng đánh giá 520 ma trận này để có được những ma trận tốt nhất cho thực thi trong những ma trận mà nhóm tác giả đã tìm thấy.

V. KẾT LUẬN

Trong bài báo này, khả năng tạo ra các ma trận MDS truy hồi đối xứng hiệu quả cho thực thi từ một ma trận MDS truy hồi đối xứng hiệu quả ban đầu, nhờ phép biến đổi lũy thừa trực tiếp đã được chỉ ra. Sau đó đã đánh giá các ma trận kết quả thu được để đạt được các ma trận tốt nhất cho thực thi. Đồng thời, nhóm tác giả cũng so sánh các ma trận thu được trong bài báo này với các ma trận thu được trong tài liệu [7] và [9]. Các ma trận MDS truy hồi hiệu quả cho thực thi sẽ có ý nghĩa trong thực thi phần cứng. Chúng có thể được sử dụng trong tầng khuếch tán của nhiều mã khối và hàm băm nhằm tiết kiệm tài nguyên và chi phí thực thi. Hơn nữa, có

thể sử dụng các ma trận này trong thiết kế tầng khuếch tán của nhiều mã khối và hàm băm hạng nhẹ hiệu quả trong tương lai.

TÀI LIỆU THAM KHẢO

[1]. S. Vaudenay, On the need for multipermutations: cryptanalysis of MD4 and SAFER. *In: Preneel B. (eds) Fast Software Encryption. FSE 1994. Lecture Notes in Computer Science,* vol. 1008. Springer, Berlin, Heidelberg, pp. 286-297, 1994.

[2]. C. Schnorr and S. Vaudenay. *Black box cryptanalysis of hash networks based on multipermutations*. In A. De Santis, editor, Advances in Cryptology - EU-ROCRYPT '94. Proceedings, volume 950 of LNCS, pages 47–57. Springer-Verlag, 1995.

[3]. M. Sajadieh, M. Dakhilalian, H. Mala, and P. Sepehrdad, "Recursive diffusion layers for block ciphers and hash functions," in *Fast Software Encryption.* Springer, 2012, pp. 385-401.

[4]. S. Wu, M. Wang, and W. Wu, "Recursive diffusion layers for (lightweight) block ciphers and hash functions," in *Selected Areas in Cryptography.* Springer, 2013, pp. 43-60.

[5]. D. Augot and M. Finiasz, "Exhaustive search for small dimension recursive mds diffusion layers for block ciphers and hash functions," in *2013 IEEE International Symposium on Information Theory Proceedings (ISIT)*. IEEE, 2013, pp.1551-1555.

[6]. S. Kolay, D. Mukhopadhyay, "Lightweight diffusion layer from the k^{th} root of the mds matrix", *IACR Cryptology ePrint Archive*, vol. 498, 2014.

[7]. D. Augot, M. Finiasz, "Direct construction of recursive mds diffusion layers using shortened bch codes", *21st International Workshop on Fast Software Encryption*, *FSE 2014*, Springer, 2014.

[8]. Tran Thi Luong, "Constructing effectively mds and recursive mds matrices by reed-solomon codes", *Journal of Science and Technology on Information Security,* Vol. 3, No. 2, pp. 10–16, 2016.

[9]. Tran Thi Luong, Nguyen Ngoc Cuong and Hoang Duc Tho, Constructing Recursive MDS Matrices Effective for Implementation from Reed-Solomon Codes and Preserving the Recursive Property of MDS Matrix of Scalar Multiplication, Journal of Informatics and Mathematical Sciences, Vol. 11, No. 2, pp. 155–177, 2019.

[10]. G. Murtaza, N. Ikram, "*Direct Exponent and Scalar Multiplication Classes of an MDS Matrix*", [EB/OL], National University of Sciences and Technology, Pakistan, (2011-01-10), pp. 2-5.

[11]. T. T. Luong, N. N. Cuong, L. T. Dung, "The preservation of good cryptographic properties of MDS matrix under direct exponent transformation", *Journal of Computer Science and Cybernetics*, vol.31, no.4, pp. 291–303, 2015.

[12]. T. T. Luong, N. N. Cuong, L. T. Dung, "A new statement about direct exponent of an MDS matrix in block ciphers", in *2015 IEEE the Seventh International Conference on Knowledge and Systems Engineering (KSE)*, IEEE, pp. 340–343, 2015. (Date Added to IEEE Xplore: 07 January 2016).

[13]. Kishan Chand Gupta, Indranil Ghosh Ray, *On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography*, In: Cuzzocrea A., Kittl C., Simos D.E., Weippl E., Xu L. (eds) Security Engineering and Intelligence Informatics. CD-ARES 2013. Lecture Notes in Computer Science, vol 8128. Springer, Berlin, Heidelberg.

[14]. Thi Luong Tran, Ngoc Cuong Nguyen, Duc Trinh Bui, 4×4 recursive MDS matrices effective for implementation from Reed-Solomon code over $GF(q)$ field, Proceedings of the 4th International Conference on Modelling, Computation and Optimization in Information Systems and Management Sciences - MCO 2021, Springer.

SƠ LƯỢC VỀ TÁC GIẢ

Trần Thị Lượng

Đơn vị công tác: Học viện Kỹ thuật mật mã.

Email: luongtranhong@gmail.com

Quá trình đào tạo: Nhận bằng Cử nhân Toán tin ứng dụng tại Trường Đại học Khoa học Tự Nhiên – Đại học Quốc gia Hà Nội năm 2006; Thạc sĩ và Tiến sĩ Kỹ thuật mật mã tại Học viện Kỹ thuật mật mã lần lượt vào năm 2012 và 2019.

Hướng nghiên cứu: Mật mã; lý thuyết mã; an toàn thông tin.

Nguyễn Ngọc Cương

Quá trình đào tạo: Nhận bằng cử nhân tại Đại học Quốc gia Hà Nội năm 1972; Tiến sĩ tại Đại học Quốc gia Hà Nội năm 1984.

Hướng nghiên cứu: Toán học tính toán; khoa học mật mã.

Hoàng Đức Thọ

Đơn vị công tác: Học viện Kỹ thuật mật mã.

Email: hdtho@actvn.edu.vn

Quá trình đào tạo: Nhận bằng Cử nhân và Thạc sĩ Công nghệ thông tin tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội lần lượt vào năm 2002 và 2007; Tiến sĩ An toàn thông tin tại Học viện FSO – Liên bang Nga năm 2014.

Hướng nghiên cứu: Mật mã; an toàn thông tin.

Hoàng Anh Công

Đơn vị công tác: Đại học Văn hóa, Thể thao và Du lịch Thanh Hóa.

Email: hoanganhbdth@gmail.com

Quá trình đào tạo: Nhận bằng Cử nhân và Thạc sĩ Khoa học máy tính tại Trường Đại học Công nghệ Thông tin và Truyền thông Thái Nguyên – Đại học Thái Nguyên lần lượt vào năm 2008 và 2013.

Hướng nghiên cứu: Khoa học máy tính; an toàn thông tin.