VỀ MỘT PHƯƠNG PHÁP SINH S-HỘP HIỆU QUẢ CÓ TÍNH CHẤT MẬT MÃ TỐT

Trần Hồng Thái*

Tóm tắt: *Trong bài báo này, chúng tôi làm rõ hơn cơ sở lý thuyết của phương pháp xây dựng S-hộp của Menyachikhin [2]. Đóng góp của chúng tôi là chứng minh rằng, nếu ta chuyển vị hai vị trí có tính chất đặc biệt của một S-hộp thì ta sẽ thu được S-hộp mới có xác suất vi sai cực đại (hoặc độ tuyến tính cực đại) tốt hơn.*

Từ khóa: S-hộp; Mã khối; Tầng phi tuyến.

1. GIỚI THIỆU

Mọi mã khối và mã dòng hiện đại đều có một hoặc nhiều thành phần phi tuyến. S-hộp là một trong các thành phần phi tuyến được dùng nhiều nhất trong các mã pháp hiện đại. Bài toán thiết kế các S-hộp có tính chất mạnh đã được xem xét trong nhiều bài báo. Các tính chất mật mã đối phó với việc ứng dụng các tấn công lên mã pháp. Các tính chất mật mã cơ bản là: khả năng kháng lại tấn công vi sai và tấn công tuyến tính, bậc phi tuyến, bậc tối thiểu của các quan hệ đa thức giữa các thành phần của các vec-tơ đầu vào và đầu ra.

Trong [2], A. Menyachikhin đã đề xuất hai thuật toán (thuật toán 9 và thuật toán 11) để sinh các S-hộp có tính chất mật mã tốt từ một S-hộp giả ngẫu nhiên cho trước. Theo đó, ý tưởng chính của 2 thuật toán này là sửa đổi S-hộp đã cho bằng cách đổi chỗ 2 vị trí của hộp thế cho nhau và kiểm tra các tính chất mật mã của chúng. Các tính chất được kiểm tra gồm xác suất vi sai cực đại và độ tuyến tính cực đại của S-hộp. Phương pháp này sau đó được đăng ký bảo vệ bản quyền của Liên bang Nga (RU Patent №2633132). Tuy nhiên, Menyachikhin không đưa ra cơ sở đảm bảo rằng các S-hộp mới sẽ có tính chất mật mã tốt hơn. Chính vì vậy, trong bài báo này chúng tôi mong muốn làm rõ cơ sở lý thuyết của phương pháp do nhóm tác giả này công bố trong [2].

Bố cục của bài báo được trình bày như sau: mục 1 giới thiệu sơ lược về mục tiêu của bài báo; mục 2 nêu các định nghĩa và khái niệm có liên quan; mục 3 trình bày một số kết quả đạt được của chúng tôi và cuối cùng là kết luận.

2. CÁC ĐỊNH NGHĨA VÀ KÝ HIỆU

Cho n là một số nguyên dương, ký hiệu V_n là không gian vec-tơ n-chiều trên trường GF(2) và $V_n^{\times} = V_n \backslash \{0\}$ với 0 là vec-tơ không trong V_n.

Cho X là một tập hợp hữu hạn các phần tử, ký hiệu #X là số phần tử của tập X.

Một ánh xạ từ V_n sang V_m được gọi là một S-hộp $n \times m$ chiều, đặc biệt nếu $m = 1$ thì được gọi là một hàm Bool n-chiều.

Một S-hộp $n \times n$ song ánh được gọi là một hộp thế n chiều.

Định nghĩa 1 ([2]): *Cho g là một S-hộp n chiều, khi đó với mọi $\alpha \in V_n$ và $\beta \in V_n$ ký hiệu:*

$$X_{\alpha,\beta}^{g} = \{x \in V_n |\ g(x) \oplus g(x \oplus \alpha) = \beta\}$$

và gọi là tập vi sai của g tại (α, β),

$$p_{\alpha,\beta}^{g} = \frac{\#X_{\alpha,\beta}^{g}}{2^n}$$

gọi là xác suất vi sai của g tại (α, β). Giá trị

$$p_g = \max_{\alpha,\beta \in V_n^{\times}} p_{\alpha,\beta}^{g}$$

được gọi là xác suất vi sai cực đại của g.

Ý nghĩa của tham số p_g là giá trị càng nhỏ thì khả năng kháng lại các thám mã vi sai càng tốt.

Bảng phân bố vi sai (DDT) của S-hộp g là một ma trận có kích cỡ $2^n \times 2^n$ mà mỗi phần tử được tính như sau:

$$T_1^g[\alpha,\beta] = \#\{x \in V_n \mid g(x) \oplus g(x \oplus \alpha) = \beta\}$$

Bảng phân bố xấp xỉ tuyến tính (LAT) của S-hộp g là một ma trận $T_2^g[\alpha,\beta]$ có kích cỡ $2^n \times 2^n$ mà mỗi phần tử được tính:

$$T_2^g[\alpha,\beta] = \#\{x \in V_n \mid \alpha \circ x = \beta \circ g(x)\} - 2^{n-1}$$

Bậc phi tuyến (nonlinear order) của f, ký hiệu là deg(f), là bậc cực đại của các số hạng xuất hiện ở dạng chuẩn tắc đại số của nó. Một hàm Bool tuyến tính là một hàm Bool có bậc phi tuyến là 1. Cho trước $a \in V_n$, ta ký hiệu l_a: $V_n \to V_1$ là hàm Bool tuyến tính gồm tổng của các bit đối số được chọn bởi các bit của a:

$$l_a(x) = \oplus_{i=0\ldots n-1} a_i x_i$$

Tương quan c(f_1, f_2) giữa hai hàm Bool f_1 và f_2 được định nghĩa là:

$$c(f_1, f_2) = 2^{1-n} \cdot \#\{x | f_1(x) = f_2(x)\} - 1$$

Định nghĩa 2 ([2])**:** *Ký hiệu $\delta_{\alpha,\beta}^g$ là giá trị tuyệt đối của giá trị tương quan giữa hàm tuyến tính đầu vào l_α và hàm tuyến tính đầu ra l_β của S-hộp g.*

$$\delta_{\alpha,\beta}^g = \left|c(l_\alpha, l_\beta \circ g)\right|$$

Ta định nghĩa độ tuyến tính cực đại của S-hộp g là:

$$\delta_g = \max_{\alpha,\beta \in V_n^\times} \delta_{\alpha,\beta}^g$$

Tham số này sẽ có ý nghĩa là giá trị này càng nhỏ thì khả năng kháng lại tấn công tuyến tính càng tốt.

Chú ý rằng, từ định nghĩa 1 về xác suất vi sai của S-hộp, ta thấy rằng nếu $x \in X_{\alpha,\beta}^g$ thì $x \oplus \alpha \in X_{\alpha,\beta}^g$. Do đó: $p_{\alpha,\beta}^g = (2i)/2^n = i/2^n$ với $i = 0, 1, ..., 2^{n-1}$. Ký hiệu P_{n-1} là tập các giá trị xác suất vi sai có thể:

$$p \in P_{n-1} = \left\{\frac{i}{2^{n-1}} | i = 0,1,..,2^{n-1}\right\},\ \#P_{n-1} = 2^{n-1} + 1$$

Ta định nghĩa tập:

$$D(g,p) = \left\{(\alpha,\beta) \in V_n^\times \times V_n | p_{\alpha,\beta}^g = p\right\}$$

Định nghĩa 3 ([2])**:** *Phổ vi sai của một S-hộp g được định nghĩa là:*

$$D(g) = \left\{\left(p, \#D(g,p)\right) \mid p \in P_{n-1}\right\},\ \#D(g) = 2^{n-1} + 1$$

Định nghĩa 4: *Cho g là một hộp thế n chiều và $x_1 \neq x_2 \in V_n$. Khi đó hộp thế g′ được xác định như sau:*

$$g'(x) = g(x),\ \forall x \neq x_1 \text{ và } x \neq x_2$$

$$g'(x_1) = g(x_2)$$

$$g'(x_2) = g(x_1)$$

được gọi là chuyển vị (x_1, x_2) của g.

3. MỘT VÀI KẾT QUẢ CỦA CHÚNG TÔI

Mệnh đề 1: *Giả sử g(x) là một hộp thế song ánh và* $\alpha_0, \beta_0 \in V_n^{\times}$. *Khi đó, với mọi* $x_1 \neq x_2$ *và đều thuộc* $X^g_{\alpha_0,\beta_0}$ *thì hộp thế g′(x) là chuyển vị* (x_1, x_2) *của g có tính chất sau:*

a) $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} + \varepsilon$, với $\varepsilon \in \{0, -4\}$ và $\#X^{g'}_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} = \#X^g_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} + \tau$, với $\tau \in \{0, +4\}$;

b) Với $(\alpha, \beta) \neq (\alpha_0, \beta_0)$ và $(\alpha, \beta) \neq (\alpha_0, \beta_0 \oplus g(x_1) \oplus g(x_2))$ *thì* $\#X^{g'}_{\alpha,\beta} = \#X^g_{\alpha,\beta} + \iota$, với $\iota \in \{0, \pm 2, \pm 4\}$.

Chứng minh:

a) Ta có nhận xét sau:

(1) $\forall x \in X^g_{\alpha_0,\beta_0} \setminus \{x_1, x_2, x_1 \oplus \alpha_0, x_2 \oplus \alpha_0\}$, ta có:

$$g'(x) \oplus g'(x \oplus \alpha_0) = g(x) \oplus g(x \oplus \alpha_0) = \beta_0 \Rightarrow x \in X^{g'}_{\alpha_0,\beta_0}$$

(2) $\forall x \in V_n \setminus X^g_{\alpha_0,\beta_0}$, ta có:

$$g'(x) \oplus g'(x \oplus \alpha_0) = g(x) \oplus g(x \oplus \alpha_0) \neq \beta_0 \Rightarrow x \notin X^{g'}_{\alpha_0,\beta_0}$$

(3) $\forall x \in \{x_1, x_2, x_1 \oplus \alpha_0, x_2 \oplus \alpha_0\}$:

Từ định nghĩa về xác suất vi sai của S-hộp ta có nếu x_1 và $x_2 \in X^g_{\alpha_0,\beta_0} \Rightarrow x_1 \oplus \alpha_0$ và $x_2 \oplus \alpha_0$ thuộc $X^g_{\alpha_0,\beta_0}$. Hơn nữa, tập $\{x_1, x_2, x_1 \oplus \alpha_0, x_2 \oplus \alpha_0\}$ là 4 điểm phân biệt nếu $x_1 \oplus x_2 \neq \alpha_0$ và là 2 điểm phân biệt nếu $x_1 \oplus x_2 = \alpha_0$.

Xét 2 trường hợp sau:

- Với x_1 và $x_2 \in X^g_{\alpha_0,\beta_0}$ và $x_2 \oplus x_1 = \alpha_0$ (nghĩa là đổi chỗ x_1 và $x_1 \oplus \alpha_0$):

  Ta có:

$$g'(x_1) \oplus g'(x_1 \oplus \alpha_0) = g(x_1) \oplus g(x_1 \oplus \alpha_0) = \beta_0 \Rightarrow x_1 \text{ và } x_2 \in X^{g'}_{\alpha_0,\beta_0}$$

$$\Rightarrow \#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} \text{ và } \#X^{g'}_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} = \#X^g_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}}$$

- Với x_1 và $x_2 \in X^g_{\alpha_0,\beta_0}$ và $x_2 \oplus x_1 \neq \alpha_0$:

  Ta có:

$g'(x_1) \oplus g'(x_1 \oplus \alpha_0) = g(x_2) \oplus g(x_1 \oplus \alpha_0) = g(x_2) \oplus g(x_1) \oplus \beta_0 \neq \beta_0$ (vì $g(x_2) \oplus g(x_1) \neq 0$)

$g'(x_2) \oplus g'(x_2 \oplus \alpha_0) = g(x_1) \oplus g(x_2 \oplus \alpha_0) = g(x_1) \oplus g(x_2) \oplus \beta_0 \neq \beta_0$

$\Rightarrow X^{g'}_{\alpha_0,\beta_0} = X^g_{\alpha_0,\beta_0} \setminus \{x_1, x_1 \oplus \alpha_0, x_2, x_2 \oplus \alpha_0\}$, nghĩa là $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} - 4$

Từ định nghĩa ta có: nếu $x \in X^g_{\alpha_0,\beta_0}$ thì $x \notin X^g_{\alpha_0,\beta}$ với $\forall\ \beta \neq \beta_0$. Do đó, 4 giá trị $\{x_1, x_1 \oplus \alpha_0, x_2, x_2 \oplus \alpha_0\} \notin X^g_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} \Rightarrow \#X^{g'}_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} = \#X^g_{\alpha_0,\beta_{0\oplus g(x_1)\oplus g(x_2)}} + 4$

Từ (1), (2) và (3), suy ra khẳng định a)

b) Lúc này, ta cần xét xem các giá trị của tập $\{x_1, x_2, x_1 \oplus \alpha, x_2 \oplus \alpha\}$ có thuộc vào tập $X^g_{\alpha,\beta}$ hay không. Ta xét các khả năng sau:

- $x_1 \in X^g_{\alpha,\beta}$ và $x_2 \in X^g_{\alpha,\beta}$ (tất nhiên $x_1 \oplus \alpha \in X^g_{\alpha,\beta}$ và $x_2 \oplus \alpha \in X^g_{\alpha,\beta}$): trường hợp này lập luận hoàn toàn tương tự mục a). Nghĩa là:

+ nếu $x_2 = x_1 \oplus \alpha$ thì $\#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta}$ và $\#X^{g'}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} = \#X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)}$

+ nếu $x_2 \neq x_1 \oplus \alpha$ thì $\#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta} - 4$ và $\#X^{g'}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} = \#X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} + 4$.

- $x_1 \in X^{g}_{\alpha,\beta}$ và $x_2 \notin X^{g}_{\alpha,\beta}$ (tất nhiên $x_1 \oplus \alpha \in X^{g}_{\alpha,\beta}$ và $x_2 \oplus \alpha \notin X^{g}_{\alpha,\beta}$):

Khi đó: $g'(x_1) \oplus g'(x_1 \oplus \alpha) = g(x_2) \oplus g(x_1) \oplus \beta \neq \beta$ và $g'(x_2) \oplus g'(x_2 \oplus \alpha) = g(x_1) \oplus g(x_2 \oplus \alpha) = g(x_1 \oplus \alpha) \oplus \beta \oplus g(x_2 \oplus \alpha) \neq \beta$ (vì $g(x_1 \oplus \alpha) \oplus g(x_2 \oplus \alpha) \neq 0, \forall x_1 \neq x_2$) $\Rightarrow x_1 \in X^{g'}_{\alpha,\beta}$ và $x_2 \notin X^{g'}_{\alpha,\beta} \Rightarrow \#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta} - 2$ và $\#X^{g'}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} = \#X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} + 2$.

- $x_2 \in X^{g}_{\alpha,\beta}$ và $x_1 \notin X^{g}_{\alpha,\beta}$ (tất nhiên $x_1 \oplus \alpha \notin X^{g}_{\alpha,\beta}$ và $x_2 \oplus \alpha \in X^{g}_{\alpha,\beta}$): tương tự trường hợp $x_1 \in X^{g}_{\alpha,\beta}$ và $x_2 \notin X^{g}_{\alpha,\beta}$. Nghĩa là $X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta} - 2$ và $\#X^{g'}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} = \#X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} + 2$.

- $x_1 \notin X^{g}_{\alpha,\beta}$ và $x_2 \notin X^{g}_{\alpha,\beta}$ (tất nhiên $x_1 \oplus \alpha \notin X^{g}_{\alpha,\beta}$ và $x_2 \oplus \alpha \notin X^{g}_{\alpha,\beta}$):

+ Với $\forall x \in X^{g}_{\alpha,\beta}$ có $g'(x) \oplus g'(x \oplus \alpha) = g(x) \oplus g(x \oplus \alpha) = \beta \Rightarrow x \in X^{g'}_{\alpha,\beta}$.

+ Với $\forall x \in V_n \setminus \{X^{g}_{\alpha,\beta} \cup \{x_1, x_2, x_1 \oplus \alpha, x_2 \oplus \alpha\}\}$ ta có $g'(x) \oplus g'(x \oplus \alpha) = g(x) \oplus g(x \oplus \alpha) \neq \beta \Rightarrow x \notin X^{g'}_{\alpha,\beta}$.

+ Với $x \in \{x_1, x_2, x_1 \oplus \alpha, x_2 \oplus \alpha\}$:

- Nếu $x_2 \oplus x_1 = \alpha \Rightarrow g(x_1) \oplus g(x_1 \oplus \alpha) \neq \beta \Rightarrow \#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta}$;
- Nếu $x_2 \neq x_1 \oplus \alpha$, không mất tính tổng quát, giả sử:

$g(x_1) \oplus g(x_1 \oplus \alpha) = \beta \oplus \Delta$, với $\Delta \neq 0$ (nghĩa là $x_1 \in X^{g}_{\alpha,\beta\oplus\Delta}$)

$g(x_2) \oplus g(x_2 \oplus \alpha) = \beta \oplus \Delta'$, với $\Delta' \neq 0$ (nghĩa là $x_2 \in X^{g}_{\alpha,\beta\oplus\Delta'}$)

Khi đó,

$g'(x_1) \oplus g'(x_1 \oplus \alpha) = g(x_2) \oplus g(x_1 \oplus \alpha) = g(x_2) \oplus g(x_1) \oplus \beta \oplus \Delta \neq \beta \oplus \Delta$

$g'(x_2) \oplus g'(x_2 \oplus \alpha) = g(x_1) \oplus g(x_2 \oplus \alpha) = g(x_1) \oplus g(x_2) \oplus \beta \oplus \Delta' \neq \beta \oplus \Delta'$

Từ biểu diễn trên ta thấy, tập $\{x_1, x_1 \oplus \alpha, x_2, x_2 \oplus \alpha\} \in X^{g'}_{\alpha,\beta}$

$\Leftrightarrow \Delta \oplus g(x_1) \oplus g(x_2) = \Delta' \oplus g(x_1) \oplus g(x_2) = 0$

$\Leftrightarrow \Delta = \Delta' = g(x_1) \oplus g(x_2)$

$\Leftrightarrow x_1, x_2 \in X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)}$

Nếu $x_1, x_2 \in X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} \Rightarrow \#X^{g'}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} = \#X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} - 4$ và $\#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta} + 4$; nếu $x_1, x_2 \notin X^{g}_{\alpha,\beta\oplus g(x_1)\oplus g(x_2)} \Rightarrow \#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta}$.

Tổng hợp lại, ta suy ra với $(\alpha, \beta) \neq (\alpha_0, \beta_0)$ và $(\alpha, \beta) \neq (\alpha_0, \beta_0 \oplus g(x_1) \oplus g(x_2))$ thì $\#X^{g'}_{\alpha,\beta} = \#X^{g}_{\alpha,\beta} + \iota$, với $\iota \in \{0, \pm 2, \pm 4\}$. □

Từ mệnh đề trên, ta thấy rằng, nếu chọn các điểm x_1, x_2 từ tập $X^{g}_{\alpha_0,\beta_0}$ với $(\alpha_0, \beta_0) \in D(g, p_g)$ thì $\#X^{g'}_{\alpha_0,\beta_0}$ có thể giảm xuống, $\#X^{g'}_{\alpha,\beta}$ có xu hướng giảm xuống, tức là đại lượng p_g sẽ giảm đi và cho S-hộp tốt hơn (an toàn hơn).

Ở đây, để thuận tiện cho trình bày, ta bổ sung ký hiệu sau: C_{max} là lực lượng của các tập $\#X^{g}_{\alpha,\beta}$ với $(\alpha, \beta) \in D(g, p_g)$.

Định lý 2: *Cho g(x) là một hộp thế song ánh và* $(\alpha_0, \beta_0) \in D(g, p_g)$. *Khi đó với mọi* $x_1 \neq x_2$ *thuộc* $X^g_{\alpha_0,\beta_0}$ *thì hộp thế g′(x) là chuyển vị* (x_1, x_2) *của g có xác suất vi sai cực đại thay đổi một lượng hoặc là 0,* $\pm 2^{1-n}$ *hoặc* $\pm 2^{2-n}$ *so với xác suất vi sai cực đại của g(x).*

Chứng minh:

Từ mệnh đề 1, nếu chọn $(\alpha_0, \beta_0) \in D(g, p_g)$ và chuyển vị 2 giá trị $g(x_1)$ và $g(x_2)$ cho nhau thì có ít nhất 1 tập $X^{g'}_{\alpha_0,\beta_0}$ sẽ không tăng (bằng hoặc giảm 4 phần tử) so với tập đạt cực đại $X^g_{\alpha_0,\beta_0}$; với các cặp $(\alpha, \beta) \neq (\alpha_0, \beta_0)$ thì $\#X^{g'}_{\alpha,\beta}$ có thể thay đổi một lượng là $\{0, \pm 2, \pm 4\}$. Vì $\#X^g_{\alpha,\beta} \leq C_{max}$, $\forall (\alpha, \beta)$ nên ta xét các trường hợp sau:

- Nếu $\exists (\alpha, \beta) \neq (\alpha_0, \beta_0)$ sao cho $\#X^{g'}_{\alpha,\beta} = \#X^g_{\alpha,\beta} + 4$ mà $\#X^g_{\alpha,\beta} = C_{max}$
  $\Rightarrow p_{g'} = p_g + 2^{2-n}$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} + 2 \Rightarrow \max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} + 2 \Rightarrow p_{g'} = p_g + 2^{1-n}$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} \Rightarrow p_{g'} = p_g$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} - 2$ và $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} \Rightarrow p_{g'} = p_g$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} - 2$ và $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} - 4$
  $\Rightarrow p_{g'} = p_g - 2^{1-n}$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} - 4$ và $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} \Rightarrow p_{g'} = p_g$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} = C_{max} - 4$ và $\#X^{g'}_{\alpha_0,\beta_0} = \#X^g_{\alpha_0,\beta_0} - 4 \Rightarrow p_{g'} = p_g - 2^{2-n}$.
- Nếu $\forall (\alpha, \beta) \neq (\alpha_0, \beta_0)$ mà $\max\{\#X^{g'}_{\alpha,\beta}\} \leq C_{max} - 6 \Rightarrow p_{g'} = p_g - 2^{2-n}$.

Từ đó, suy ra đ.p.c.m. □

Nhận xét: khi chuyển vị 2 giá trị $g(x_1)$ và $g(x_2)$, thì tập $X^{g'}_{\alpha,\beta}$ chỉ bị thay đổi tại các điểm $\{x_1, x_2, x_1 \oplus \alpha_0, x_2 \oplus \alpha_0\}$. Tập $\{x_1, x_2, x_1 \oplus \alpha_0, x_2 \oplus \alpha_0\}$ là 4 điểm phân biệt nếu $x_1 \oplus x_2 \neq \alpha_0$ và là 2 điểm phân biệt nếu $x_1 \oplus x_2 = \alpha_0$ sẽ được bổ sung hoặc loại bỏ khỏi tập $X^g_{\alpha,\beta}$ để tạo thành tập $X^{g'}_{\alpha,\beta}$. Do đó, nếu ta chọn x_1, x_2 từ tập $X^g_{\alpha_0,\beta_0}$ với $(\alpha_0, \beta_0) \in D(g, p_g)$, xu hướng tập $\{x_1, x_2, x_1 \oplus \alpha, x_2 \oplus \alpha\}$ được bổ sung vào các tập $X^g_{\alpha,\beta}$ với (α, β) thuộc các lớp $D_1(g, p_g)$, $D_2(g, p_g)$, $D_3(g, p_g)$, ... nhiều hơn, khi đó, ta có thể tìm được các S-hộp có tính chất tốt hơn. Ngược lại nếu ta chọn x_1, x_2 từ tập $X^g_{\alpha_0,\beta_0}$ với $(\alpha_0, \beta_0) \in D_3(g, p_g)$ hoặc $D_4(g, p_g)$ thì xu hướng tập $\{x_1, x_2, x_1 \oplus \alpha, x_2 \oplus \alpha\}$ được bổ sung vào các tập $X^g_{\alpha,\beta}$ với (α, β) thuộc các lớp $D_0(g, p_g)$, $D_1(g, p_g)$, $D_2(g, p_g)$ và khi đó ta khó tìm được các S-hộp có tính chất tốt hơn.

Kết quả trên có một số ý nghĩa: trước tiên, đây là cơ sở để xây dựng các S-hộp có tính chất mật mã tốt một cách hiệu quả mà nhóm tác giả Menyachikhin đưa ra; thứ hai nó cũng lý giải tại sao ta cần phải chọn vị trí thay đổi trong 1 trong các tập $X^g_{\alpha_0,\beta_0}$ tương ứng của cặp $(\alpha, \beta) \in D(g, p_g)$ mới có ý nghĩa (vì lúc đó, ta mới kiểm soát được giá trị p_g mà phụ thuộc trực tiếp vào $\#X^g_{\alpha_0,\beta_0}$).

Dựa trên kết quả của Fuller (trong [1]), chúng tôi thu được một kết quả nhỏ khác đối với đại lượng δ_g. Trước tiên, chúng tôi phát biểu lại định lý 3 như sau:

Định lý 3 (định lý 6.4.4 trong [1])**:** *Cho g(x) là một S-hộp song ánh. Khi đó, với mọi $x_1 \neq x_2$, g′(x) là chuyển vị (x_1, x_2) của g(x) có độ phi tuyến thay đổi hoặc là 0 hoặc ±2.*

Ta rút ra hệ quả sau:

Hệ quả 4: *Cho g(x) là một S-hộp song ánh. Khi đó, với mọi $x_1 \neq x_2$, g′(x) là chuyển vị (x_1, x_2) của g(x) có độ tuyến tính cực đại δ_g, thay đổi một lượng hoặc là 0 hoặc $\pm 2^{2-n}$ so với độ tuyến tính cực đại của S-hộp gốc δ_g.*

Chứng minh:

Từ định nghĩa ta có:

$$\delta_{\alpha,\beta}^{g} = \frac{|\#\{x|\alpha \circ x = \beta \circ g(x)\} - 2^{n-1}|}{2^{n-1}} = \frac{T_2[\alpha,\beta]}{2^{n-1}}$$

do đó

$$\delta_g = \max_{\alpha,\beta \in V_n^{\times}} \frac{T_2[\alpha,\beta]}{2^{n-1}}$$

Mặt khác, ta lại có [3]:

$$\begin{aligned} NL(g(x)) &= 2^{n-1} - \max_{\alpha,\beta \in V_n^{\times}} T_2[\alpha,\beta] \\ &= 2^{n-1} - 2^{n-1}.\delta_g \end{aligned}$$

Trong đó, NL(g(*x*)) là độ phi tuyến của S-hộp g(*x*).

$$\Rightarrow \delta_g = \frac{NL(g(x))}{2^{n-1}} - 1$$

$$\Rightarrow \delta_{g'} - \delta_g = \frac{NL\big(g'(x)\big) - NL(g(x))}{2^{n-1}}$$

Áp dụng định lý 3, khi độ phi tuyến của S-hộp mới g′(*x*) thay đổi là {0, ±2} thì đại lượng độ tuyến tính cực đại của S-hộp mới sẽ thay đổi tương ứng là $\{0, \pm 2^{2-n}\}$. □

4. KẾT LUẬN

Phương pháp sinh S-hộp mà Menyachikhin (trong [1]) là một trong những phương pháp heuristic rất hữu hiệu để xây dựng các S-hộp có tính chất mật mã mạnh. Ý nghĩa quan trọng của phương pháp là ta có thể xây dựng các S-hộp mạnh (có các tính chất mật mã tốt) mới mà không tương đương affine với các S-hộp đã cho với độ phức tạp tính toán chấp nhận được. Tuy nhiên, hạn chế của phương pháp là chưa xem xét sự thay đổi các tính chất mật mã khác của S-hộp mới.

Đóng góp trong bài báo này của chúng tôi là làm rõ cơ sở lý thuyết của phương pháp xây dựng S-hộp của Menyachikhin. Trước tiên, chúng tôi chứng minh rằng, nếu ta chuyển vị hai vị trí có tính chất đặc biệt của một S-hộp (trong tập X_{α_0,β_0}^{g} là tập các giá trị *x* thỏa mãn sai khác đầu vào α_0, sai khác đầu ra là β_0 và (α_0, β_0) là cặp sai khác cho ta giá trị vi sai cực đại), ta có thể thu được S-hộp mới có đại lượng xác suất vi sai cực đại tốt hơn. Tương tự, chúng tôi cũng thu được một kết quả tương tự với giá trị độ tuyến tính cực đại của S-hộp (khác biệt là việc chuyển vị hai vị trí bất kỳ).

TÀI LIỆU THAM KHẢO

[1]. Fuller, J.E., *"Analysis of affine equivalent Boolean functions for cryptography"*. 2003, Queensland University of Technology.

[2]. Menyachikhin, A., *"Spectral-linear and spectral-differential methods for generating S-boxes having almost optimal cryptographic parameters"*. Математические вопросы криптографии, 2017. **8**(2): p. 97-116.

[3]. Dunkelman, O. and S. Huang, *"Reconstructing an S-box from its Difference Distribution Table"*. https://eprint.iacr.org/, 2018.

ABSTRACT

TOWARD EFFICIENT METHOD FOR GENERATE S-BOX
WITH GOOD CRYPTOGRAPHIC PROPERTIES

In this paper, we further clarify the theoretical basis of the S-box construction method of Menyachikhin [2]. Our contribution is to prove that if we transpose two special locations in a given S-box, we will obtain a new S-box with a better maximum differential probability (the same with maximum linear deviation).

Keywords: S-box construction; Blockcipher; Maximum linear deviation.

Nhận bài ngày 31 tháng 3 năm 2020
Hoàn thiện ngày 19 tháng 6 năm 2020
Chấp nhận đăng ngày 03 tháng 8 năm 2020

Địa chỉ: Viện KH-CN Mật mã/ Ban Cơ yếu Chính phủ.
*Email: thai_tranhong@ymail.com.