XÂY DỰNG CÁC MA TRẬN MDS CẶP ĐÔI TỪ MÃ REED-SOLOMON

TS. Trần Thị Lượng
Học viện Kỹ thuật mật mã

Bài báo này giới thiệu về MDS cặp đôi - một ma trận có dạng đối xứng đặc biệt và phương pháp xây dựng các ma trận này nhờ một mã cyclic nổi tiếng, đó là mã Reed-Solomon. Những ma trận dạng này có thể hữu ích trong việc nâng cao tốc độ xử lý hoặc hiệu quả trong thiết kế phần cứng.

Tác giả Thierry P. Berger (năm 2014) đã trình bày cách xây dựng tổng quát các ma trận MDS cổ điển mà không cần tính toán đệ quy nhưng lại có tính đối xứng mạnh để đẩy nhanh tốc độ xử lý với một số tối thiểu các bảng tra hoặc để thực hiện với một số lượng tối thiểu các cổng trong một mạch. Tác giả gọi loại ma trận đặc thù này là *"các ma trận cặp đôi dyadic matrix"*, bởi vì chúng liên quan tới các mã cặp đôi. Tác giả giới thiệu một cách xây dựng tổng quát các ma trận MDS cặp đôi tự nghịch đảo từ các mã Reed-Solomon (RS) và đề cập đến khía cạnh cài đặt của những ma trận MDS cặp đôi này để xây dựng các mã khối hiệu quả.

MA TRẬN CẶP ĐÔI

Một ma trận đối xứng khối là một ma trận vuông có kích cỡ chẵn $r = 2s$ để nếu $A_{i,j}$ với i, j thuộc $\{1, 2\}$ biểu thị bốn ma trận con kích thước của A, thì khi đó $A_{1,1} = A_{2,2}$, và $A_{1,2} = A_{2,1}$. Khi đó, một ma trận cặp đôi A là một ma trận vuông có kích cỡ 2^v sao cho A là ma trận khối đối xứng

và bốn ma trận con của nó là các ma trận đối xứng khối đệ quy. Tên của các ma trận cặp đôi xuất phát từ các mã cặp đôi (dyadic code), là một họ của các mã Abel, đó là các mã lý tưởng khi chúng được xét trong một đại số trên nhóm dịch $(GF(2)^n, +)$. Để xem chi tiết có thể tìm trong [2, 3]. Một điều thú vị là dạng của các ma trận cặp đôi này cũng giống với dạng của các ma trận Hadamard.

Kết quả chính của [1] là một cách xây dựng tổng quát các ma trận MDS cặp đôi tự nghịch đảo từ mã *RS* với kích cỡ bất kỳ $r = 2^v$ và trên trường hữu hạn bất kỳ $GF(2)^m$ (dưới phỏng đoán MDS $r \leq 2^{m-1}$).

Định nghĩa 1 (*Ma trận đối xứng khối*). Giả sử là một ma trận $2s \times 2s$ trên một vành R. Đặt $M = \begin{bmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{bmatrix}$ là ma trận với sự phân tách các khối vuông. Ma trận M là đối xứng-khối (block-systemetric) nếu $M_{1,1} = M_{2,2}$, và $M_{1,2} = M_{2,1}$.

Ta quan tâm tới các ma trận đối xứng khối có tính đệ quy, là những ma trận được gọi là các ma trận cặp đôi.

Định nghĩa 2 (*Ma trận cặp đôi*). Giả sử M là một ma trận $2^v x 2^v$ trên vành R. Người ta có thể định nghĩa đệ quy một ma trận cặp đôi (đối xứng khối đệ quy) như sau:

Nếu $v = 0$, M là ma trận cặp đôi.

Nếu $v > 0$, M là ma trận cặp đôi khi và chỉ khi M là đối xứng khối và mỗi ma trận khối con phân biệt của nó cỡ $2^{v-1} \times 2^{v-1}$ $M_{1,1}$ và $M_{1,2}$ là ma trận cặp đôi.

Mục đích chính của tác giả Berger trong [1] là xây dựng được một số ma trận cặp đôi là MDS.

Dưới đây là một ví dụ đầu tiên của ma trận cặp đôi trên $GF(2^4)$. Giả sử a là nghiệm của x^4+x+1, đó là một nghiệm nguyên thủy của $GF(16) = GF(2)(a)$. Giả sử M là ma trận 4×4 sau đây:

$$M = \begin{bmatrix} a^3 & a^{12} & 1 & a^{10} \\ a^{12} & a^3 & a^{10} & 1 \\ 1 & a^{10} & a^3 & a^{12} \\ a^{10} & 1 & a^{12} & a^3 \end{bmatrix}$$

Lưu ý rằng $M_{1,1} = M_{2,2} = \begin{bmatrix} a^3 & a^{12} \\ a^{12} & a^3 \end{bmatrix}$ và $M_{1,2} = M_{2,1} = \begin{bmatrix} 1 & a^{10} \\ a^{10} & 1 \end{bmatrix}$

Tất cả các ma trận con trên là đối xứng khối, vì vậy M là ma trận cặp đôi.

MỘT SỐ THUỘC TÍNH CỦA MA TRẬN CẶP ĐÔI

Đặt $r = 2^v$ với một số nguyên v cố định. Đối với một vành cố định R, chúng ta ký hiệu D_v là tập các ma trận cặp đôi có kích cỡ $r = 2^v$ trên R. Xét mệnh đề sau đây.

Mệnh đề 1 [1].

1) D^v là một module-R, tức là $(D_v, +)$ là một nhóm giao hoán và D_v là bền vững (stable) bởi phần tử nhân vô hướng $\lambda \in R$.

2) D_v là bền vững dưới phép nhân ma trận.

3) Nếu R là một vành giao hoán, thì tích của các ma trận cặp đôi là giao hoán.

4) Nếu R là một vành hữu hạn và A là một ma trận cặp đôi khả nghịch, thì A^{-1} là ma trận cặp đôi.

Áp dụng công thức tích của hai ma trận cho trường hợp riêng $A=C$ và $B=D$, ta có hệ quả sau đây:

Hệ quả 1 [1]. Nếu là vành giao hoán với đặc số 2, thì bình phương của một ma trận cặp đôi là một ma trận đường chéo.

Có thể thấy rằng các tính chất này cũng giống với các tính chất của các ma trận Hadamard.

MÃ REED-SOLOMON (RS)

Có nhiều cách khác nhau để giới thiệu về họ mã. Tác giả Berger trình bày các mã này như sự ước lượng của các đa thức.

Cho $K=GF(2^m)$. Xét vành đa thức $R=K[X]/(X^{2^m} - X)$. Vành R là đẳng cấu với các ứng dụng của K vào chính nó [4], tức là tất cả các ứng dụng của K vào K là một đa thức với bậc nhỏ hơn 2^m.

Đặt $P_k = \{P(X) \in R \mid deg\ (P(X)) < k\}$. Tập P_k là một K - không gian vectơ của R có số chiều là k.

Đặt $S=(a_1, a_2, ..., a_n)$ là một tập được sắp gồm các phần tử phân biệt của K.

Định nghĩa 3 *(Mã RS).* Mã Reed-Solomon $RS_{k,S}$ với số chiều k (độ dài là n*) và giá S* là mã thu được bằng cách ước lượng các phần tử của P_k trên *S:*

$$RS_{k,S} = \{(P(a\ ), \ldots, P(a_n)) \in K^n \mid P(X) \in \mathcal{P}_k\}.$$

Bởi vì P_k là một K - không gian con của R, nên mã $RS_{k,S}$ là K-tuyến tính.

Đa thức bất kỳ khác không có bậc chắc chắn nhỏ hơn k sẽ có nhiều nhất $k-1$ nghiệm. Sử dụng thực tế này, ta có thể suy ra rằng khoảng cách tối thiểu của mã trên thỏa mãn $d \geq n - (k-1)$, do đó, mã này là MDS và $k+d = n+1$.

Sử dụng ước lượng của cơ sở kinh điển $(1,X,X^2 ...,X^{k-1})$ của P_k, ta khôi phục ma trận sinh cổ điển của mã Reed Solomon ([5]):

$$\begin{bmatrix} 1 & 1 & \ldots & \ldots & 1 \\ a_1 & a_2 & \ldots & \ldots & a_n \\ a_1^2 & a_2^2 & \ldots & \ldots & a_n^2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_1^{k-1} & a_2^{k-1} & \ldots & \ldots & a_n^{k-1} \end{bmatrix}$$

Các ma trận MDS từ mã

Nếu chọn $n=2r$ và $k=r$, thu được một mã MDS với các tham số $[2r,r,r+1]$. Một mã như vậy là phù hợp để có được một ma trận MDS: bởi vì như vậy là đủ để có thể xây dựng được ma trận sinh của nó dưới dạng hệ thống $G=(I_r \mid A)$ để có được một ma trận MDS A trên K.

Tuy nhiên, ta sẽ xem xét cấu trúc của chi tiết hơn.

Nếu $A=[a_{i,j}]$, thì hàng đầu tiên của G là $G_1=(1,0,...,0,a_1,1,a_{1,2},...,a_{1,r})$. Hàng này tương ứng với ước lượng của đa thức sau: $P_1(X) = b_1^{-1} \prod_{i=2}^{r}(X - a_i)$ trong đó $b_1 = \prod_{i=2}^{r}(a_1 - a_i)$. Thật vậy, $deg\ (P_1\ (X)) = r-1 < k = r; P_1\ (a_i) = 1$ và $P_1\ (a_i) = 0$ với I từ 2 đến r. Có thể suy ra rằng $a_{1,i} = P_1\ (a_{r+i})$.

Tương tự, đặt $P_i(X) = b_i^{-1} \prod_{j=1,j\neq i}^{r}(X - a_j))$ với $b_i = \prod_{j=2,j\neq i}^{r}(a_i - a_j)$ cho i từ 1 đến r. Ta thu được $a_{i,j} = P_i(a_{r+j})$ với mọi i và j.

Một giới hạn chung của cách xây dựng này đến từ các phỏng đoán MDS là, ngoại trừ một số trường hợp đặc biệt $(k \in \{1,2,n-1,n-2\})$ thì chiều dài tối đa của một mã MDS trên một trường hữu hạn kích cỡ q là $n=q+1$. Vì vậy, đối với ma trận MDS trên $GF(2^m)$, vì chiều dài mã của ta là chẵn, nên kích thước tối đa của một ma trận MDS là $2^{m-1} \times 2^{m-1}$.

Giới hạn tương tự đối với trường hợp $m=8$ cũng đưa ra một ma trận kích cỡ $r = 2^7 = 128$. Giá trị $r=128$ này là quá lớn đối với các ứng dụng. May mắn thay, việc xây dựng của tác giả có thể được thực hiện bằng cách không cần sử dụng toàn bộ cơ sở $B = (b_1,...,b_m)$ của K trên $GF(2)$, chỉ cần một tập được sắp $(b_1,...,b_s)$ gồm s các phần tử độc lập tuyến tính của K, dẫn đến một ma trận MDS cặp đôi có kích cỡ 2^{s-1}. Vì vậy, dễ dàng có thể xây dựng một ma trận MDS cặp đôi hoạt động trên 8 khối có kích cỡ 8.

XÂY DỰNG CÁC MÃ MDS CẶP ĐÔI TỰ NGHỊCH ĐẢO TỪ CÁC MÃ RS

Giả sử $n=2^v$ với $v \leq m$. Giả sử $V \subset K$ là một không gian vectơ có số chiều v trên $GF(2)$. Tác giả chọn một cơ sở $B=(b_1,...,b_v)$ của V.

Định nghĩa $S_B=(a_0,a_1,...,a_{n-1})$ như sau: $a_0=0, a_1=b_1, a_2=b_2, a_3=b_1+b_2, ..., a_i=\sum_{j=0}^{v-1} i_j\ b_j$, $i = \sum_{j=0}^{v-1} i_j\ 2^j$ trong đó là biểu diễn nhị phân của số nguyên i.

Ví dụ, nếu $B = (1,a,b)$, thì $S_B = (0,1,a,1 + a,b,1 + b,a + b,1 + a + b)$.

Kết quả chính trong [1] của Berger là định lý sau đây:

Định lý 1 [1]. Ma trận MDS đạt được từ mã Reed-Solomon RS_{r,S_B} là ma trận cặp đôi. Hơn nữa là tự nghịch đảo.

Chi tiết các chứng minh của định lý, độc giả xem thêm trong [1].

SO SÁNH VỚI CÁC CÔNG TRÌNH TRƯỚC ĐÓ VỀ CÁC MÃ GOPPA CẶP ĐÔI

Trong [6], Paulo S.L.M. Barreto và Rafael Misoczki đã đề xuất lớp mã Goppa cặp đôi cho một kiểu hệ mật khóa công khai McEliece. Họ đưa ra một thuật toán xây dựng các ma trận Cauchy cặp đôi trên $GF(2^m)$. Rõ ràng đó là các ma trận MDS cặp đôi như được định nghĩa trong [1].

Có một liên kết mạnh giữa các ma trận Cauchy và các ma trận phần dư trong dạng hệ thống của các mã *RS* tổng quát (các mã GRS). Do đó, tác giả Berger phỏng đoán rằng cách xây dựng của tác giả và thuật toán được giới thiệu trong [6] dẫn tới các tập giống nhau của các ma trận MDS cặp đôi.

Hơn nữa, các ma trận Cauchy cặp đôi đến từ một vài mã GRS rất cụ thể được đưa ra chủ yếu từ các mã *RS* bằng cách nhân phần thứ hai của giá với cùng một phần tử vô hướng.

Với phương pháp xây dựng ma trận MDS tự nghịch đảo từ các mã RS trong [1], tác giả bài báo này đã tiến hành cài đặt chương trình và thực hiện trên Maple. Từ đó, đã thu được một số ma trận MDS cặp đôi tự nghịch đảo từ mã RS. Dưới đây là hai ma trận ví dụ cỡ 4 và cỡ 8 đã thu được:

$$Mhex := \begin{bmatrix} ED & C0 & D8 & F4 \\ C0 & ED & F4 & D8 \\ D8 & F4 & ED & C0 \\ F4 & D8 & C0 & ED \end{bmatrix}$$

$$Mhex := \begin{bmatrix} 9 & DA & B7 & 4D & 29 & 83 & 51 & D3 \\ DA & 9 & 4D & B7 & 83 & 29 & D3 & 51 \\ B7 & 4D & 9 & DA & 51 & D3 & 29 & 83 \\ 4D & B7 & DA & 9 & D3 & 51 & 83 & 29 \\ 29 & 83 & 51 & D3 & 9 & DA & B7 & 4D \\ 83 & 29 & D3 & 51 & DA & 9 & 4D & B7 \\ 51 & D3 & 29 & 83 & B7 & 4D & 9 & DA \\ D3 & 51 & 83 & 29 & 4D & B7 & DA & 9 \end{bmatrix}$$

KẾT LUẬN

Tác giả Berger [1] đã giới thiệu về ma trận cặp đôi và một phương pháp xây dựng các ma trận MDS cặp đôi phù hợp cho các ứng dụng mật mã. Các ma trận này có thể được xây dựng từ các mã RS. Theo tác giả, một công việc mang tính lý thuyết tiếp theo cần làm là tìm kiếm các ma trận MDS cặp đôi khác so với các ma trận được xây dựng từ mã RS. Một vấn đề mở là có sự tồn tại của các ma trận MDS cặp đôi không tương đương với các ma trận đến từ mã RS trong trường hợp chiều dài đầy đủ, nghĩa là $r=2^{(m-1)}$. Có thể thấy rằng các ma trận cặp đôi có dạng giống hệt với các ma trận Hadamard. Do đó, có thể có các ma trận cặp đôi không xuất phát từ các mã RS. Những ma trận này có khả năng ứng dụng trong thiết kế và xây dựng các mã khối góp phần nâng cao độ an toàn và tính hiệu quả trong cài đặt phần cứng, và nâng cao tốc độ xử lý trong phần mềm.❖

TÀI LIỆU THAM KHẢO

1. Thierry P. Berger, Construction of dyadic MDS matrices for cryptographic applications, arXiv: 1402.0972v1 [cs. CR] 5-2014.
2. Florence J. MacWilliams. Binary codes which are ideals in the group algebra of an abelian group. Bell Syst. Tech. J., vol. 49,pages 9871011, 1970.
3. B. Sundar Rajan and Moon Ho Lee. Quasi-cyclic dyadic codes in the Walsh-Hadamard transform domain. IEEE Transactions on Information Theory, 48(8):2406-2412, 2002.
4. Rudolf Lidl and Harald Niederreiter. Finite Fields / Rudolf Lidl, Harald Niederreiter ; foreword by P.M. Cohn. Cambridge University Press, Cambridge, New York, 2nd ed. edition, 1997.
5. Florence J. MacWilliams. Binary codes which are ideals in the group algebra of an abelian group. Bell Syst. Tech. J., vol. 49,pages 9871011, 1970.
6. Rafael Misoczki and Paulo S. L. M. Barreto. Compact McEliece Keys from Goppa Codes. In Selected Areas in Cryptography - SAC 2009, volume 5867 of Lecture Notes in Computer Science, pages 376-392. Springer, 2009.