# Một số kết quả về tính giả ngẫu nhiên và siêu giả ngẫu nhiên của cấu trúc Feistel

**Nguyễn Bùi Cương, Hoàng Đình Linh**

***Tóm tắt*— Cấu trúc mã khối đóng vai trò rất quan trọng trong việc thiết kế một thuật toán mã khối an toàn. Tính giả ngẫu nhiên và siêu giả ngẫu nhiên của một cấu trúc mã khối đã và đang thu hút sự quan tâm nghiên cứu trong cộng đồng mật mã. Trong bài báo này, chúng tôi trình bày một số kết quả lý thuyết liên quan tới việc đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên của cấu trúc Feistel (là một trong nhiều cấu trúc thường được sử dụng bên cạnh SPN, ARX…) bằng cách sử dụng kỹ thuật hệ số H do J. Patarin đề xuất.**

***Abstract*— Block cipher constructions play an important role in designing a secured block cipher algorithm. Pseudorandomness and super-pseudorandomness of a block cipher construction has been attracting universal interests of the cryptographic communication. In this paper, we present some theoretic results that related in evaluating the pseudorandomness and super-pseudorandomness of the Feistel structure (which is a frequent used structure beside SPN, ARX…) by using the H coefficient technique proposed by J. Patarin.**

***Từ khóa— mã khối; cấu trúc Feistel; giả ngẫu nhiên; siêu giả ngẫu nhiên.***

***Keywords— block cipher; Feistel structure; pseudorandomness; super-pseudorandomness.***

## I. GIỚI THIỆU

Một hàm mật mã có sử dụng khóa như một mã khối có thể được xem như một hàm ngẫu nhiên, hoặc một hoán vị ngẫu nhiên tương ứng với khóa được chọn ngẫu nhiên. Độ an toàn mạnh nhất mà ta có thể thiết lập cho một hàm ngẫu nhiên $f$ (hoặc một hoán vị ngẫu nhiên $c$) chính là: $f$ (hoặc $c$) chỉ có thể phân biệt được với một hàm được chọn ngẫu nhiên đều $f^*$ (hoặc hoán vị được chọn ngẫu nhiên đều $c^*$) với một xác suất thành công không đáng kể, kể cả khi sử dụng một thuật toán kiểm tra xác suất $\mathcal{A}$ có năng lực không bị hạn chế (thường được sử dụng để phân biệt với số lượng lớn các truy vấn thích nghi lên hàm $f$ (hoặc hoán vị $c$)).

Trước đây đã có những nghiên cứu liên quan đến vấn đề này. Trong đó, một trường hợp lý tưởng (có độ an toàn tuyệt đối) là khi một mã khối không thể phân biệt được với một hoán vị được chọn ngẫu nhiên đều. Tuy nhiên trong thực tế, ta rất khó chứng minh tính không thể phân biệt được của các hàm mật mã thực tế với hàm được chọn ngẫu nhiên đều, kể cả khi sử dụng số lượng truy vấn lớn. Năm 1988, Luby và Rackoff [1] đã đưa ra các định nghĩa chính thức về tính giả ngẫu nhiên và siêu giả ngẫu nhiên của mã khối. Đồng thời đã chứng minh rằng, cấu trúc Feistel 3-vòng là giả ngẫu nhiên và 4-vòng là siêu giả ngẫu nhiên. Sau đó, Patarin đã trình bày kỹ thuật hệ số H [2] và sử dụng để chứng minh lại 2 kết quả này. Các chứng minh của Patarin sử dụng cách tiếp cận ban đầu của kỹ thuật hệ số H, cũng như của Luby-Rackoff là khá dài và phức tạp. Sau đó, Gilbert và Minier [3] đã sử dụng một cách tiếp cận đơn giản hơn nhưng khá hiệu quả, dựa trên 2 định lý chính của Patarin để đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên cho lược đồ L và R.

Trong khuôn khổ của bài báo này, chúng tôi trình bày một cách chứng minh khác dựa trên hai định lý chính của Patarin về tính giả ngẫu nhiên và siêu giả ngẫu nhiên cho cấu trúc Feistel với số vòng tùy ý. Cách tiếp cận này cũng đã được Gilbert và Minier [3] sử dụng để đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên cho lược đồ L và R.

Bố cục của bài báo gồm 4 Mục. Sau Mục Giới thiệu, Mục II trình bày một số khái niệm, phương pháp sử dụng kỹ thuật hệ số H do Patarin đề xuất để đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên của một số cấu trúc mã khối theo mô hình Luby-Rackoff được trình bày. Trong Mục III, chúng tôi đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên của cấu trúc Feistel với số vòng tùy ý. Và cuối cùng là Mục kết luận.

## II. MỘT SỐ CƠ SỞ LÝ THUYẾT

### *A. Ký hiệu*

Trong bài báo này, chúng tôi sử dụng một số ký hiệu sau: $\mathbb{I}_n$ là ký hiệu tập $\mathbb{Z}_2^n$, $\mathbb{F}_{n,m}$ là tập tất cả các hàm từ $\mathbb{I}_n$ vào $\mathbb{I}_m$. $\mathbb{F}_n$ là tập tất cả các hàm từ $\mathbb{I}_n$ vào $\mathbb{I}_n$. $\mathbb{P}_n$ là tập tất cả các hoán vị trên $\mathbb{I}_n$. Khi đó, ta có:

$$\left|\mathbb{F}_{n,m}\right| = 2^{m.2^n}\ ;\ \left|\mathbb{P}_n\right| = \left(2^n\right)!\ .$$

*B. Một số khái niệm*

Trước tiên, chúng tôi giới thiệu định nghĩa một bộ phân biệt giả ngẫu nhiên:

**Định nghĩa 1 (Định nghĩa 6 [4]).** *Cho $n,m>1$. Một bộ phân biệt giả ngẫu nhiên là một thuật toán tất định $\mathcal{A}$ có khả năng tính toán không hạn chế (nhưng vẫn hữu hạn), thuật toán này có quyền truy vấn một hàm cho trước $F:\mathbb{I}_n \to \mathbb{I}_m$ bằng cách hỏi các giá trị $x \in \mathbb{I}_n$, để nhận được câu trả lời là $y = F(x)$ . Tùy theo các câu trả lời này, thuật toán $\mathcal{A}$ cho đầu ra 0 hoặc 1.*

Một hàm được chọn ngẫu nhiên của $\mathbb{F}_{n,m}$ được định nghĩa như một biến ngẫu nhiên $f$ của $\mathbb{F}_{n,m}$ , và có thể được xem như phân phối xác suất $\left(\mathcal{P}[f=\varphi]\right)_{\varphi\in\mathbb{F}_{n,m}}$ trên $\mathbb{F}_{n,m}$. Hàm được chọn ngẫu nhiên (tương ứng hoán vị được chọn ngẫu nhiên) ở đây được hiểu là hàm (tương ứng hoán vị) được rút ngẫu nhiên từ $\mathbb{F}_{n,m}$ (tương ứng $\mathbb{P}_n$) phù hợp với một phân phối xác suất cố định. Từ đó, ta có định nghĩa một hàm ngẫu nhiên hoàn thiện (perfect random function) (tương ứng hoán vị ngẫu nhiên hoàn thiện (perfect random permutation)) như sau:

**Định nghĩa 2. (Định nghĩa 1 [3]).** *Hàm ngẫu nhiên hoàn thiện $f^*$ của $\mathbb{F}_{n,m}$ là phần tử được rút đều từ $\mathbb{F}_{n,m}$. Nói cách khác, $f^*$ được gắn với phân phối xác suất đều trên $\mathbb{F}_{n,m}$. Ta định nghĩa hoán vị ngẫu nhiên hoàn thiện $c^*$ trên $\mathbb{I}_n$ là phần tử được rút đều từ $\mathbb{P}_n$. Nói cách khác, $c^*$ được gắn với phân phối xác suất đều trên $\mathbb{P}_n$.*

Tiếp theo, chúng ta định nghĩa lợi thế (advantage) một bộ phân biệt $\mathcal{A}$ trong việc phân biệt một hàm được chọn ngẫu nhiên $F$ với một hàm ngẫu nhiên hoàn thiện $F^*$:

**Định nghĩa 3. (Định nghĩa 7 [4]).** *Cho F là một hàm được chọn ngẫu nhiên và $F^*$ là một hàm ngẫu nhiên hoàn thiện. Lợi thế một bộ phân biệt giả ngẫu nhiên $\mathcal{A}$ cho việc phân biệt giữa F với $F^*$ là:*

$$\mathrm{Adv}_{\mathcal{A}}\left(F,F^*\right) := \left|\mathcal{P}\left[\mathcal{A}^F=1\right] - \mathcal{P}\left[\mathcal{A}^{F^*}=1\right]\right|.$$

Để đơn giản, chúng ta ký hiệu $p^* = \mathcal{P}\left[\mathcal{A}^{F^*}=1\right]$ và $p = \mathcal{P}\left[\mathcal{A}^{F}=1\right]$.

Bộ phân biệt giả ngẫu nhiên định nghĩa ở trên cho phép chỉ thực hiện truy vấn mã hóa. Bộ phân biệt siêu giả ngẫu nhiên là bộ phân biệt được cho phép thực hiện cả truy vấn giải mã.

**Định nghĩa 4 (Định nghĩa 8 [4]).** *Cho $N>1$. Một bộ phân biệt siêu giả ngẫu nhiên là một thuật toán tất định $\mathcal{A}$ với khả năng tính toán không hạn chế (nhưng vẫn hữu hạn), thuật toán này có quyền truy vấn một hoán vị cho trước $C \in \mathbb{P}_N$ bằng cách hỏi giá trị $x \in \mathbb{I}_N$ và lựa chọn hoặc là ảnh $y = C(x)$ hoặc là nghịch ảnh $y = C^{-1}(x)$. Tùy theo câu trả lời nhận được, thuật toán $\mathcal{A}$ đưa đầu ra 0 hoặc 1.*

Lợi thế của bộ phân biệt siêu giả ngẫu nhiên có trong việc phân biệt một hoán vị được chọn ngẫu nhiên $C$ và một hoán vị ngẫu nhiên hoàn thiện $C^*$ được định nghĩa tương tự như trường hợp bộ phân biệt giả ngẫu nhiên.

Các hàm ngẫu nhiên mà chúng ta muốn xem xét phân biệt với các hàm ngẫu nhiên hoàn thiện, thông thường được xây dựng bằng việc nhúng các hàm ngẫu nhiên hoàn thiện $f_1^*, f_2^*, ..., f_r^*$ vào một cấu trúc toàn thể $\Phi$. Miền xác định và miền giá trị của $f_1^*, f_2^*, ..., f_r^*$ có kích thước có thể thay đổi, nó thường nhỏ hơn kích thước miền xác định và miền giá trị của hàm $\Phi\left(f_1^*, f_2^*, ..., f_r^*\right)$. Một cấu trúc $\Phi$ như vậy đôi khi được gọi là bộ sinh hàm (hoặc bộ sinh hoán vị). Khi đó, ta có định nghĩa về tính giả ngẫu nhiên của một bộ sinh hàm (hoặc bộ sinh hoán vị) như sau:

**Định nghĩa 5 (Định nghĩa 9 [4]):** *Một bộ sinh hàm $\Phi$ được gọi giả ngẫu nhiên nếu với mọi đa thức P(N), Q(N), tồn tại số nguyên $N_0$ sao cho $\forall N \geq N_0$ và tất cả các bộ phân biệt giả ngẫu nhiên $\mathcal{A}$ được cho phép thực hiện $q \leq Q(N)$ truy vấn thì:*

$$\mathrm{Adv}_{\mathcal{A}}\left(\Phi\left(f_1^*,...,f_r^*\right), F^*\right) \leq \frac{1}{P(N)}$$

Các bộ tạo hoán vị siêu giả ngẫu nhiên cũng được định nghĩa tương tự như vậy với việc xem xét các bộ phân biệt siêu giả ngẫu nhiên.

*C. Kỹ thuật hệ số H*

Trong mục này chúng tôi trình bày hai định lý chính của Patarin được sử dụng để đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên của một số cấu trúc mã khối theo mô hình Luby-Rackoff. Đây là một công cụ rất hiệu quả để đánh giá cận của lợi thế phân biệt của một hàm (tương ứng hoán vị) ngẫu nhiên với một hàm (tương ứng hoán vị) được chọn ngẫu nhiên đều.

Ký hiệu $\mathcal{X}$ là tập $\mathbb{I}_n^q$ tất cả các bộ $q$ phần tử $X=\left(X_1,...,X_q\right), \forall i\neq j: X_i \neq X_j$. Đầu tiên, đối với bộ phân biệt giả ngẫu nhiên $\mathcal{A}$ chỉ có quyền thực hiện các truy vấn mã hóa, ta có:

**Định lý 1 (Định lý 1 [3]).** *Cho $f\in\mathbb{F}_{n,m}$ là một hàm được chọn ngẫu nhiên; $f^*\in\mathbb{F}_{n,m}$ là một hàm ngẫu nhiên hoàn thiện; q là một số nguyên dương. Nếu tồn tại tập $\mathcal{Y}\subset\mathbb{I}_m^q$ và 2 số dương $\varepsilon_1$ và $\varepsilon_2$ thỏa mãn:*

*i.* $|\mathcal{Y}|\geq(1-\varepsilon_1)|\mathbb{I}_m|^q$ ;

*ii.* $\forall X\in\mathcal{X}, \forall Y\in\mathcal{Y}, \mathcal{P}\left[X\xrightarrow{f}Y\right]\geq(1-\varepsilon_2)\frac{1}{|\mathbb{I}_m|^q}$.

*Thì với bộ phân biệt $\mathcal{A}$ bất kỳ sử dụng q truy vấn mã hóa, ta có:*

$$Adv_{\mathcal{A}}\left(f,f^*\right)\leq\varepsilon_1+\varepsilon_2.$$

Đối với các bộ phân biệt siêu giả ngẫu nhiên $\mathcal{A}$ có quyền thực hiện cả truy vấn mã hóa và giải mã, ta có kết quả sau:

**Định lý 2 (Định lý 4 [3]).** *Cho $c\in\mathbb{P}_n$ là một hoán vị ngẫu nhiên; $c^*\in\mathbb{P}_n$ là một hoán vị ngẫu nhiên hoàn thiện; q là một số nguyên dương, và $\varepsilon>0$. Nếu với mọi $X,Y\in\mathcal{X}$ mà:*

$$\mathcal{P}\left[X\xrightarrow{c}Y\right]\geq(1-\varepsilon)\frac{1}{|\mathbb{I}_n|^q}.$$

*thì với bất kỳ bộ phân biệt $\mathcal{A}$ được cho phép thực hiện q truy vấn mã hóa hoặc giải mã, ta có:*

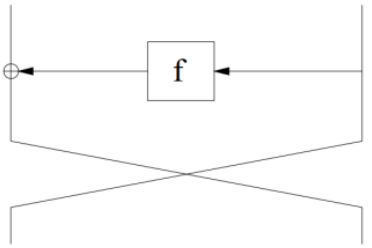
$$Adv_{\mathcal{A}}\left(c,c^*\right)\leq\varepsilon+\frac{q(q-1)}{2\times 2^n}.$$

## III. TÍNH GIẢ NGẪU NHIÊN VÀ SIÊU GIẢ NGẪU NHIÊN CỦA CẤU TRÚC FEISTEL

*A. Mô tả cấu trúc Feistel*

Cấu trúc Feistel 1-vòng (Hình 1) là một hoán vị $2n$-bit sử dụng một hàm vòng $n$-bit thỏa mãn:

$$\phi(f)(\langle L,R\rangle)=\langle R,L\oplus f(R)\rangle$$




Hình 1. Cấu trúc Feistel 1-vòng

Khi đó, cấu trúc Feistel $r$-vòng là hợp của $r$ hàm Feistel 1-vòng, biến đổi $r$ hàm $n$-bit $f_1,\cdots,f_r$ thành một hoán vị $2n$-bit:

$$\phi(f_1,f_2,...,f_r)=\phi(f_r)\circ...\circ\phi(f_1).$$

Trong các phần tiếp theo, chúng tôi xem xét đánh giá tính giả ngẫu nhiên và siêu giả ngẫu nhiên của cấu trúc Feistel khi thay thế các hàm vòng bởi các hàm được chọn ngẫu nhiên đều từ không gian các hàm $n$-bit ánh xạ sang $n$-bit.

*B. Tính giả ngẫu nhiên của cấu trúc Feistel*

Ta có khẳng định sau:

**Khẳng định 1.** *Cấu trúc Feistel 1-vòng và 2-vòng đều không là giả ngẫu nhiên.*

*Chứng minh.* Chúng ta chỉ ra rằng chỉ với lần lượt 1 hoặc 2 truy vấn lựa chọn là đủ để phân biệt $f=\phi\left(f_1^*\right)$ và $f=\phi\left(f_1^*,f_2^*\right)$ ($f_1^*,f_2^*\in\mathbb{F}_n$ là các hàm ngẫu nhiên hoàn thiện độc lập) với $F^*\in\mathbb{F}_{2n}$ ngẫu nhiên hoàn thiện với xác suất lớn.

*Đối với cấu trúc Feistel 1-vòng.*

Gọi $\mathcal{A}_1$ là thuật toán phân biệt, được hoạt động như sau:

1. $\mathcal{A}_1$ chọn 1 giá trị $X_1=(L,R)\in\mathbb{I}_{2n}$.
2. $\mathcal{A}_1$ truy vấn lên hàm $f$ bất kỳ trên không gian hàm $\mathbb{F}_{2n}$ để thu được giá trị $Y_1=f(X_1)=(S,T)$.
3. $\mathcal{A}_1$ kiểm tra giá trị $S$ bên trái của $Y_1$ có bằng $R$ hay không.
4. Nếu bằng $R$ thì $\mathcal{A}_1$ trả ra giá trị 1, nếu không thì $\mathcal{A}_1$ trả ra giá trị 0.

Với $p_1^*$ là xác suất $\mathcal{A}_1$ trả ra giá trị 1 khi $f$ được chọn ngẫu nhiên đều từ $\mathbb{F}_{2n}$. Khi đó,

$p_1^* = 2^{-n}$ vì tất cả các giá trị của S có cùng xác suất xuất hiện là $2^{-n}$.

Với $p_1$ là xác suất $\mathcal{A}_1$ trả ra giá trị 1 khi $f = \phi\left(f_1^*\right)$(cấu trúc Feistel 1-vòng). Khi đó, $p_1 = 1$, vì

$$\phi\left(f_1^*\right)(L,R) = \left(R, L \oplus f_1^*(R)\right), \forall L,R \in \mathbb{I}_n.$$

Từ đó, ta có lợi thế phân biệt của $\mathcal{A}_1$ là:

$$Adv_{\mathcal{A}_1}\left(\phi\left(f_1^*\right), F^*\right) = \left|p_1 - p_1^*\right| = 1 - 2^{-n} > \frac{1}{3n}, \quad \forall n \geq 1.$$

Do đó, cấu trúc Feistel 1-vòng không là giả ngẫu nhiên.

*Đối với cấu trúc Feistel 2-vòng.*

Gọi $\mathcal{A}2$ là thuật toán phân biệt, được hoạt động như sau:

1. $\mathcal{A}_2$ chọn 1 giá trị $X_1 = (L,R) \in \mathbb{I}_{2n}$.
2. $\mathcal{A}_2$ truy vấn lên hàm *f* bất kỳ trên không gian hàm $\mathbb{F}_{2n}$ để thu được giá trị của $Y_1 = f(X_1) = (S,T) \in \mathbb{I}_{2n}$.
3. $\mathcal{A}_2$ chọn 1 giá trị $X_2 = (L',R) \in \mathbb{I}_{2n}$ với $L' \neq L$.
4. $\mathcal{A}_2$ truy vấn lên hàm *f* để thu được giá trị của $Y_2 = f(X_2) = (S',T')$.
5. $\mathcal{A}_2$ kiểm tra điều kiện $S \oplus L = S' \oplus L'$.
6. Nếu thỏa mãn thì $\mathcal{A}_2$ trả ra giá trị 1, nếu không thì $\mathcal{A}_2$ trả ra giá trị 0.

Với $p_2^*$ là xác suất $\mathcal{A}_1$ trả ra giá trị 1 khi $f$ được chọn ngẫu nhiên đều từ $\mathbb{F}_{2n}$ thì $p_2^* = 2^{-n}$.

Với $p_2$ là xác suất $\mathcal{A}_1$ trả ra giá trị 1 khi $f = \phi\left(f_1^*, f_2^*\right)$(cấu trúc Feistel 2-vòng) thì $p_2 = 1$ (vì $S = L \oplus f_1(R), S' = L' \oplus f_1(R)$).

Do đó, lợi thế phân biệt của $\mathcal{A}_2$ là:

$$Adv_{\mathcal{A}_2}\left(\phi\left(f_1^*, f_2^*\right), F^*\right) = \left|p_2 - p_2^*\right| = 1 - 2^{-n} > \frac{1}{3n}, \forall n \geq 1.$$

Vậy cấu trúc Feistel 2-vòng không phải là giả ngẫu nhiên□

*Đối với cấu trúc Feistel r-vòng* ($r \geq 3$).

Cấu trúc Feistel 3-vòng là giả ngẫu nhiên đã được đưa ra đầu tiên bởi Luby và Rackoff, kết quả này đã được trình bày trong nhiều tài liệu [1, 4, 5]. Sau đây là phát biểu của định lý:

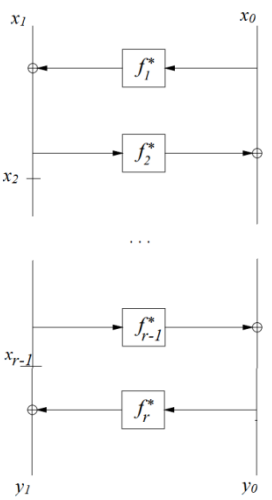
**Định lý 3 (Định lý 10 [4]).** *Cho $f_1^*, f_2^*, f_3^* \in \mathbb{F}_n$ là các hàm ngẫu nhiên hoàn thiện độc lập. Gọi $F^* \in \mathbb{F}_{2n}$ là một hàm ngẫu nhiên hoàn thiện. Đối với một bộ phân biệt giả ngẫu nhiên bất kỳ $\mathcal{A}$ được cho phép thực hiện q truy vấn mã hóa thích nghi, chúng ta có:*

$$Adv_{\mathcal{A}}\left(\phi\left(f_1^*, f_2^*, f_3^*\right), F^*\right) \leq \frac{q(q-1)}{2^n}.$$

Một cách trực giác, chúng ta sẽ suy luận rằng khi số vòng càng tăng thì càng khó phân biệt với một hàm được chọn ngẫu nhiên đều hơn. Hay nói cách khác, cấu trúc Feistel 3-vòng là giả ngẫu nhiên thì các cấu trúc Feistel với số vòng lớn hơn 3 cũng là giả ngẫu nhiên. Tuy nhiên, để chứng tỏ điều này cũng cần những lập luận có căn cứ khoa học. Sau đây, chúng tôi chứng minh cho trường hợp tổng quát, với $r \geq 3$thì cấu trúc Feistel *r*-vòng là giả ngẫu nhiên.

**Mệnh đề 1.** *Cho $f_1^*, f_2^*, ..., f_{r-1}^*, f_r^* \in \mathbb{F}_n; r \geq 3$ là các hàm ngẫu nhiên hoàn thiện độc lập. Gọi $F^* \in \mathbb{F}_{2n}$ là một hàm ngẫu nhiên hoàn thiện. Đối với một bộ phân biệt giả ngẫu nhiên bất kỳ $\mathcal{A}$ được cho phép thực hiện q truy vấn mã hóa thích nghi, chúng ta có:*

$$Adv_{\mathcal{A}}\left(\phi\left(f_1^*, f_2^*, ..., f_{r-1}^*, f_r^*\right), F^*\right) \leq \frac{(r-1)q(q-1)}{2 \times 2^n}.$$




Hình 2. Cấu trúc Feistel *r*-vòng

*Chứng minh.* Chúng ta sẽ so sánh hàm $\phi\left(f_1^*, f_2^*,..., f_{r-1}^*, f_r^*\right)$ với hàm ngẫu nhiên hoàn thiện $F^* \in \mathbb{F}_{2n}$.

Ký hiệu $X = (X_i)_{i\in[1..q]} = \left(x_i^1, x_i^0\right) \in \mathbb{I}_{2n}$ là các đầu vào của $\phi\left(f_1^*, f_2^*,..., f_{r-1}^*, f_r^*\right)$ và các đầu ra tương ứng là $Y = (Y_i)_{i\in[1..q]} = \left(y_i^1, y_i^0\right) \in \mathbb{I}_{2n}$.

Đối với mỗi

$$\left(y_i^1, y_i^0\right) = \phi\left(f_1^*, f_2^*,..., f_{r-1}^*, f_r^*\right)\left(x_i^1, x_i^0\right)$$

ta ký hiệu $x_i^2, x_i^3,..., x_i^{r-1}$ là các giá trị trung gian (Hình 2). Cụ thể:

$$\begin{aligned} &x_i^2 = x_i^1 \oplus f_1^*\left(x_i^0\right),\\ &x_i^0 \oplus f_2^*\left(x_i^2\right) = x_i^3,\\ &\cdots\\ &f_{r-1}^*\left(x_i^{r-1}\right) \oplus x_i^{r-2} = y_i^0,\\ &f_r^*\left(y_i^0\right) = x_i^{r-1} \oplus y_i^1. \end{aligned}$$

Ta ký hiệu $x^0, x^1, x^2, x^3,..., x^{r-1}, y^0, y^1$ tương ứng lần lượt là các bộ $q$ phần tử các từ $n$-bit

$$\left(x_i^0\right)_{i\in[1..q]}, \left(x_i^1\right)_{i\in[1..q]}, \left(x_i^2\right)_{i\in[1..q]}, \left(x_i^3\right)_{i\in[1..q]},$$
$$..., \left(x_i^{r-1}\right)_{i\in[1..q]}, \left(y_i^0\right)_{i\in[1..q]}, \left(y_i^1\right)_{i\in[1..q]}.$$

Ta định nghĩa $\mathcal{X}$ là tập tất cả các bộ $q$ phần tử $X$ của các từ khác nhau đôi một của $\mathbb{I}_{2n}$ (tức là sao cho với $i, j$ phân biệt bất kỳ thuộc $[1..q]$ thì $x_i^0 \neq x_j^0$ hoặc $x_i^1 \neq x_j^1$); và định nghĩa $\mathcal{Y}$ là tập các bộ $q$ phần tử $Y$ của các từ $\mathbb{I}_{2n}$ sao cho các bộ $q$ phần tử $y_0$ tương ứng đều chứa các từ $\mathbb{I}_n$ khác nhau đôi một:

$$\mathcal{Y} = \left\{\left(Y_1,...,Y_q\right) \in \left(\mathbb{I}_{2n}\right)^q \mid y^0 \in \mathbb{I}_n^{\neq}\right\}.$$

Để thiết lập cận dưới của kích thước tập $\mathcal{Y}$, ta có:

$$\begin{aligned} |\mathcal{Y}| &= |\mathbb{I}_{2n}|^q \left(1 - \mathcal{P}\left[y^0 \notin \mathbb{I}_n^{\neq}\right]\right)\\ &\geq |\mathbb{I}_{2n}|^q \left(1 - \sum_{i,j\in[1..q], i\neq j} P\left[y_i^0 = y_j^0\right]\right)\\ &\geq |\mathbb{I}_{2n}|^q \left(1 - \frac{q(q-1)}{2} \times 2^{-n}\right)\\ &\geq |\mathbb{I}_{2n}|^q \left(1 - \frac{q(q-1)}{2\times 2^n}\right). \end{aligned}$$

Với bộ $q$ phần tử $X$ bất kỳ của $\mathcal{X}$ và bộ $q$ phần tử $Y$ bất kỳ của $\mathcal{Y}$, ta có:

$$\mathcal{P}\left[X \xrightarrow{\phi\left(f_1^*, f_2^*,..., f_{r-1}^*, f_r^*\right)} Y\right]$$

$$= \sum_{x^2, x^3,..., x^{r-1}\in\mathbb{I}_n} \mathcal{P}\left[\begin{array}{l} \left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right)\\ \wedge\left(x^0 \oplus f_2^*\left(x^2\right) = x^3\right)\\ \wedge\cdots\\ \wedge\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right)\\ \wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right) \end{array}\right]$$

$$\geq \sum_{x^2, x^3,..., x^{r-1}\in\mathbb{I}_n^{\neq}} \mathcal{P}\left[\begin{array}{l} \left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right)\wedge\\ \cdots\wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right) \end{array}\right]$$
$$\times\mathcal{P}\left[\begin{array}{l} \left(f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right)\\ \wedge\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right) \end{array}\right].$$

Vì $x^{r-2} \in \mathbb{I}_n^{\neq}$, nên theo tính chất của một hàm ngẫu nhiên hoàn thiện được trong [6] suy ra:

$$\mathcal{P}\left[f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right] = \frac{1}{2^{nq}}.$$

Tương tự, vì $x^{r-1} \in \mathbb{I}_n^{\neq}$, suy ra:

$$\mathcal{P}\left[f_{r-1}^*\left(x^{r-1}\right) = x^{r-2} \oplus y^0\right] = \frac{1}{2^{nq}}.$$

Do đó,

$$\mathcal{P}\left[\begin{array}{l}\left(f_{r-2}^{*}\left(x^{r-2}\right)=x^{r-1}\oplus x^{r-3}\right)\\ \wedge\left(f_{r-1}^{*}\left(x^{r-1}\right)\oplus x^{r-2}=y^{0}\right)\end{array}\right]$$
$$\geq \mathcal{P}\left[\left(f_{r-2}^{*}\left(x^{r-2}\right)=x^{r-1}\oplus x^{r-3}\right)\right]$$
$$\times\mathcal{P}\left[\left(f_{r-1}^{*}\left(x^{r-1}\right)\oplus x^{r-2}=y^{0}\right)\right]$$
$$=\frac{1}{2^{2nq}}.$$

Vậy,

$$\mathcal{P}\left[X\xrightarrow{\phi\left(f_1^{*},f_2^{*},...,f_{r-1}^{*},f_r^{*}\right)}Y\right]$$
$$\geq \sum_{x^2,x^3,...,x^{r-1}\in\mathbb{I}_n^{\neq}}\frac{1}{2^{2nq}}$$
$$\times\mathcal{P}\left[\begin{array}{l}\left(x^{2}=x^{1}\oplus f_1^{*}\left(x^{0}\right)\right)\wedge\\ \cdots\wedge\left(f_r^{*}\left(y^{0}\right)=x^{r-1}\oplus y^{1}\right)\end{array}\right].$$

Ký hiệu

$$B=\sum_{x^2,x^3,...,x^{r-1}\in\mathbb{I}_n^{\neq}}\mathcal{P}\left[\begin{array}{l}\left(x^{2}=x^{1}\oplus f_1^{*}\left(x^{0}\right)\right)\wedge\\ \cdots\wedge\left(f_r^{*}\left(y^{0}\right)=x^{r-1}\oplus y^{1}\right)\end{array}\right].$$

Ta có:

$$B=\mathcal{P}\left[\begin{array}{l}\left(f_1^{*}(x^{0})\oplus x^{1}\right)\in\mathbb{I}_n^{\neq}\wedge\\ \cdots\wedge\left(f_r^{*}(y^{0})\oplus y^{1}\right)\in\mathbb{I}_n^{\neq}\end{array}\right]$$
$$=1-\mathcal{P}\left[\begin{array}{l}\left(f_1^{*}(x^{0})\oplus x^{1}\right)\notin\mathbb{I}_n^{\neq}\vee\\ \cdots\vee\left(f_r^{*}(y^{0})\oplus y^{1}\right)\notin\mathbb{I}_n^{\neq}\end{array}\right]$$
$$\geq 1-\sum_{i<j}\mathcal{P}\left[f_1^{*}(x_i^0)\oplus x_i^1=f_1^{*}(x_j^0)\oplus x_j^1\right]$$
$$-\cdots-\sum_{i<j}\mathcal{P}\left[f_r^{*}(y_i^0)\oplus y_i^1=f_r^{*}(y_j^0)\oplus y_j^1\right].$$

Ta có

$$\mathcal{P}\left[f_1^{*}(x_i^0)\oplus f_1^{*}(x_j^0)=x_i^1\oplus x_j^1\right]\leq\frac{1}{2^n}.$$

Thật vậy, nếu $x_i^0\neq x_j^0$, với $\delta=x_i^1\oplus x_j^1$ cho trước bất kỳ, theo tính chất đối với một hàm ngẫu nhiên hoàn thiện được đưa ra trong [6] ta có:

$$\mathcal{P}\left[f_1^{*}(x_i^0)\oplus f_1^{*}(x_j^0)=x_i^1\oplus x_j^1\right]=\frac{1}{2^n}.$$

Nếu $x_i^0=x_j^0$ thì $x_i^1\neq x_j^1$, khi đó:

$$\mathcal{P}\left[f_1^{*}(x_i^0)\oplus f_1^{*}(x_j^0)=x_i^1\oplus x_j^1\right]=0.$$

Áp dụng với $\frac{q(q-1)}{2}$ cặp $(i,j)$ của $[1..q]$ ta thu được:

$$\sum_{i<j}\mathcal{P}\left[f_1^{*}(x_i^0)\oplus x_i^1=f_1^{*}(x_j^0)\oplus x_j^1\right]\leq\frac{q(q-1)}{2\times 2^n}.$$

Tương tự,

$$\sum_{i<j}\mathcal{P}\left[f_2^{*}(x_i^2)\oplus x_i^0=f_2^{*}(x_j^2)\oplus x_j^0\right]\leq\frac{q(q-1)}{2\times 2^n}$$
$$\cdots$$
$$\sum_{i<j}\mathcal{P}\left[f_r^{*}(y_i^0)\oplus y_i^1=f_r^{*}(y_j^0)\oplus y_j^1\right]=\frac{q(q-1)}{2\times 2^n}$$

Do đó, $B\geq 1-\frac{r-2}{2}\times\frac{q(q-1)}{2^n}$. Từ đó, ta có:

$$\mathcal{P}\left[X\xrightarrow{\phi\left(f_1^{*},f_2^{*},...,f_{r-1}^{*},f_r^{*}\right)}Y\right]$$
$$\geq\frac{1}{2^{2nq}}\left(1-\frac{r-2}{2}\times\frac{q(q-1)}{2^n}\right).$$

Áp dụng Định lý 1 với $\varepsilon_1=\frac{q(q-1)}{2\times 2^n}$ $\varepsilon_2=\frac{r-2}{2}\times\frac{q(q-1)}{2^n}$, ta thu được:

$$Adv_{\mathcal{A}}^{q}\left(\phi\left(f_1^{*},f_2^{*},...,f_{r-1}^{*},f_r^{*}\right),F^{*}\right)\leq\frac{r-1}{2}\times\frac{q(q-1)}{2^n}\square$$

Khi $r=3$ thì kết quả thu được là giống như cận của Luby và Rackoff trong Định lý 3.

*C. Tính siêu giả ngẫu nhiên của cấu trúc Feistel*

Ta có khẳng định sau:

**Khẳng định 2.** *Cấu trúc Feistel 1-vòng, 2-vòng và 3-vòng đều không là siêu giả ngẫu nhiên.*

*Chứng minh.* Trước tiên, ta có nhận xét rằng cấu trúc Feistel 1-vòng và 2-vòng không phải là

giả ngẫu nhiên nên chúng cũng không là siêu giả ngẫu nhiên.

*Đối với cấu trúc Feistel 3-vòng.* Cấu trúc này không là siêu giả ngẫu nhiên. Thật vậy, ta có thể xây dựng bộ phân biệt như sau:

Gọi $\mathcal{A}_3$ là thuật toán phân biệt, được hoạt động như sau:

1. $\mathcal{A}_3$ chọn 1 giá trị $X_1=(L,R)\in\mathbb{I}_{2n}$
2. $\mathcal{A}_3$ truy vấn lên hàm *f* bất kỳ trên không gian hàm $\mathbb{F}_{2n}$ để thu được giá trị $Y_1=f(X_1)=(S,T)\in\mathbb{I}_{2n}$.
3. $\mathcal{A}_3$ chọn 1 giá trị $X_2=(L',R)\in\mathbb{I}_{2n}$ với $L'\neq L$.
4. $\mathcal{A}_3$ truy vấn lên hàm *f* để thu được giá trị $Y_2=f(X_2)=(S',T')$.
5. $\mathcal{A}_3$ chọn 1 giá trị
$$X_3=(S',T'\oplus L\oplus L')\in\mathbb{I}_{2n}.$$
6. $\mathcal{A}_3$ truy vấn lên hàm $f^{-1}$ để thu được giá trị $Y_3=f^{-1}(X_3)=(L'',R'')$.
7. $\mathcal{A}_3$ kiểm tra điều kiện $R''\oplus R=S\oplus S'$, nếu thỏa mãn thì $\mathcal{A}_3$ trả ra giá trị 1, nếu không thì $\mathcal{A}_3$ trả ra giá trị 0.

Với $p_3^*$ là xác suất mà $\mathcal{A}_3$ trả ra 1 khi $f$ là hoán vị ngẫu nhiên hoàn thiện trên $\mathbb{F}_{2n}$, khi đó $p_3^*\approx 2^{-n}$.

Với $p_3$ là xác suất mà $\mathcal{A}_3$ trả ra 1 khi $f=\phi\left(f_1^*,f_2^*,f_3^*\right)$, thì khi đó $p_3=1$. Thật vậy, ta có:

$$f(L,R)=(S,T)$$
$$\Leftrightarrow\begin{cases}S=R\oplus f_2^*\left(L\oplus f_1^*(R)\right)\\ T=L\oplus f_1^*(R)\oplus f_3^*\left(R\oplus f_2^*\left(L\oplus f_1^*(R)\right)\right).\end{cases}$$

Tương tự,

$$f(L',R)=(S',T')$$
$$\Leftrightarrow\begin{cases}S'=R\oplus f_2^*\left(L'\oplus f_1^*(R)\right)\\ T'=L'\oplus f_1^*(R)\oplus f_3^*\left(R\oplus f_2^*\left(L'\oplus f_1^*(R)\right)\right).\end{cases}$$

$$f^{-1}(S,T)=(L,R)$$
$$\Leftrightarrow\begin{cases}L=T\oplus f_3^*(S)\oplus f_1^*\left(S\oplus f_2^*\left(T\oplus f_3^*(S)\right)\right)\\ R=S\oplus f_2^*\left(T\oplus f_3^*(S)\right).\end{cases}$$

Do đó,

$$f^{-1}(S',T'\oplus L\oplus L')=(L'',R'')$$
$$\Rightarrow R''=S'\oplus f_2^*\left(T'\oplus L\oplus L'\oplus f_3^*(S')\right)$$
$$=S'\oplus f_2^*\left(L\oplus f_1^*(R)\right)$$
$$=S'\oplus S\oplus R.$$

Vậy $R''\oplus R=S'\oplus S$.

Do đó, lợi thế phân biệt của $\mathcal{A}_3$ là:

$$Adv_{\mathcal{A}_3}\left(\phi\left(f_1^*,f_2^*,f_3^*\right),C^*\right)$$
$$=\left|p_3^*-p_3\right|\approx 1-2^{-n}\geq\frac{1}{2n},\forall n\geq 1.$$

Vậy cấu trúc Feistel 3-vòng không là siêu giả ngẫu nhiên□

*Đối với cấu trúc Feistel r-vòng* $(r\geq 4)$. Ta có mệnh đề sau:

**Mệnh đề 2.** *Cho* $f_1^*,f_2^*,...,f_{r-1}^*,f_r^*\in\mathbb{F}_n$; $r\geq 4$ *là các hàm ngẫu nhiên hoàn thiện độc lập. Gọi* $C^*\in\mathbb{P}_{2n}$ *là một hoán vị ngẫu nhiên hoàn thiện. Đối với một bộ phân biệt siêu giả ngẫu nhiên bất kỳ* $\mathcal{A}$ *được cho phép thực hiện q truy vấn mã hóa hoặc giải mã thích nghi, chúng ta có:*

$$Adv_{\mathcal{A}}\left(\phi\left(f_1^*,f_2^*,...,f_{r-1}^*,f_r^*\right),C^*\right)\leq\frac{r-2}{2}\times\frac{q(q-1)}{2^n}+\frac{q(q-1)}{2\times 2^{2n}}.$$

*Chứng minh.* Chúng ta sẽ so sánh hàm $\phi\left(f_1^*,f_2^*,...,f_{r-1}^*,f_r^*\right)$ với hoán vị ngẫu nhiên hoàn thiện $C^*\in\mathbb{P}_{2n}$.

Ký hiệu $X=(X_i)_{i\in[1..q]}=\left(x_i^1,x_i^0\right)\in\mathbb{I}_{2n}$ là các đầu vào của $\phi\left(f_1^*,f_2^*,...,f_{r-1}^*,f_r^*\right)$ và các đầu ra tương ứng $Y=(Y_i)_{i\in[1..q]}=\left(y_i^1,y_i^0\right)\in\mathbb{I}_{2n}$.

Đối với mỗi

$$\left(y_i^1, y_i^0\right) = \phi\left(f_1^*, f_2^*, ..., f_{r-1}^*, f_r^*\right)\left(x_i^1, x_i^0\right)$$

ta ký hiệu $x_i^2, x_i^3, ..., x_i^{r-1}$ là các giá trị trung gian như Hình 2. Cụ thể:

$$x_i^2 = x_i^1 \oplus f_1^*\left(x_i^0\right),$$

$$x_i^0 \oplus f_2^*\left(x_i^2\right) = x_i^3,$$

$$\cdots$$

$$f_{r-1}^*\left(x_i^{r-1}\right) \oplus x_i^{r-2} = y_i^0,$$

$$f_r^*\left(y_i^0\right) = x_i^{r-1} \oplus y_i^1.$$

Cuối cùng ta ký hiệu $x^0, x^1, x^2, x^3, ..., x^{r-1}$, $y^0, y^1$ tương ứng lần lượt là các bộ $q$ phần tử các từ $n$-bit

$$\left(x_i^0\right)_{i\in[1..q]}, \left(x_i^1\right)_{i\in[1..q]}, \left(x_i^2\right)_{i\in[1..q]}, \left(x_i^3\right)_{i\in[1..q]},$$

$$..., \left(x_i^{r-1}\right)_{i\in[1..q]}, \left(y_i^0\right)_{i\in[1..q]}, \left(y_i^1\right)_{i\in[1..q]}.$$

Ta định nghĩa $\mathcal{X}$ là tập tất cả các bộ $q$ phần tử $X$ của các từ khác nhau đôi một của $\mathbb{I}_{2n}$ (tức là sao cho với $i, j$ phân biệt bất kỳ thuộc [1...q] thì $x_i^0 \neq x_j^0$ hoặc $x_i^1 \neq x_j^1$) và định nghĩa $\mathcal{Y}$ là tập các bộ $q$ phần tử $Y$ của các từ $\mathbb{I}_{2n}$ khác nhau từng đôi một như sau:

$$\mathcal{Y} = \left\{\left(Y_1, ..., Y_q\right) \in \left(\mathbb{I}_{2n}\right)^q \mid Y \in \mathbb{I}_{2n}^{\neq}\right\}.$$

Với bộ $q$ phần tử $X$ bất kỳ của $\mathcal{X}$ và bộ $q$ phần tử $Y$ bất kỳ của $\mathcal{Y}$, ta có:

$$\mathcal{P}\left[X \xrightarrow{\phi\left(f_1^*, f_2^*, ..., f_{r-1}^*, f_r^*\right)} Y\right]$$

$$= \sum_{x^2, x^3, ..., x^{r-1} \in \mathbb{I}_n} \mathcal{P}\begin{bmatrix}\left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right) \\ \wedge\left(x^0 \oplus f_2^*\left(x^2\right) = x^3\right) \\ \wedge\cdots \\ \wedge\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right) \\ \wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right)\end{bmatrix}$$

$$\geq \sum_{x^2, x^3, ..., x^{r-1} \in \mathbb{I}_n^{\neq}} \mathcal{P}\begin{bmatrix}\left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right) \wedge \\ \cdots \wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right)\end{bmatrix} \times$$

$$\times\mathcal{P}\begin{bmatrix}\left(f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right) \\ \wedge\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right)\end{bmatrix}.$$

Vì $x^{r-2} \in \mathbb{I}_n^{\neq}$, nên theo tính chất đối với hàm ngẫu nhiên hoàn thiện được đưa ra trong [6] suy ra

$$\mathcal{P}\left[f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right] = \frac{1}{2^{nq}}.$$

Tương tự, vì $x^{r-1} \in \mathbb{I}_n^{\neq}$, suy ra

$$\mathcal{P}\left[f_{r-1}^*\left(x^{r-1}\right) = x^{r-2} \oplus y^0\right] = \frac{1}{2^{nq}}.$$

Do đó,

$$\mathcal{P}\begin{bmatrix}\left(f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right) \\ \wedge\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right)\end{bmatrix}$$

$$\geq \mathcal{P}\left[\left(f_{r-2}^*\left(x^{r-2}\right) = x^{r-1} \oplus x^{r-3}\right)\right]$$

$$\times\mathcal{P}\left[\left(f_{r-1}^*\left(x^{r-1}\right) \oplus x^{r-2} = y^0\right)\right]$$

$$= \frac{1}{2^{2nq}}.$$

Vậy,

$$\mathcal{P}\left[X \xrightarrow{\phi\left(f_1^*, f_2^*, ..., f_{r-1}^*, f_r^*\right)} Y\right]$$

$$\geq \sum_{x^2, x^3, ..., x^{r-1} \in \mathbb{I}_n^{\neq}} \frac{1}{2^{2nq}} \times$$

$$\times\mathcal{P}\begin{bmatrix}\left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right) \wedge \\ \cdots \wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right)\end{bmatrix}.$$

Ký hiệu:

$$B = \sum_{x^2, x^3, ..., x^{r-1} \in \mathbb{I}_n^{\neq}} \mathcal{P}\begin{bmatrix}\left(x^2 = x^1 \oplus f_1^*\left(x^0\right)\right) \wedge \\ \cdots \wedge\left(f_r^*\left(y^0\right) = x^{r-1} \oplus y^1\right)\end{bmatrix}.$$

Ta có

$$B=\mathcal{P}\left[\begin{array}{l}\left(f_1^*(x^0)\oplus x^1\right)\in\mathbb{I}_n^{\neq}\wedge\\ \cdots\wedge\left(f_r^*(y^0)\oplus y^1\right)\in\mathbb{I}_n^{\neq}\end{array}\right]$$

$$=1-\mathcal{P}\left[\begin{array}{l}\left(f_1^*(x^0)\oplus x^1\right)\notin\mathbb{I}_n^{\neq}\vee\\ \cdots\vee\left(f_r^*(y^0)\oplus y^1\right)\notin\mathbb{I}_n^{\neq}\end{array}\right]$$

$$\geq 1-\sum_{i<j}\mathcal{P}\left[f_1^*(x_i^0)\oplus x_i^1=f_1^*(x_j^0)\oplus x_j^1\right]$$

$$-\cdots-\sum_{i<j}\mathcal{P}\left[f_r^*(y_i^0)\oplus y_i^1=f_r^*(y_j^0)\oplus y_j^1\right].$$

Suy ra:

$$\mathcal{P}\left[f_1^*(x_i^0)\oplus f_1^*(x_j^0)=x_i^1\oplus x_j^1\right]\leq\frac{1}{2^n}.$$

Thật vậy, nếu $x_i^0\neq x_j^0$, thì với $\delta=x_i^1\oplus x_j^1$ cho trước bất kỳ, ta có:

$$\mathcal{P}\left[f_1^*(x_i^0)\oplus f_1^*(x_j^0)=x_i^1\oplus x_j^1\right]=\frac{1}{2^n}.$$

Nếu $x_i^0=x_j^0$ thì $x_i^1\neq x_j^1$, khi đó:

$$\mathcal{P}\left[f_1^*(x_i^0)\oplus f_1^*(x_j^0)=x_i^1\oplus x_j^1\right]=0.$$

Áp dụng với $\frac{q(q-1)}{2}$ cặp $(i,j)$ của $[1..q]$ ta thu được:

$$\sum_{i<j}\mathcal{P}\left[f_1^*(x_i^0)\oplus x_i^1=f_1^*(x_j^0)\oplus x_j^1\right]\leq\frac{q(q-1)}{2\times 2^n}$$

Tương tự,

$$\sum_{i<j}\mathcal{P}\left[f_2^*(x_i^2)\oplus x_i^0=f_2^*(x_j^2)\oplus x_j^0\right]\leq\frac{q(q-1)}{2\times 2^n}$$

…

$$\sum_{i<j}\mathcal{P}\left[f_r^*(y_i^0)\oplus y_i^1=f_r^*(y_j^0)\oplus y_j^1\right]\leq\frac{q(q-1)}{2\times 2^n}$$

Do đó, $B\geq 1-\frac{r-2}{2}\times\frac{q(q-1)}{2^n}$.

Cuối cùng:

$$\mathcal{P}\left[X\xrightarrow{\phi\left(f_1^*,f_2^*,\ldots,f_{r-1}^*,f_r^*\right)}Y\right]$$

$$\geq\frac{1}{2^{2nq}}\left(1-\frac{r-2}{2}\times\frac{q(q-1)}{2^n}\right).$$

Áp dụng Định lý 2 cho việc đánh giá $Adv_{\mathcal{A}}\left(\phi\left(f_1^*,f_2^*,\ldots,f_{r-1}^*,f_r^*\right),C^*\right)$ trong mệnh đề 2 với $\varepsilon=\frac{r-2}{2}\times\frac{q(q-1)}{2^n}$, ta có:

$$Adv_{\mathcal{A}}^q\left(\phi\left(f_1^*,f_2^*,\ldots,f_{r-1}^*,f_r^*\right),C^*\right)$$

$$\leq\frac{r-2}{2}\times\frac{q(q-1)}{2^n}+\frac{q(q-1)}{2\times 2^{2n}}\square$$

Khi $r=4$, chúng ta thu được cận lợi thế tốt hơn cận của Patarin phát biểu trong Định lý 4 của tài liệu [5]. Tuy nhiên, trong chứng minh của Patarin cũng có thể đạt được cận này bằng biến đổi đơn giản, nhưng đã được nới lỏng cận để thu được kết quả là $\frac{q^2}{2^n}$ như của Luby và Rackoff trong [1].

## IV. KẾT LUẬN

Trong bài báo này, chúng tôi đã xây dựng được các bộ phân biệt giả ngẫu nhiên cho trường hợp 1-vòng và 2-vòng để chứng minh rằng cấu trúc Feistel 1-vòng và 2-vòng không là giả ngẫu nhiên, cũng như bộ phân biệt siêu giả ngẫu nhiên cho trường hợp 3-vòng để chứng minh cấu trúc này không là siêu giả ngẫu nhiên. Hơn nữa, chúng tôi đưa ra chứng minh tổng quát về tính giả ngẫu nhiên và siêu giả ngẫu nhiên của cấu trúc Feistel theo mô hình Luby-Rackoff với số vòng tùy ý. Tuy nhiên, một điểm đáng lưu ý là các cận đạt được không giảm khi số vòng tăng.

Các kết quả đạt được có ý nghĩa trong việc chứng tỏ rằng cấu trúc Feistel với số vòng lớn hơn hoặc bằng 3 là giả ngẫu nhiên, và cấu trúc Feistel với số vòng lớn hơn hoặc bằng 4 là siêu giả ngẫu nhiên. Tương đồng, một số nghiên cứu trên thế giới có một số kết quả cải tiến cho kết quả này và thu được một số cận nhỏ hơn khi số vòng tăng như trong [7, 8, 9], nhưng yêu cầu cách tiếp cận khác. Đây là một vấn đề mở triển vọng cho các nghiên cứu tiếp theo.

## TÀI LIỆU THAM KHẢO

[1]. Luby M. , Rackoff C., "How to construct pseudorandom permutations from pseudorandom functions", SIAM Journal on Computing. 17 (2), pp. 373-386, 1988.

[2]. Patarin J., "The "coefficients H" technique", Selected Areas in Cryptography, Springer, pp. 328-345, 2008.

[3]. Gilbert H., Minier M., "New results on the pseudorandomness of some blockcipher constructions", Fast Software Encryption, Springer, pp. 248-266, 2001.

[4]. Piret G.-F., "Block ciphers: security proofs, cryptanalysis, design, and fault attacks", UCL, 2005.

[5]. Patarin J., "Pseudorandom permutations based on the DES scheme", EUROCODE'90, Springer, pp. 193-204, 1991.

[6]. Goldwasser S., Bellare M., "Lecture notes on cryptography", Summer course Cryptography and computer security at MIT. 1999, pp. 1999, 1996.

[7]. Patarin J., "Security of random Feistel schemes with 5 or more rounds", Advances in Cryptology–CRYPTO 2004, Springer, pp. 106-122, 2004 .

[8]. Patarin J., "About Feistel schemes with six (or more) rounds", Fast Software Encryption, Springer, pp. 103-121, 1998.

[9]. Patarin J., "Luby-Rackoff: 7 rounds are enough for $2^{n(1-\varepsilon)}$ security", Advances in Cryptology-CRYPTO 2003, Springer, pp. 513-529, 2003.

## SƠ LƯỢC VỀ TÁC GIẢ

**ThS. Nguyễn Bùi Cương**

Đơn vị công tác: Viện Khoa học-Công nghệ Mật mã - Ban Cơ yếu Chính phủ.

Email: nguyenbuicuong@gmail.com

Quá trình đào tạo: Nhận bằng cử nhân Toán học tại Đại học Sư phạm Hà Nội năm 2004. Nhận bằng Thạc sĩ Toán học tại Đại học Khoa học tự nhiên - Đại học Quốc gia Hà Nội năm 2006.

Hướng nghiên cứu hiện nay: Khoa học mật mã, mã hóa đối xứng.

**CN. Hoàng Đình Linh**

Đơn vị công tác: Viện Khoa học-Công nghệ Mật mã - Ban Cơ yếu Chính phủ.

Email: linhhd@bcy.gov.vn

Quá trình đào tạo: Nhận bằng cử nhân Toán học tại Đại học Khoa học tự nhiên-Đại học Quốc gia Hà Nội năm 2014.

Hướng nghiên cứu hiện nay: Nghiên cứu, thiết kế, đánh giá độ an toàn chứng minh được của các thuật toán mã hóa đối xứng.