MỞ ĐẦU

1. Động lực nghiên cứu

Sự phát triển mạnh mẽ của công nghệ số và việc sử dụng dữ liệu dùng chung hiện nay đặt ra yêu cầu cao đối với: i) Định danh và xác thực thiết bị, bảo vệ an toàn phần cứng và dữ liệu; ii) Bảo mật khóa mã trong mã hóa mật ở lớp vật lý. **Bảo mật phần cứng** có nhiệm vụ đảm bảo các mục tiêu trên ở lớp vật lý trước phát triển mạnh mẽ của các phương thức tấn công phần cứng, đặc biệt là sự lây lan của mã độc phần cứng.

Mạch tạo hàm không thể sao chép về vật lý (*PUF: Physically Unclonable Function*) là một trong các kỹ thuật nền tảng, tương tác trực tiếp với thực thể vật lý nhằm đạt được mục tiêu bảo mật ở lớp vật lý. PUF có tính nguyên bản, đặc thù đối với một thực thể vật lý cụ thể và đặc biệt là khả năng chống sao chép ở mức vật lý. Với mong muốn tìm hiểu và phát triển thiết kế PUF cho một số ứng dụng bảo mật cụ thể, nghiên cứu sinh lựa chọn đề tài:

"Nghiên cứu nâng cao hiệu năng RO PUF dùng trong bảo mật phần cứng". (RO PUF: Ring Oscillator PUF/Mạch PUF dao động vòng)

Hiệu năng của một sơ đồ PUF gắn với ứng dụng cụ thể. Trong luận án này, hiệu năng RO PUF được đánh giá theo **độ tin cậy** trong định danh và xác thực thiết bị và **tính ổn định** của chuỗi bit đáp ứng đầu ra của PUF, phục vụ các ứng dụng mã hóa bảo mật. Từ mục tiêu chung là nghiên cứu các giải pháp nâng cao hiệu năng mạch RO PUF, dùng trong các ứng dụng bảo mật phần cứng, nghiên cứu sinh xác định mục tiêu nghiên cứu cụ thể:

- Đề xuất mô hình trích xuất đặc trưng cục bộ của mạch RO PUF, ứng dụng trong định danh và xác thực thiết bị;
- Nghiên cứu các kỹ thuật ổn định chuỗi bit ra đáp ứng RO PUF;
- Thiết kế mạch ứng dụng và thực nghiệm kiểm chứng kết quả trên FPGA.

2. Đối tượng và phạm vi nghiên cứu

Đối tượng nghiên cứu là mạch RO PUF. Về lý thuyết, nghiên cứu mô hình thống kê của tần số mạch RO PUF, tham số định lượng phẩm chất RO PUF và tính khả thi của các ứng dụng RO PUF cụ thể. Về thực nghiệm, phát triển các ứng dụng của mạch RO PUF trong việc tách và xác thực dữ liệu định danh (*ID: Identification*) cho thiết bị, tạo chuỗi bit ra ổn định và duy nhất, phục vụ mã hóa bảo mật.

3. Đóng góp của luận án

- Đề xuất giải pháp trích xuất đặc trưng tần số của RO PUF trên cơ sở phân tích ảnh hưởng của nhiệt độ môi trường.

- Đề xuất sơ đồ tách và xác thực ID cho thiết bị sử dụng RO PUF thực thi trên FPGA sử dụng các tham số khoảng cách và mức ngưỡng xác thực dựa trên độ đo Euclid.

- Đề xuất kỹ thuật ổn định trực tiếp chuỗi bit trích xuất từ RO PUF và đánh giá hiệu quả đề xuất bằng thực nghiệm trên FPGA.

4. Cấu trúc của luận án

Ngoài phần Mở đầu, Kết luận, luận án gồm 4 chương.

Chương 1: Tổng quan về mạch tạo hàm không thể sao chép về vật lý

Chương 1 giới thiệu khái quát về mạch tạo hàm không thể sao chép về vật lý (PUF): Khái niệm, phân loại, một số sơ đồ PUF điển hình, các tham số và chỉ tiêu đánh giá hiệu năng PUF.

Chương 2: Thiết kế RO PUF trên FPGA

Chương 2 trình bày các giải pháp kỹ thuật cụ thể khi thiết kế mạch RO PUF trên FPGA, mô hình thống kê đề xuất dùng để khảo sát đặc tính của tần số RO, một số kết luận rút ra về đặc tính tần số RO từ phân tích số liệu thực nghiệm. Trên cơ sở đó, nghiên cứu sinh đề xuất sử dụng đặc trưng cục bộ của tần số RO tạo ID cho thiết bị.

Chương 3: Ứng dụng RO PUF định danh và xác thực ID cho thiết bị

Chương 3 đề xuất sơ đồ định danh và xác thực ID ứng dụng RO PUF, phương pháp sử dụng độ đo Euclid trong xây dựng các tham số định lượng phẩm chất mạch RO PUF; thực thi thiết kế trên các linh kiện FPGA Xilinx Spartan-6, Xilinx Spartan-3E và Xilinx Artix-7.

Chương 4: Kỹ thuật ổn định chuỗi bit trích xuất từ RO PUF

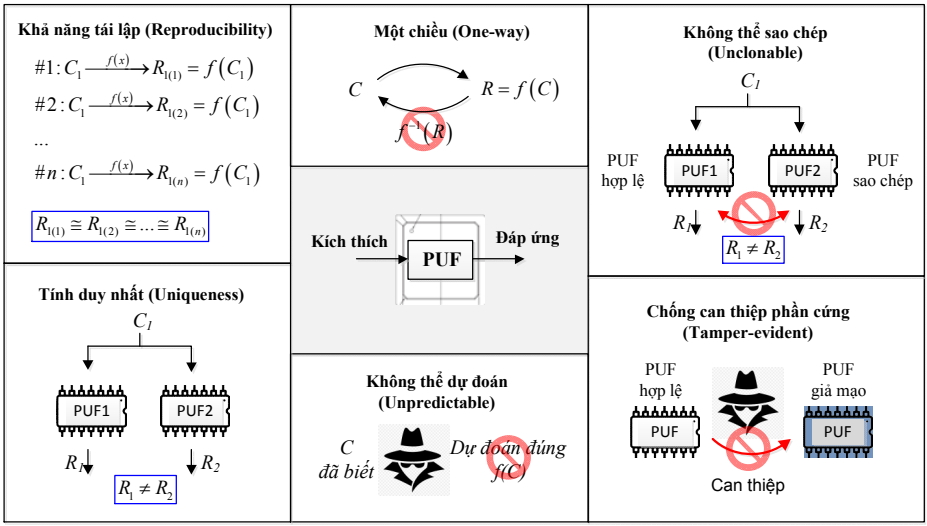
Chương 4 đề xuất các giải pháp ổn định dữ liệu ra mạch RO PUF nhằm tạo chuỗi bit ổn định và duy nhất, hướng tới các ứng dụng trong an toàn, bảo mật phần cứng đặc thù.

Cuối mỗi chương có kết luận chương khái quát kết quả nghiên cứu và công bố tương ứng. Phần kết luận chung tóm tắt kết quả đạt được và những đóng góp về khoa học của luận án, gợi mở một số hướng nghiên cứu tiếp theo.

Chương 1: Tổng quan về mạch tạo hàm không thể sao chép về vật lý

1.1. Khái quát về PUF

Mạch tạo hàm không thể sao chép về vật lý (*PUF: Physically Unclonable Function*) là kỹ thuật trích xuất dữ liệu đặc trưng gắn với thực thể vật lý. Dữ liệu này là riêng biệt và không thể sao chép như vân tay sinh trắc học đối với mỗi người cụ thể. Các nghiên cứu về PUF tập trung vào việc đề xuất các kiến trúc PUF, xác lập tham số và phương pháp đánh giá một sơ đồ PUF, tìm kiếm hướng ứng dụng PUF trong thực tế. Các thiết kế PUF khai thác những thăng giáng ngẫu nhiên nội tại hình thành trong quá trình chế tạo các cấu kiện điện tử để tách ra dữ liệu đặc trưng. Những lĩnh vực ứng dụng điển hình của PUF là định danh và xác thực thiết bị (chống giả mạo), tạo khóa mã bảo mật, tạo số ngẫu nhiên, bảo vệ IP và một số ứng dụng khác liên quan đến bảo mật phần cứng ở cấp độ vật lý.



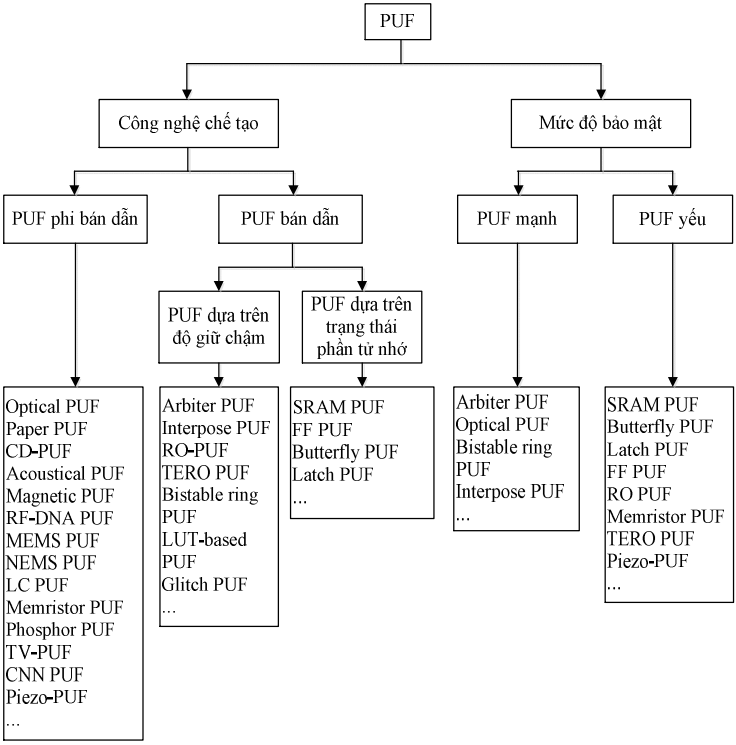
Hình 1.1: Cấu trúc cơ bản của PUF và các thuộc tính thiết yếu

Cấu trúc cơ bản và các thuộc tính thiết yếu của PUF được trình bày trên Hình 1.1. Tương ứng với mỗi mẫu dữ liệu kích thích (*Challenge*) ở đầu vào, ở đầu ra sẽ có một mẫu dữ liệu đáp ứng (*Response*). Mẫu đáp ứng PUF có bản chất là đại lượng thống kê, không thể dự đoán, duy nhất và độc lập. Trong trường hợp lý tưởng, mẫu đáp ứng PUF không thể được mô hình hóa bằng các

công cụ toán. Các cặp mẫu kích thích – mẫu đáp ứng (*CRP: Challenge-Response Pair*) là không thể sao chép về mặt vật lý.

1.2. Phân loại PUF

Các sơ đồ PUF có thể được phân loại dựa trên phương pháp chế tạo và mức độ bảo mật (Hình 1.2).



Hình 1.2: Phân loại PUF

Theo công nghệ chế tạo, *PUF phi bán dẫn* sử dụng các vật liệu khác vật liệu bán dẫn để tạo cấu trúc PUF; *PUF bán dẫn* khai thác sự bất đồng nhất về mặt vật lý gây ra bởi những thăng giáng không kiểm soát được, xuất hiện trong quá trình chế tạo để tạo ra dữ liệu đặc trưng cho mỗi IC.

Đa số các thiết kế PUF được thực thi trên nền bán dẫn. Theo nguồn thăng giáng, các PUF bán dẫn được phân thành *PUF dựa trên độ giữ chậm* (Khai thác sự khác biệt về độ giữ chậm đường truyền tín hiệu bên trong mạch) và

PUF dựa trên trạng thái của các phần tử nhớ (Khai thác tính ngẫu nhiên trong trạng thái đầu của ô nhớ).

Theo kích thước tập CRP, các PUF có thể được phân thành *PUF yếu* (Độ dài dữ liệu đáp ứng là hàm tuyến tính hay đa thức của số phần tử tập CRP) và *PUF mạnh* (Độ dài dữ liệu đáp ứng là hàm mũ của số phần tử tập CRP). PUF mạnh chế áp được các tấn công giả lập, PUF yếu thích hợp cho việc tạo khóa mã và chuỗi khởi tạo cho các ứng dụng tạo số giả ngẫu nhiên.

1.3. Các tham số đánh giá hiệu năng của PUF

1.3.1. Mô hình toán của PUF

- Lớp PUF $\mathcal{P}$: Mô tả hoàn chỉnh của một kiểu kiến trúc PUF cụ thể. Thủ tục khởi tạo $\mathcal{P}.Create\left(r^C\right)$, với đối số ngẫu nhiên $r^C \leftarrow \{0,1\}^*$ là phép thử nhị phân, dùng để tạo các thực thể của $\mathcal{P}$.

- Thực thể PUF *puf*: Thể hiện rời rạc của $\mathcal{P}$, tạo ra bởi thủ tục $\mathcal{P}.Create$:

$$\mathcal{P} \equiv \left\{ puf_i \leftarrow \mathcal{P}.Create\left(r_i^C\right) : \forall i, r_i^C \leftarrow \{0,1\}^* \right\} \tag{1.1}$$

$puf\left(x\right)$: *puf* được cấu hình theo biến trạng thái *x*.

- Hàm ước lượng PUF của $puf\left(x\right)$: $puf\left(x\right).Eval$

- Đáp ứng của *puf*: Đại lượng được tạo ra từ ước lượng PUF.

Thực nghiệm PUF:

Một thực nghiệm $\left(N_{puf}, N_{chal}, N_{meas}\right)$ trên một lớp PUF $\mathcal{P}$ là một mảng $N_{puf} \times N_{chal} \times N_{meas}$ giá trị đáp ứng PUF thu nhận được đối với N_{puf} thực thể PUF ngẫu nhiên của lớp $\mathcal{P}$, được kích thích bởi tập N_{chal} kích thích ngẫu nhiên, từ N_{meas} lần kích hoạt riêng biệt.

$$E_{\mathcal{P}}\left(N_{puf}, N_{chal}, N_{meas}\right) \rightarrow Y_{E(P)} = \left[y_i^{(j)}\left(x_k\right) \leftarrow puf_i\left(x_k\right).Eval\left(r_j^E\right) \right] \tag{1.2}$$

Với $\forall 1 \le i \le N_{puf} : puf_i \leftarrow \mathcal{P}$,

$\forall 1 \le k \le N_{chal} : x_k \leftarrow \mathcal{X}_{\mathcal{P}}$,

$\forall 1 \le j \le N_{meas} : r_j^E \leftarrow \{0,1\}^*$

Khi tính tới điều kiện thực nghiệm α, mô hình có dạng: $E_{\mathcal{P}}^{\alpha}\left(N_{puf}, N_{chal}, N_{meas}\right)$.

1.3.2. Các tham số định lượng phẩm chất PUF

- *Khoảng cách nội* (*Intra-distance*) là biến ngẫu nhiên mô tả khoảng cách giữa hai đáp ứng PUF đối với cùng một thực thể PUF và sử dụng cùng một kích thích.

$$D_{puf_i}^{intra}(x) \triangleq dist\left[Y_i(x); Y_i^{'}(x)\right] \tag{1.3}$$

$Y_i(x)$ và $Y_i^{'}(x)$ là hai ước lượng ngẫu nhiên và riêng biệt của puf_i với cùng một kích thích x.

- *Khoảng cách tương quan* (*Inter-distance*) là biến ngẫu nhiên mô tả khoảng cách giữa hai đáp ứng PUF từ hai thực thể PUF sử dụng cùng một kích thích:

$$D_{\mathcal{P}}^{inter} \triangleq dist\left[Y(x); Y^{'}(x)\right] \tag{1.4}$$

$Y(x)$, $Y^{'}(x)$ là các đáp ứng khi tác động cùng một kích thích x lên hai thực thể PUF ngẫu nhiên và tách biệt $PUF \leftarrow \mathcal{P}$ và $PUF^{'}\left(\neq PUF\right) \leftarrow \mathcal{P}$.

Các tham số của phân bố xác suất $D_{\mathcal{P}}^{intra}$ và $D_{\mathcal{P}}^{inter}$ thường được sử dụng trong đánh giá chất lượng PUF là giá trị trung bình và độ lệch chuẩn.

1.3.3. Các chỉ tiêu chất lượng của PUF

Một sơ đồ PUF được đánh giá qua khả năng thực thi (*Constructibility*), khả năng ước lượng (*Evaluability*), khả năng tái lập (*Reproducibility*), tính duy nhất (*Uniqueness*), khả năng định danh (*Identifiability*), tính không thể giả lập về vật lý (*Physical Unclonability*), tính không thể dự đoán (*Unpredictability*),…

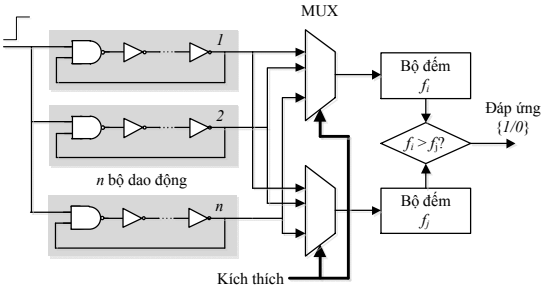
Kết luận chương 1

Chương 1 trình bày khái quát về PUF, phân loại và một số sơ đồ PUF phổ biến, tình hình nghiên cứu trong nước và trên thế giới về PUF. Để có thể xây dựng tham số định lượng hiệu năng của PUF cho các ứng dụng cụ thể, nghiên cứu sinh trình bày kết quả các nghiên cứu quan trọng trong việc xây dựng mô hình toán của PUF, các tham số định lượng phẩm chất một thiết kế PUF. Cuối chương trình bày một số lĩnh vực ứng dụng PUF và các công trình liên quan.

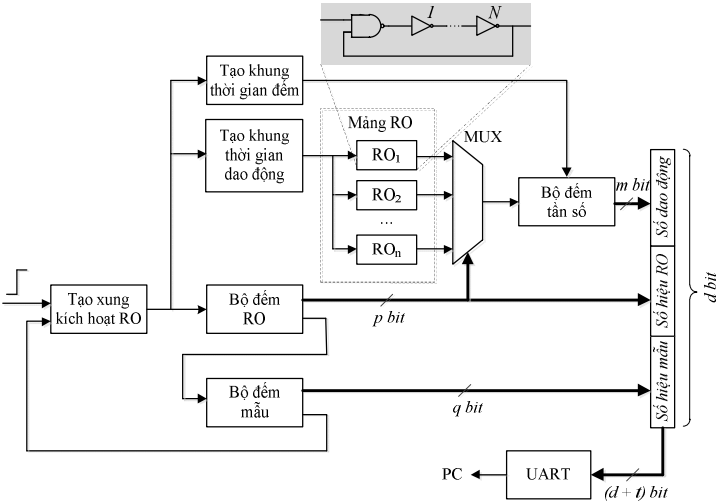
Chương 2: Thiết kế RO PUF trên FPGA

2.1. Thiết kế phần cứng RO PUF trên FPGA

Đặc điểm nổi bật trong thiết kế PUF trên FPGA là hầu hết các mạch PUF không tuân thủ quy tắc thiết kế logic số thông thường, trong đó cấu hình mạch vật lý có thể bị sửa đổi, cắt bỏ trong giai đoạn tối ưu hóa mạch logic. RO PUF là một trong số các sơ đồ PUF có độ phức tạp ít nhất có thể thực thi trên FPGA đảm bảo yêu cầu tính đồng nhất và đối xứng trong mạch vật lý.



Hình 2.1: Mạch RO PUF cơ bản



Hình 2.2: Sơ đồ chức năng mạch RO PUF đề xuất

Để khảo sát ảnh hưởng của các nhân tố biến thiên lên tần số RO, nghiên cứu sinh đề xuất thiết kế RO PUF thu nhận dữ liệu tần số của các RO (Hình 2.2) trên cơ sở cải tiến thiết kế cơ bản Suh và Devadas năm 2007 (Hình 2.1).

Phần tử giữ chậm (bộ đảo) của RO được cấu hình từ một LUT nguyên bản. Việc thiết kế được thực thi bằng công cụ Xilinx ISE/FPGA Editor. N bộ đảo (N chẵn) và một cổng NAND được kết nối để tạo RO cơ bản, sau đó đóng gói RO cơ bản bằng kỹ thuật *hard macro*. Macro RO được sao chép ra các vị trí khác nhau trên FPGA tạo thành các thực thể RO. Các mạch bổ trợ của thiết kế gồm giao diện *UART* và các mạch tạo xung đồng bộ. Bộ đếm RO tạo p bit dữ liệu điều khiển bộ chọn kênh, tuần tự chuyển mạch $RO_1 - RO_n$ tới đầu vào bộ đếm tần số trong một chu kỳ lấy mẫu. Bộ đếm tần số đo số dao động RO trong khoảng thời gian ΔT_{mea} được thiết lập bởi bộ tạo khung thời gian đếm. Bộ đếm mẫu được dùng để đếm và khống chế số mẫu. d bit dữ liệu truyền sẽ được bổ sung t bit dữ liệu đệm để tạo khung dữ liệu phù hợp, truyền qua UART tới máy tính. Giá trị tần số tuyệt đối RO được tính bằng tích trị số đếm của bộ đếm tần số với $1/\Delta T_{mea}$. Trong thiết kế cụ thể này, chọn $N = 16$, $p = 5$, $n = 2^p = 32$, $\Delta T_{mea} = 20ms$, $m = 24$, $q = 16$, $(d + t) = 48$. Thiết kế có tính tùy biến cao và có thể chuyển đổi linh hoạt giữa các công nghệ FPGA.

2.2. Mô hình thống kê của tần số RO PUF

Tần số tuyệt đối của RO có thể được mô hình hóa bởi biểu thức:

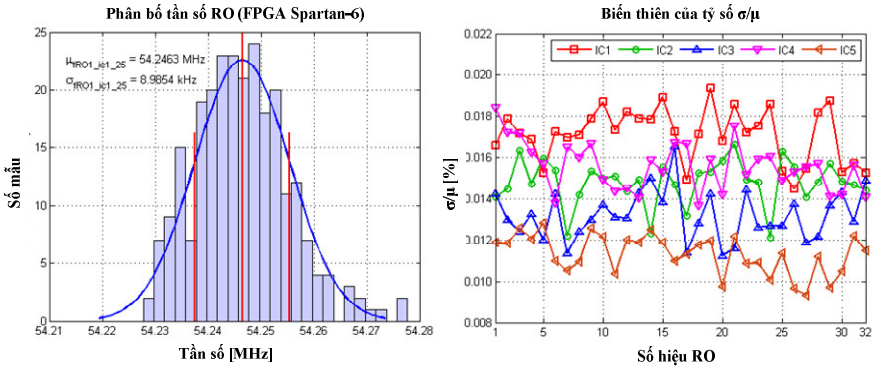
$$f_{RO} = f_{nominal} + \Delta f_{local} + \Delta f_{global} + \Delta f_{OP} \qquad (2.1)$$

Trong đó, $f_{nominal}$ là tần số RO danh định (là tần số đo được khi thiết bị danh định hoạt động ở điều kiện danh định, 25°C, 1,0 V). Δf_{global} và Δf_{local} là các biến thiên tần số tương ứng gây ra bởi biến thiên toàn cục (biến thiên công nghệ giữa các chip và sự thay đổi nhiệt độ môi trường, có tác động đồng đều lên các RO) và biến thiên cục bộ (biến thiên công nghệ bên trong chip); Δ_{OP} là độ lệch tần số gây ra bởi điều kiện hoạt động.

2.3. Khảo sát ảnh hưởng của các nhân tố biến thiên lên tần số RO.

2.3.1. Ảnh hưởng của thăng giáng tức thời

Thăng giáng tức thời (*temporal variation*) là thăng giáng ngẫu nhiên xuất hiện tại bất cứ điều kiện hoạt động nào. Ảnh hưởng này được định lượng qua độ ổn định $\left(1 - \sigma/\mu\right)\left[\times 100\%\right]$, trong đó μ và σ tương ứng là giá trị trung bình và độ lệch chuẩn của phân bố tần số. Hình 2.3 trình bày biểu đồ phân bố của dữ liệu tần số đối với RO_5/IC_1 và biến thiên tỷ số σ/μ đối với 5 IC FPGA Spartan-6. Thăng giáng tức thời có ảnh hưởng không đáng kể tới các tần số RO đo được và có thể bỏ qua trong các phân tích tiếp theo.



Hình 2.3: Biểu đồ phân bố tần số của RO_1/IC_1 với 256 mẫu (a) và tỷ số σ/μ của 32 RO trên 5 IC FPGA Spartan-6 (b)

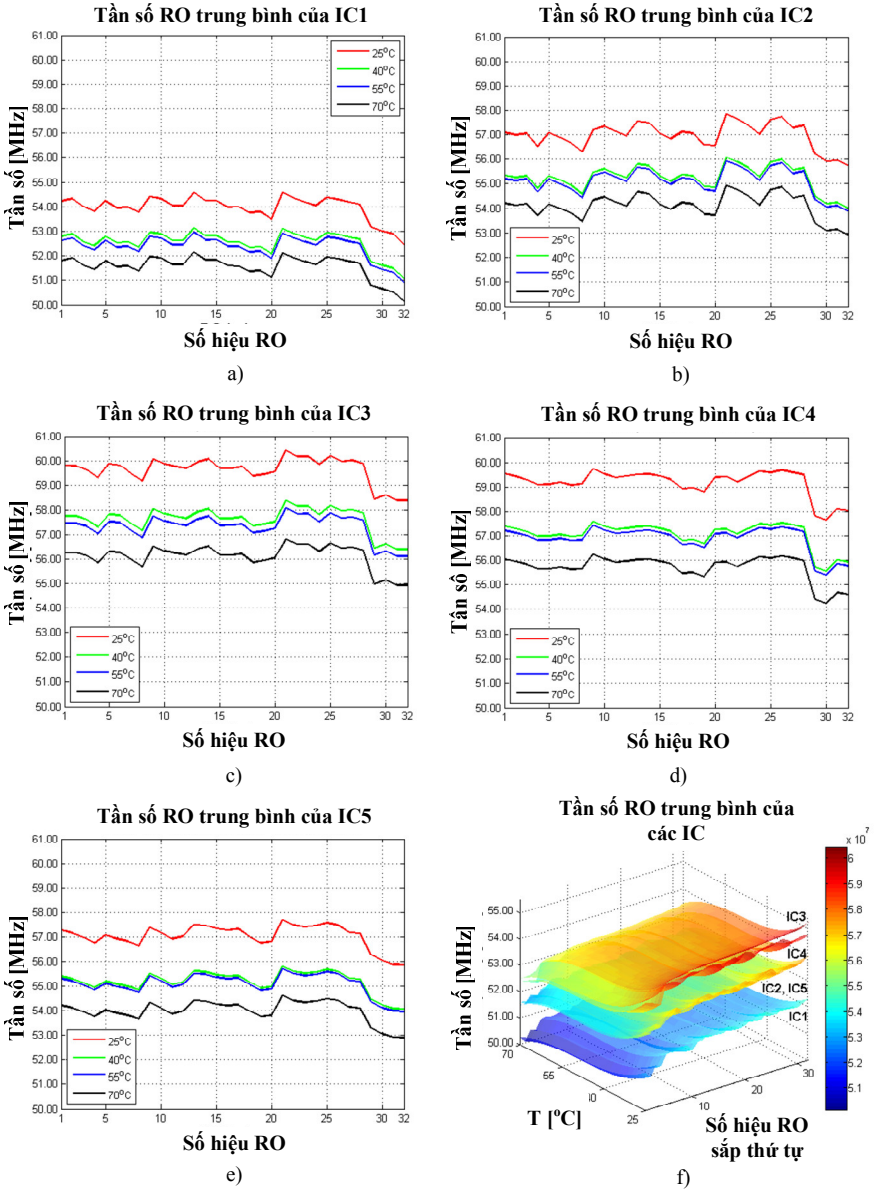
2.3.2. Ảnh hưởng của nhiệt độ môi trường

Khảo sát 5 FPGA Spartan-6 tại 25°C, 40°C, 55°C, và 70°C; 6 FPGA Spartan-3E trong khoảng 25°C – 80°C, bước 5°C. Các phép đo được lặp lại 256 lần với mỗi RO tại mỗi điểm nhiệt độ. Các tần số RO trung bình được biểu diễn trên Hình 2.4(a)-(e) và được kết hợp thành mặt 3D trên Hình 2.4(f). Sự dịch chuyển của các tần số RO trung bình thể hiện giá trị trung bình của Δf_{OP} gây ra bởi điều kiện hoạt động (Phương trình (2.1)). Trị số tuyệt đối của các tần số RO không đặc trưng cho RO; trị số này giảm khi nhiệt độ tăng và ngược lại.

2.3.3. Ảnh hưởng của các biến thiên toàn cục và cục bộ

Với các biến thiên toàn cục (biến thiên giữa các chip), tần số của một RO xác định thay đổi đáng kể giữa các chip. Nhiệt độ là một nhân tố toàn cục do nó tác động đồng đều lên các RO tương tự biến thiên toàn cục xuất hiện từ quá trình chế tạo. Tác động này khá đáng kể nên các tần số RO có tính duy nhất (*uniqueness*) thấp và không thể được sử dụng trực tiếp để đặc trưng cho các cấu kiện vật lý.

Biến thiên cục bộ (biến thiên bên trong chip) được thể hiện qua tương quan của mẫu hình biến thiên tần số RO (dạng đường gấp khúc trên các đồ thị Hình 2.4 (a)-(e). Mẫu hình này của một chip đơn tương đối ổn định đối với nhiệt độ, đồng thời khác biệt giữa các chip khác nhau. Có thể khai thác tính ổn định cao của biến thiên cục bộ mạch RO PUF để tách ra các đặc trưng nguyên bản của IC.



Hình 2.4: (a)-(e) Biến thiên tần số RO, (f) Mô tả 3D của thay đổi tần số RO theo nhiệt độ (25°C, 40°C, 55°C, và 70°C) đo với 5 linh kiện FPGA Spartan-6.

Kết luận chương 2

Chương 2 đề xuất mô hình thống kê của tần số RO. Từ sơ đồ RO PUF truyền thống, nghiên cứu sinh đề xuất thiết kế RO PUF đơn giản, thực thi trên các họ FPGA Xilinx Spartan-3E và Spartan-6 nhằm khảo sát mô hình thống kê của tần số RO trong các điều kiện hoạt động khác nhau, cụ thể là sự thay đổi của nhiệt độ môi trường. Qua phân tích số liệu thực nghiệm, có thể thấy các thăng giáng tức thời có tác động không đáng kể lên tần số RO và có thể bỏ qua. Nhiệt độ và các nhân tố biến thiên toàn cục tác động lớn đến trị số tuyệt đối của tần số RO, tuy nhiên mức độ tác động là đồng đều đối với các RO trong mảng RO và do đó có thể loại bỏ bằng kỹ thuật ghép cặp RO. Chỉ các biến thiên cục bộ mới bền vững trước ảnh hưởng của điều kiện hoạt động và có mẫu hình đặc trưng cho chip FPGA cụ thể. Đây là cơ sở cho việc đề xuất nguyên lý định danh và xác thực thiết bị sẽ được trình bày trong chương 3.

Chương 3: Ứng dụng RO PUF định danh và xác thực ID cho thiết bị

3.1. Cơ sở của việc định danh và xác thực ID cho thiết bị

3.1.1. Phương pháp truyền thống

Độ tin cậy xác thực được đánh giá qua trị số tỷ lệ lỗi cân bằng (*EER: Equal Error Rate)*, độ tin cậy cao khi *EER* nhỏ và ngược lại. ***Độ tin cậy tốt nhất của các phương pháp định danh và xác thực truyền thống[1] tương ứng với*** $EER \approx 10^{-6}$.

3.1.2. Sử dụng độ đo Euclid định lượng một số tham số của RO PUF

Để định lượng sự tương đồng/khác biệt giữa các vectơ mẫu ID, nghiên cứu sinh đề xuất các tham số khoảng cách dựa trên độ đo Euclid sau.

Xét ID có dạng là một vector $(n-1)$ chiều $R\left(\left\{df_i \middle| i=\overline{1,n-1}\right\}\right)$, với $df_i = f_i - f_{i+1}$ là tần số hiệu của cặp tần số RO liên tiếp f_i, f_{i+1}, n là số RO có trong mảng RO. Khoảng cách giữa hai vector R_i và R_j:

$$d\left(R_i, R_j\right) = \sqrt{\sum_{k=1}^{n-1}\left(df_{ik} - df_{jk}\right)^2} \tag{3.1}$$

Trong đó df_{ik}, $i=\overline{1,N}$, $k=\overline{1,n-1}$, là tọa độ thứ k của vector R_i; N là số IC trong tập IC khảo sát. Khoảng cách chuẩn hóa được xác định bởi:

$$d_{norm} = \frac{d\left(R_i, R_j\right)}{2^{k_{norm}}\sqrt{n-1}} \tag{3.2}$$

k_{norm} là hệ số chuẩn hóa: $k_{norm} = \left\lceil \log_2\left(\max\left\{\left|df_{ik}\right|, i=\overline{1,N}, k=\overline{1,n-1}\right\}\right)\right\rceil + 1$

Khoảng cách nội chuẩn hóa giữa vector mẫu ID và vector ID danh định:

$$d_{intra}\left(R_l, R\right) = \frac{d\left(R_l, R\right)}{2^{k_{norm}}\sqrt{n-1}} \tag{3.3}$$

Trong đó R_l là vectơ mẫu ID của lần đo thứ l; R là vectơ ID danh định của IC, được xác định từ thống kê trên tập vector mẫu ID có số phần tử lớn. Trị số mong muốn của d_{intra} là xấp xỉ bằng 0 .

---

[1] Maes, R. (2013). *Physically unclonable functions: Constructions, properties and applications*. Springer Science & Business Media.

Khoảng cách tương quan chuẩn hóa giữa các vector ID danh định được xác định bởi:

$$d_{inter}\left(R_p,R_q\right)=\frac{d\left(R_p,R_q\right)}{2^{k_{norm}}\sqrt{n-1}} \tag{3.4}$$

Với R_p, R_q, $p,q=\overline{1,N}, p\neq q$, tương ứng là vector ID danh định của IC_p và IC_q trong tập IC khảo sát. Trị số mong muốn của d_{inter} là:

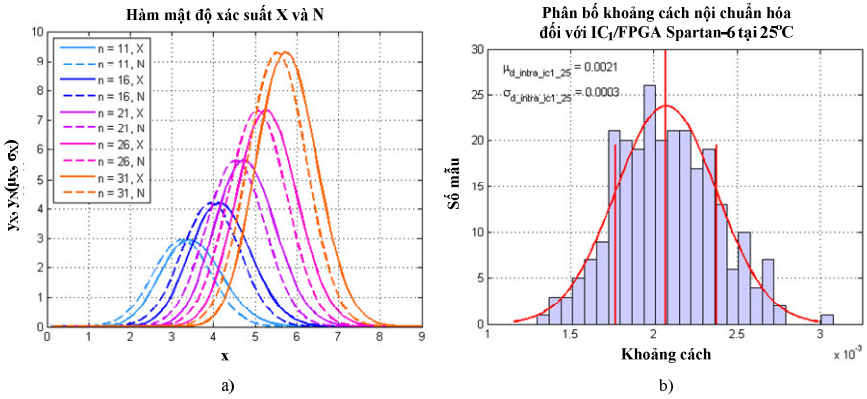
$$\min\left\{d_{inter}\left(R_p,R_q\right),\forall p,q=\overline{1,N},p\neq q\right\}>d_{thr} \tag{3.5}$$

Với d_{thr} là mức ngưỡng xác thực.

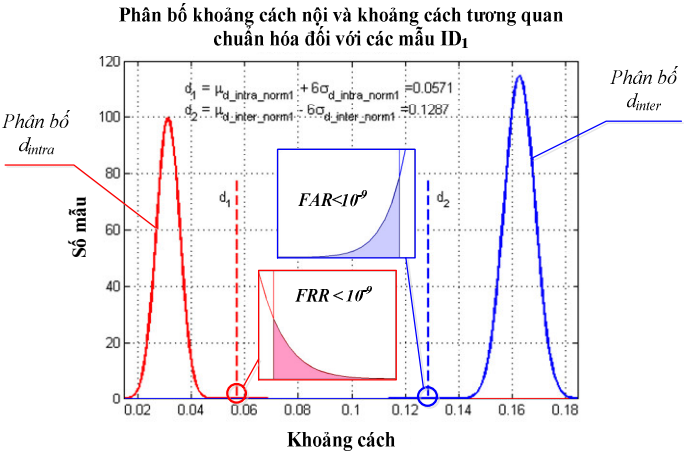
3.1.3. Đặc trưng thống kê của khoảng cách Euclid

Khái quát các thành phần df_i và $\left(df_{ik}-df_{jk}\right)$ thành biến ngẫu nhiên X_i có phân bố chuẩn với giá trị trung bình bằng 0 và phương sai bằng 1.

Xét n biến ngẫu nhiên X_i, $i=\overline{1,n}$, cùng tuân theo quy luật chuẩn hóa $\mathcal{N}\left(0,1\right)$. Khi đó, biến ngẫu nhiên $Y_i=\sqrt{\sum_{i=1}^{n}X_i^2}$ tuân theo quy luật phân bố $\mathcal{X}$ với n bậc tự do. Khi n lớn, Y_i có phân bố chuẩn với giá trị trung bình và phương sai xác định (Hình 3.1).



Hình 3.1: (a) Đồ thị các hàm mật độ xác suất $\mathcal{X}$ và $\mathcal{N}\left(\mu_{\mathcal{X}},\sigma_{\mathcal{X}}\right)$; (b) Biểu đồ phân bố khoảng cách nội chuẩn hóa của một IC FPGA Spartan-6



Hình 3.2: Cơ sở xác định mức ngưỡng xác thực.

Ở mức 6σ (6 lần độ lệch chuẩn tính từ tham số mục tiêu), tỷ lệ bất định chỉ là 2×10^{-9}. Trong phân bố khoảng cách nội chuẩn hóa và khoảng cách tương quan chuẩn hóa, các đường d_1, d_2 xác định ở mức 6σ đảm bảo tỷ lệ chấp nhận nhầm (*FAR: False Acceptance Rate*) và tỷ lệ loại bỏ nhầm (*FRR: False Rejection Rate*) nhỏ hơn 10^{-9}. Có thể chọn $d_1 \le d_{thr} \le d_2$.

Cận dưới của d_{thr} có thể được xác định từ điều kiện:

$$d_{thr} \ge \max\left\{\mu_{d_{inntra\_i}}\right\} + 6\max\left\{\sigma_{d_{inntra\_i}}\right\},\ i=\overline{1,N}, \tag{3.6}$$

$\mu_{d_{inntra\_i}}$ và $\sigma_{d_{inntra\_i}}$: Giá trị trung bình và độ lệch chuẩn của các mẫu thuộc IC_i trong tập IC khảo sát.

Cận trên của d_{thr} cần nhỏ hơn khoảng cách cực tiểu giữa các ID danh định:

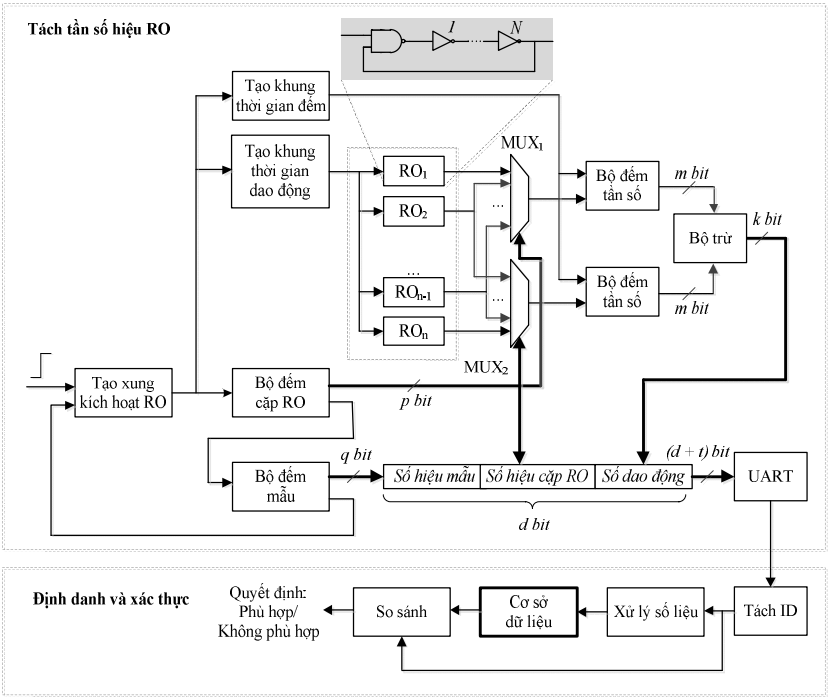
$$d_{thr} \le \min\left\{d_{inter\_i\_j\_norm}\middle|i,j\in\overline{1,N}, i\ne j\right\}, \tag{3.7}$$

$d_{inter\_i\_j\_norm}\middle|i,j\in\overline{1,N}, i\ne j$: Khoảng cách giữa các ID danh định trong tập N IC khảo sát.

Như vậy, chọn d_{thr} từ các điều kiện (3.6) và (3.7) sẽ đảm bảo xác suất để một mẫu ID bị xác thực nhầm nhỏ hơn 2×10^{-9}.

3.2. Thiết kế kỹ thuật sơ đồ định danh và xác thực ID

Hình 3.3 trình bày sơ đồ định danh và xác thực ID ứng dụng RO PUF.



Hình 3.3: Sơ đồ định danh và xác thực ID ứng dụng RO PUF

Sơ đồ gồm hai phần:

- **Mạch tách tần số hiệu RO**

Mạch có nhiệm vụ tạo tần số hiệu RO theo phương pháp ghép cặp liên tiếp, thực thi trên FPGA.

- **Giao thức định danh và xác thực**

- Bộ tách ID chuyển mẫu dữ liệu nối tiếp thu nhận được từ UART thành cấu trúc vector $(n-1)$ chiều, mỗi chiều là trị số tần số hiệu RO.

- Khối Xử lý số liệu tính toán trên tập mẫu vector ID để tạo vector ID danh định, mẫu khoảng cách nội, các khoảng cách tương quan giữa các ID danh định, xác định mức ngưỡng xác thực và lưu vào cơ sở dữ liệu.

- Trong pha xác thực, mẫu ID được kết hợp tuần tự với các ID danh định trong cơ sở dữ liệu và tạo dữ liệu khoảng cách Euclid. Bộ so sánh so sánh khoảng cách này với mức ngưỡng. Nếu khoảng cách nhỏ hơn mức ngưỡng, mẫu ID được coi là tạo bởi IC đã được đăng ký. Nếu khoảng cách lớn hơn mức ngưỡng, mẫu ID được coi là tạo bởi IC chưa đăng ký.

3.3. Thực nghiệm định danh và xác thực ID cho thiết bị

3.3.1. Ước lượng tính ổn định của ID

Thực thi sơ đồ đề xuất trên 4 IC Spartan-6, 6 IC Spartan-3E, 8 IC Artix-7, thu 256 mẫu dữ liệu tần số hiệu df cho mỗi IC tại mỗi điểm nhiệt độ (25^{o}C-80^{o}C, bước 5^{o}C với Spartan-6, Spartan-3E; nhiệt độ phòng với Artix-7). Với mỗi mẫu df, xác định mẫu ID dạng $R=\left\{df_i, i=\overline{1,n-1}\right\}$. Từ tập mẫu ID, xác định ID danh định $R_{nom}=\left\{mean\left(df_i\right), i=\overline{1,n-1}\right\}$; tính các mẫu khoảng cách nội chuẩn hóa từ mỗi mẫu ID tới ID danh định theo công thức (3.3). Các tham số thống kê được trình bày trong Bảng 3.1 và Bảng 3.2.

Bảng 3.1: Giá trị trung bình của khoảng cách nội chuẩn hóa $\left[\times 10^{-3}\right]$ (Spartan-6)

	25^{o}C	**30^{o}C**	**35^{o}C**	**40^{o}C**	**45^{o}C**	**50^{o}C**	**55^{o}C**	**60^{o}C**	**65^{o}C**	**70^{o}C**	**75^{o}C**	**80^{o}C**
IC_1	*2,1*	*2,1*	*2,1*	*2,0*	*2,0*	*2,0*	*1,9*	*1,9*	*1,9*	*1,9*	*1,8*	*1,8*
IC_2	*2,1*	*2,1*	*2,1*	*2,1*	*2,1*	*2,1*	*2,1*	*2,0*	*2,0*	*2,0*	*2,1*	*2,0*
IC_3	*2,1*	*2,1*	*1,9*	*2,1*	*2,1*	*2,0*	*2,0*	*2,1*	*1,9*	*1,9*	*1,9*	*1,9*
IC_4	*2,3*	*2,0*	*2,0*	*2,1*	*2,1*	*2,0*	*2,0*	*2,1*	*1,9*	*1,9*	*2,0*	*1,9*

Bảng 3.2: Độ lệch chuẩn của khoảng cách nội chuẩn hóa $\left[\times 10^{-4}\right]$ (FPGA Spartan-6)

	25^{o}C	**30^{o}C**	**35^{o}C**	**40^{o}C**	**45^{o}C**	**50^{o}C**	**55^{o}C**	**60^{o}C**	**65^{o}C**	**70^{o}C**	**75^{o}C**	**80^{o}C**
IC_1	*3,04*	*3,64*	*3,20*	*3,26*	*3,11*	*3,06*	*3,32*	*2,86*	*3,03*	*3,12*	*2,90*	*2,75*
IC_2	*3,30*	*3,46*	*3,16*	*3,04*	*3,41*	*3,49*	*3,14*	*3,19*	*3,22*	*2,85*	*3,30*	*3,13*
IC_3	*3,21*	*6,84*	*3,10*	*3,24*	*3,36*	*3,42*	*3,01*	*3,55*	*3,12*	*2,88*	*2,80*	*2,95*
IC_4	*6,40*	*3,06*	*3,28*	*3,06*	*3,19*	*3,16*	*3,43*	*3,09*	*3,58*	*2,84*	*3,13*	*3,17*

Bảng 3.3: Tham số thống kê khoảng cách nội chuẩn hóa $\left[\times 10^{-3}\right]$ khi định danh và xác thực tại điều kiện nhiệt độ bất kỳ (FPGA Spartan-6)

Tham số	**IC_1**	**IC_2**	**IC_3**	**IC_4**
$\mu_{d_{intra}}$	*4,9*	*6,2*	*5,9*	*5,3*
$\sigma_{d_{intra}}$	*1,8*	*2,5*	*2,3*	*2,2*

Bảng 3.4: Xác định mức ngưỡng xác thực $\left[\times 10^{-3}\right]$

Điều kiện thực nghiệm	Tham số	FPGA Spartan-6	FPGA Spartan-3E	FPGA Artix-7
Tại nhiệt độ nhất định	$\max\left\{\mu_{d_{intra}}\right\}$	*2,3*	*8,0*	-
	$\max\left\{\sigma_{d_{intra}}\right\}$	*0,7*	*2,9*	-
	d_{thr}	*6,4*	*25,5*	-
Trên toàn dải nhiệt độ	$\max\left\{\mu_{d_{intra}}\right\}$	*6,2*	*10,0*	*0,99*
	$\max\left\{\sigma_{d_{intra}}\right\}$	*2,5*	*3,4*	*0,44*
	d_{thr}	*21,1*	*30,3*	*3,60*

Chọn mức ngưỡng: $d_{thr} = \max\left\{\mu_{d_{intra}}\right\} + 6 \times \max\left\{\sigma_{d_{intra}}\right\}$ (3.8)

Khi định danh và xác thực trong cùng điều kiện nhiệt độ, $\max\left\{\mu_{d_{intra}}\right\}$ và $\max\left\{\sigma_{d_{intra}}\right\}$ được chọn là các giá trị lớn nhất của Bảng 3.1 và Bảng 3.2. Khi định danh và xác thực tại nhiệt độ bất kỳ, $\max\left\{\mu_{d_{intra}}\right\}$ và $\max\left\{\sigma_{d_{intra}}\right\}$ được chọn từ tham số thống kê dữ liệu tần số hiệu tổng hợp (Bảng 3.3). Mức ngưỡng xác thực khi này có thể lớn hơn so với trường hợp trước. Mức ngưỡng xác thực đối với các FPGA khác nhau được tổng hợp trong Bảng 3.4.

3.3.2. Ước lượng tính duy nhất của ID

Các ID danh định đảm bảo tính duy nhất khi mức ngưỡng xác thực nhỏ hơn khoảng cách chuẩn hóa cực tiểu giữa chúng (Bảng 3.5). Tại 25°C, khoảng cách chuẩn hóa cực tiểu là $105,9 \times 10^{-3}$ (IC_1-IC_2) lớn hơn mức ngưỡng $6,4 \times 10^{-3}$ (Bảng 3.4) $\sim 16,5$ lần.

Thực nghiệm trên toàn dải nhiệt độ, khoảng cách chuẩn hóa giữa các ID danh định của 4 IC Spartan-6 được trình bày trong Bảng 3.6. Khoảng cách cực tiểu giữa các các ID danh định là $101,9 \times 10^{-3}$ (IC_1- IC_2), lớn hơn các mức ngưỡng (Bảng 3.4) $\sim 15,9$ và $\sim 4,8$ lần khi xác thực tại cùng nhiệt độ và tại nhiệt độ bất kỳ. Bảng 3.7 trình bày khoảng cách chuẩn hóa giữa các ID của các IC Spartan-3E, Artix-7. Có thể thấy khoảng cách chuẩn hóa cực tiểu lớn hơn nhiều lần mức ngưỡng khi xác thực tại cùng nhiệt độ và tại nhiệt độ bất kỳ.

Bảng 3.5: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$ tại điều kiện thực nghiệm xác định (FPGA Spartan-6)

	25°C			**30°C**			**35°C**		
	IC_2	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**
IC_1	*105,9*	*113,1*	*150,8*	*105,0*	*112,4*	*150,4*	*105,2*	*112,5*	*149,7*
IC_2		*112,9*	*161,6*		*113,1*	*162,4*		*112,7*	*161,1*
IC_3			*177,0*			*176,5*			*175,6*
	40°C			**45°C**			**50°C**		
	IC_2	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**
IC_1	*105,7*	*112,6*	*148,9*	*106,8*	*112,8*	*148,3*	*106,2*	*112,9*	*147,2*
IC_2		*112,2*	*160,3*		*111,4*	*159,4*		*110,5*	*157,4*
IC_3			*174,9*			*174,4*			*172,6*
	55°C			**60°C**			**65°C**		
	IC_2	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**
IC_1	*105,9*	*113,1*	*145,8*	*106,2*	*113,1*	*146,0*	*106,8*	*113,7*	*145,1*
IC_2		*109,4*	*156,0*		*109,3*	*155,7*		*108,7*	*154,7*
IC_3			*171,6*			*170,1*			*169,5*
	70°C			**75°C**			**80°C**		
	IC_2	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**	**IC_2**	**IC_3**	**IC_4**
IC_1	*107,4*	*114,0*	*145,0*	*107,7*	*114,1*	*143,7*	*108,4*	*114,1*	*143,3*
IC_2		*108,1*	*153,2*		*107,9*	*152,2*		*107,1*	*151,1*
IC_3			*168,2*			*167,4*			*166,6*

Bảng 3.6: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$ (Spartan-6)

IC_2	**IC_3**	**IC_4**	
101,9	*108,0*	*142,3*	**IC_1**
	108,2	*154,7*	**IC_2**
		169,2	**IC_3**

Bảng 3.7: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$ (Spartan-6, Artix-7)

FPGA Spartan-3E						**FPGA Artix-7**							
IC_2	**IC_3**	**IC_4**	**IC_5**	**IC_6**		**IC_2**	**IC_3**	**IC_4**	**IC_5**	**IC_6**	**IC_7**	**IC_8**	
146,1	*176,5*	*103,5*	*187,2*	*162,5*	**IC_1**	*21,8*	*13,3*	*17,0*	*16,2*	*22,6*	*17,5*	*16,7*	**IC_1**
	203,9	*161,8*	*234,9*	*160,2*	**IC_2**		*20,0*	*27,7*	*16,7*	*27,0*	*20,2*	*23,8*	**IC_2**
		154,4	*207,0*	*209,5*	**IC_3**			*18,2*	*12,3*	*20,6*	*16,5*	*16,8*	**IC_3**
			161,8	*161,3*	**IC_4**				*19,9*	*21,0*	*19,8*	*14,3*	**IC_4**
				185,4	**IC_5**					*17,9*	*16,2*	*15,7*	**IC_5**
											21,4	*18,1*	**IC_6**
												16,8	**IC_7**

3.3.3. So sánh mức tiêu thụ tài nguyên phần cứng

Mạch tách tần số hiệu được thực thi trên các FPGA Xilinx Spartan-6, Spartan-3E, và Artix-7 (Công nghệ 45 nm, 90 nm, 28 nm tương ứng). Thiết kế tham chiếu được thực thi trên ASIC (Công nghệ CMOS 65 nm công suất thấp của TSMC). Vì các được thực thi trên các công nghệ khác nhau, việc so sánh mức tiêu thụ tài nguyên phần cứng chỉ giới hạn ở so sánh quy mô của thiết kế. Thiết kế tham chiếu chiếm 0,241 mm^2 (10,7%) diện tích bán dẫn, gồm 4096 RO và các mạch điều khiển, giao tiếp, mỗi RO gồm 80 bộ đảo và một cổng NAND. Các RO được phân vào 16 nhóm×256 RO, mỗi nhóm có một bộ chọn kênh 256:1 và một bộ đếm tần số RO. Như vậy, thiết kế đề xuất nhỏ gọn hơn và do đó chiếm ít diện tích bán dẫn và tiêu thụ ít năng lượng hơn thiết kế tham chiếu.

3.3.4. Đánh giá hiệu quả của phương pháp

- RO PUF có độ đồng nhất trong cấu trúc vật lý cao với việc sử dụng kỹ thuật *hard macro*.

- Việc sử dụng tần số hiệu thay vì các trị số tuyệt đối của tần số giúp loại trừ được ảnh hưởng của biến thiên nhiệt độ môi trường lên đáp ứng của RO PUF.

- Nhờ sử dụng biên độ thay cho hàm dấu nên khai thác được nhiều thông tin hơn trong dữ liệu PUF với cùng số lượng các RO được sử dụng, giữ cho thiết kế nhỏ gọn với số lượng hạn chế các RO cần dùng, đạt hiệu quả về năng lượng tiêu thụ và diện tích bán dẫn.

- Việc sử dụng khoảng cách Euclid thay cho khoảng cách Hamming giúp khai thác tốt hơn dữ liệu tần số RO. Sơ đồ xác thực sử dụng mức ngưỡng dựa trên khoảng cách Euclid cho phép xác thực chính xác với độ tin cậy cao hơn các phương pháp đã có, thể hiện qua xác suất xác thực nhầm nhỏ hơn 2×10^{-9}, giảm ít nhất 3 bậc độ lớn so với trị số *EER* nhỏ nhất trong thiết kế tham chiếu.

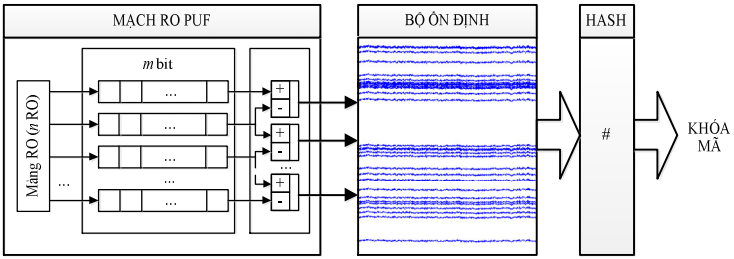
Kết luận chương 3

Trên cơ sở kết quả phân tích lý thuyết và thực nghiệm về các yếu tố ảnh hưởng đến tần số RO trong chương 2, chương 3 đề xuất thiết kế ứng dụng RO PUF định danh và xác thực ID dựa trên việc sử dụng các tham số độ đo Euclid. Mức ngưỡng được xác định chặt chẽ từ tiêu chuẩn thống kê, đảm bảo độ tin cậy xác thực cao hơn so với các phương pháp đã có. Thiết kế kết hợp thực thi mảng RO trên chip và việc xử lý số liệu trên máy tính, do vậy có tính gọn nhẹ, tiêu thụ ít tài nguyên phần cứng và năng lượng, đồng thời có thể được chuyển đổi linh hoạt giữa các nền tảng phần cứng.

Chương 4: Kỹ thuật ổn định chuỗi bit trích xuất từ RO PUF

4.1. Khảo sát về tính ổn định và các phương pháp ổn định chuỗi bit của RO PUF

Cần tạo chuỗi bit ổn định trên chip từ các mẫu vector ID thu nhận được. Các mẫu này luôn có sự thăng giáng nhỏ do tần số RO có bản chất là đại lượng thống kê.



Hình 4.1: Thủ tục tạo khóa mã từ dữ liệu PUF và sử dụng hàm băm

Mô hình tổng quát quá trình tạo khóa mã được trình bày trên Hình 4.1. Các tần số RO tuyệt đối và các tần số hiệu được đo, tính toán trên chip. Các chuỗi bit trong dữ liệu tần số hiệu thay đổi nhỏ qua mỗi lần kích hoạt mạch. Bộ ổn định (*stabilizer*) tạo chuỗi bit ra ổn định và duy nhất, khi được tác động bởi hàm băm (*hash*) sẽ tạo ra khóa mã ngẫu nhiên và bí mật. Trong chương này, nghiên cứu sinh trình bày các thuật toán và giải pháp kỹ thuật ổn định chuỗi bit ra của một sơ đồ RO PUF.

4.2. Các phương pháp ổn định chuỗi bit ra mạch RO PUF

* Phương pháp trung bình mẫu

Giả sử tần số hiệu RO danh định của cặp RO_j là df_{j0}, $j = \overline{1, n_{ring} - 1}$, với n_{ring} là số RO trong mảng RO. Tần số hiệu RO_j của mẫu thứ i là:

$$df_{ij} = df_{j0} + \delta_{ij} \tag{4.1}$$

Với δ_{ij} là sai lệch của trị số mẫu đối với tần số hiệu danh định. Tần số hiệu trung bình của RO_j được xác định bởi:

$$df_{mean,j} = \frac{1}{n_{sample}} \sum_{i=1}^{n_{sample}} df_{ij} = df_{j0} + \frac{1}{n_{sample}} \sum_{i=1}^{n_{sample}} \delta_{ij} \tag{4.2}$$

Bảng 4.1: Thuật toán tính giá trị trung bình của tần số hiệu RO

Bước	Tác vụ
1	Khởi tạo mảng RO.
2	Thu nhận dữ liệu df .
3	Đặt mẫu df đầu tiên làm giá trị tham chiếu (dạng chuỗi bit): $df_{j0} = df_{1j}$
4	Tính $\Delta_i = df_{ij} - df_{j0}$, $i = \overline{1, n_{sample}}$
5	Tính $\Delta = \sum_{i=1}^{n_{sample}} \Delta_i = \sum_{i=1}^{n_{sample}} df_{ij} - n_{sample} df_{j0}$
6	Tính $df_{mean,j} = \frac{1}{n_{sample}} \sum_{i=1}^{n_{sample}} df_{ij} = \frac{\Delta}{n_{sample}} + df_{j0}$
7	Loại bỏ phần biến thiên trong $df_{mean,j}$ ở bước 6 để nhận được $df_{mean,j}$ trung bình

Với n_{sample} là số mẫu tần số hiệu RO. Trị số cực đại của $\left| \frac{1}{n_{sample}} \sum_{i=1}^{n_{sample}} \delta_{ij} \right|$ đối với tất cả các cặp RO xác định số bit cần loại bỏ để thu được chuỗi bit duy nhất.

*** Thuật toán tách chuỗi bit ổn định bằng cách loại bỏ phần thăng giáng trong dữ liệu tần số hiệu**

Phương pháp trực tiếp tách ra chuỗi bit ổn định là loại bỏ phần thăng giáng trong dữ liệu tần số hiệu RO. Từ thực nghiệm, tiến hành xác định độ dài dữ liệu thăng giáng N_{EX} xét ở trường hợp xấu nhất và loại bỏ. Chuỗi bit được tạo thành bằng cách kết hợp các phần không đổi của df .

*** Thuật toán tách chuỗi bit ổn định sử dụng mặt nạ dữ liệu thích nghi**

Vì các giá trị mẫu df khác biệt nhau một số bit trọng số nhỏ, có thể tách ra chuỗi bit không đổi bằng cách áp dụng mặt nạ dữ liệu lên các giá trị mẫu df . Thuật toán tạo mặt nạ dữ liệu df được trình bày trong Bảng 4.2. Chuỗi bit thành phần ổn định được tách ra bằng cách kết hợp df_{j0} và mặt nạ qua một thủ tục được gọi là trích xuất khóa mã:

$$key0_{ij,k} = \begin{cases} df_{j0,k} & ,mask_{ij,k} = 1 \\ 0 & ,mask_{ij,k} = 0 \end{cases} \quad (4.3)$$

Trong đó, $mask_{ij,k}$ là bit thứ k của mặt nạ thành phần $mask_{ij}$ tương ứng với mẫu thứ i của tần số hiệu RO_j. Chuỗi bit toàn phần được ghép bởi các chuỗi bit đơn. Để tăng tính ổn định của chuỗi bit ra, có thể kết hợp kỹ thuật lấy trung bình vào thuật toán Bảng 4.2

*** Thuật toán trích xuất phần tử lặp lại nhiều nhất từ phân bố thống kê**

Hiện tượng đột biến trong dữ liệu df thường xảy ra tại các biên của trị số lũy thừa 2, đặc biệt khi số bit dữ liệu df cần cắt bỏ không đủ lớn. Để khắc phục, nghiên cứu sinh đề xuất phương pháp trích xuất phần dữ liệu lặp lại nhiều nhất từ phân bố thống kê các mẫu dữ liệu df sau cắt bit (Bảng 4.3).

4.3. Thực thi thiết kế tạo chuỗi bit ổn định trên FPGA

Thiết kế tạo chuỗi bit ổn định bằng phương pháp cắt bit kết hợp lấy trung bình mẫu df và phương pháp mặt nạ dữ liệu được thực thi trên FPGA Xilinx Artix-7. Mảng RO được thiết kế với cùng phương pháp như đối với mạch tách tần số hiệu RO trên FPGA Artix-7.

Bảng 4.2: Thuật toán tạo mặt nạ dữ liệu thích nghi với dữ liệu tần số hiệu đầu vào.

Bước	Tác vụ
1	Khởi tạo mảng RO.
2	Thu nhận dữ liệu df: $(df)_{n_{sample} \times (n_{ring}-1)}$
3	Với mỗi RO_j, đặt mẫu df đầu tiên df_{1j} làm giá trị tham chiếu (dạng chuỗi bit): $df_{j0} = df_{1j}$
4	Đối với mỗi mẫu df_{ij} tính: $df_{xor\_ij} = df_{ij} \oplus df_{j0}$
5	Tính các mặt nạ trung gian: $mask\_temp_j = \bigcup_{i=1}^{n} df_{xor\_ij}, j = \overline{1, n_{ring}-1}$ Lọc bỏ tất cả các bit {0} trong khoảng giới hạn bởi các bit {1} của $mask\_temp_j$ để nhận được $mask\_temp1_j$.
6	Đảo bit $mask\_temp1_j$ để nhận được mặt nạ cần tạo $(mask)$

Bảng 4.3: Thuật toán tách chuỗi bit ổn định từ các phần dữ liệu lặp lại nhiều nhất

Bước	Tác vụ
1	Khởi tạo mảng RO.
2	for $i = 1$ to n_{ic} for $j = 1$ to n_{key_sample} for $k = 1$ to n_{sample} Tính df_{mean} từ các trị số mẫu df ; end; Tách chuỗi bit $df_{1,mean}$ từ df_{mean} bằng phương pháp cắt bit, lưu $df_{1,mean}$ vào RAM; end; end;
3	Tính phân bố tần số của $df_{1,mean}$.
4	Tách các mẫu $df_{1,mean}$ có tần suất xuất hiện lớn nhất, gán bằng $df_{2,mean}$
5	Ghép các phần tử $df_{2,mean}$ để tạo chuỗi bit ra

Ghi chú: n_{ic} : Số IC; n_{key_sample} : Số mẫu khóa mã; n_{sample} : Số mẫu df

Kết luận chương 4

Chương 4 đề xuất các giải pháp kỹ thuật và thuật toán ổn định chuỗi bit tạo ra bởi RO PUF để có thể tạo khóa mã hoặc tạo mã khởi tạo phục vụ các ứng dụng mã hóa hoặc tạo số ngẫu nhiên. Phương pháp loại bỏ phần thăng giáng bằng cách cắt đi một số không đổi các bit trọng số thấp trong dữ liệu tần số hiệu dựa trên giả thiết các tần số hiệu RO có mức thăng giáng tương đương. Nhằm thích ứng với mức thăng giáng không đều trong dữ liệu tần số hiệu và tăng độ dài chuỗi bit ra, phương pháp mặt nạ dữ liệu dựa trên thuật toán tạo mặt nạ cập nhật theo mẫu dữ liệu đến. Phương pháp tần xuất cực đại dựa trên phân tích thống kê chọn giữ lại phần ổn định trong dữ liệu tần số hiệu. Các phương pháp trên có thể được kết hợp với kỹ thuật lấy trung bình mẫu nhằm loại bỏ các dữ liệu đột biến và tăng tính ổn định của chuỗi bit tách ra.

Chuỗi bit tạo ra có tính ngẫu nhiên cao, không thể dự đoán, đảm bảo tính duy nhất và có thể được tạo trực tiếp trên chip mà không cần phải có thêm các mô-đun phụ trợ. Kết quả thực nghiệm khẳng định hiệu quả của các phương pháp ổn định chuỗi bit.

KẾT LUẬN

I. Một số kết quả đạt được của luận án

1. Xây dựng mô hình thống kê của tần số RO, phân tích định tính và định lượng mức độ ảnh hưởng của nhiệt độ môi trường, điều kiện hoạt động lên các thành phần trong tần số RO. Từ đó chỉ ra, chỉ các thành phần biến thiên cục bộ mới bền vững trước các nhân tố tác động và đặc trưng cho thiết bị, có thể được sử dụng để tách ra ID cho thiết bị.

2. Đề xuất sơ đồ tách và xác thực ID cho thiết bị sử dụng mạch RO PUF thực thi trên FPGA, trong đó sử dụng các tham số khoảng cách và mức ngưỡng xác thực dựa trên độ đo Euclid. Kết quả thực nghiệm cho thấy phương pháp đề xuất đã nâng cao hiệu năng tách và xác thực ID trên hai phương diện:

- Giao thức tách và xác thực ID rõ ràng, định lượng các tham số khoảng cách và mức ngưỡng với độ chính xác cao, khắc phục hạn chế của việc sử dụng độ đo Hamming là lượng tử hóa các tham số khoảng cách.

- Độ tin cậy xác thực cao (được định lượng qua xác suất xác thực nhầm thiết bị, trị số này nhỏ hơn nhiều 2×10^{-9}) so với các thiết kế đã có.

3. Đề xuất các phương pháp ổn định chuỗi bit tạo ra bởi RO PUF để có thể tạo khóa mã hoặc tạo mã khởi tạo, phục vụ các ứng dụng mã hóa hoặc tạo số ngẫu nhiên. Chuỗi bit tạo ra có tính ngẫu nhiên cao, không thể dự đoán, đảm bảo tính duy nhất và có thể được tạo trực tiếp trên chip mà không cần phải có thêm phần cứng phụ trợ.

II. Hướng phát triển tiếp theo

Trên cơ sở những kết quả đã đạt được, trong các nghiên cứu tiếp theo về RO PUF, nghiên cứu sinh sẽ khắc phục những hạn chế và đề xuất một số nội dung nghiên cứu mới.

1. Tiếp tục cải tiến, nâng cao hiệu quả phương pháp định danh và xác thực thiết bị ứng dụng RO PUF, thực thi các kỹ thuật ổn định chuỗi bit trên FPGA.

2. Nghiên cứu ứng dụng RO PUF trong bảo vệ lõi IP, tạo số ngẫu nhiên thực sự, tạo khóa bảo mật phù hợp với các ứng dụng cụ thể.

3. Thực thi RO PUF trên công nghệ ASIC nhằm nâng cao hơn nữa hiệu năng RO PUF, khắc phục những hạn chế của công nghệ FPGA.

4. Thực thi các hình thức tấn công đối với mạch RO PUF để kiểm nghiệm và đề xuất các giải pháp nâng cao độ tin cậy của các thiết kế ứng dụng RO PUF.