BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

TRẦN VĂN TOÀN

NGHIÊN CỨU NÂNG CAO HIỆU NĂNG RO PUF DÙNG TRONG BẢO MẬT PHẦN CỨNG

LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – 2023

BỘ GIÁO DỤC VÀ ĐÀO TẠO BỘ QUỐC PHÒNG

HỌC VIỆN KỸ THUẬT QUÂN SỰ

TRẦN VĂN TOÀN

NGHIÊN CỨU NÂNG CAO HIỆU NĂNG RO PUF DÙNG TRONG BẢO MẬT PHẦN CỨNG

LUẬN ÁN TIẾN SĨ KỸ THUẬT

Chuyên ngành: KỸ THUẬT ĐIỆN TỬ

Mã số: 9 52 02 03

NGƯỜI HƯỚNG DẪN KHOA HỌC:

PGS. TS. HOÀNG VĂN PHÚC

HÀ NỘI – 2023

LỜI CAM ĐOAN

Tôi cam đoan luận án và các kết quả trình bày trong luận án là công trình nghiên cứu của tôi dưới sự hướng dẫn của các cán bộ hướng dẫn. Các số liệu, kết quả trình bày trong luận án là hoàn toàn trung thực và chưa được công bố trong bất cứ công trình nào trước đây. Các kết quả dùng để tham khảo đều đã được trích dẫn đầy đủ và theo đúng quy định.

Hà Nội, ngày 24 tháng 3 năm 2023

Tác giả

Trần Văn Toàn

LỜI CẢM ƠN

Trong quá trình học tập, nghiên cứu và thực hiện luận án, nghiên cứu sinh đã nhận được nhiều sự giúp đỡ và đóng góp quý báu.

Trước tiên, nghiên cứu sinh xin bày tỏ lòng biết ơn sâu sắc đến thầy giáo, PGS. TS. Hoàng Văn Phúc bởi những chỉ dẫn sâu sắc trong định hướng nghiên cứu. Xin chân thành cảm ơn thầy giáo, PGS. TS. Trịnh Quang Kiên bởi sự hướng dẫn chi tiết và kịp thời về nội dung nghiên cứu.

Nghiên cứu sinh cũng chân thành cảm ơn các thầy giáo trong khoa Vô tuyến điện tử, tập thể bộ môn Kỹ thuật Vi xử lý, Khoa Vô tuyến điện tử, Học viện Kỹ thuật Quân sự bởi sự giúp đỡ tận tình, tạo điều kiện mọi mặt cho quá trình học tập, nghiên cứu; chân thành cảm ơn cán bộ Phòng thí nghiệm Bộ môn Công nghệ hóa học, Khoa Hóa - Lý Kỹ thuật, Học viện Kỹ thuật Quân sự đã tạo điều kiện cho nghiên cứu sinh sử dụng trang thiết bị của Phòng thí nghiệm để tiến hành các thực nghiệm.

Nghiên cứu sinh chân thành cảm ơn Phòng Sau đại học, Học viện Kỹ thuật Quân sự bởi sự hỗ trợ kịp thời, giúp nghiên cứu sinh đảm bảo tiến độ học tập; cảm ơn Hệ Quản lý học viên sau đại học, Học viện Kỹ thuật Quân sự đã tạo nhiều thuận lợi trong công tác. Cuối cùng, nghiên cứu sinh bày tỏ lòng biết ơn đối với gia đình, bạn bè, đồng nghiệp, lãnh đạo chỉ huy khoa Kỹ thuật cơ sở, Học viện Phòng không - Không quân bởi sự động viên tinh thần quý báu và tạo điều kiện mọi mặt.

Xin chân thành cảm ơn!

MỤC LỤC

DANH MỤC CÁC TỪ VIẾT TẮT

Từ viết tắt	Tiếng Anh	Tiếng Việt
APUF	Arbiter PUF	PUF trọng tài
ASIC	Application-Specific Integrated Circuit	Mạch tích hợp chuyên dụng
BPUF	Butterfly PUF	PUF với các bộ chốt ghép chéo
BR PUF	Bistable Ring PUF	PUF mạch vòng ổn định kép
BRAM	Block RAM	RAM khối
CCD	Charge-Coupled Device	Linh kiện ghép điện tích
CNN PUF	Convolutional Neural Network PUF	PUF sử dụng mạng nơron tích chập
CoLPUF	Configurable LFSR-based PUF	PUF dựa trên LFSR có thể cấu hình
CRO PUF	Configurable RO PUF	RO PUF có thể cấu hình
CRP	Challenge-Response Pair	Cặp mẫu kích thích – mẫu đáp ứng
DFF PUF	D Flip Flop PUF	PUF dựa trên FF D
DRAM	Dynamic RAM	RAM động
ECC	Error Correcting Code	Mã sửa lỗi

EER	Equal Error Rate	Tỷ lệ lỗi cân bằng
FAR	False Acceptance Rate	Tỷ lệ chấp nhận nhầm
FF	Flip Flop	Mạch lật
FF PUF	Flip Flop PUF	PUF dựa trên Flip Flop
FFXORPUF	Feed-Forward XOR PUF	PUF tiếp thuận, ghép cổng XOR các đầu ra
FPGA	Field Programable Gate Array	Mảng cổng logic khả trình
FRR	False Rejection Rate	Tỷ lệ loại bỏ nhầm
FSM	Finite State Machine	Máy trạng thái hữu hạn
HDL	Hardware Description Language	Ngôn ngữ mô tả phần cứng
IC	Integrated Circuit	Mạch tích hợp
ID	Identity, Identification	Định danh
IoT	Internet of Things	Interner vạn vật
IPUF	Interpose PUF	PUF xen kẽ
LFSR	Linear Feedback Shift Register	Thanh ghi dịch hồi tiếp tuyến tính
LUT	Look-Up Table	Bảng tra
LPUF	Latch PUF	PUF dựa trên bộ chốt
MEMS PUF	Micro-Electro-Mechanical Systems PUF	PUF sử dụng cảm biến vi cơ điện tử

MOSFET	Metal Oxide Semiconductor Field Effect Transistor	Transistor hiệu ứng trường dựa trên mặt ghép ôxit kim loại – bán dẫn
MUX	Multiplexer	Bộ ghép kênh
NEMS PUF	Nano-Electro-Mechanical Switch PUF	PUF sử dụng chuyển mạch vi cơ điện tử
PDL	Programmable Delay Line	Đường giữ chậm khả trình
POF	Physical One-way Function	Hàm vật lý một chiều
PRF	Pseudo-Random Function	Hàm giả ngẫu nhiên
PRNG	Pseudo-Random Number Generator	Bộ tạo số giả ngẫu nhiên
PUF	Physically Unclonable Function	Mạch tạo hàm không thể sao chép về vật lý
RAM	Random Access Memory	Bộ nhớ truy xuất ngẫu nhiên
RF-DNA PUF	Radio-Frequency DNA PUF	PUF DNA tần số vô tuyến
RNG	Random Number Generator	Bộ tạo số ngẫu nhiên
RO	Ring Oscillator	Bộ/mạch dao động vòng
RO PUF	Ring Oscillator PUF	PUF dao động vòng
ROC	Receiver-Operating Characteristic	Đặc tuyến hoạt động
ROM	Read-Only Memory	Bộ nhớ chỉ đọc

SoC	System-on-Chip	Hệ thống trên chip
SRAM	Static RAM	RAM tĩnh
TDC	Time-to-Digital Converter	Bộ chuyển đổi thời gian-số
TERO PUF	Transient Effect Ring Oscillator PUF	PUF dao động vòng dựa trên hiệu ứng quá độ
TV PUF	Threshold Voltage PUF	PUF sử dụng điện áp ngưỡng
UART	Universal Asynchronous Receiver-Transmitter	Giao diện truyền số liệu nối tiếp không đồng bộ
XRRO PUF	XOR Reconfiguration RO PUF	RO PUF tái cấu hình sử dụng cổng XOR

DANH MỤC HÌNH VẼ

DANH MỤC BẢNG

DANH MỤC KÝ HIỆU TOÁN HỌC

Ký hiệu	Ý nghĩa
f_{RO}	Tần số mạch dao động vòng
$f_{nominal}$	Tần số danh định
Δf_{local}	Biến thiên tần số cục bộ
Δf_{global}	Biến thiên tần số toàn cục
Δf_{OP}	Biến thiên tần số gây ra bởi điều kiện hoạt động
N	Số bộ đảo trong mạch RO
n	Số RO trong mảng RO
m	Độ rộng dữ liệu đếm của bộ đếm tần số RO
q	Độ rộng dữ liệu đếm của bộ đếm mẫu
p	Độ rộng dữ liệu điều khiển bộ chọn kênh RO
ΔT_{mea}	Khoảng thời gian đếm của bộ đếm tần số RO
f	Tần số
df	Tần số hiệu/Gia số tần số
d_{intra}	Khoảng cách nội
d_{inter}	Khoảng cách tương quan
μ	Trung bình thống kê
σ	Độ lệch chuẩn
d_{thr}	Mức ngưỡng
n_{ic}	Số IC khảo sát
n_{sample}	Số mẫu
n_{key_sample}	Số mẫu khóa mã

DANH MỤC CÁC THUẬT NGỮ VÀ ĐỊNH NGHĨA

Thuật ngữ	Ý nghĩa
Bảo vệ IP sử dụng PUF (*PUF-based IP protection*)	Sử dụng kỹ thuật PUF bảo vệ quyền sở hữu trí tuệ về mặt kỹ thuật, như bảo vệ sự toàn vẹn và chống sao chép file **.bit* dùng để cấu hình phần cứng FPGA.
Chuỗi khởi tạo (*Seed*)	Số ngẫu nhiên được dùng để khởi tạo bộ tạo số giả ngẫu nhiên
Đặc tuyến hoạt động (*Receiver-Operating Characteristic*)	Đồ thị biểu diễn hàm FRR theo FAR, thể hiện tương quan giữa tính ổn định và tính duy nhất trong định danh và xác thực thiết bị sử dụng PUF.
Đáp ứng (*Response*)	Dữ liệu ra sơ đồ PUF tương ứng với một kích thích cụ thể.
Định danh (*Identity, Identification*)	Dữ liệu gán cho một thiết bị nhằm phân biệt nó với các thiết bị khác. Dữ liệu này có thể là quy ước hay được tạo từ đặc tính vật lý của thiết bị.
Hàm băm (*Hash function*)	Hàm bất kỳ có thể được sử dụng để ánh xạ dữ liệu có kích thước tùy ý thành dữ liệu có kích thước cố định
Khoảng cách Hamming (*Hamming distance*)	Số bit khác nhau giữa hai chuỗi bit có cùng độ dài.

Khoảng cách Hamming tương đối (*Fractional Hamming distance*)	Tỷ số của khoảng cách Hamming giữa hai chuỗi bit và độ dài của chúng.
Khoảng cách nội (*Intra-distance*)	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
Khoảng cách tương quan (*Inter-distance*)	Biến ngẫu nhiên mô tả khoảng cách giữa hai đáp ứng PUF từ hai thực thể PUF sử dụng cùng một kích thích
Ước lượng PUF (*PUF evaluation*)	Hàm biểu thị phép đo PUF
Kích thích (*Challenge*)	Dữ liệu vào dùng để cấu hình sơ đồ PUF
Lớp PUF (*PUF Class*)	Mô hình toán học mô tả hoàn chỉnh của một kiểu kiến trúc PUF cụ thể, gồm thủ tục khởi tạo dùng để tạo các thực thể PUF
PUF bán dẫn (*Silicon PUF*)	Thiết kế PUF khai thác đặc trưng thăng giáng nội tại xuất hiện trong quá trình chế tạo cấu kiện bán dẫn.
PUF phi bán dẫn (*Non-Silicon PUF*)	Thiết kế PUF khai thác đặc trưng ngẫu nhiên của các vật liệu phi bán dẫn
Tấn công kênh bên (*Side-channel attack*)	Hình thức khai thác lỗ hổng bảo mật nhằm đánh cắp thông tin hoặc tác động đến chương trình thực thi của một hệ thống bằng cách gián tiếp đo hoặc tách các hiệu ứng vật lý của phần cứng hệ thống.

Tấn công dựa trên mô hình (*Modeling attack*)	Hình thức tấn công bằng kỹ thuật học máy (*machine learning*), dựa trên tập dữ liệu vào/ra xây dựng bản sao mô hình của hệ thống.
Thực thể PUF (*PUF instance*)	Cấu trúc vật lý thực tế của mạch PUF khi thực thi sơ đồ PUF trên phần cứng.

MỞ ĐẦU

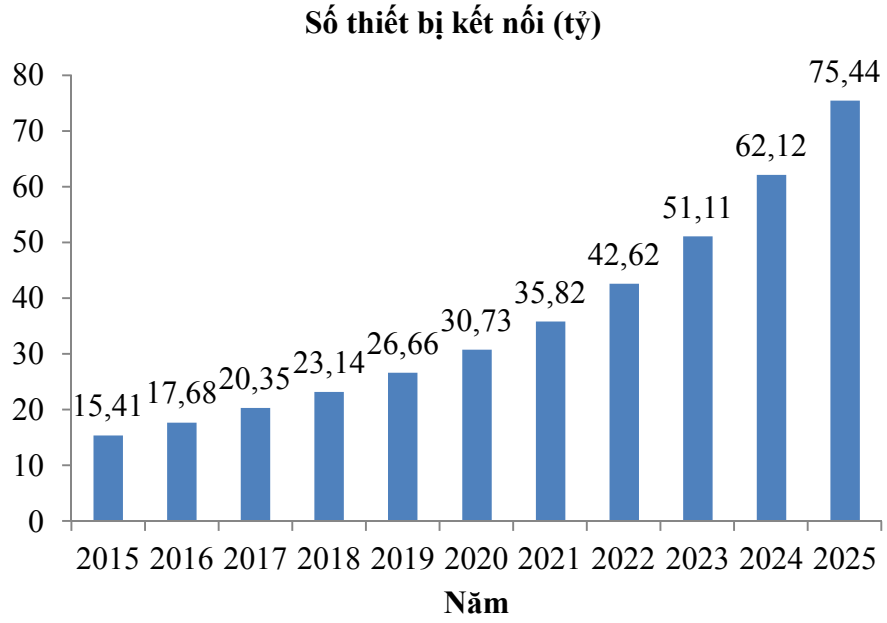
1. Động lực nghiên cứu

Ngày nay, những tiến bộ trong công nghệ điện tử - số đã và đang làm gia tăng mạnh mẽ chủng loại và số lượng các thiết bị điện tử, công nghệ thông tin và truyền thông, cũng như phương thức kết nối giữa chúng nhằm dùng chung dữ liệu. Đặc biệt, sự phổ biến của công nghệ mạng không dây đã dẫn đến sự hình thành nền tảng số Internet vạn vật (*IoT: Internet of Things*), trong đó hàng tỷ thực thể cấu kiện đa dạng về chủng loại được kết nối với nhau và chia sẻ dữ liệu nhằm mở rộng và gia tăng giá trị các dịch vụ [1]. Theo ước tính của *Statistica*[1], tổng số các thiết bị kết nối trên thế giới đến năm 2025 sẽ xấp xỉ 75,44 tỷ (Hình i) [2]. Cùng với đó, các hình thức tấn công mạng nhằm vào IoT cũng phát triển nhanh chóng về quy mô và phương thức [3,4] (Phát tán mã độc, tấn công từ chối dịch vụ…). Điều này đặt ra yêu cầu cao đối với việc xác định chính xác chủ thể tham gia hệ thống truyền tin. Đây là nhiệm vụ định danh (*Identification*) và xác thực (*Authentication*) thiết bị trong bảo vệ an toàn phần cứng và dữ liệu.

Trong lĩnh vực quốc phòng an ninh phát sinh sự thâm nhập của linh kiện giả qua mạng cung ứng vật tư cho các hãng chế tạo vũ khí [5,6]. Linh kiện giả có thể là linh kiện tái chế, phế phẩm, sản xuất không giấy phép, sao chép hoặc đã bị can thiệp phần cứng [7], gây ra nguy cơ giảm độ tin cậy và tuổi thọ của vũ khí, trang bị kỹ thuật, suy giảm năng lực tác chiến của lực lượng vũ trang. Theo khảo sát của *Trenton Systems*[2], năm 2020,

[1] Công ty Đức thành lập năm 2007, hoạt động trong lĩnh vực kinh doanh dữ liệu thống kê thị trường và tiêu dùng.
[2] Công ty Mỹ thành lập năm 1989, hoạt động trong lĩnh vực chế tạo phần cứng máy tính chuyên dụng cho quân sự, thương mại và công nghiệp.

linh kiện giả chiếm khoảng 15% trong tổng số phụ tùng và linh kiện thay thế trong biên chế trang bị của quân đội Mỹ, gây thiệt hại trên 7,5 tỷ USD/năm tương đương 11.000 việc làm trong ngành công nghiệp bán dẫn [8]. Đối với quân đội ta, quá trình hiện đại hóa vũ khí trang bị liên quan đến việc tham gia vào chuỗi cung ứng linh kiện, vật tư và vũ khí toàn cầu. Do đó, việc nhận biết và loại bỏ linh kiện giả là một yêu cầu thiết yếu, nhằm đảm bảo tính nguyên bản của các cấu kiện điện tử, nắm chắc lý lịch và phẩm chất của vũ khí, trang bị kỹ thuật.



Hình i: Số thiết bị kết nối vào IoT từ năm 2015 đến năm 2025

Cùng với việc xác định chính xác chủ thể tham gia hệ thống truyền tin, cần bảo mật dữ liệu truyền bằng các kỹ thuật mã hóa/giải mã mật nhằm chống lại sự truy cập trái phép. Một mặt cần xây dựng các giao thức và thuật toán mã hóa đáp ứng được các mục tiêu bảo đảm an toàn thông tin; mặt khác cần phân tích mức độ an toàn của các cấu trúc mã hóa bằng cách giả lập tấn công, cố gắng phá vỡ chúng. Cụ thể, đối với hầu hết các cấu trúc mã hóa dùng khóa mã, cần đáp ứng các yêu cầu về bảo mật việc tạo, lưu trữ

và sử dụng khóa mã. Mức độ bảo mật của một hệ thống mã hóa (được đánh giá qua nỗ lực phá vỡ chúng khi không biết khóa mã) tương quan theo hàm mũ với độ dài (bit) của đoạn dữ liệu được sử dụng làm khóa mã. Ở lớp vật lý, các khóa mã thường được lưu ở một vùng nhớ số bền vững (*non-volatile digital memory*) trên một chip bán dẫn. Đối phương có thể can thiệp vào sự hoạt động của hệ thống mã hóa bằng nhiều cách, ở cả cấp độ phần mềm và phần cứng. Ngày nay, các phương thức tấn công phần cứng đã phát triển mạnh mẽ, điển hình là tấn công kênh bên (khai thác thông tin rò rỉ qua thời gian hoạt động, công suất tiêu thụ, bức xạ điện từ…), làm lây lan mã độc phần cứng (*hardware Trojan*) hay can thiệp để dựng lại cấu trúc phần cứng của thiết bị. Do đó, cần phát triển các kỹ thuật và cấu trúc vật lý có khả năng chống lại các tấn công phần cứng và đạt được các mục tiêu bảo mật ở lớp vật lý.

Hai tác vụ trên (định danh và xác thực thiết bị, mã hóa mật) là những nhiệm vụ điển hình của lĩnh vực bảo đảm an toàn thông tin và bảo mật phần cứng. **Bảo mật phần cứng** bao gồm các kỹ thuật nhằm xác định và phân tích tác động của các nguy cơ gây tổn hại phần cứng, giảm thiểu tác hại cho phần cứng khi bị tấn công, phát triển các thiết kế phần cứng có khả năng tự sửa chữa [9].

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. Kể từ khi ra đời, PUF đã được nghiên cứu rộng rãi trên mọi phương diện, từ kỹ thuật tạo PUF, phương pháp xử lý dữ liệu đáp ứng PUF cho đến phát triển các ứng dụng PUF trong bảo mật phần cứng cũng như cải tiến chất lượng PUF nhằm tăng tính

bền vững trước tấn công phần cứng… 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"***.

Hiệu năng của một sơ đồ PUF gắn với ứng dụng cụ thể. Trong luận án này, hiệu năng PUF được đánh giá theo **độ tin cậy** trong định danh và xác thực thiết bị[3] và **tính ổn định** của chuỗi bit đáp ứng đầu ra của PUF, phục vụ các ứng dụng mã hóa bảo mật. Dưới đây trình bày kết quả của các nghiên cứu đã có trên thế giới trong lĩnh vực này.

*** Định danh và xác thực thiết bị**

Từ phân tích định tính tiêu chuẩn định danh và xác thực thiết bị, các tác giả trong [10,11] đề xuất cách tính mức ngưỡng xác thực dựa trên tỷ lệ chấp nhận nhầm (*FAR: False Acceptance Rate*) và tỷ lệ loại bỏ nhầm (*FRR: False Rejection Rate*). Phân tích thực nghiệm các hệ thống định danh và xác thực dựa trên các đáp ứng 64-bit đối với một số sơ đồ PUF, các tác giả trong [10] chỉ ra, sơ đồ ***PUF dao động vòng (RO PUF: Ring Oscillator PUF) với việc so sánh ghép cặp các mạch dao động vòng (RO: Ring Oscillator) có khả năng định danh và xác thực tốt nhất với tỷ lệ lỗi cân bằng[4] (EER: Equal Error Rate) xấp xỉ 10^{-6}***. Ngoài ra, một số công trình nghiên cứu tạo dữ liệu định danh (*ID: Identification*) và xác thực thiết bị dựa trên RO PUF theo hướng tiếp cận khác. Trong [12], các tác giả đã đề xuất đại lượng Q là khái quát hóa khoảng cách giữa các vector ID với các tọa độ là tần số RO. Trên cơ sở phân bố xác suất của biến ngẫu nhiên Q,

[3] Thuật ngữ "thiết bị", "linh kiện", "cấu kiện", "chip" trong luận án này được dùng để chỉ mạch tích hợp (*IC: Integrated Circuit*).

[4] Với phương pháp đang xét, mức ngưỡng được chọn từ điều kiện cân bằng FAR và FRR: $FAR = FRR = EER$. Độ tin cậy được đánh giá qua EER. Độ tin cậy cao khi EER nhỏ và ngược lại.

các tác giả áp dụng kỹ thuật kiểm nghiệm Kolmogorov-Smirnov [13,14] để xác thực các IC. Trong [15], mỗi mẫu tần số hiệu RO trung bình được định nghĩa là trung bình cộng các mẫu tần số hiệu RO thành phần, được tính từ tập các cặp RO cho trước. Từ tập các mẫu tần số hiệu RO trung bình, các tác giả áp dụng phương pháp truyền thống dựa trên *EER* để xác định mức ngưỡng, dùng trong xác thực thiết bị. Hạn chế của các phương pháp là độ chính xác của mức ngưỡng không cao do sử dụng các độ đo khoảng cách Hamming [13], loại bỏ biến thiên cục bộ (quy luật biến thiên tần số hiệu RO giữa các RO trên cùng một chip) [15]. Ngoài ra, các tác giả chưa xét tác động của điều kiện hoạt động và các nhân tố biến thiên khác lên việc định danh và xác thực cấu kiện.

*** Ổn định dữ liệu đáp ứng PUF**

Để có thể ứng dụng PUF trong các nhiệm vụ liên quan đến mã hóa bảo mật, cần có các giải pháp nhằm ổn định dữ liệu đáp ứng PUF. Trong [16], các tác giả đề xuất sơ đồ mã hóa sửa lỗi (*ECC: Error Correcting Code*) nhằm duy trì sự ổn định của dữ liệu ra PUF ngay cả khi điều kiện hoạt động thay đổi. Các tác giả trong [17] đề xuất sơ đồ RO PUF cải tiến dựa trên mã hóa Lehmer-Gray và giải mã BCH. Bộ giải mã này là thành phần chính của sơ đồ tạo dữ liệu bổ trợ (*helper data*). Các khóa mã được tạo ra thông qua một thủ tục gọi là tích lũy entropy. Trong [18], các tác giả thay thế hàm băm bằng bộ giải mã BCH nhằm nâng cao hiệu suất của bộ tách dùng giải thuật mờ (*fuzzy extractor*). Nhìn chung, các hướng tiếp cận trên được đề xuất đối với sơ đồ RO PUF truyền thống với chuỗi bit thu nhận được từ hàm dấu, không hiệu quả về mặt khai thác thông tin. Ngoài ra, các sơ đồ tạo khóa mã đó khá phức tạp và tiêu thụ nhiều tài nguyên phần cứng, cũng như chưa kiểm nghiệm khóa mã được tạo vào một sơ đồ mã hóa mật thực tế. Đối với lĩnh vực ứng dụng này, luận án giới hạn ở việc

ổn định chuỗi bit ra, làm cơ sở cho các nghiên cứu tiếp theo như tạo số ngẫu nhiên hay khóa mã phục vụ mã hóa bảo mật.

Từ việc khảo sát các nghiên cứu hiện có về PUF, có thể thấy việc nâng cao hiệu năng sơ đồ PUF là một yêu cầu thiết yếu nhằm nâng cao tính phổ dụng của PUF trong bảo mật phần cứng. Điều này đặc biệt có ý nghĩa trước bối cảnh phát triển mạnh mẽ của IoT và việc sử dụng dữ liệu dùng chung hiện nay.

2. Mục tiêu và nhiệm vụ của luận án

*** Mục tiêu chung:**

Nghiên cứu các giải pháp nâng cao hiệu năng mạch RO PUF, dùng trong các ứng dụng bảo mật phần cứng.

*** Mục tiêu 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.

3. Đối tượng và phạm vi nghiên cứu

*** Đối tượng nghiên cứu:** Mạch RO PUF.

*** Phạm vi nghiên cứu:**

- 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 ID cho thiết bị, tạo chuỗi bit ra ổn định và duy nhất, phục

vụ mã hóa bảo mật.

4. Phương pháp nghiên cứu

Từ mục tiêu nghiên cứu đã đề ra, nghiên cứu sinh sử dụng một số phương pháp nghiên cứu sau.

- Khảo sát các nghiên cứu đã có, tập trung vào RO PUF trên các phương diện như mô hình toán, phương pháp xây dựng mạch vật lý, cơ chế tạo dữ liệu đáp ứng, các ứng dụng của RO PUF trong bảo mật phần cứng.

- Đánh giá khả năng phát triển các ứng dụng của phần cứng thực thi thiết kế PUF, cụ thể là các họ FPGA Xilinx Spartan-3E, Spartan-6 và Artix-7.

- Thử nghiệm mạch phần cứng thực thi thiết kế RO PUF trong các điều kiện môi trường khác nhau.

- Phân tích thống kê dữ liệu thực nghiệm, rút ra kết luận về đặc tính vật lý cần nghiên cứu.

- Sử dụng các công cụ hỗ trợ thiết kế và mô phỏng trong thiết kế logic số: Xilinx ISE, Xilinx Vivado, Mentor Graphics Modelsim; phần mềm tính toán và mô phỏng Matlab-Simulink.

5. Tình hình nghiên cứu trong và ngoài nước

Hướng nghiên cứu mới về PUF xuất hiện trong khoảng hai thập kỷ gần đây, có triển vọng ứng dụng rộng rãi trong an toàn thông tin và bảo mật phần cứng.

Tại Việt Nam, hướng nghiên cứu này bước đầu được triển khai tại một số cơ sở nghiên cứu trọng điểm. Nhóm nghiên cứu của Học viện Kỹ thuật Quân sự do PGS. TS. Hoàng Văn Phúc chủ trì đã phát triển thiết kế RO PUF kết hợp bộ chuyển đổi thời gian-số (*TDC: Time-to-Digital Converter*) [19]. Ngoài ra, thuộc về lĩnh vực bảo mật phần cứng có thể kể đến một số

nhóm nghiên cứu về thiết kế vi mạch, hướng tới ứng dụng trong lĩnh vực an toàn, bảo mật thông tin. Các nhóm nghiên cứu thuộc Ban Cơ yếu Chính phủ tập trung vào việc thực thi các loại mã mật và các giao thức bảo mật thông tin trong ngành cơ yếu. Tại Đại học Bách khoa Hà Nội, các nhà khoa học đã thực hiện nhiều nghiên cứu về bảo mật thông tin và mã mật, đặc biệt là các giải pháp bảo mật sử dụng kỹ thuật hỗn loạn, nhưng chủ yếu tập trung trên nền tảng phần mềm [20]. Nhóm nghiên cứu tại Phòng thí nghiệm Hệ thống tích hợp thông minh (SISLAB) của Đại học Quốc gia Hà Nội do PGS. TS. Trần Xuân Tú chủ trì đã có nhiều công bố khoa học trong lĩnh vực bảo mật phần cứng, tập trung vào thiết kế các lõi phần cứng mã mật tốc độ cao, công suất tiêu thụ thấp cho các hệ thống Internet vạn vật [21,22]. Tại Đại học Khoa học Tự nhiên – Đại học Quốc gia TP. Hồ Chí Minh, Phòng thí nghiệm Xử lý tín hiệu số và hệ thống nhúng (DESLAB) do TS. Lê Đức Hùng chủ trì cũng tập trung vào thiết kế các vi mạch số và hệ thống nhúng tiết kiệm năng lượng, các bộ vi xử lý cấu trúc RISC-V và các lõi mã mật nhẹ [23]. Các nhóm nghiên cứu khác tại Đại học Bách khoa TP. Hồ Chí Minh, Đại học Sư phạm Kỹ thuật TP. Hồ Chí Minh và Đại học Giao thông vận tải cũng thực hiện các nghiên cứu về thiết kế vi mạch số, vi mạch tương tự, vi mạch tần số vô tuyến nhưng chưa có công bố về lĩnh vực bảo mật phần cứng và PUF.

Các công trình nghiên cứu trên thế giới về lĩnh vực này rất phong phú, tập trung trên một số hướng chủ yếu dưới đây.

i) Đề xuất các kiến trúc PUF mới, nâng cao hiệu quả và tính linh hoạt trong cấu hình phần cứng, kiểm chứng mức độ an toàn phần cứng mạch PUF trước các hoạt động tấn công phần cứng.

Khái niệm về PUF dần được hình thành từ các khái niệm về hàm vật lý một chiều (*POF: Physical One-way Function*), hàm giả ngẫu nhiên

(*PRF: Pseudo-Random Function*) [24] với ý tưởng chung là lợi dụng các thăng giáng ngẫu nhiên gắn với bản chất vật lý đặc trưng cho thiết bị cụ thể để tạo dữ liệu định danh (*ID: Identity*) cho thiết bị. POF và PRF đa dạng về vật liệu và dạng tín hiệu thăng giáng, phức tạp về mặt thiết lập cấu hình thiết bị tạo dữ liệu đáp ứng nên chỉ phù hợp với các ứng dụng chuyên biệt. Xét trên phương diện vật liệu nền, PUF phi bán dẫn tương tự như POF và PRF nên ít được tập trung nghiên cứu. Ngược lại, hầu hết các nghiên cứu về PUF đều phát triển trên nền bán dẫn, theo hai hướng chính là lợi dụng độ giữ chậm trong cấu kiện bán dẫn và mạch kết nối; lợi dụng trạng thái phần tử nhớ [10]. Nhiều sơ đồ tạo PUF đã được đề xuất, bao gồm các sơ đồ cơ bản và các sơ đồ cải tiến nhằm nâng cao khả năng của mạch PUF chống lại các hình thức tấn công phần cứng.

ii) Phát triển các công cụ lý thuyết nhằm tiếp cận, mô tả tính chất vật lý của mạch PUF, xử lý dữ liệu đáp ứng PUF.

Do PUF có bản chất là kỹ thuật gắn trực tiếp với nền vật lý, việc mô hình hóa toán học PUF như đối với các lĩnh vực kỹ thuật truyền thống là đặc biệt khó khăn và thường chỉ giới hạn áp dụng trong phạm vi cụ thể. Tuy nhiên, các nhà khoa học đã cố gắng phác thảo một số đặc tính tổng quan về PUF dưới hình thức toán học. Phần 1.3.1 sẽ trình bày chi tiết về mô hình toán của PUF. Trên cơ sở đó, giới nghiên cứu đề xuất một số tham số định lượng phẩm chất của PUF và các chỉ tiêu đánh giá hiệu năng mạch PUF. Đặc điểm nổi bật trong các công cụ lý thuyết mô hình hóa PUF là sự tồn tại của các đại lượng xác xuất và các chỉ tiêu định tính "lớn", "nhỏ". Điều này là do dữ liệu PUF có bản chất là đại lượng thống kê và việc đánh giá hiệu năng của mạch PUF phải gắn với ứng dụng cụ thể.

iii) Phát triển các lĩnh vực ứng dụng PUF.

Về phương diện thực thi phần cứng, sự phát triển của công nghệ vi mạch khả trình (ASIC, FPGA…) tạo điều kiện thuận lợi cho việc phát triển các ứng dụng PUF. Như sẽ trình bày trong phần 2.1.1, hầu hết các thiết kế PUF được thực thi trên các họ FPGA (*Field Programmable Gate Array: Mảng cổng logic khả trình*) bởi khả năng của công nghệ này cho phép sử dụng tài nguyên phong phú, chỉnh sửa thiết kế dễ dàng, có thể tái cấu hình nhiều lần và chuyển đổi linh hoạt giữa các họ linh kiện.

6. Đóng góp của luận án

Luận án có một số đóng góp về khoa học như sau.

- 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.

7. Bố cục của luận án

Luận án được cấu trúc thành bốn 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.

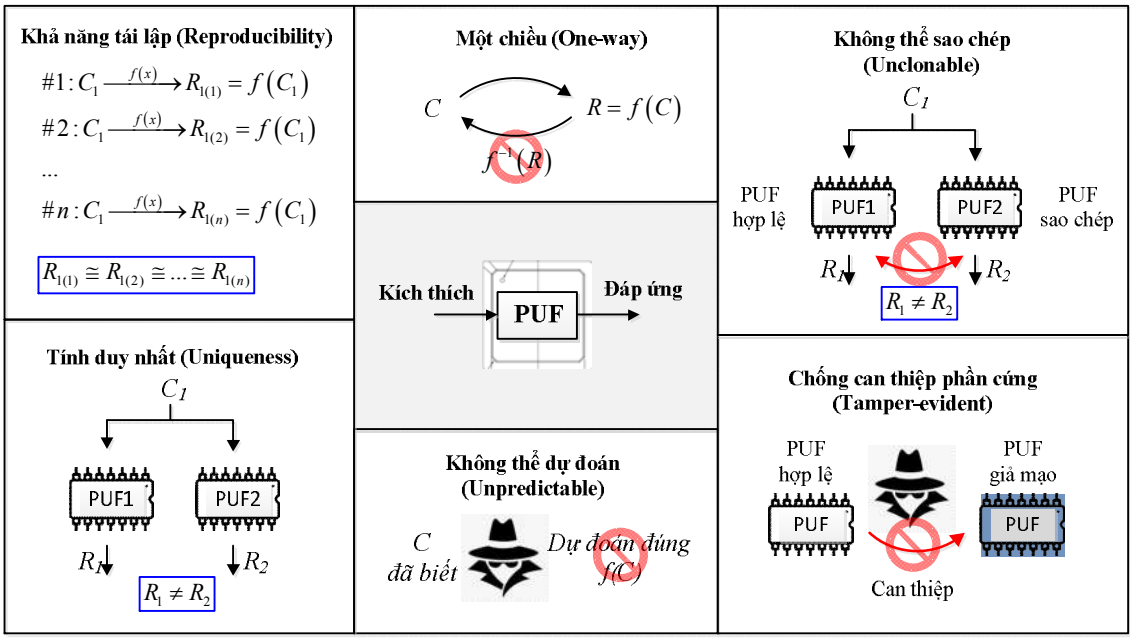
Cuối mỗi chương có kết luận chương khái quát kết quả nghiên cứu và công bố tương ứng. Phần kết luận chung tóm tắt kết quả đạt được và những đóng góp về khoa học của luận án, gợi mở một số hướng nghiên cứu tiếp theo.

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. Đây là hướng nghiên cứu mới được phát triển trong khoảng hai thập kỷ gần đây. 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. Thông thường, các ảnh hưởng này là rất nhỏ và chỉ thể hiện ở thang hiển vi. Các phép đo với độ chính xác cao các thể hiện này cho phép tách ra các đặc tính nguyên bản và đặc thù. Việc xây dựng các kiến trúc PUF là thiết kế các sơ đồ có khả năng khuếch đại các thăng giáng vi mô lên mức có thể quan sát được. Ngay cả khi quá trình chế tạo được giám sát chặt chẽ, do tác động của các yếu tố ngẫu nhiên và không điều khiển được, không thể tạo ra hai cấu kiện đồng nhất về mặt vật lý.

Cấu trúc cơ bản và các thuộc tính thiết yếu của PUF được trình bày trên Hình 1.1 [25]. 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.

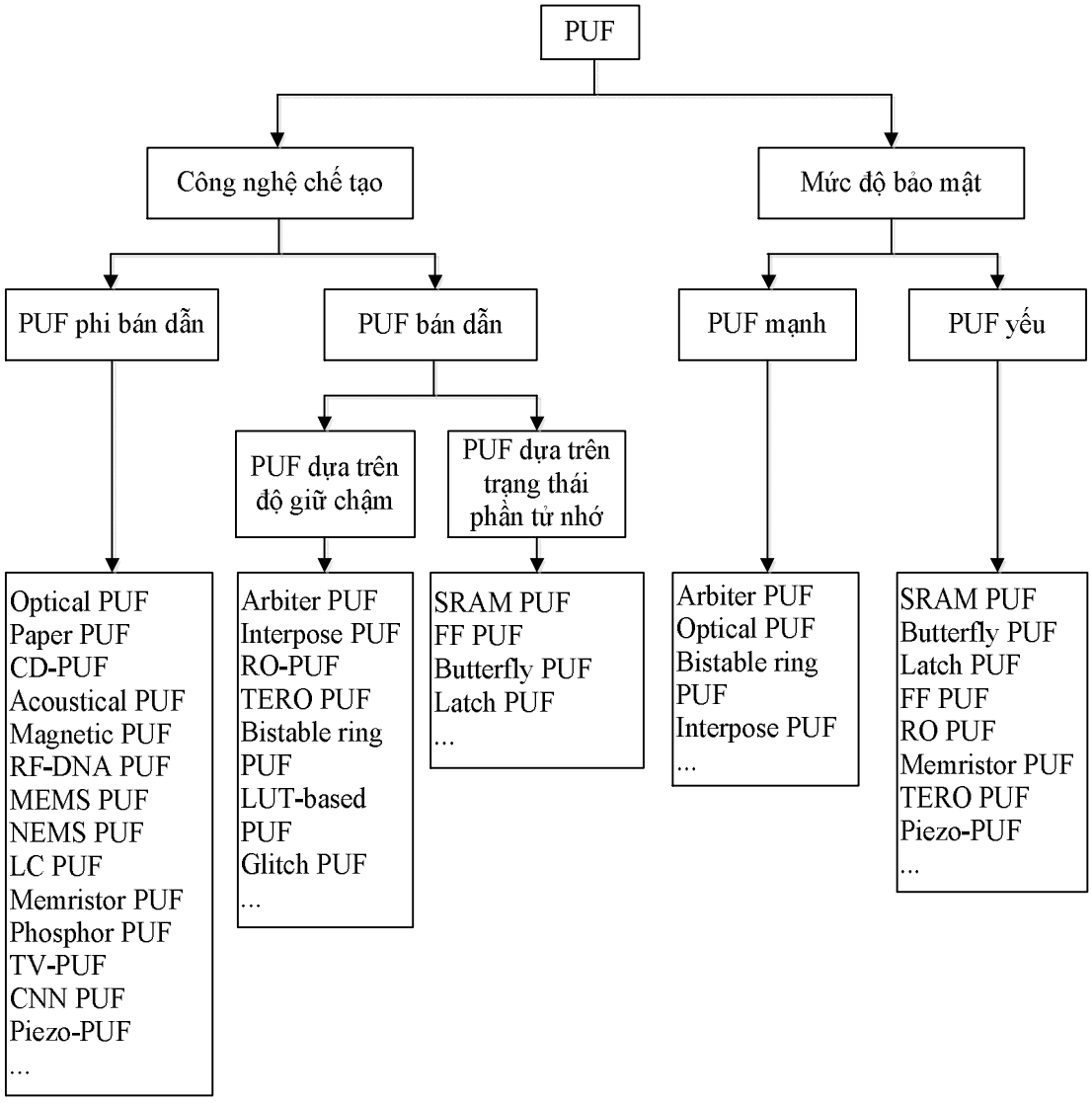


Hình 1.1: Cấu trúc cơ bản của PUF và các thuộc tính thiết yếu [25]

Thiết kế PUF được thực thi trên các thiết bị khác nhau tạo ra các thực thể PUF (*PUF instance*) khác nhau. Đối với mỗi lần kích hoạt mạch PUF, tương ứng một mẫu kích thích đầu vào, các mẫu đáp ứng đầu ra đối với các thực thể PUF khác nhau là khác nhau (thể hiện *tính duy nhất* và *tính không thể sao chép*). Đối với cùng một thực thể PUF và cùng một kích thích đầu vào, các mẫu đáp ứng đầu ra tương ứng các lần kích hoạt mạch PUF là khác nhau (thể hiện *tính không thể dự đoán*). Tập các mẫu này có các tham số thống kê đặc trưng cho thực thể PUF đang xét (thể hiện *khả năng tái lập/tính ổn định*). Quá trình tạo kích thích – đáp ứng là *một chiều*. Từ tập CRP không thể dựng lại chính xác cấu trúc vật lý mạch PUF. Vì thăng giáng về tham số vật lý xuất hiện trong quá trình chế tạo có tính đặc thù và nguyên bản, việc can thiệp phần cứng sẽ làm thay đổi tham số vật lý mạch PUF và do đó thay đổi CRP. Đây là khả năng *chống can thiệp phần cứng* đối với thiết bị. Như vậy, các thiết bị được cấy mạch PUF có thể được định danh chính xác dựa trên đặc trưng thống kê của các mẫu đáp ứng PUF.

1.2. Phân loại PUF

Các thiết kế PUF rất đa dạng về cơ sở vật lý, cấu trúc dữ liệu CRP và gắn với ứng dụng cụ thể. Các sơ đồ PUF có thể được phân loại dựa trên phương pháp chế tạo và mức độ bảo mật [25], như được trình bày trên Hình 1.2.



Hình 1.2: Phân loại PUF [25]

1.2.1. Phân loại PUF theo công nghệ chế tạo

Theo công nghệ chế tạo, PUF được phân thành hai nhóm chính: PUF phi bán dẫn (*Non-Silicon PUF*) và PUF bán dẫn (*Silicon PUF*) [26]. Với sự

phát triển của công nghệ vi mạch khả trình và các công cụ hỗ trợ thiết kế, đa số các thiết kế PUF được thực thi trên nền bán dẫn.

PUF phi bán dẫn sử dụng các vật liệu khác vật liệu bán dẫn để tạo cấu trúc PUF, gồm PUF quang, PUF sợi giấy, PUF CD, PUF âm thanh, PUF từ,.. Dưới đây giới thiệu khái quát một số sơ đồ PUF phi bán dẫn.

- PUF quang (*Optical PUF*) [27]: Đĩa quang chứa các hạt có cấu trúc vi mô ($\sim 500\mu m$) có tác dụng tán xạ tia laser chiếu tới. Hình ảnh tán xạ được thu nhận bởi camera CCD và truyền về máy tính. Hàm băm Gabor tác động lên dữ liệu ảnh tán xạ và tạo chuỗi bit đặc trưng.

- PUF sợi giấy (*Paper PUF*) [28]: Cấu trúc sợi giấy ngẫu nhiên và duy nhất được chiếu tia laser. Hình ảnh tán xạ được mã hóa và liên kết với nội dung tài liệu để tạo chữ ký số kết hợp cho dữ liệu.

- PUF CD (*CD PUF*) [29]: Kích thước các vùng ghi (*"land"*) và vùng nền (*"pit"*) trong cấu trúc vi mô của CD được đo nhằm tách ra thăng giáng về độ lệch giữa kích thước thực và kích thước thiết kế xuất hiện trong quá trình chế tạo. Dữ liệu này được chuyển đổi thành chuỗi bit chứa thông tin định danh CD.

- PUF âm thanh (*Acoustical PUF*) [30]: Dây giữ chậm siêu âm được sử dụng để giữ chậm tín hiệu điện (chuyển đổi tín hiệu điện thành các dao động cơ và ngược lại). Phổ tần đặc trưng của dây giữ chậm được phân tích và tách ra các bit định danh tín hiệu.

- PUF từ (*Magnetic PUF*) [31]: Các mẫu hạt trong vật liệu từ có tính duy nhất nguyên bản về từ tính. Đặc tính này được ứng dụng trong xác thực thẻ tín dụng.

- PUF DNA tần số vô tuyến (*RF-DNA PUF*) [32]: Các đơn vị cấu trúc đồng nhất dạng đĩa phủ sợi kim loại bố trí ngẫu nhiên được đặt trong trường điện

từ. Tín hiệu tán xạ sóng điện từ có tính ngẫu nhiên, được thu nhận bởi một ma trận anten và được dùng để tách ra thông tin đặc trưng cho đơn vị cấu trúc.

- PUF sử dụng cảm biến vi cơ điện tử (*MEMS PUF*) [33]: Các hệ thống vi cơ điện tử (*MEMS: Micro-Electro-Mechanical Systems*) bao gồm các phần tử cơ và cơ điện tử tiểu hình hóa (kích thước thay đổi từ dưới 1 μm tới một vài mm) được tạo ra bởi công nghệ chế tạo các cấu kiện vi mô. MEMS PUF lợi dụng tính duy nhất (*uniqueness*) cao của tín hiệu cảm biến MEMS để tạo các chuỗi bit duy nhất dùng cho tạo khóa mã bảo mật. MEMS PUF tích hợp nhiều phép đo đặc tính của vật liệu trong một CRP.

- PUF sử dụng chuyển mạch vi cơ điện tử (*NEMS PUF*) [34]: Lợi dụng hiệu ứng ma sát lăn trong các chuyển mạch vi cơ điện tử (*NEMS: Nano-Electro-Mechanical Switch*) kích thước micro và nano để tạo cấu trúc PUF có độ tin cậy và tính ổn định cao.

- PUF sử dụng khung dao động LC (*LC PUF*) [35]: Khung dao động LC gồm điện dung là một đĩa nhựa nhỏ (~ 1 mm^2) phủ kim loại ở hai mặt ghép nối tiếp với điện cảm là một cuộn dây kim loại. Đặt khung LC trong trường điện từ, tiến hành quét tần số và xác định tần số cộng hưởng của mạch. Sự sai lệch nhỏ về đỉnh cộng hưởng thể hiện thăng giáng nội tại và được sử dụng để tách đặc tính PUF.

- PUF sử dụng điện trở nhớ (*Memristor PUF*) [36]: Các điện trở nhớ (*memristor*) có đặc tính phi tuyến cao, khi thay thế cho linh kiện CMOS trong mạch PUF tạo ra đáp ứng có độ bất định 50% và độ tin cậy cao.

- PUF sử dụng phốtpho (*Phosphor PUF*) [37]: Đơn vị cấu trúc chứa các hạt phốtpho được phủ nhựa. Khi chiếu tia cực tím lên đơn vị cấu trúc, xảy ra hiện tượng phát lân quang. Tán xạ này có tính ngẫu nhiên và khó bị sao

chép, được sử dụng để tạo định danh số cho đơn vị cấu trúc.

- PUF sử dụng điện áp ngưỡng (*TV PUF*) [38]: PUF khai thác sự nhạy của điện áp ngưỡng (*TV: Threshold Voltage*) MOSFET đối với các thăng giáng ngẫu nhiên.

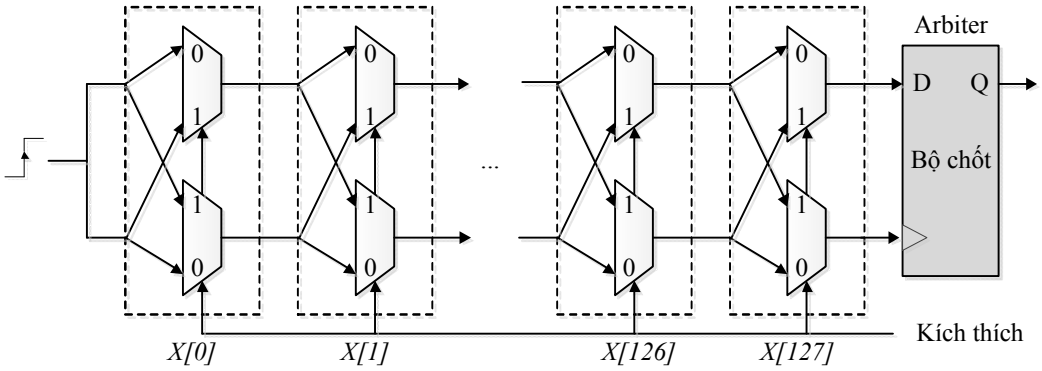
- PUF sử dụng mạng nơron tích chập (*CNN PUF*) [39]: Quá trình học sâu (*deep learning*) sử dụng mạng nơron tích chập (*CNN: Convolutional Neural Network*) được áp dụng vào phân tích tín hiệu băng gốc thu nhận được bởi một máy thu vô tuyến, từ đó tách ra dữ liệu có tính duy nhất phục vụ định danh thiết bị.

- PUF dựa trên hiệu ứng áp điện (*Piezo-PUF*) [40]: Năng lượng được thu bởi bộ thu năng lượng áp điện từ cảm ứng vi điện cơ đặt trong chân không có tính phi tuyến cao và có thể được sử dụng để tạo dữ liệu PUF.

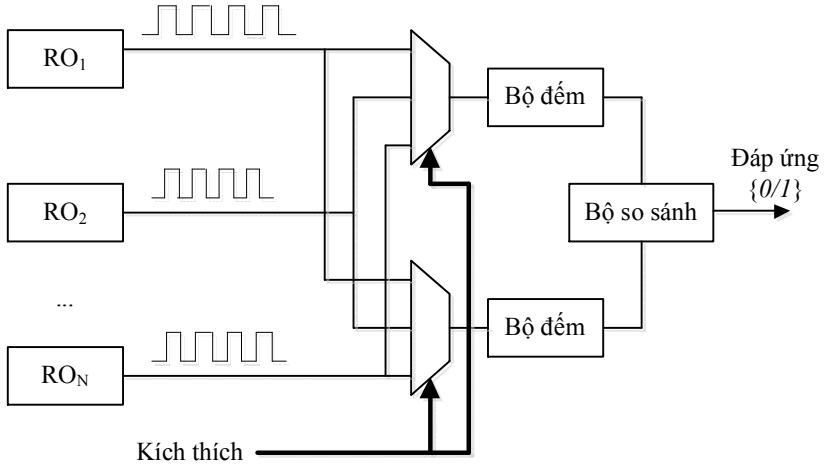
PUF bán dẫn khai thác sự bất đồng nhất về mặt vật lý gây ra bởi những thăng giáng không kiểm soát được, xuất hiện trong quá trình chế tạo để tạo ra dữ liệu đặc trưng cho mỗi IC. Theo nguồn thăng giáng, các PUF bán dẫn được phân thành hai nhóm chính là PUF dựa trên độ giữ chậm (*delay-based PUF*) và PUF dựa trên trạng thái của các phần tử nhớ (*memory-based PUF*).

PUF dựa trên độ giữ chậm khai thác sự khác biệt về độ giữ chậm đường truyền tín hiệu bên trong mạch. Một số PUF thuộc loại này là PUF trọng tài, PUF dao động vòng …

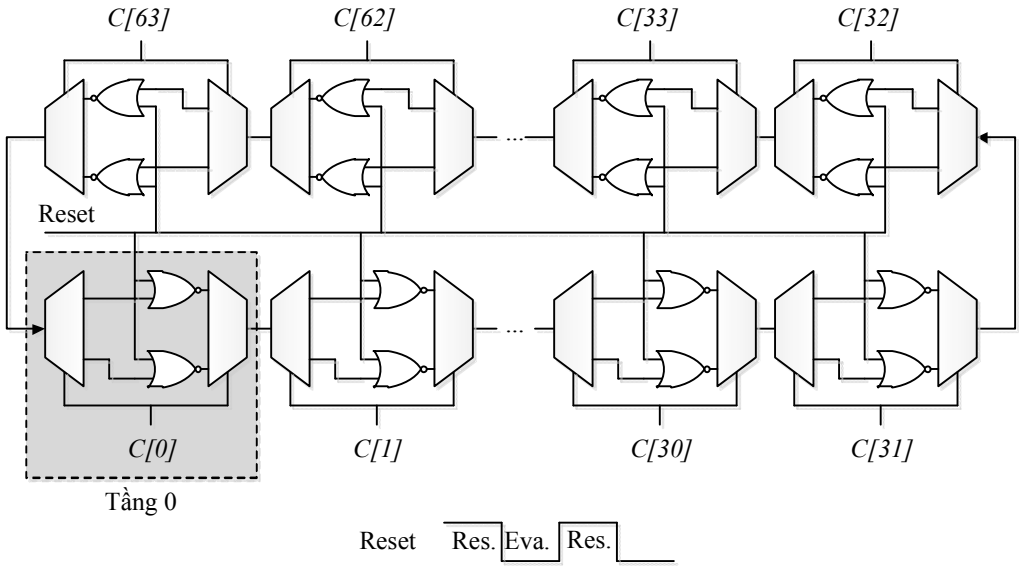
- PUF trọng tài (*APUF: Arbiter PUF*) [41] gồm hai đường giữ chậm đồng nhất về mặt vật lý trên chip được kích hoạt đồng thời. Mạch so sánh (*Arbiter*, là FF được kích bởi sườn xung) được dùng để xác định sườn trước xung tới, thiết lập mức logic $\{0\}$ hay $\{1\}$ ở đầu ra tùy vào đường truyền nào có độ giữ chậm nhỏ hơn .



a)



b)



c)

Hình 1.3: PUF dựa trên độ giữ chậm [25]: (a) APUF; (b) RO PUF; (c) BR PUF

- PUF dao động vòng (*RO PUF: Ring Oscillator PUF*) [24,42] khai thác sự khác biệt về tần số mạch dao động vòng gây ra bởi đặc tính giữ chậm của các mạch đảo và đường hồi tiếp tín hiệu qua cổng NAND.

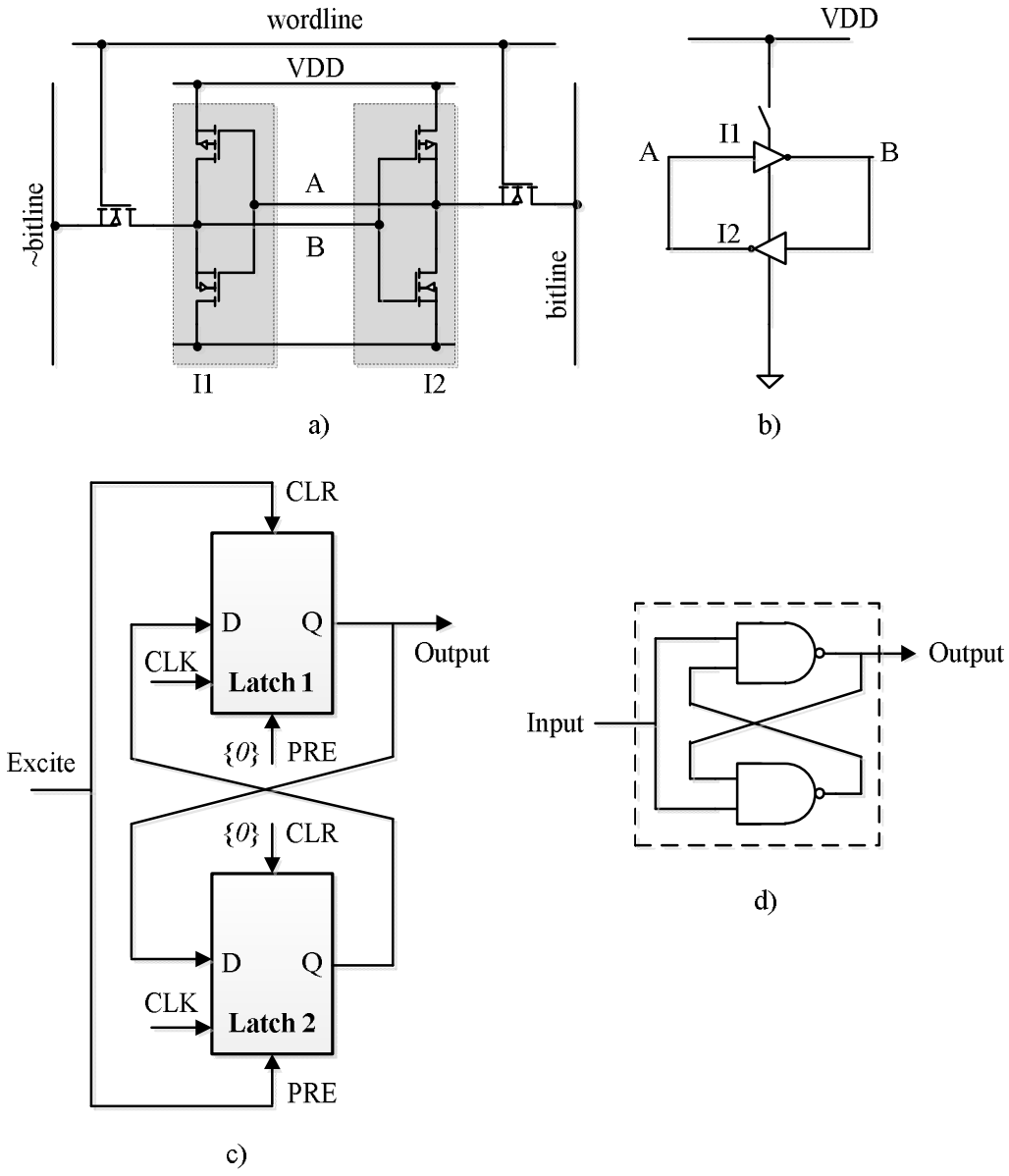
- PUF mạch vòng ổn định kép (*BR PUF: Bistable Ring PUF*) [43] gồm một số chẵn các cổng đảo, tạo nên hai trạng thái ổn định có thể có dạng $\{101010...\}$ hoặc $\{010101...\}$. Mỗi cổng đảo có độ giữ chậm cấu hình được bởi một bit kích thích. Các đáp ứng được tạo ra từ hai trạng thái xác lập có thể có của một vòng ổn định kép sau khi loại bỏ tín hiệu *Reset* (dùng để thiết lập trạng thái ổn định ban đầu của vòng).

Các PUF dựa trên trạng thái phần tử nhớ khai thác tính ngẫu nhiên trong trạng thái đầu của ô nhớ. Một số PUF thuộc loại này là PUF dựa trên RAM tĩnh, PUF với các bộ chốt ghép chéo, PUF dựa trên bộ chốt,…

- PUF dựa trên RAM tĩnh (*SRAM PUF*) [44,45]: Ô nhớ RAM tĩnh (*SRAM: Static RAM*) có cấu trúc logic gồm hai bộ đảo ghép chéo, có hai trạng thái ổn định. Thăng giáng từ quá trình chế tạo tạo ra sự bất đồng nhất ngẫu nhiên về vật lý trong ô nhớ, xác định đặc tính cấp nguồn. Sau khi được cấp nguồn, các ô nhớ có xu hướng lưu trữ logic $\{0\}$, logic $\{1\}$ hoặc bất kỳ. Sự phân bố của ba loại trạng thái này của các ô nhớ trên cả bộ nhớ là ngẫu nhiên.

- PUF với các bộ chốt ghép chéo (*BPUF: Butterfly PUF*) [46] được đề xuất nhằm khắc phục nhược điểm của SRAM PUF. Trạng thái của ô nhớ SRAM được giả lập trên logic tái cấu hình FPGA bằng cách ghép chéo hai bộ chốt dữ liệu, cho phép hai trạng thái logic ổn định. Trạng thái không ổn định được tạo ra bằng cách sử dụng chức năng *Clear*/*Preset* của bộ chốt. Điều này tương đương với sự chuyển trạng thái của các ô nhớ SRAM sau khi cấp nguồn nuôi, nhưng không cần một thiết bị cấp nguồn thực sự. Tiếp

theo, trạng thái ổn định của một ô BPUF được xác định bởi tính bất đồng nhất về vật lý giữa các bộ chốt và mối ghép chéo.



Hình 1.4: PUF dựa trên trạng thái phần tử nhớ: (a)-(b) Sơ đồ nguyên lý và sơ đồ logic của ô nhớ SRAM [45]; (c) BPUF [46]; (d) PUF dựa trên bộ chốt SR [47].

- PUF dựa trên bộ chốt (*LPUF: Latch PUF*) [47] có kiến trúc tương tự với SRAM PUF và BPUF. Thay vì ghép chéo hai bộ đảo hay hai bộ chốt, hai cổng NOR/NAND được ghép chéo tạo nên mạch chốt NOR đơn giản. Dưới

tác dụng của tín hiệu *Reset*, bộ chốt trở nên không ổn định và tiếp tục hội tụ về một trạng thái ổn định tùy vào sự bất đồng nhất nội tại giữa các linh kiện.

1.2.2. Phân loại PUF theo mức độ bảo mật

Theo kích thước tập CRP, các PUF có thể được phân vào hai nhóm: PUF yếu và PUF mạnh [48-50]. Tương quan giữa số phần tử tập CRP và độ dài dữ liệu đáp ứng PUF đối với PUF yếu là tuyến tính hay đa thức, đối với PUF mạnh là theo hàm mũ.

PUF mạnh chế áp được các tấn công giả lập (*emulation attack*) khi đối phương cố gắng lưu trữ tất cả CRP vào bộ nhớ trong khi PUF yếu dễ bị phá bởi các tấn công dạng này. Các PUF mạnh điển hình là APUF và BR PUF. Đối với các PUF yếu, đối phương có thể kích hoạt mạch PUF với tất cả kích thích có thể có trong một khoảng thời gian hữu hạn. Các PUF yếu phổ biến là SRAM PUF, RO PUF, RS LPUF… Về mặt ứng dụng, các PUF mạnh có thể được sử dụng trực tiếp để xác thực thiết bị mà không cần phần cứng mã hóa bổ sung, trong khi các PUF yếu thích hợp cho việc tạo khóa mã và chuỗi khởi tạo (*seed*) 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

Trong công trình [10], Maes và cộng sự bước đầu thiết lập mô hình toán cho PUF, làm cơ sở cho việc đánh giá hiệu năng các sơ đồ PUF và nghiên cứu ứng dụng PUF trong các tác vụ bảo mật phần cứng.

Lớp PUF (*PUF class*), ký hiệu là $\mathcal{P}$, là mô tả hoàn chỉnh của một kiểu kiến trúc PUF cụ thể. Lớp PUF gồm thủ tục khởi tạo $\mathcal{P}.Create$ dùng để tạo các thực thể của $\mathcal{P}$. Nhìn chung, $\mathcal{P}.Create$ là hàm xác suất, được

biểu diễn tường minh bởi $\mathcal{P}.Create\left(r^C\right)$, với đối số ngẫu nhiên $r^C \leftarrow \{0,1\}^*$ là phép thử nhị phân.

Thực thể PUF (*PUF instance*) *puf* là một thể hiện rời rạc của lớp PUF $\mathcal{P}$, được tạo ra bởi thủ tục $\mathcal{P}.Create$. Lớp PUF có thể được coi là tập tất cả các thực thể của nó:

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

Cấu trúc của nhiều lớp PUF cho phép thực thể PUF *puf* có thể được cấu hình theo biến trạng thái *x* ký hiệu là $puf\left(x\right)$. $puf\left(x\right)$ là cấu trúc vật lý chi tiết của một kiến trúc PUF. Phần có thể cấu hình của một trạng thái được gọi chung là **kích thích (*Challenge*)**, được cấp tới thực thể PUF qua một đầu vào. Tập các kích thích có thể có x đối với một thực thể PUF thuộc lớp $\mathcal{P}$ được ký hiệu là $\mathcal{X}_\mathcal{P}$.

Khởi tạo một thực thể PUF bất kỳ:

$$puf_i \leftarrow \mathcal{P}.Create\left(r_i^C \leftarrow \{0,1\}^*\right) \Leftrightarrow PUF \leftarrow \mathcal{P}.Create \Leftrightarrow PUF \leftarrow \mathcal{P}$$

Mỗi thực thể PUF *puf* có một hàm **ước lượng PUF (*PUF evaluation*)** $puf.Eval$ tạo ra đại lượng biểu thị một phép đo của puf. $puf.Eval$ phụ thuộc trạng thái được biểu diễn bởi thực thể PUF: $puf\left(x\right).Eval$.

$puf\left(x\right).Eval$ cũng là một hàm xác suất có biểu diễn tường minh là $puf\left(x\right).Eval\left(r^E \leftarrow \{0,1\}^*\right)$. Đại lượng tạo ra được gọi là **đáp ứng (*Response*)** của thực thể PUF. Lớp tất cả các giá trị đáp ứng mà một thực thể PUF thuộc lớp PUF $\mathcal{P}$ có thể tạo ra được ký hiệu là $\mathcal{Y}_\mathcal{P}$.

Ước lượng ngẫu nhiên của thực thể PUF puf_i đối với kích thích *x*:

$$y_i^{(j)}(x) \leftarrow puf_i(x).Eval\left(r_j^E \leftarrow \{0,1\}^*\right)$$
$$\Leftrightarrow Y_i(x) \leftarrow puf_i(x).Eval \Leftrightarrow Y_i(x) \leftarrow puf_i(x)$$

Ước lượng ngẫu nhiên của một thực thể PUF ngẫu nhiên đối với kích thích x:

$$Y(x) \leftarrow PUF(x).Eval \Leftrightarrow Y(x) \leftarrow PUF(x)$$

Với nhiều lớp PUF, đầu ra tạo bởi thực thể PUF khi được kích hoạt bị ảnh hưởng bởi các tham số vật lý như nhiệt độ môi trường, mức điện áp nguồn nuôi,… Khi đó, đầu ra được ký hiệu là $puf(x).Eval^{\alpha}$, với $\alpha = (T_{env})$ chỉ thị điều kiện nhiệt độ môi trường T_{env}. Khi bỏ qua α, có thể coi việc kích hoạt được tiến hành ở điều kiện hoạt động danh định.

*** Thực nghiệm PUF:**

Một đáp ứng PUF nhìn chung là một biến ngẫu nhiên. Để đánh giá tính hữu dụng của một lớp PUF cần có thông tin về phân bố xác suất của các đáp ứng PUF. Thông tin này được rút ra từ thực nghiệm.

Các giá trị đáp ứng PUF có thể được phân thành:

i) Các đáp ứng từ các thực thể PUF khác nhau;

ii) Các đáp ứng từ cùng một thực thể PUF tương ứng các kích thích khác nhau.

iii) Các đáp ứng từ cùng một thực thể PUF của cùng một kích thích tương ứng các lần kích hoạt khác nhau.

Một thực nghiệm $(N_{puf}, N_{chal}, N_{meas})$ 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.

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

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

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

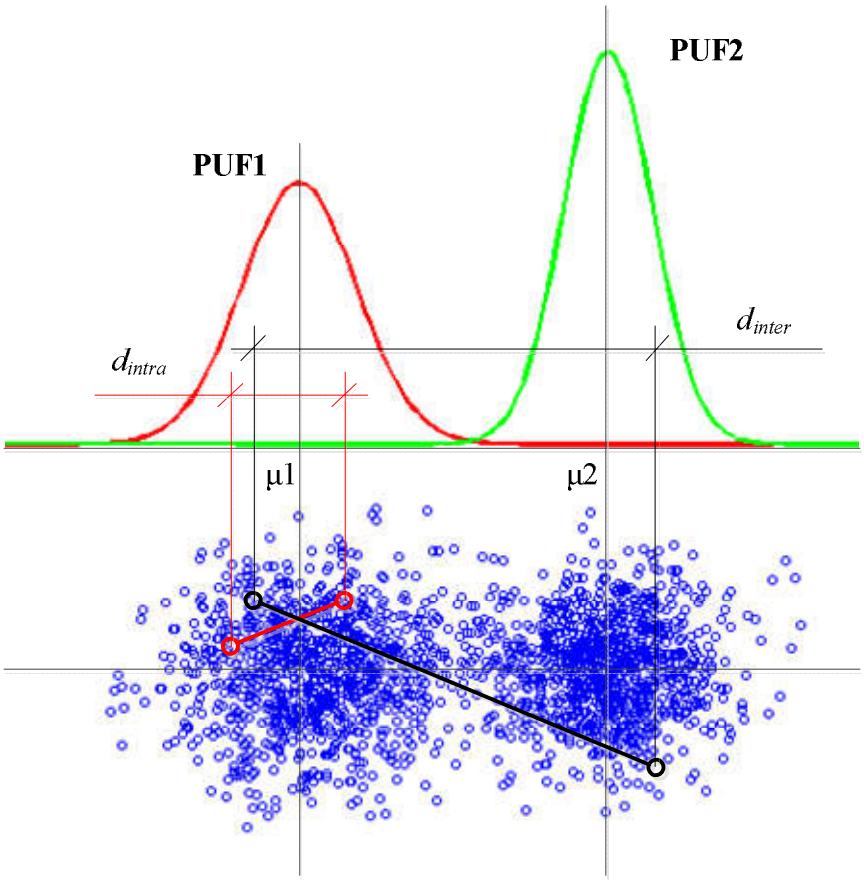
$\forall 1 \le j \le N_{meas} : r_j^E \leftarrow \{0,1\}^*$

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

Tùy vào ứng dụng cụ thể, việc đánh giá chất lượng của một thiết kế PUF căn cứ trên các các chỉ tiêu khác nhau. Đây là điểm đặc biệt so với các lĩnh vực kỹ thuật truyền thống. Các chỉ tiêu đánh giá chất lượng PUF thường dựa trên các tham số định lượng chính mà quan trọng nhất là **khoảng cách nội (*Intra-distance*)** và **khoảng cách tương quan (*Inter-distance*)**.

Đối với một kích thích cụ thể, khoảng cách tương quan giữa hai thực thể PUF là khoảng cách giữa hai đáp ứng xuất hiện khi đồng thời cấp kích thích này tới đầu vào hai thực thể PUF. Đối với một kích thích cụ thể, khoảng cách nội giữa hai lần kích hoạt một thực thể PUF là khoảng cách giữa hai đáp ứng xuất hiện khi tuần tự cấp kích thích này tới đầu vào thực thể PUF. Cả hai khoảng cách này đều được đo đối với cặp đáp ứng tương ứng với **cùng một kích thích**. Hình 1.5 minh họa các tham số khoảng cách này. Mô tả toán học của các tham số khoảng cách được trình bày dưới đây.



Hình 1.5: Minh họa khoảng cách nội và khoảng cách tương quan

*** Khoảng cách nội**

Khoảng cách nội của đáp ứng PUF 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:

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

Với $Y_i(x)$ và $Y_i^{'}(x)$ là hai ước lượng ngẫu nhiên và riêng biệt của thực thể PUF puf_i với cùng một kích thích x. Khoảng cách nội của đáp ứng PUF đối với một thực thể PUF ngẫu nhiên và một kích thích ngẫu nhiên là biến ngẫu nhiên:

$$D_{\mathcal{P}}^{intra}(x) \triangleq D_{PUF \leftarrow \mathcal{P}}^{intra}(\mathcal{X} \leftarrow \mathcal{X}_{\mathcal{P}}) \tag{1.4}$$

Hàm khoảng cách $dist[,;,]$ có thể có độ đo bất kỳ trên tập đáp ứng $\mathcal{Y}$. Thông thường, các đáp ứng có dạng vector ký số nhị phân (*bit vector*) và độ đo khoảng cách được sử dụng là khoảng cách Hamming hoặc khoảng cách Hamming tương đối.

Từ các đáp ứng quan sát được $\mathcal{Y}_{Exp(\mathcal{P})}$ có thể tính được tập khoảng cách nội đáp ứng $D^{intra}_{Exp(\mathcal{P})}$:

$$D^{intra}_{Exp(\mathcal{P})} = dist\left[y_i^{(j_1)}(x_k); y_i^{(j_1)}(x_k) \right] \Big| \begin{matrix} \forall 1 \le i \le N_{puf}; \forall 1 \le k \le N_{chal}; \\ \forall 1 \le j_1 \ne j_2 \le N_{meas} \end{matrix} \quad (1.5)$$

Các tham số của phân bố xác xuất $D^{intra}_{\mathcal{P}}$ được cho bởi:

- Trung bình thống kê:

$$\mu^{intra}_{\mathcal{P}} = \overline{D^{intra}_{Exp(\mathcal{P})}} = \frac{2}{N_{puf} N_{chal} N_{meas} (N_{meas} - 1)} \sum D^{intra}_{Exp(\mathcal{P})} \quad (1.6)$$

- Độ lệch chuẩn:

$$\sigma^{intra}_{\mathcal{P}} = \sqrt{\frac{2}{N_{puf} N_{chal} N_{meas} (N_{meas} - 1) - 2} \sum \left(D^{intra}_{Exp(\mathcal{P})} - \mu^{intra}_{\mathcal{P}} \right)^2} \quad (1.7)$$

Các biến thiên về nhiệt độ môi trường và điện áp nguồn nuôi trong điều kiện thực nghiệm có ảnh hưởng đến khoảng cách nội giữa các đáp ứng PUF. Khoảng cách nội giữa hai đáp ứng PUF ước lượng trên cùng thực thể PUF và với cùng một kích thích, nhưng ở các điều kiện khác nhau α_1 và α_2 thông thường lớn hơn khoảng cách nội giữa các đáp ứng ước lượng trong cùng điều kiện.

*** Khoảng cách tương quan**

Khoảng cách tương quan của đáp ứng PUF là biến ngẫu nhiên mô tả

khoảng cách giữa hai đáp ứng PUF từ hai thực thể PUF sử dụng cùng một kích thích:

$$D_{\mathcal{P}}^{inter} \triangleq dist\left[Y(x);Y'(x)\right] \tag{1.8}$$

Với $Y(x)$, $Y'(x)$ 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 $PUF'(\neq PUF) \leftarrow \mathcal{P}$. Khoảng cách tương quan của đáp ứng PUF đối với một kích thích ngẫu nhiên là biến ngẫu nhiên:

$$D_{\mathcal{P}}^{inter} \triangleq D_{\mathcal{P}}^{inter}\left(\mathcal{X} \leftarrow \mathcal{X}_{\mathcal{P}}\right) \tag{1.9}$$

Từ các đáp ứng quan sát được $\mathcal{Y}_{Exp(\mathcal{P})}$ có thể tính được tập khoảng cách tương quan của đáp ứng $D_{Exp(\mathcal{P})}^{inter}$:

$$D_{Exp(\mathcal{P})}^{inter} = dist\left[y_{i_1}^{(j)}(x_k); y_{i_2}^{(j)}(x_k)\right]\Big|^{\forall 1 \le i_1 \ne i_2 \le N_{puf}; \forall 1 \le k \le N_{chal}; \forall 1 \le j \le N_{meas}} \tag{1.10}$$

Các tham số của phân bố xác xuất $D_{\mathcal{P}}^{inter}$ được cho bởi:

- Trung bình thống kê:

$$\mu_{\mathcal{P}}^{inter} = \overline{D_{Exp(\mathcal{P})}^{inter}} = \frac{2}{N_{puf}\left(N_{puf}-1\right)N_{chal}N_{meas}} \sum D_{Exp(\mathcal{P})}^{inter} \tag{1.11}$$

- Độ lệch chuẩn:

$$\sigma_{\mathcal{P}}^{inter} = \sqrt{\frac{2}{N_{puf}\left(N_{puf}-1\right)N_{chal}N_{meas}-2} \sum\left(D_{Exp(\mathcal{P})}^{inter} - \mu_{\mathcal{P}}^{inter}\right)^2} \tag{1.12}$$

Khoảng cách tương quan giữa các đáp ứng PUF cũng chịu ảnh hưởng của các biến thiên trong điều kiện thực nghiệm.

1.3.3. Các chỉ tiêu chất lượng của PUF

Một sơ đồ PUF được đánh giá [10] 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 sao chép về vật lý (*Physical Unclonability*), tính không thể dự đoán (*Unpredictability*),…

*** Khả năng thực thi**

Lớp PUF $\mathcal{P}$ có thể thực thi được nếu có thể dễ dàng thực hiện hàm $Create$ và tạo ra một thực thể PUF ngẫu nhiên:

$$puf \leftarrow \mathcal{P}.Create\left(r^C \leftarrow \{0,1\}^*\right) \tag{1.13}$$

*** Khả năng ước lượng**

Lớp PUF $\mathcal{P}$ có thể ước lượng nếu nó khả thi, đối với bất kỳ thực thể PUF ngẫu nhiên $puf \in \mathcal{P}$ và bất kỳ kích thích ngẫu nhiên $x \in \mathcal{X}_{\mathcal{P}}$, có thể dễ dàng ước lượng đáp ứng:

$$y \leftarrow puf(x).Eval\left(r^E \leftarrow \{0,1\}^*\right). \tag{1.14}$$

*** Khả năng tái lập**

Lớp PUF $\mathcal{P}$ thể hiện khả năng tái lập nếu nó có thể ước lượng và:

$$\Pr\left(D_{\mathcal{P}}^{intra} small\right) high^{5}. \tag{1.15}$$

*** Tính duy nhất**

Lớp PUF $\mathcal{P}$ có tính duy nhất nếu nó có thể ước lượng và:

$$\Pr\left(D_{\mathcal{P}}^{inter} high\right) high. \tag{1.16}$$

[5] Ký hiệu trong công thức: *small* ~ nhỏ, *high* ~ lớn.

*** Khả năng định danh**

Lớp PUF $\mathcal{P}$ có khả năng định danh nếu nó có thể tái lập và có tính duy nhất, cụ thể:

$$\Pr\left(D_{\mathcal{P}}^{intra} < D_{\mathcal{P}}^{inter}\right) high. \tag{1.17}$$

*** Tính không thể sao chép về vật lý**

Lớp PUF $\mathcal{P}$ là không thể sao chép về vật lý nếu nó có thể ước lượng, khó tác động để hàm $\mathcal{P}.Create$ tạo ra hai thực thể PUF phân biệt puf và $puf' \in \mathcal{P}$ thỏa mãn:

$$\Pr\left(dist\left[Y \leftarrow puf\left(X\right); Y' \leftarrow puf'\left(X\right)\right] < D_{\mathcal{P}}^{inter}\left(X\right)\right) high, \tag{1.18}$$

với $X \leftarrow \mathcal{X}_{\mathcal{P}}$

Ở trường hợp cực hạn, khó tạo ra hai thực thể PUF thỏa mãn:

$$\Pr\left(dist\left[Y \leftarrow puf\left(X\right); Y' \leftarrow puf'\left(X\right)\right] > D_{\mathcal{P}}^{intra}\left(X\right)\right) small \tag{1.19}$$

*** Tính không thể dự báo**

Lớp PUF $\mathcal{P}$ thể hiện tính không thể dự báo nếu nó có thể ước lượng và khó thỏa mãn điều kiện thiết lập dưới đây. Với một thực thể PUF ngẫu nhiên $puf \in \mathcal{P}$, giả định các quy tắc sau:

- Pha học mẫu: Kích hoạt puf đối với tập hạn chế các kích thích và ghi nhận các đáp ứng. Tập kích thích là $\mathcal{X}_{\mathcal{P}}^{'}$ với các phần tử được chọn ngẫu nhiên (tính không thể dự đoán yếu) hoặc thích nghi (tính không thể dự đoán mạnh).

- Pha kích hoạt: Cho trước kích thích ngẫu nhiên $X \leftarrow \mathcal{X}_{\mathcal{P}} \setminus \mathcal{X}_{\mathcal{P}}^{'}$, dự đoán đáp ứng Y_{pred} khi kích hoạt puf bởi kích thích X. Y_{pred} được tạo bởi thuật

toán dự báo $predict$ hình thành trong pha học mẫu trên:

$$Y_{pred} \leftarrow predict(X) \tag{1.20}$$

Nếu điều kiện:

$$\Pr\left(dist\left[Y_{pred} \leftarrow predict(X); Y \leftarrow puf(X)\right] < D_{\mathcal{P}}^{inter}(X)\right) high \tag{1.21}$$

khó thỏa mãn, lớp PUF $\mathcal{P}$ được xem là không thể dự báo.

Đối với các PUF bán dẫn sử dụng độ đo khoảng cách Hamming, các chỉ tiêu chất lượng có thể được cụ thể hóa như sau [11].

*** Tính duy nhất**

Tiến hành đo lường mức độ biến thiên của các mẫu đáp ứng của cùng một tập mẫu kích thích thu được từ các chip khác nhau. Nếu X_i và X_j là các đáp ứng $n-bit$ của chip thứ i và thứ j của cùng kích thích C, tính duy nhất U được định lượng qua khoảng cách tương quan trung bình giữa k cấu kiện:

$$U = \frac{2}{k(k-1)} \sum_{i=1}^{k-1} \sum_{j=i+1}^{k} \frac{HD(X_i, X_j)}{n} \times 100\% \tag{1.22}$$

Trong đó, $HD(X_i, X_j)$ là khoảng cách Hamming giữa các chuỗi $n-bit$ X_i và X_j. Giá trị lý tưởng của U là 50%.

*** Tính ngẫu nhiên**

Tính ngẫu nhiên được định lượng qua độ đo R xác định mức phân bố đều của tỷ lệ các bit $\{0\}$ và bit $\{1\}$ trong đáp ứng PUF:

$$R_{y_i} = \frac{1}{n} \sum_{j=1}^{n} r_{i,j} \times 100\% \tag{1.23}$$

Với $r_{i,j}$ là bit thứ j trong mẫu đáp ứng $n-bit$ đối với chip thứ i. Giá trị lý tưởng của R là 50%.

*** Tính ổn định**

Tính ổn định xác định khả năng của PUF trong việc tạo ra cùng một đáp ứng một cách hiệu quả từ mẫu kích thích đã cho, xét tại các điều kiện hoạt động khác nhau (biến thiên về điện áp nguồn nuôi, nhiệt độ môi trường) có tính đến sự lão hóa của cấu kiện. Đối với chip thứ i, khoảng cách nội trung bình được xác định bởi:

$$HD_i^{intra} = \frac{1}{s}\sum_{t=1}^{s}\frac{HD\left(X_i, X_{i,t}\right)}{n} \times 100\% \tag{1.24}$$

Khi đó, tính ổn định của PUF được định nghĩa bởi:

$$S_{y_i} = 100\% - HD_i^{intra} \tag{1.25}$$

Giá trị lý tưởng của S là 100% . Trị số S trung bình đối với k chip được tính bởi:

$$S_{avg} = \frac{1}{k}\sum_{i=1}^{k} S_{y_i} \tag{1.26}$$

Các chỉ tiêu chất lượng của các cấu trúc PUF có thể thay đổi tùy vào ứng dụng PUF cụ thể.

1.4. Ứng dụng của PUF

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 lớp vật lý.

1.4.1. Định danh và xác thực thiết bị

Do đặc tính không thể sao chép về vật lý, PUF được ứng dụng vào

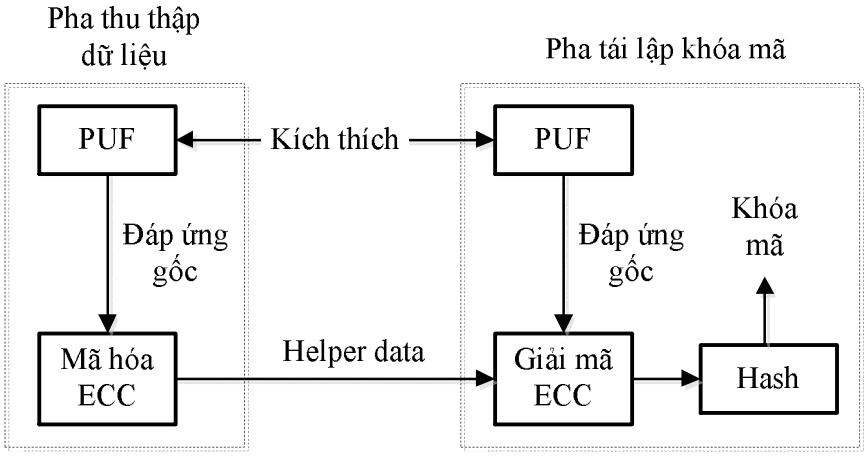
công nghệ chống giả mạo. Các đáp ứng PUF có thể được sử dụng trực tiếp tương tự như lược đồ nhận dạng vân tay sinh trắc. Trong pha tập hợp dữ liệu (*enrollment*), các CRP của các thực thể PUF được lưu vào cơ sở dữ liệu cùng với định danh (ID) của hệ vật lý gắn thực thể PUF. Trong pha xác thực (*authentication*), CRP của hệ cần xác minh sẽ được so với một mẫu CRP bất kỳ trong cơ sở dữ liệu. Nếu các đáp ứng đủ gần, việc xác thực là thành công và ngược lại. Mẫu CRP đã sử dụng sẽ bị loại khỏi cơ sở dữ liệu nhằm loại trừ nguy cơ tấn công lặp. Quá trình xác thực sẽ căn cứ vào mức ngưỡng được xác định theo đặc trưng thống kê của các tham số khoảng cách cũng như yêu cầu của ứng dụng cụ thể.

Một số thiết kế hệ thống xác thực dựa trên PUF đã được phát triển trên FPGA. Thiết kế PUF dựa trên DRAM trong [51] tạo chuỗi bit ổn định được sử dụng làm ID 128-bit cho chip. Trong [52], các tác giả trình bày phương pháp tạo ID cho chip sử dụng RO cấu hình được, đề xuất sơ đồ tái kích hoạt trực giao (*orthogonal reinitialization*) nhằm cải thiện tính lặp lại (*repeatability*) của dữ liệu được sử dụng làm ID. Trong [53], các tác giả đề xuất giao thức xác thực dựa trên so sánh các mẫu đáp ứng từ một APUF. Các tác giả trong [54] đề xuất giao thức bảo mật bảo đảm xác thực lẫn nhau giữa các thiết bị kết nối. …

1.4.2. Tạo khóa mã bảo mật

Độ an toàn của một lược đồ mã hóa phụ thuộc việc bảo mật khóa mã. Các đáp ứng PUF từ bản chất vật lý chứa tạp và nhạy với điều kiện môi trường nên không thể được sử dụng trực tiếp làm khóa mã, do đó cần một cơ chế sửa lỗi trên chip (*on-chip*).

Theo cách tiếp cận truyền thống, quá trình tạo khóa mã bảo mật gồm hai pha (Hình 1.6):



Hình 1.6: Ứng dụng PUF tạo khóa mã bảo mật [25]

i) Thu thập dữ liệu (enrollment): Dữ liệu bổ trợ (*helper data*) được tính từ các mẫu đáp ứng PUF sử dụng mạch mã hóa sửa lỗi (ECC);

ii) Tái lập khóa mã (key regeneration): Pha tái lập khóa mã loại bỏ tạp khỏi đáp ứng PUF. Với dữ liệu bổ trợ, bộ giải mã ECC bù lỗi phát sinh trong dữ liệu PUF do sự thay đổi của nhiệt độ và điện áp.

1.4.3. Tạo số ngẫu nhiên

Số ngẫu nhiên được sử dụng rộng rãi trong mã hóa bảo mật để tạo khóa mã, tạo các chuỗi khởi tạo ngẫu nhiên... Thông thường, các số ngẫu nhiên được tạo bởi các bộ tạo số giả ngẫu nhiên (*PRNG: Pseudo-Random Number Generator*) bằng các thuật toán giả lập tính ngẫu nhiên. Yêu cầu đặt ra đối với các chuỗi khởi tạo (*seed*) dùng cho các thuật toán này là phải đảm bảo tính duy nhất, hoàn toàn ngẫu nhiên và không thể dự đoán. Đáp ứng PUF có thể được dùng như các chuỗi khởi tạo cho PRNG. Trong [55], chuỗi khởi tạo được tạo bởi PUF có chứa logic điều khiển để đảm bảo các số ngẫu nhiên được tạo ra là phi chu kỳ. Trong [56-58], các chuỗi khởi tạo ngẫu nhiên thực sự được tách từ tạp trong mẫu khởi động của SRAM và được dùng làm đầu vào cho bộ tạo số ngẫu nhiên không xác định (*nondeterministic RNG*).

1.4.4. Bảo vệ IP

Sự phát triển của các công cụ trợ giúp thiết kế làm tăng tính linh hoạt trong thiết kế số, dễ dàng chuyển giao, cập nhật thiết kế qua mã HDL, đồng thời cũng đặt ra vấn đề bảo vệ sở hữu trí tuệ đối với các thiết kế, chống linh kiện giả. Công trình [59] đề xuất kỹ thuật mã hóa/giải mã file cấu hình thiết kế (*bitstream*) sử dụng khóa mã bảo mật tách ra từ PUF. Các giải pháp cải tiến kỹ thuật này gồm: Xác thực khóa mã theo chu kỳ [60]; sử dụng khóa mã tạo từ PUF cho cả mã hóa và xác thực MAC [45]; phát triển giao thức dựa trên mã hóa công khai để bảo vệ IP trên FPGA [44], theo đó các khóa riêng không tách khỏi FPGA và làm tăng tính bảo mật của cả hệ thống. Các tác giả trong [61] đề xuất cơ chế xác thực sử dụng kết hợp PUF và máy trạng thái hữu hạn (*FSM: Finite State Machine*) để bảo vệ IP cho các hệ thống trên chip (*SoC: System-on-Chip*) trên FPGA.

PUF đã và đang thu hút sự chú ý mạnh mẽ của cộng đồng nghiên cứu trong những năm gần đây, cả trên phương diện lý thuyết và thực nghiệm. Các ứng dụng PUF trên nền VLSI thương mại hiện có đã hiện thực hóa PUF từ chỗ là mô hình toán lý tưởng trở thành các nguyên mẫu đặc biệt hữu dụng, được ứng dụng rộng rãi trong lĩnh vực bảo mật phần cứng. Tuy nhiên, các thiết kế phần cứng PUF không phải luôn có cùng đặc tính kỳ vọng với PUF lý tưởng và chính điều này tạo ra nguy cơ đối với bảo mật phần cứng như tính nhạy cảm với tấn công dựa trên mô hình… Các nghiên cứu về PUF hiện tại và tương lai tập trung chủ yếu vào tìm hiểu khả năng và giới hạn của PUF qua việc phát triển các thiết kế PUF mới với việc cải thiện các đặc tính PUF, các hình thức tấn công tiềm tàng đối với PUF [62].

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, hướng phát triển của việc nghiên cứu và ứng dụng PUF. Từ nghiên cứu tổng quan về PUF trong chương 1, nghiên cứu sinh xác định phạm vi nghiên cứu cụ thể phù hợp với công nghệ thiết kế số hiện có và lĩnh vực ứng dụng quan tâm. Nội dung này sẽ được trình bày trong chương 2.

CHƯƠNG 2: THIẾT KẾ RO PUF TRÊN FPGA

2.1. Thiết kế phần cứng RO PUF trên FPGA

2.1.1. Thiết kế PUF trên FPGA

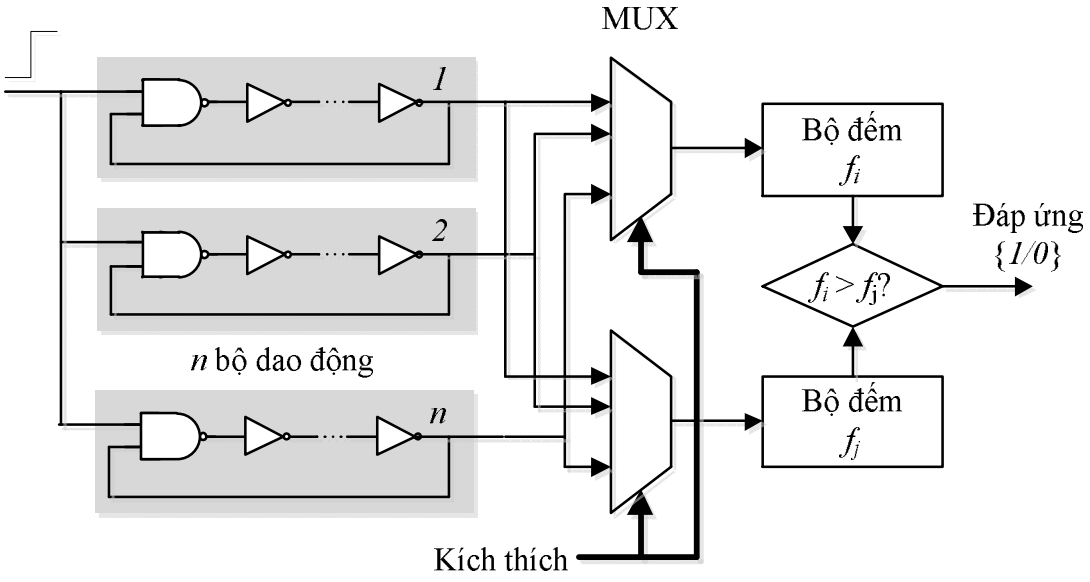
Ngày nay, công nghệ logic khả trình đã và đang phát triển mạnh mẽ, có khả năng cung cấp tài nguyên phần cứng lớn với chi phí thấp cũng như đảm bảo sự linh hoạt trong thiết kế đối với các ứng dụng cụ thể. So với các công nghệ logic khả trình khác (ASIC, DSP…), FPGA có một số ưu thế như thời gian phát triển sản phẩm ngắn, chi phí thiết kế thấp, khả năng tái sử dụng cao, dễ dàng nâng cấp, chuyển đổi giữa các họ linh kiện do có thể dùng chung mã nguồn HDL cho các công nghệ khác nhau [63]… Vì vậy, FPGA được ứng dụng rộng rãi trong nhiều lĩnh vực như y sinh, cảm ứng xa, điện tử dân dụng, hệ thống điều khiển công nghiệp... [64-67]. Việc phát triển các ứng dụng cụ thể trên nền FPGA đối với người sử dụng trở nên dễ dàng nhờ các công cụ hỗ trợ thiết kế.

Nhiều thiết kế PUF đã được nghiên cứu và phát triển trên ASIC và đặc biệt là FPGA. Các hãng sản xuất FPGA lớn hiện nay như *Xilinx*, *Intel* và *Microsemi* đã bắt đầu tích hợp PUF vào sản phẩm nhằm mục đích bảo mật [68-70]. Việc phát triển các thiết kế PUF trên FPGA là một hướng nghiên cứu quan trọng nhằm khai thác các ưu thế của công nghệ này. Tuy nhiên, 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. Mạch vật lý của PUF yêu cầu tính đồng nhất và đối xứng cao. Điều này khó đạt được đối với công nghệ tái cấu hình mạch logic, ngoại trừ một số sơ đồ PUF có độ phức tạp ít nhất, trong đó có RO PUF. Số lượng các nghiên cứu về RO PUF chiếm một phần đáng kể trong các thiết kế đề xuất

thực thi trên FPGA (Bảng PL1.1). Trong chương này, nghiên cứu sinh trình bày các kỹ thuật và phương pháp đặc biệt trong thiết kế mạch RO PUF trên FPGA, đề xuất mô hình thống kê của tần số RO và phân tích số liệu thực nghiệm để rút ra đặc tính của các nhân tố ảnh hưởng đến tần số RO.

2.1.2. Kiến trúc RO PUF trên FPGA

Thiết kế cơ bản của RO PUF trên FPGA [42] được trình bày trên Hình 2.1. Mảng RO gồm n RO có cấu trúc mạch vật lý đồng nhất. Kích thích được chọn là các bit dữ liệu điều khiển hai bộ ghép kênh, nhằm chọn ra cặp tần số RO f_i và $f_j (i \neq j)$ trong tập các tần số $f_1 - f_n$. Do các biến thiên tham số vật lý từ quá trình chế tạo và tác động của các điều kiện hoạt động khác nhau, các tần số tuyệt đối RO thường khác biệt giữa các RO trên một chip đơn cũng như đối với mỗi RO trên các chip khác nhau.



Hình 2.1: Sơ đồ RO PUF cơ bản [42]

Giá trị bit đáp ứng r_{ij} được xác định bởi biểu thức [71]:

$$r_{ij} = \begin{cases} 1 & : f_i > f_j \\ 0 & : others \end{cases} \quad (2.1)$$

$$\Leftrightarrow r_{ij} = \text{sgn}(f_i - f_j) - 1 \quad (2.2)$$

RO PUF thuộc lớp các PUF yếu bởi tập kích thích chỉ có hữu hạn phần tử dùng để định cấu hình RO PUF. Sau khi được thực thi, tần số RO được thiết lập dựa trên các bit kích thích. Việc thay đổi kích thích đầu vào sẽ dẫn tới sự khác biệt tần số và đáp ứng đầu ra.

Có thể thấy một số hạn chế của thiết kế này là:

- Với việc sử dụng hàm dấu[6] để tạo dữ liệu đáp ứng, phần lớn thông tin bị loại bỏ (giá trị tần số, dấu của tần số hiệu,..);

- Để tách ra ID tin cậy và duy nhất, mỗi RO chỉ được sử dụng một lần để tạo ra một bit đơn và tránh hiện tượng tương quan[7] (*correlation*) trong dữ liệu đáp ứng. Với n RO (n chẵn), thiết kế cơ bản thành lập $n/2$ cặp RO dùng trong so sánh tần số, từ đó tạo $n/2$ bit đáp ứng.

- Các RO rất nhạy với sự biến thiên nhiệt độ môi trường cũng như các nhân tố biến thiên toàn cục khác, việc so sánh trực tiếp các giá trị tần số RO cũng sẽ phụ thuộc nhiệt độ: Trong một dải nhiệt độ, $f_i > f_j$, trong dải nhiệt độ khác, $f_i < f_j$ [13]…

Do các nguyên nhân trên, sơ đồ cơ bản hầu như không khả thi trong việc tách ra ID cho thiết bị. Từ thiết kế RO PUF cơ bản, nhiều nghiên cứu đã được tiến hành theo các hướng sau:

[6] Trong trường hợp chung, trị số tần số RO là đại lượng thống kê, do đó có thể coi đối số (f_i - f_j) của hàm sgn luôn khác 0, r_{ij} chỉ nhận giá trị *0* hoặc *1*, đại diện cho bit $\{0\}$ và bit $\{1\}$.

[7] Nếu trong so sánh trị số tần số, các RO được ghép cặp bất kỳ thì sẽ xảy ra trường hợp: $f_a > f_b$ tạo một bit $\{1\}$, $f_b > f_c$ tạo một bit $\{1\}$. Khi đó, đương nhiên sẽ có $f_a > f_c$ và bit $\{1\}$ tạo ra là tương quan với các bit đáp ứng đã tạo trên. Với $n!$ hoán vị có thể có từ n RO, số bit độc lập có thể tạo ra là $\log_2(n!)$. Để đơn giản hóa thiết kế, các tác giả trong [42] chọn phương pháp ghép cặp trong đó mỗi RO chỉ được sử dụng một lần. Từ n RO thành lập $n/2$ cặp RO, tạo $n/2$ bit đáp ứng.

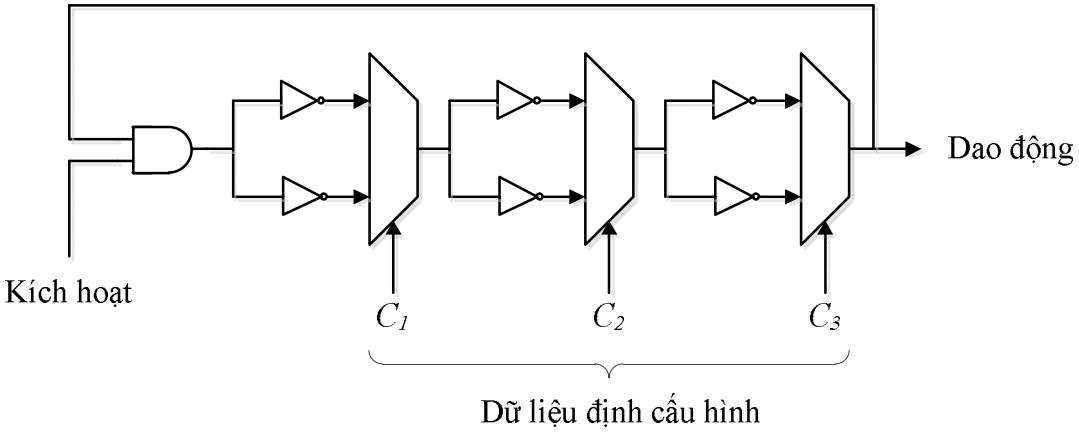
i) Cải tiến chất lượng mạch vật lý RO PUF: Tăng tính linh hoạt trong khả năng định cấu hình mạch RO, tăng tính đồng nhất và đối xứng trong thiết kế vật lý mảng RO.

ii) Nâng cao hiệu quả tách dữ liệu đáp ứng RO PUF.

Để tăng tính linh hoạt trong khả năng định cấu hình mạch RO, các biến thể sau được đề xuất.

*** RO PUF có thể cấu hình**

Sơ đồ RO PUF có thể cấu hình (*CRO PUF: Configurable RO PUF*) [71] được trình bày trên Hình 2.2. Một bộ ghép kênh được dùng để chọn một trong hai bộ đảo tại mỗi tầng của RO. Một RO N tầng có thể được cấu hình để tạo 2^N tần số khác nhau. Phương pháp này sử dụng các cấu hình có sự khác biệt về độ trễ lớn nhất nhằm giảm tạp trong các đáp ứng RO PUF, cải thiện độ tin cậy của RO PUF.



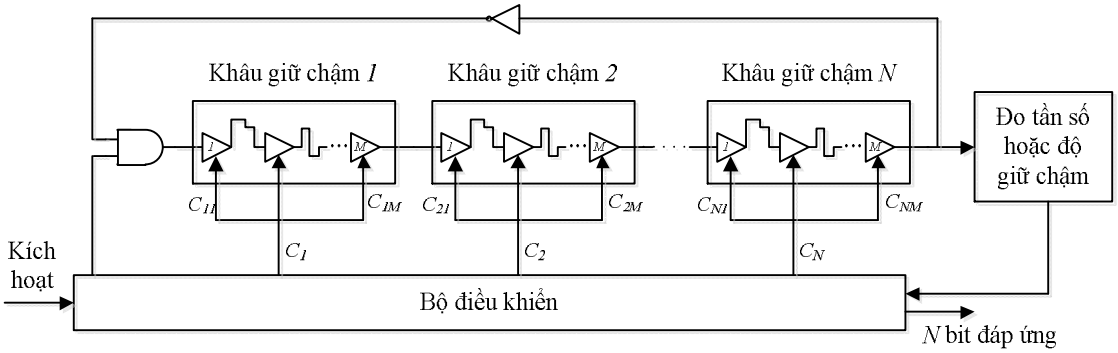
Hình 2.2: Sơ đồ RO PUF có thể cấu hình [71]

Các tác giả trong [72-74] cải tiến thiết kế trên và tạo nhiều bit đầu ra hơn với cùng diện tích bán dẫn trên các FPGA của Xilinx. Gao trong [75] đề xuất thiết kế CRO PUF khác có tính linh hoạt và độ tin cậy cao với việc xây dựng RO PUF ở mức bộ đảo thay vì ở mức RO. Tuy nhiên, các kỹ

thuật này trong khi cải thiện được độ tin cậy lại yêu cầu tài nguyên phần cứng lớn. Để khắc phục điều này, các tác giả trong [76] đề xuất thiết kế RO PUF mắc chéo nhằm nâng cao tính linh hoạt và độ tin cậy trong khi giảm thiểu mức tiêu thụ tài nguyên phần cứng. Trọng tâm của thiết kế là chọn các bộ đảo từ nhiều cặp RO bằng việc sử dụng các LUT. Trong [77,78], các tác giả xây dựng CRO PUF với độ trễ khả trình.

*** RO PUF đơn**

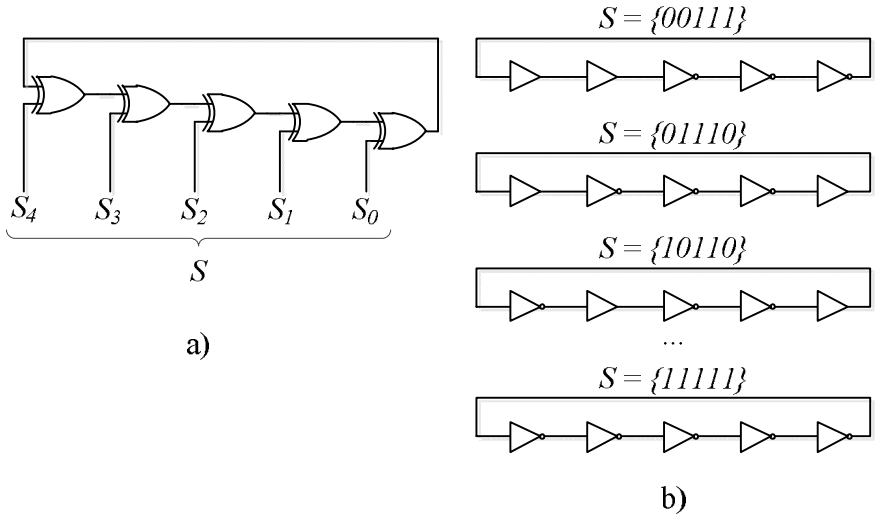
RO PUF đơn (*Loop PUF*) [79] chỉ gồm một mạch RO, trong đó các bộ đảo được thay thế bởi phần tử trễ điều khiển được. RO PUF đơn so sánh các tần số RO tương ứng các cấu hình RO PUF khác nhau theo phương pháp tuần tự thay vì song song trong quá trình tạo bit đáp ứng (Hình 2.3).



Hình 2.3: Sơ đồ RO PUF đơn [79]

*** RO PUF tái cấu hình sử dụng cổng XOR**

RO PUF tái cấu hình sử dụng cổng XOR (*XRRO PUF*) [80] sử dụng các cổng XOR thay cho các bộ đảo trong sơ đồ RO PUF cơ bản (Hình 2.4). Cổng XOR đóng vai trò là bộ đệm hay bộ đảo tùy vào bit điều khiển (bit trạng thái) có giá trị $\{0\}$ hay $\{1\}$. Bằng cách thay đổi dữ liệu điều khiển các cổng XOR sao cho số bộ đảo trong mạch là số lẻ, có thể thay đổi độ giữ chậm của mạch và do đó thay đổi tần số RO.



Hình 2.4: RO dựa trên các cổng XOR (a) và phương pháp cấu hình (b) [80]

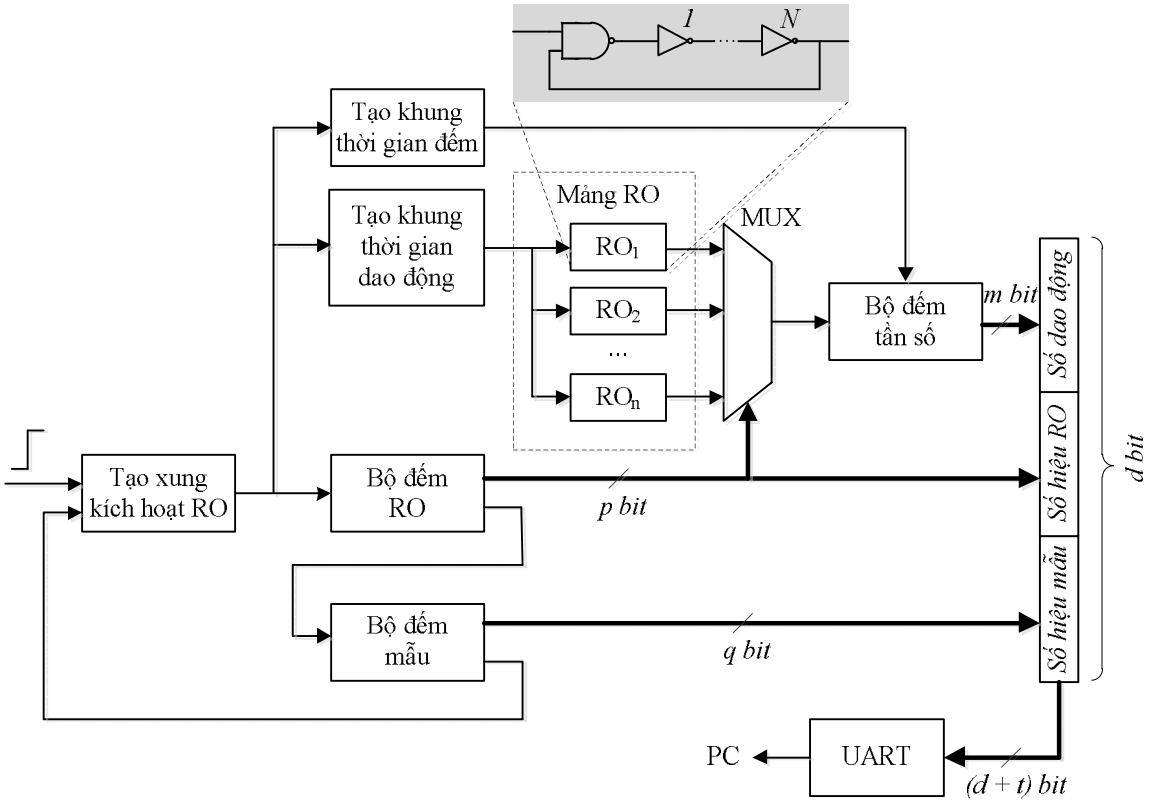
Để tăng tính đồng nhất và đối xứng trong thiết kế vật lý mảng RO, Merli và cộng sự trong [81] sử dụng kỹ thuật *hard macro* trong thiết kế số trên FPGA Spartan-3E để tạo các macro (khối thiết kế cơ sở) và sao chép ra các vị trí khác nhau trên FPGA.

Để cải thiện hiệu quả xử lý dữ liệu, các công trình nghiên cứu tập trung nâng cao số bit đáp ứng có thể tách ra từ cùng một tập n tần số RO. Trong thiết kế cơ bản, với phương pháp so sánh ghép cặp, từ n RO có thể tạo ra $n/2$ bit đáp ứng. Trong [82], phương pháp so sánh ghép cặp liên tiếp có thể tạo ra $(n-1)$ bit đáp ứng. Yin và cộng sự trong [83] nhóm các RO trong cùng một điều kiện, qua đó tăng số bit đáp ứng từ $O(n)$ lên $O(n\log_2 n)$. Để đảm bảo độ tin cậy, mức ngưỡng R_{th} được chọn sao cho khác biệt giữa các tần số trong các nhóm không nhỏ hơn R_{th}. Trong [84], để giảm các thăng giáng hệ thống và tách ra các thăng giáng xảy ra trong quá trình chế tạo, các tác giả thiết kế bộ khử thăng giáng dựa trên kỹ thuật ngoại suy đa thức bám theo quy luật biến thiên của thăng giáng hệ thống…

Nhìn chung, các thiết kế biến thể làm tăng quy mô của mạch vật lý.

Về mặt thực thi phần cứng, các bộ ghép kênh chiếm nhiều tài nguyên và có cấu trúc nối mạch phức tạp hơn nhiều các phần tử logic khác. Ngoài ra, các phương pháp đã đề xuất chưa làm rõ quy mô tác động của các nhân tố biến thiên lên tần số RO, cơ chế khai thác đặc tính của các nhân tố biến thiên để có thể tách ra ID cho thiết bị.

Để khảo sát ảnh hưởng của các nhân tố biến thiên lên tần số RO, từ mạch RO PUF cơ bản (Hình 2.1), nghiên cứu sinh xây dựng thiết kế RO PUF có sơ đồ chức năng được trình bày trên Hình 2.5. Sơ đồ gồm mảng RO mô-đun hóa, các khối điều khiển và giao tiếp được duy trì tối thiểu nhằm tách và thu nhận dữ liệu tần số tuyệt đối của các RO. Sơ đồ chức năng chi tiết và mạch vật lý trên FPGA tương ứng được trình bày trên Hình PL 1.1 và Hình PL1.2, Hình PL1.3.



Hình 2.5: Sơ đồ chức năng mạch RO PUF đề xuất

Phần tử giữ chậm (bộ đảo) của RO được cấu hình từ một LUT nguyên bản. Nhằm duy trì tính đồng nhất về mạch vật lý của các RO, N bộ đảo (N chẵn) và một cổng NAND trong mạch RO cơ bản được kết nối thủ công, sử dụng công cụ Xilinx ISE/FPGA Editor. Sau đó, sử dụng kỹ thuật *hard macro* đóng gói RO cơ bản để tạo ra một macro RO. Macro RO được sao chép ra các vị trí khác nhau trên FPGA tạo thành các thực thể RO (Sau đây gọi tắt là RO). Vì chưa cần ghép cặp các RO, mạch chỉ sử dụng một bộ đếm tần số nhằm tiết kiệm tài nguyên phần cứng và loại bỏ sai số đếm gây ra bởi khác biệt về phần cứng thực thi các bộ đếm. Các RO được bố trí sao cho mảng RO có cấu trúc đối xứng và giảm thiểu khác biệt về độ trễ giữa các kết nối RO tới bộ đếm tần số. Các dao động RO được ghép kênh trước khi cấp tuần tự tới bộ đếm. Các mạch bổ trợ của thiết kế gồm giao diện truyền số liệu nối tiếp không đồng bộ (*UART: Universal Asynchronous Receiver-Transmitter*) và các mạch tạo xung đồng bộ cho hoạt động của hệ thống. Xung kích hoạt RO được tạo ra từ việc chia tần xung nhịp hệ thống (*clock*), có chu kỳ lặp lại đủ lớn cho việc truyền dữ liệu nối tiếp qua giao diện UART. Bộ đếm RO tạo p bit dữ liệu điều khiển bộ chọn kênh, tuần tự chuyển mạch RO_1 – RO_n tới đầu ra trong một chu kỳ lấy mẫu. Bộ đếm tần số được tái lập (*reset*) đầu mỗi chu kỳ chuyển mạch RO, đo số dao động RO trong khoảng thời gian được thiết lập bởi bộ tạo khung thời gian đếm. Bộ đếm mẫu được kích bởi sườn trước xung kết thúc đếm của bộ đếm RO, được dùng để đếm và khống chế số mẫu. Để truyền qua giao diện UART, d bit dữ liệu truyền sẽ được bổ sung t bit dữ liệu đệm để tạo khung dữ liệu phù hợp.

Trong thiết kế cụ thể này, với mục đích khảo sát đặc tính tần số của một tập RO tương đối khác biệt về độ giữ chậm, chọn $N = 16$, $p = 5$, $n = 2^p = 32$. Khoảng thời gian đo ΔT_{mea} được chọn đủ lớn để giảm thiểu sai

số tính tần số RO (bằng tích của trị số đếm được của bộ đếm tần số RO với $1/\Delta T_{mea}$), $\Delta T_{mea} = 20ms$. Từ đó xác định được độ rộng dữ liệu đếm của bộ đếm tần số $m = 24$. Chọn $q = 16$ để có thể linh hoạt chọn số lượng lớn mẫu cần thu nhận (đến 2^q mẫu). Để đảm bảo truyền không lỗi qua UART, khung dữ liệu truyền được chọn có độ rộng $(d + t) = 48$.

Thiết kế có tính tùy biến cao và có thể chuyển đổi linh hoạt giữa các công nghệ FPGA chỉ với một số thay đổi nhỏ. Họ FPGA Xilinx Artix-7 và phần mềm thiết kế Vivado không hỗ trợ việc tạo các macro, tuy nhiên có thể sử dụng lệnh để gán các phần tử logic cho các LUT. Quá trình này cần được giám sát chặt chẽ nhằm đảm bảo tính đồng nhất và đối xứng cho thiết kế, giảm thiểu sự mất cân bằng về độ trễ lan truyền gây ra bởi khác biệt về đường truyền giữa các RO và bộ đếm[8]. Ở mức HDL, các khối chức năng được tùy biến tối đa với việc sử dụng các tham số tĩnh. Điều này giúp quản lý thiết kế chặt chẽ và thuận tiện trong liên kết với các thiết kế lớn hơn.

2.2. Mô hình thống kê của tần số RO PUF

Hiện tượng biến thiên tham số cấu kiện bán dẫn đã được nghiên cứu rộng rãi nhằm tạo cơ sở cho việc đề ra các giải pháp ổn định tham số, cải tiến công nghệ chế tạo IC [85,86]. Nhìn chung, các đặc tính điện của IC chịu ảnh hưởng bởi điều kiện tổng quát PVT (*Process, Voltage, Temperature/Công nghệ, điện áp nguồn nuôi, nhiệt độ làm việc*). Các nguồn biến thiên gồm:

i) *Các nhân tố môi trường* là các biến thiên xảy ra trong quá trình hoạt động của mạch, bao gồm:

[8] Với FPGA có tần số xung đồng hồ hệ thống 50 MHz và các RO có tần số dưới 100 MHz, sai số đếm là không đáng kể và có thể bỏ qua [J1].

- Sự thay đổi nhiệt độ của chip hay nhiệt độ môi trường làm việc của chip.

Khi nhiệt độ tăng, dòng cực máng giảm. Nhiệt độ mặt ghép của transistor là tổng của nhiệt độ môi trường và mức tăng nhiệt độ gây ra bởi sự tiêu thụ công suất của IC. Nhiệt độ trên chip thay đổi theo các mức tiêu thụ công suất khác nhau.

- Biến thiên điện áp nguồn nuôi.

Trị số điện áp nguồn nuôi có thể lệch khỏi giá trị danh định tới $\pm 10\%$, thay đổi theo không gian (vị trí trên chip) và thời gian, gây ra bởi dung sai của mạch ổn áp, tác động của bức xạ hồng ngoại lên mạch nguồn hay tạp âm nhiệt.

- Biến thiên tham số do việc đóng/mở các van bán dẫn…

Các biến thiên dạng này chủ yếu phụ thuộc vào thiết kế cấp nguồn, bố trí các thành phần trong mạch.

ii) *Các nhân tố vật lý* là các biến thiên xảy ra trong quá trình chế tạo, được gọi là các biến thiên công nghệ (*process variation*). Biến thiên dạng này gắn kết lâu dài với linh kiện như biến thiên về độ dày các lớp vật liệu, kích thước phẳng và nồng độ tạp chất…, từ đó gây ra biến thiên trong các tham số quan trọng của linh kiện và mạch. Các tham số này đối với transistor là độ dài kênh L và điện áp ngưỡng V_t; đối với mạch là độ rộng và khoảng cách giữa các đường nối, độ dày các lớp kim loại và cách điện,

Các biến thiên công nghệ được phân thành:

- Biến thiên giữa các lô sản xuất (*lot to lot variation*);

- Biến thiên giữa các phiến (*wafer to wafer variation*);

- Biến thiên giữa các chip (*interdie variation*);

- Biến thiên bên trong chip (*intradie variation*).

Biến thiên giữa các lô và giữa các phiến thường được gộp chung với biến thiên giữa các chip. Hình 2.6 minh họa biến thiên dạng này. Quá trình cấy ion gây ra sự khác biệt trong nồng độ tạp chất vùng tâm phiến so với vùng ngoại vi, tương ứng với sự khác biệt về điện áp ngưỡng theo vị trí trên phiến. Ngoài ra, sau quá trình quang khắc, các chip ở cạnh phiến khác biệt chút ít với các chip ở tâm phiến về độ dài kênh. Các biến thiên tham số này gây ra sự khác biệt khoảng 20% trong trị số tần số mạch dao động vòng. Hình 2.7 minh họa biến thiên giữa các chip và biến thiên bên trong chip đối với tham số biến thiên là độ dày lớp điện môi sau quá trình phẳng hóa cơ học.

Gọi P là tham số khái quát cho các tham số mô hình cấu kiện tích cực hoặc thụ động dùng trong mô phỏng đặc tính của thiết kế như:

- Dạng hình học của cấu kiện MOSFET: Độ dày lớp ôxit cực cổng; độ dài, độ rộng kênh dẫn;

- Độ khuếch tán tạp chất;

- Điện áp ngưỡng, dòng rò;

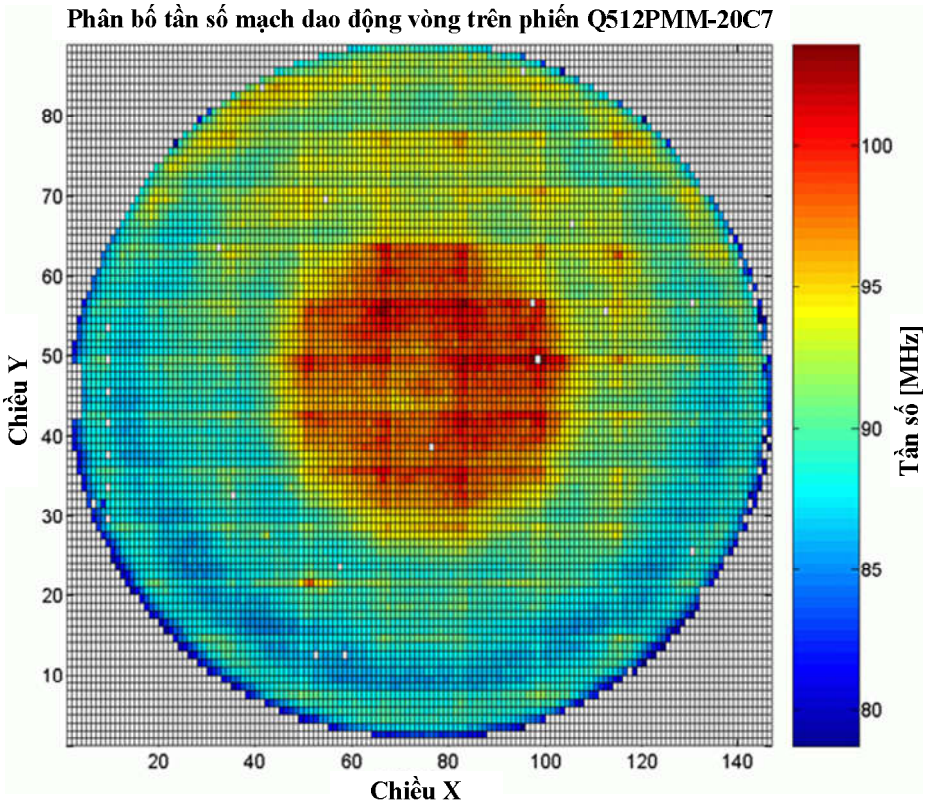
- Độ rộng mạch nối và khoảng cách giữa các mạch nối, độ dày lớp kim loại mạch nối, độ dày lớp vật liệu cách điện, kích thước tiếp điểm;

- Trở kháng tiếp điểm, trở kháng mạch nối, hằng số điện môi lớp cách điện…

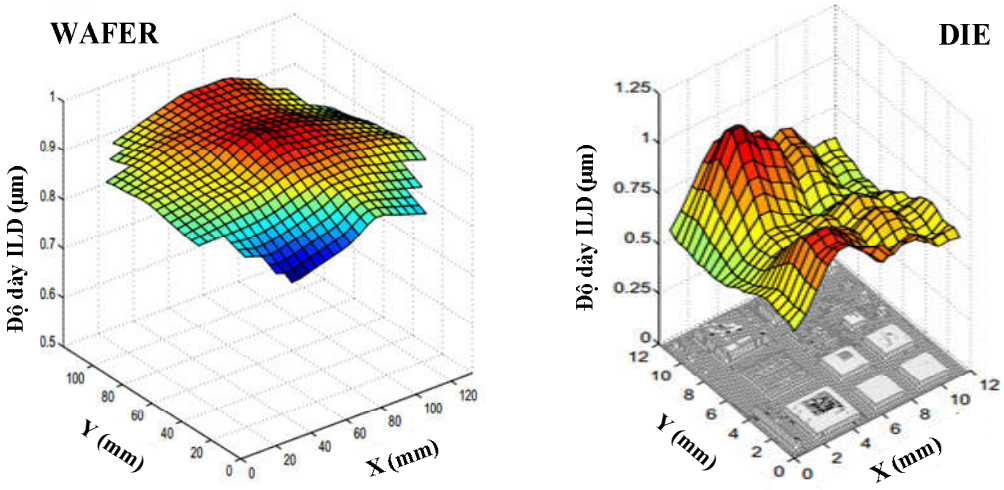
Tham số P có thể được mô hình hóa [86] bởi phương trình:

$$P = P_0 + \tilde{P}_{interdie} + \tilde{P}_{intradie} + P_\varepsilon \qquad (2.3)$$

Trong đó, P_0 là trị số thiết kế danh định, $\tilde{P}_{interdie}$ là biến thiên tham số giữa các chip, $\tilde{P}_{intradie}$ là biến thiên tham số bên trong chip, P_ε là các biến thiên chưa biết còn lại.



Hình 2.6 Phân bố tần số mạch dao động vòng thực thi trên công nghệ CMOS 90-nm theo vị trí trên phiến [85]



Hình 2.7: Minh họa biến thiên độ dày lớp điện môi của phiến (trái) và chip (phải) [86].

Biến thiên tham số giữa các chip là sự khác biệt về trị số một vài tham số của loạt các chip hầu như đồng nhất (được tạo ra từ cùng một phiến, từ các phiến khác nhau hoặc từ các lô khác nhau). Trị số trung bình thống kê của các tham số thay đổi đều đối với tập chip khảo sát. Chi tiết hơn, $\tilde{P}_{interdie}$ có thể được biểu diễn dưới dạng các biến thiên thành phần được giả định là các nguồn thăng giáng độc lập về mặt vật lý và có một kiểu phân bố thống kê nào đó:

$$\tilde{P}_{intradie} = \tilde{P}_{fab-to-fab} + \tilde{P}_{lot-to-lot}(fab) + \tilde{P}_{wafer-to-wafer}(lot) + \tilde{P}_{die-to-die}(wafer) \quad (2.4)$$

$\tilde{P}_{interdie}$ có phân bố chuẩn:

$$\tilde{P}_{interdie} \sim N\left(0, \sigma^2_{interdie}\right) \quad (2.5)$$

Biến thiên tham số bên trong chip là sự lệch tham số theo khác biệt về vị trí không gian bên trong mỗi chip. Khác với biến thiên tham số giữa các chip, biến thiên tham số bên trong chip liên quan đến sự bất đồng nhất trong cấu trúc nội tại gây ra bởi các bước công nghệ. $\tilde{P}_{intradie}$ có thể được biểu diễn dưới dạng hàm của các tọa độ không gian (x, y):

$$\tilde{P}_{intradie}(x, y) = \mathcal{W}(\omega, x, y) = \omega_0 + \omega_x x + \omega_y y \quad (2.6)$$

với ω được biểu thị qua các hệ số ω_0, ω_x và ω_y là các biến ngẫu nhiên theo các tọa độ phẳng (x, y).

Như vậy, mô hình trên tách biệt các nhân tố môi trường và các nhân tố vật lý, đồng thời mô tả tổng quan bản chất vật lý của các biến thiên tham số giữa các chip và biến thiên tham số bên trong chip. Biến thiên bên trong chip nhỏ hơn nhiều biến thiên giữa các chip, khó kiểm soát và thường bị bỏ qua trong thiết kế. Ngoại trừ biến thiên bên trong chip, các loại biến thiên

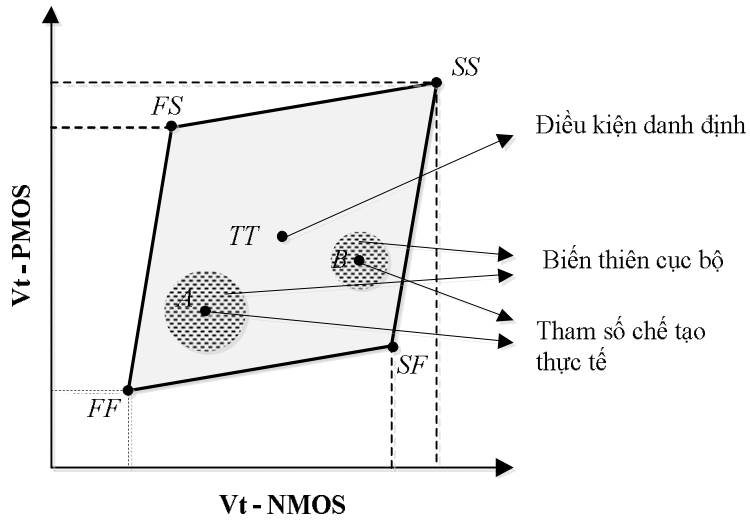
khác có thể kiểm soát được và bù tham số.

Biến thiên tham số về mặt vật lý trong mạch RO thể hiện ở biến thiên thời gian giữ chậm, qua đó gây nên sự thay đổi tần số RO. Trong biểu thức thực nghiệm đề xuất dưới đây nhằm mô tả đặc trưng thống kê tần số RO, tham số P trong công thức (2.3) được cụ thể hóa bằng tần số RO. Đặc điểm nổi bật của RO PUF là tần số tuyệt đối RO phụ thuộc nhiều vào biến thiên của nhiệt độ môi trường và điện áp nguồn nuôi [42]. Trong biểu thức tần số RO đề xuất, nghiên cứu sinh sẽ kết hợp các nhân tố môi trường vào biến thiên giữa các chip thành đại lượng thể hiện biến thiên tác động đồng đều lên các chip khảo sát; kết hợp biến thiên bên trong chip và các nhân tố khác (đại lượng P_ε trong công thức (2.3)) thành đại lượng thể hiện biến thiên tác động cục bộ bên trong chip. Tần số tuyệt đối của RO có thể được mô hình hóa bởi biểu thức:

$$f_{RO} = f_{nominal} + \Delta f_{local} + \Delta f_{global} + \Delta f_{OP} \quad (2.7)$$

Trong đó, $f_{norminal}$ là tần số RO danh định (tần số đo được khi thiết bị hoạt động ở điều kiện danh định, trong trường hợp này là 25^{o}C, 1,0 V). Trị số này không đổi đối với mọi RO, mọi FPGA và bất kỳ điều kiện làm việc nào. Các thành phần còn lại trong công thức (2.7) là các nhân tố biến thiên. Δf_{global} và Δf_{local} tương ứng 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. Minh họa các thành phần danh định, biến thiên cục bộ được trình bày trên Hình 2.8. Trên đồ thị đặc trưng PVT [87], *corner TT* (*Typical/Danh định*) tương ứng điều kiện danh định, các *corner FF*, *FS*, *SF*, *SS* là tổ hợp của các điều kiện cực hạn *F* (*Fast/Nhanh*) và *S*

(*Slow/Chậm*).



Hình 2.8: Minh họa các thành phần danh định và biến thiên cục bộ

Trong quá trình chế tạo, dưới các tác động của biến thiên toàn cục (quy định bởi đặc điểm công nghệ như khác biệt về mật độ khuếch tán tạp chất giữa vùng trung tâm và vùng biên của phiến cũng như giữa các phiến trong một lô, giữa các lô…), tham số cấu kiện lệch khỏi *TT* về các điểm *A*, *B*… Kết hợp với tác động của các biến thiên cục bộ (thăng giáng ngẫu nhiên bên trong chip), tham số cấu kiện lệch về các vùng phân bố ngẫu nhiên với tâm là các điểm *A*, *B*.

Nghiên cứu thực nghiệm khảo sát đối với 5 linh kiện FPGA thực thi thiết kế RO PUF trên Hình 2.5 với 32 RO, mỗi RO được tạo bởi 16 bộ đảo và một cổng NAND. Tại mỗi điều kiện thực nghiệm, mỗi FPGA được kích hoạt để tạo ra 256 mẫu dữ liệu. Các mẫu này được truyền trực tiếp tới máy tính qua UART để xử lý tiếp theo.

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

Từ mô hình thống kê tần số RO đề xuất (công thức (2.7)) và số liệu thu nhận được từ mạch RO PUF (Hình 2.5), dưới đây phân tích tác động

của các nhân tố biến thiên lên tần số RO với một số quy ước:

- Tách biến thiên gây ra bởi nhiệt độ môi trường khỏi Δf_{OP} và coi là nhân tố biến thiên toàn cục do giả định nhiệt độ môi trường có tác động đồng đều lên các mạch RO trong một IC. Tuy nhiên, biến thiên gây ra bởi nhiệt độ môi trường vẫn được xét riêng trong phần 2.3.2 nhằm kiểm nghiệm giả định trên và làm nổi bật phân tích đặc tính biến thiên giữa các chip.

- Tác động của biến thiên nguồn nuôi chưa được xét đến.

- Khảo sát Δf_{OP} (biến thiên gây ra do điều kiện hoạt động) chỉ giới hạn trong ảnh hưởng của các thăng giáng tức thời.

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 [88]. Với một RO đơn, có thể khảo sát thăng giáng này như đối với biến thiên của Δf_{OP} tại điều kiện làm việc danh định. Giá trị tần số được đo nhiều lần đối với $5\text{IC}\times 32\text{RO}$ trong cùng điều kiện hoạt động (nhiệt độ môi trường 25^{o}C, điện áp lõi 1,0 V). Các tần số của một RO cụ thể do đó biến thiên dưới tác động của thăng giáng ngẫu nhiên trong nhiệt độ môi trường và điện áp nguồn cung cấp. 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 các mẫu tần số RO.

Hình 2.9 trình bày biểu đồ phân bố của dữ liệu tần số thu được sau 256 lần đo đối với RO_5/IC_1 (FPGA Spartan-6) và RO_8/IC_2 (FPGA Spartan-3E). Các tham số thống kê của phân bố tần số RO cùng độ ổn định tương ứng được trình bày trong Bảng 2.1. Có thể thấy tỷ số σ/μ nhỏ hơn nhiều giá trị kỳ vọng (1%), tương ứng với độ ổn định cao.

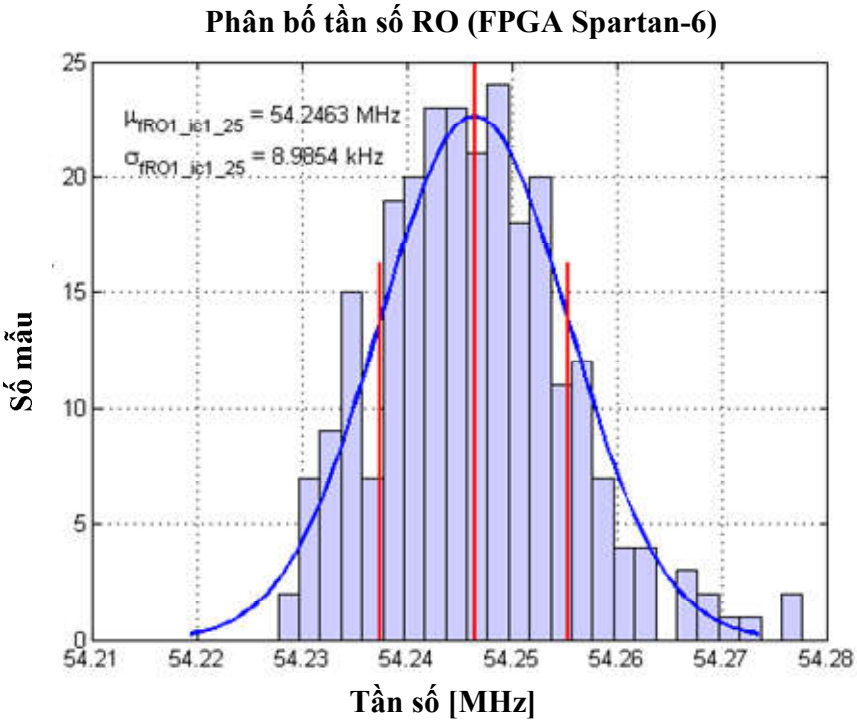
Biến thiên của tỷ số σ/μ đối với $5\text{IC}\times 32\text{RO}$ FPGA Spartan-6 và $6\text{IC}\times 32\text{RO}$ FPGA Spartan-3E được trình bày trên Hình 2.10. Đối với các FPGA Spartan-6 (Hình 2.10(a)), tỷ số σ/μ của các RO có giá trị cực tiểu là *0,0093*% (RO_{27}/IC_5) và giá trị cực đại là *0,0194*% (RO_{19}/IC_1), tương ứng với độ ổn định *99,99*% và *99,98*%. Khoảng biến thiên độ ổn định tần số RO đối với 5 FPGA Spartan-6 và 6 FPGA Spartan-3E tại 25°C và tại nhiệt độ bất kỳ trong khoảng nhiệt độ khảo sát được trình bày trên Bảng 2.2. Kết quả này chỉ ra rằng thăng giáng tức thời có ảnh hưởng không đáng kể tới các tần số RO và có thể được bỏ qua trong các phân tích tiếp theo.

Bảng 2.1: Khảo sát độ ổn định của tần số RO dưới tác động của các thăng giáng tức thời

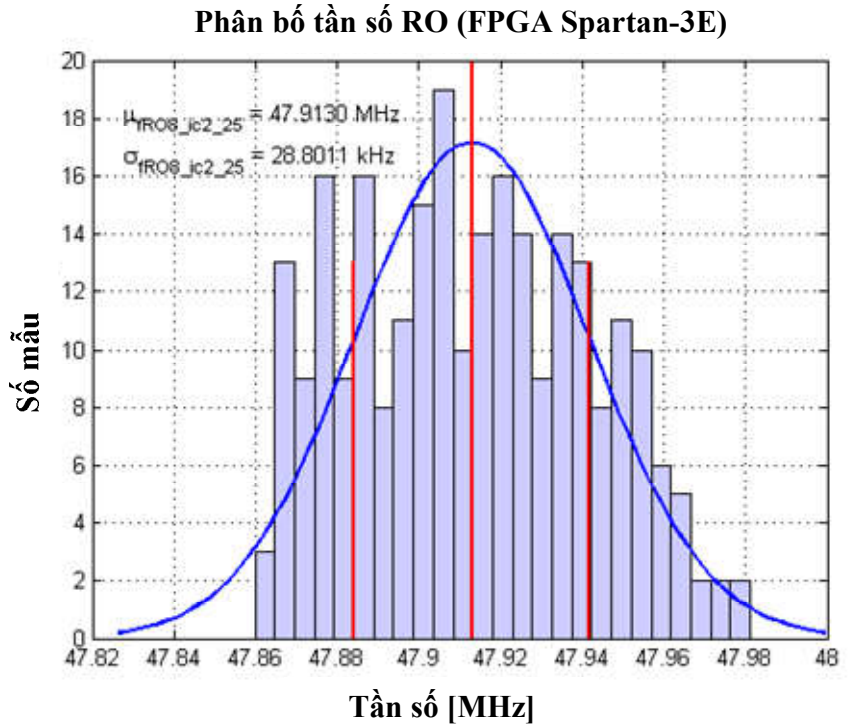
Tham số	**RO_1/IC_1 (FPGA Spartan-6)**	**RO_8/IC_2 (FPGA Spartan-3E)**
Tần số trung bình [MHz]	*54,25*	*47,91*
Độ lệch chuẩn [kHz]	*8,99*	*28,80*
σ/μ [%]	*0,02*	*0,06*
Độ ổn định [%]	*99,98*	*99,94*

Bảng 2.2: Khảo sát khoảng biến thiên độ ổn định tần số RO

Tham số	**25°C**		**25°C – 70°C (80°C)**	
	FPGA Spartan-6	**FPGA Spartan-3E**	**FPGA Spartan-6**	**FPGA Spartan-3E**
min σ/μ [%]	*0,0093* (RO_{27}/IC_5)	*0,0471* (RO_{29}/IC_1)	*0,0093*	*0,0090*
Độ ổn định [%]	*99,99*	*99,95*	*99,99*	*99,91*
max σ/μ [%]	*0,0194* (RO_{19}/IC_1)	*0,1168* (RO_9/IC_4)	*0,1343*	*0,1466*
Độ ổn định [%]	*99,98*	*99,88*	*99,87*	*99,85*

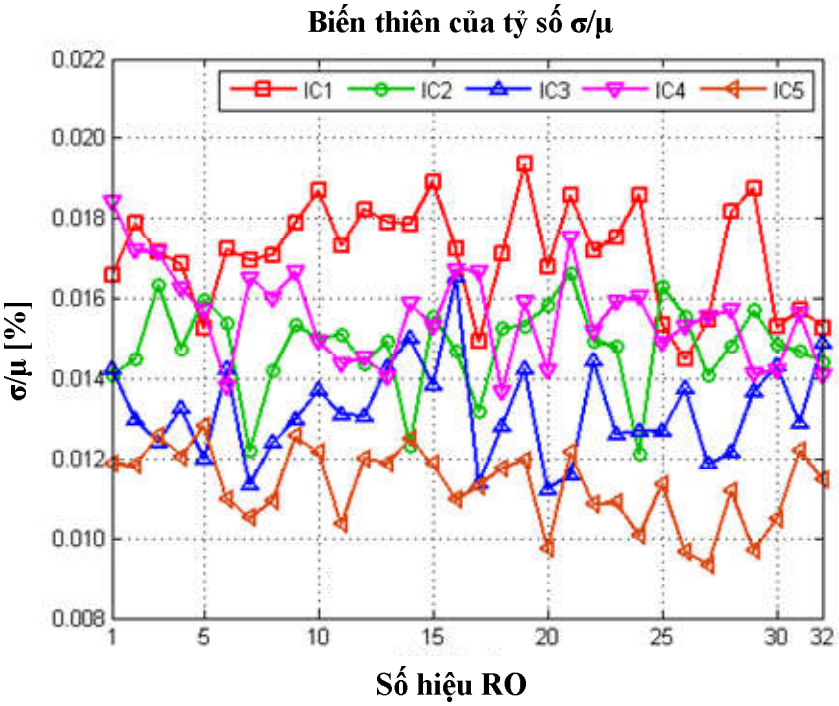


a)

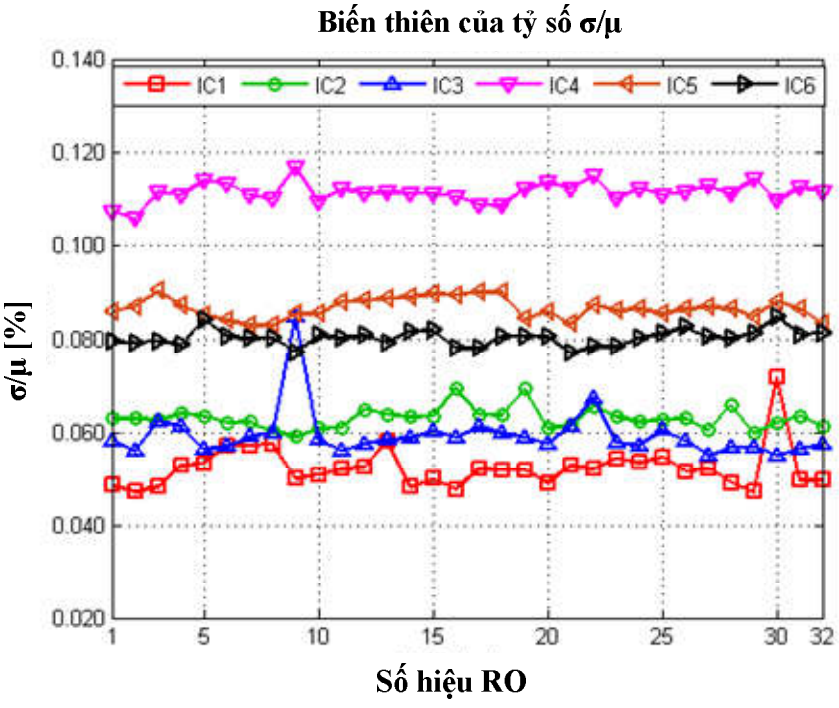


b)

Hình 2.9: Biểu đồ phân bố tần số của RO_1/IC_1 (FPGA Spartan-6) (a) và RO_8/IC_2 (FPGA Spartan-3E) (b) ước lượng từ 256 mẫu tại nhiệt độ 25^{o}C.



a)



b)

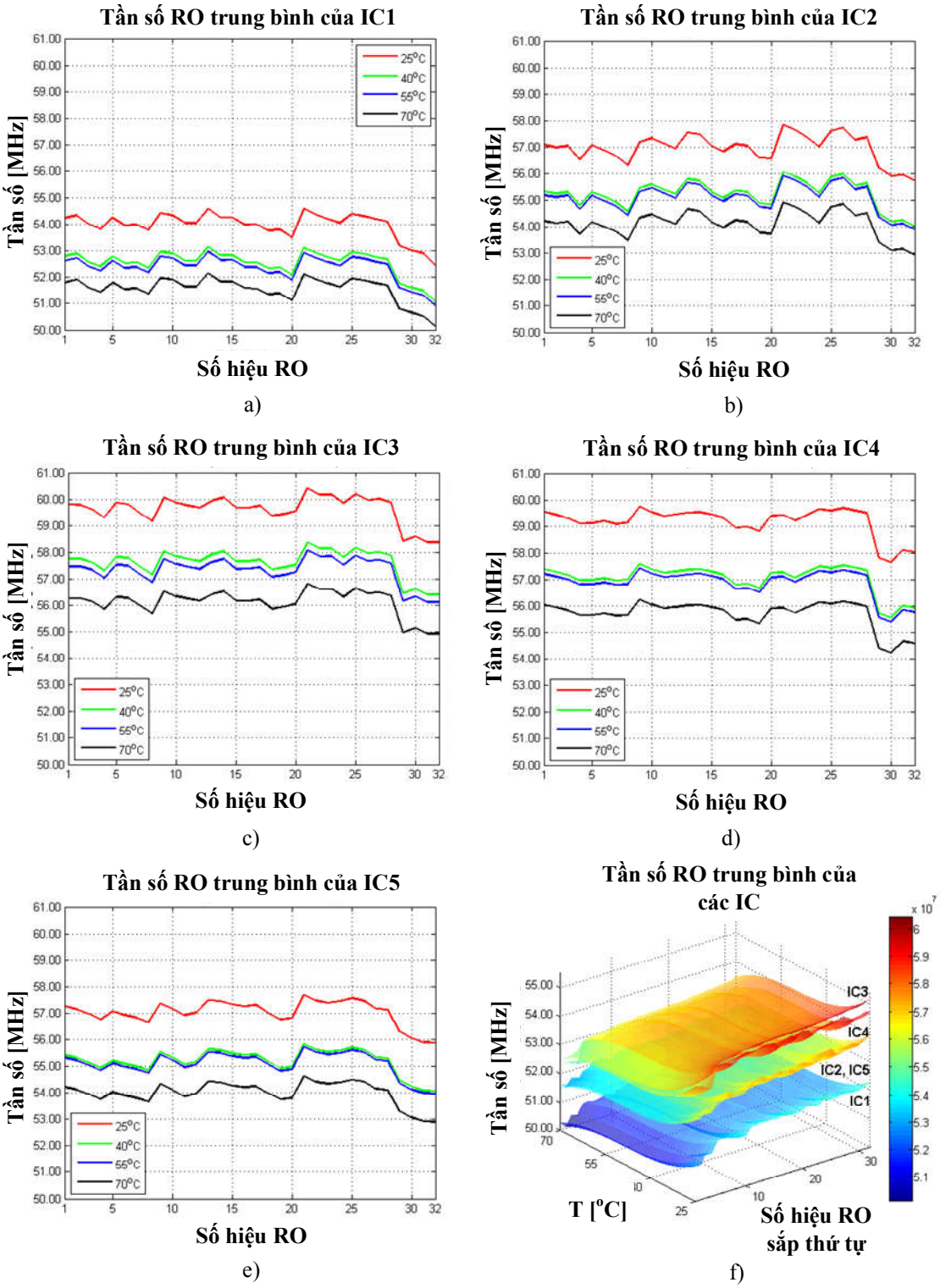
Hình 2.10: Tỷ số σ/μ của 32 RO trên 5 IC FPGA Spartan-6 (a) và 6 IC FPGA Spartan-3E (b) ước lượng từ 256 mẫu tại nhiệt độ 25^{o}C.

2.3.2. Ảnh hưởng của nhiệt độ môi trường

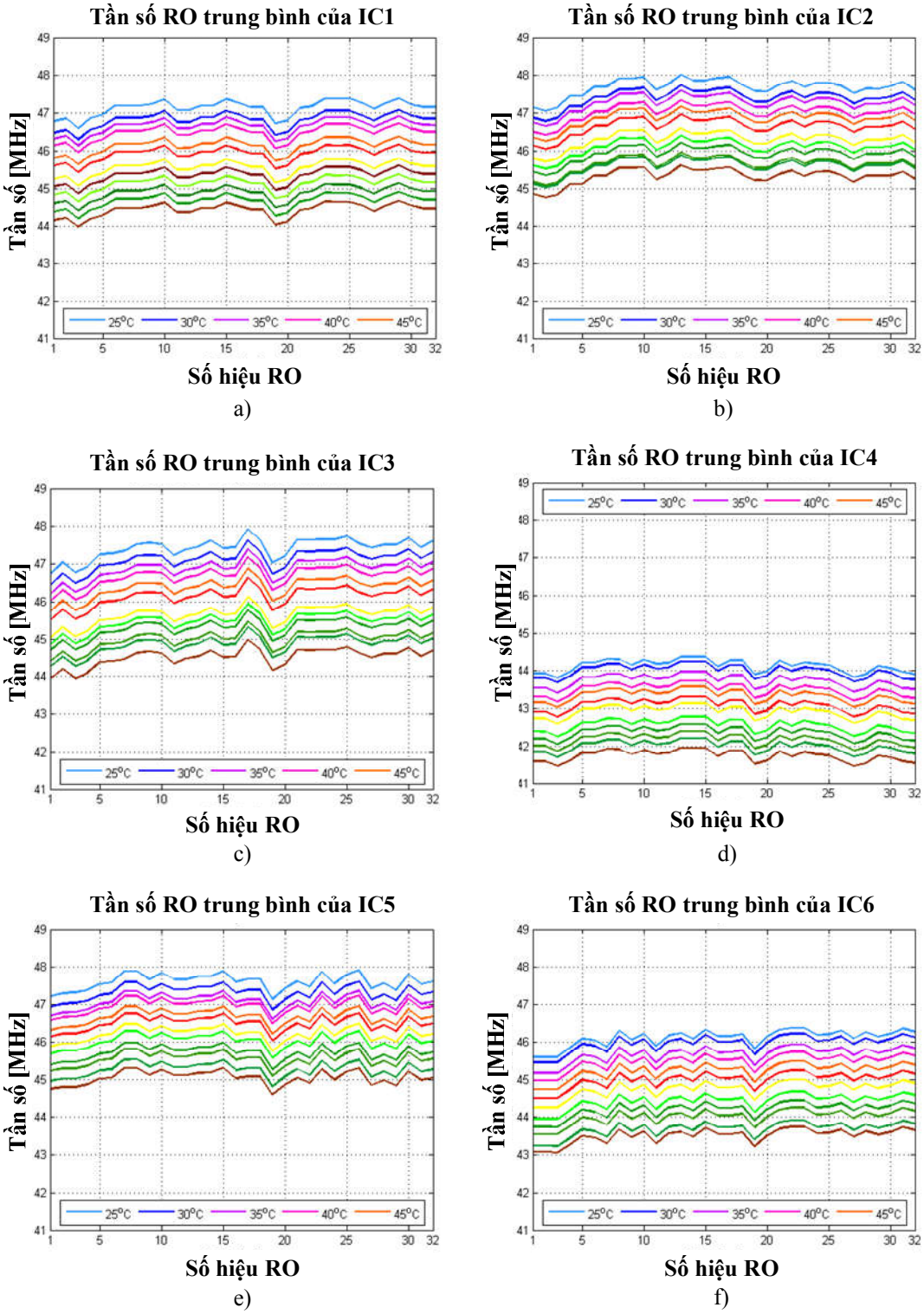
Để định lượng sự phụ thuộc của các tần số RO vào nhiệt độ môi trường, tiến hành đo tần số RO đối với các FPGA ở nhiều nhiệt độ khác nhau. Khảo sát 5 FPGA Spartan-6 tại 25^{o}C, 40^{o}C, 55^{o}C, và 70^{o}C. Các phép đo được lặp lại 256 lần với mỗi RO trong 32 RO để tính các tần số trung bình của chúng. Các kết quả chính được biểu diễn trên Hình 2.11(a) – (e) và được kết hợp thành một mặt 3D trên Hình 2.11(f). Các tần số RO trung bình của các IC được sắp xếp theo chiều tăng của các tần số trung bình trong IC_3 nhằm giữ cho mặt 3D trơn và thể hiện rõ xu hướng thay đổi. Sự dịch chuyển của các giá trị tần số RO trung bình thể hiện giá trị trung bình của Δf_{OP} gây ra bởi điều kiện hoạt động trong công thức (2.7).

Các đồ thị trên cho thấy xu hướng biến thiên giá trị trung bình của tần số tuyệt đối RO theo nhiệt độ. Tần số RO giảm khi nhiệt độ tăng và ngược lại. Khi nhiệt độ tăng từ 25^{o}C đến 70^{o}C, tần số trung bình của các RO thay đổi trong khoảng $2{,}34 - 3{,}59$ MHz (FPGA Spartan-6). Đối với mọi công nghệ, sự biến thiên tần số RO là không tuyến tính do sự phụ thuộc của dòng transistor vào nhiệt độ là phi tuyến [85]. Nhiệt độ thay đổi từ 40^{o}C đến 55^{o}C chỉ làm giảm tần số RO trong khoảng $97{,}8$ kHz – $0{,}29$ MHz. Mức khác biệt này vẫn lớn hơn nhiều so với thăng giáng tức thời, do vậy giá trị tuyệt đối của các tần số RO không đặc trưng cho RO.

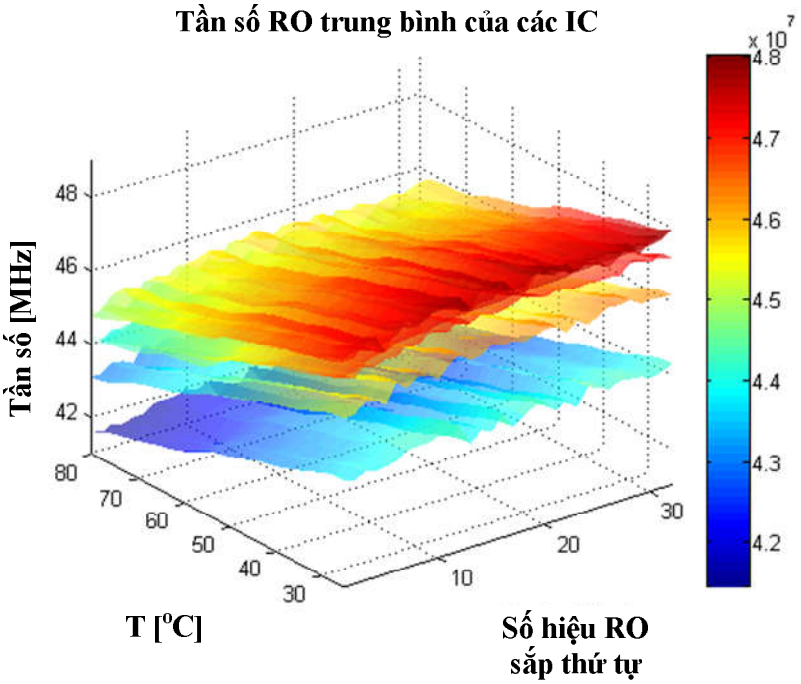
Phân tích số liệu thực nghiệm đối với thiết kế RO PUF đề xuất thực thi trên 6 FPGA Spartan-3E, đo 256 lần, lưới nhiệt độ khảo sát 25^{o}C – 80^{o}C với bước 5^{o}C, ta nhận được kết quả tương tự (Hình 2.12 và Hình 2.13).



Hình 2.11: (a) – (e) Biến thiên tần số RO theo nhiệt độ; (f) Mô tả 3D của biến thiên tần số RO theo nhiệt độ đo với 5 linh kiện FPGA Spartan-6.



Hình 2.12: Biến thiên tần số RO theo nhiệt độ (25°C – 80°C, bước 5°C) đo với 6 linh kiện FPGA Spartan-3E.



Hình 2.13: Mô tả 3D của biến thiên tần số RO theo nhiệt độ đo với 6 linh kiện FPGA Spartan-3E.

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

Các biến thiên xuất hiện từ quá trình chế tạo là kết hợp của các biến thiên cục bộ (bên trong chip) và toàn cục (giữa các chip), tương ứng được biểu diễn bởi Δf_{local} và Δf_{global} trong phương trình (2.7). Với các biến thiên toàn cục, từ Hình 2.11(f) có thể thấy tần số của một RO xác định thay đổi đáng kể giữa các chip. Ví dụ, tần số của RO_5 dịch lên *5,61* MHz từ IC_1 đến IC_3 ở 25°C. Các mặt trên Hình 2.11(f) cùng dịch lên hoặc xuống giữa các IC, hiện tượng này cũng xảy ra giữa các mức nhiệt độ khác nhau. Ví dụ, các tần số RO tăng khoảng *1,73* MHz đến *3,41* MHz từ IC_1 đến IC_2 ở bất kỳ nhiệt độ nào. Có thể coi 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

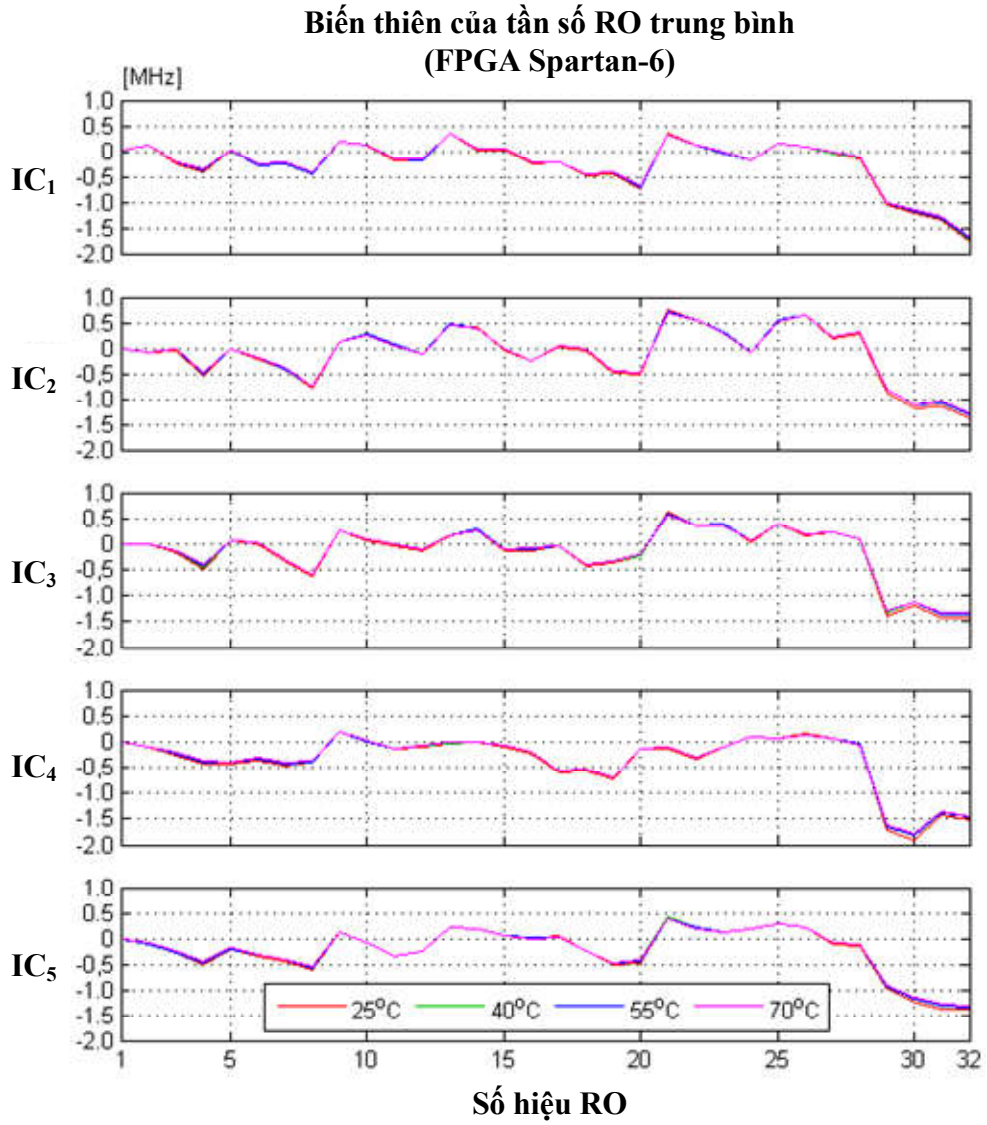
(*uniqueness*) thấp và không thể được sử dụng trực tiếp để đặc trưng cho các cấu kiện vật lý.

Tiếp theo, xét ảnh hưởng của các biến thiên cục bộ qua sự khác biệt trong tần số RO, khảo sát đối với mọi RO trên một chip đơn. Từ số liệu đo, các giá trị trung bình của 32 tần số RO được trình bày trên Hình 2.11(a) – (e). Các gợn trên các bề mặt gây ra bởi tính không đồng nhất giữa các tập RO sắp thứ tự thể hiện ảnh hưởng của Δf_{local} trong công thức (2.7).

Đối với tập các RO khảo sát, theo các nghiên cứu đã có, hiện tượng hai hay nhiều tần số RO gần nhau về trị số là khá phổ biến. Trên Hình 2.11(f), đối với IC_1 tại 25°C, khác biệt về tần số trung bình của RO_{14} và RO_{15} chỉ là *1,88* kHz. Với độ lệch chuẩn của thăng giáng ngẫu nhiên tương ứng RO_{14} và RO_{15} là *9,70* kHz và *10,26* kHz, nếu sử dụng phương pháp tạo bit đáp ứng bằng so sánh ghép cặp dễ dẫn đến hiện tượng bất định. Đặc biệt, đối với các cặp RO_8 – RO_{18}, RO_{23} – RO_{27}, RO_{21} – RO_{13}. Do đó cần phải loại bỏ một số tần số RO trong trường hợp sử dụng phương pháp so sánh ghép cặp để tách bit đáp ứng. Như sẽ trình bày trong chương tiếp theo, điều này là không cần thiết đối với phương pháp vector ID đề xuất.

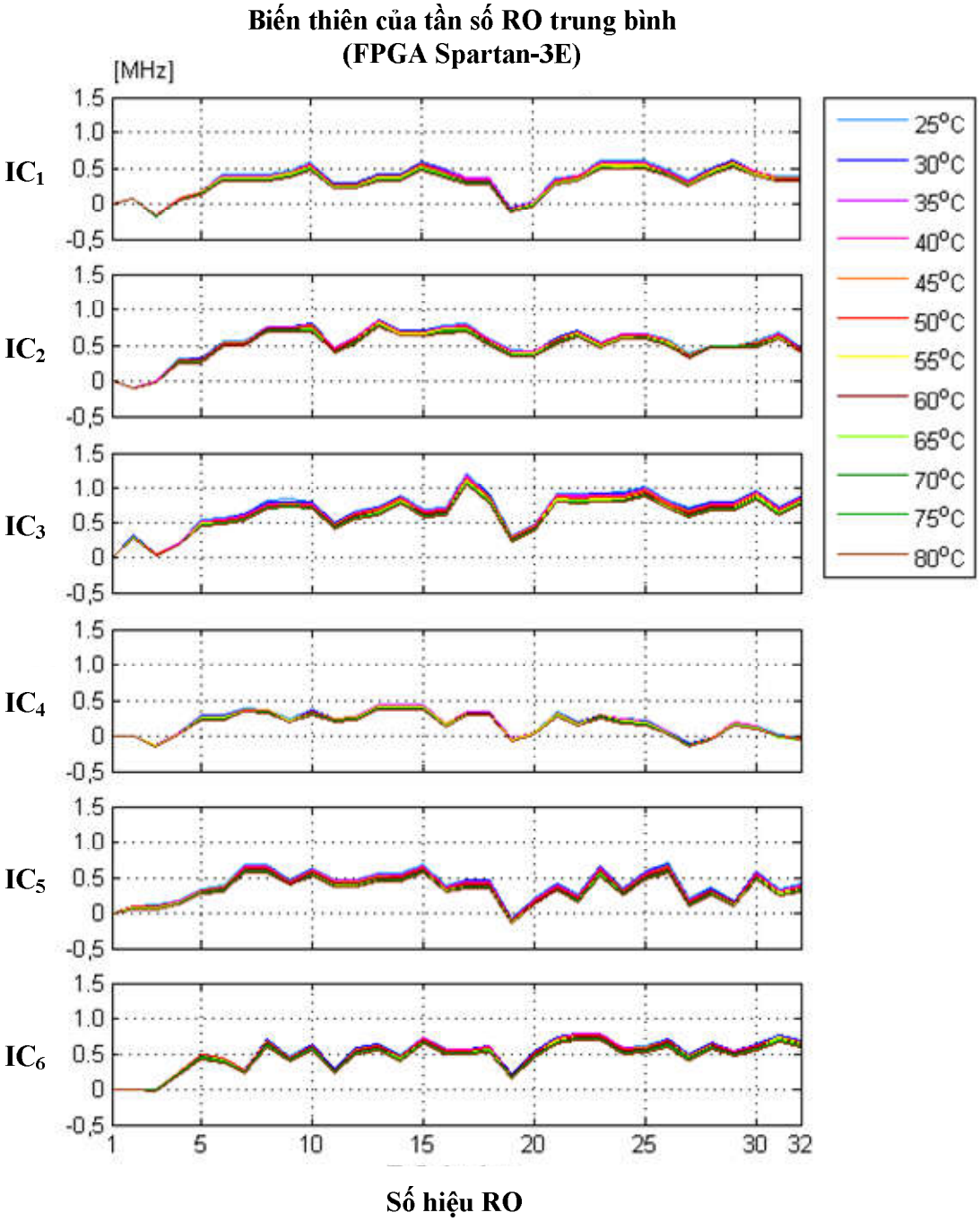
Các sai biệt cục bộ khá nhỏ. Khi dịch các f_{RO_i} về 0, giá trị cực đại của thăng giáng tần số các RO còn lại chỉ là *111,7* kHz đối với mọi IC và mọi điểm nhiệt độ khảo sát (*161,2* kHz đối với 6 IC FPGA Spartan-3E, 25°C – 80°C, bước 5°C). Giá trị này cùng bậc với thăng giáng tức thời. Như vậy đặc điểm biến thiên của các tần số RO tương đối ổn định đối với nhiệt độ. Điều này có thể quan sát được trên Hình 2.11(a) – (e), trong đó các đường gấp khúc đối với một chip FPGA đơn hầu như có cùng dạng tại mọi nhiệt độ. Biểu diễn tần số RO trung bình quy chuẩn về điểm 0 đối với 5 FPGA Spartan-6 được trình bày trên Hình 2.14 (Hình 2.15 đối với 6 FPGA

Spartan-3E, khảo sát tại lưới nhiệt độ 25°C – 80°C, bước 5°C)[9]. Từ Hình 2.14 và Hình 2.15 có thể thấy, mỗi IC được đặc trưng bởi một dạng đường gấp khúc. Điều này có nghĩa là 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 2.14: Đồ thị kết quả khảo sát biến thiên cục bộ với tần số quy chuẩn về điểm 0 của 5 IC FPGA Spartan-6 tại các nhiệt độ khác nhau.

[9] Tần số RO sau khi loại bỏ tần số định thiên được gọi là tần số RO quy chuẩn về điểm 0.



Hình 2.15: Đồ thị kết quả khảo sát biến thiên cục bộ với tần số quy chuẩn về điểm 0 của 6 IC FPGA Spartan-3E tại các nhiệt độ khác nhau.

Nội dung nghiên cứu này được trình bày chi tiết trong các công trình [J1, C1].

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 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 giá trị 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

Khái niệm dữ liệu định danh (*ID: Identity*) của thiết bị gồm:

- Định danh quy ước: Thiết bị được cấy một mạch định danh tần số vô tuyến hoặc được gán một chuỗi số, chuỗi dữ liệu nhị phân hay mã vạch duy nhất, lưu trong một vùng nhớ bền vững trên chip. Các giải pháp này làm tăng giá thành hệ thống, không có khả năng chống can thiệp phần cứng hiệu quả, độ tin cậy xác thực không cao.

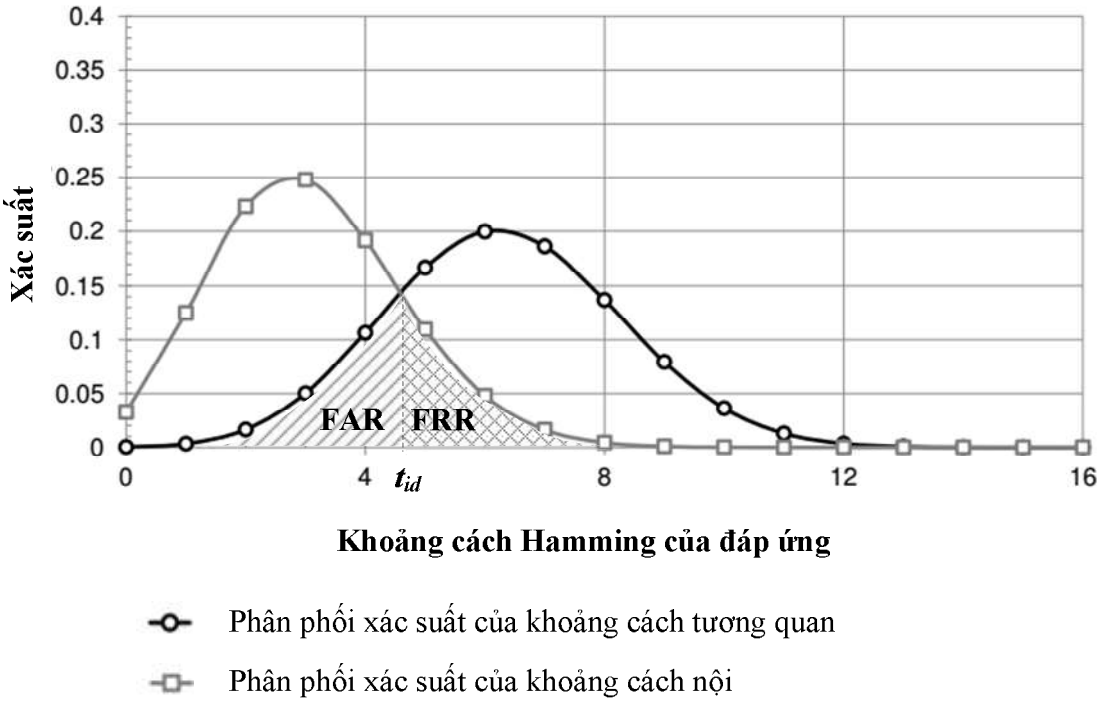
- Định danh vật lý: Khai thác đặc trưng vật lý (*inherent identifying feature*) của thiết bị để tạo dữ liệu định danh.

PUF được coi là vân tay sinh trắc *on-chip*, mở ra triển vọng định danh và xác thực thiết bị gần với nền vật lý. Các tác giả trong [11] sử dụng trực tiếp các đáp ứng RO PUF, đề xuất giao thức hai pha (tập hợp dữ liệu và xác thực), lập biểu đồ phân bố khoảng cách nội và khoảng cách tương quan, xác định mức ngưỡng dựa trên vị trí tương đối của hai biểu đồ này. Do bit đáp ứng tạo bởi hàm dấu (so sánh tần số RO), dữ liệu khoảng cách có dạng rời rạc (sử dụng độ đo là khoảng cách Hamming hoặc khoảng cách Hamming tương đối[10]) và độ tin cậy xác thực bị hạn chế bởi độ dài mẫu đáp ứng/độ phức tạp hệ thống. Công trình [10] là khảo cứu khá toàn diện và chi tiết về PUF, bao quát cơ sở lý thuyết và kiểm nghiệm hiệu năng của

[10] Với các dữ liệu $n-bit$, khoảng cách Hamming giữa chúng lấy giá trị trong tập $\{0,1,2...,n-1,n\}$, khoảng cách Hamming tương đối giữa chúng lấy giá trị trong tập $\left\{0,\frac{1}{n},\frac{2}{n},...,\frac{n-1}{n},1\right\}$.

các sơ đồ PUF đối với một số ứng dụng cụ thể. Đối với việc ứng dụng PUF định danh và xác thực thiết bị, các tác giả trong [10] bước đầu thiết lập cơ sở lý thuyết, đề xuất các biểu thức định lượng tính ổn định (*reliability/security*), tính duy nhất (*uniqueness*) và thực thi phần cứng các thiết kế PUF tương ứng. Trong luận án này, nghiên cứu sinh sử dụng các kết quả trong công trình [10] làm kết quả tham chiếu chính khi nghiên cứu nâng cao hiệu năng RO PUF (độ tin cậy định danh và xác thực thiết bị, độ ổn định dữ liệu đáp ứng RO PUF).

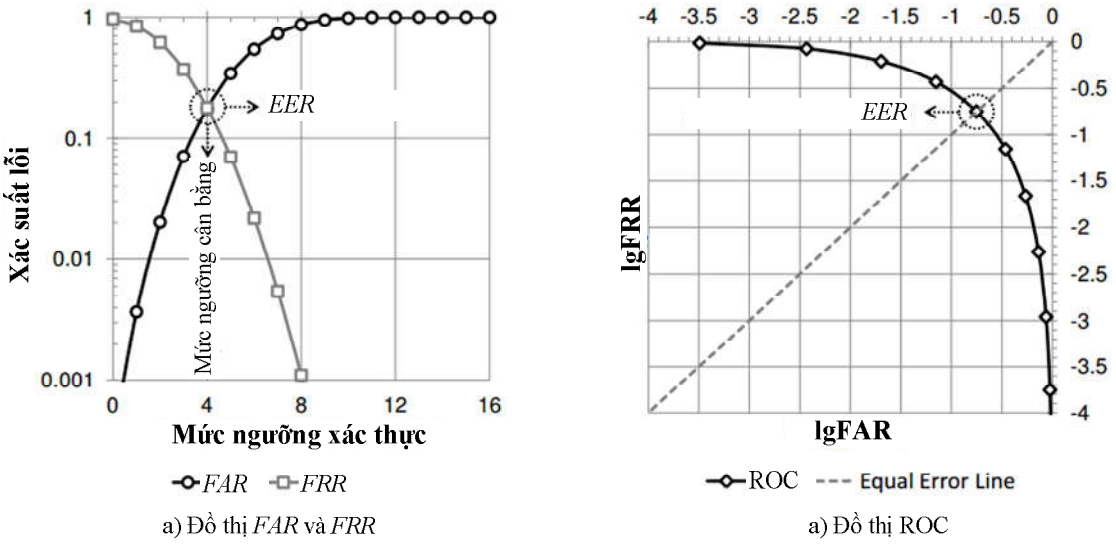
Một lớp PUF có khả năng định danh cao khi đối với tập mẫu đáp ứng của nó, các khoảng cách nội nhỏ hơn khoảng cách tương quan với xác suất lớn. Đồ thị phân phối xác suất của khoảng cách nội và khoảng cách tương quan theo độ đo Hamming đối với DFF PUF được trình bày trên Hình 3.1.



Hình 3.1: Phân phối khoảng cách nội và khoảng cách tương quan đối với các đáp ứng 16-bit của DFF PUF thu được từ thực nghiệm [10].

Vùng chồng lấn giữa hai đồ thị thể hiện tính mờ của việc xác thực: Nếu một mẫu đo khoảng cách giữa các đáp ứng rơi vào vùng này, nó có thể được coi là khoảng cách nội (khẳng định thực thể cần xác thực đã được đăng ký) hoặc khoảng cách tương quan (khẳng định thực thể cần xác thực chưa được đăng ký). Do vậy, cần một mức ngưỡng thực tế t_{id} để phân định kết quả xác thực. Mức ngưỡng này được xác định từ điều kiện cân bằng sai số gây ra do việc loại bỏ nhầm thực thể cần xác thực và chấp nhận nhầm thực thể lạ. Về mặt đồ thị, mức ngưỡng được xác định từ giao điểm *EER* (tỷ lệ lỗi cân bằng) của hai đường *FRR* (tỷ lệ loại bỏ nhầm) và *FAR* (tỷ lệ chấp nhận nhầm) trên Hình 3.2(a). Mức ngưỡng cao giảm thiểu nguy cơ loại bỏ nhầm, nhưng lại làm tăng nguy cơ chấp nhận nhầm, và ngược lại. Như vậy, cần xác định mức ngưỡng từ điều kiện thỏa hiệp giữa tính ổn định và tính duy nhất. Điều này được thể hiện rõ hơn khi biểu diễn *EER* là giao của đặc tuyến hoạt động (*ROC*, biểu diễn *FRR* là hàm của *FAR*) và đường cân bằng sai số (phân giác góc phần tư thứ ba hệ trục tọa độ Đề-các với các trục theo thang lôgarit trên Hình 3.2(b)). Nhánh trái ROC thể hiện xu hướng tăng tính duy nhất, nhánh hướng xuống bên phải thể hiện xu hướng tăng tính ổn định.

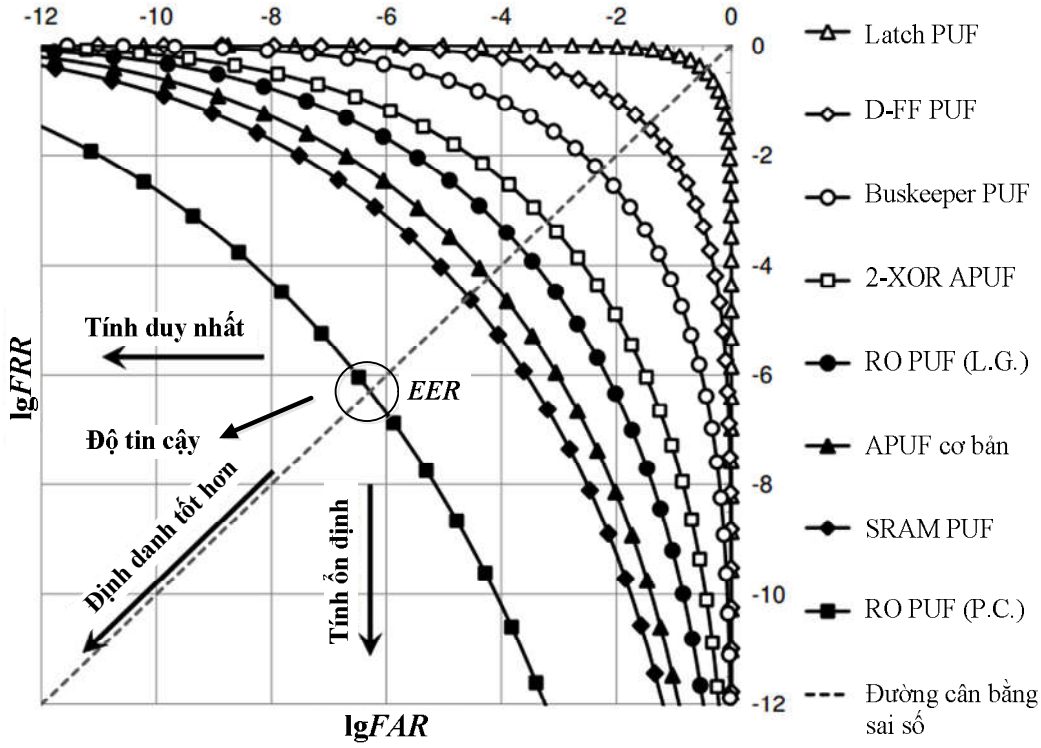
Phân tích các hệ thống định danh dựa trên các đáp ứng 64-bit đối với một số sơ đồ PUF (Hình 3.3), các tác giả trong [10] chỉ ra RO PUF với việc ghép cặp RO có khả năng định danh và xác thực tốt nhất với $EER \approx 10^{-6}$. Trong trường hợp đang xét, **độ tin cậy** xác thực được đánh giá qua trị số *EER*. Độ tin cậy cao khi *EER* nhỏ và ngược lại. ***Độ tin cậy cao nhất của các phương pháp định danh và xác thực truyền thống tương ứng với*** $\boldsymbol{EER \approx 10^{-6}}$.



a) Đồ thị *FAR* và *FRR*

a) Đồ thị ROC

Hình 3.2: Xác định mức ngưỡng định danh dựa trên *FAR* và *FRR* [10]



Hình 3.3: So sánh các đường ROC của các hệ định danh dựa trên các đáp ứng 64-bit của một số sơ đồ PUF [10]; RO PUF (P.C.)/(L.G.): Thiết kế RO PUF ghép cặp RO [42] và kết hợp mã hóa Lehmer-Gray [16].

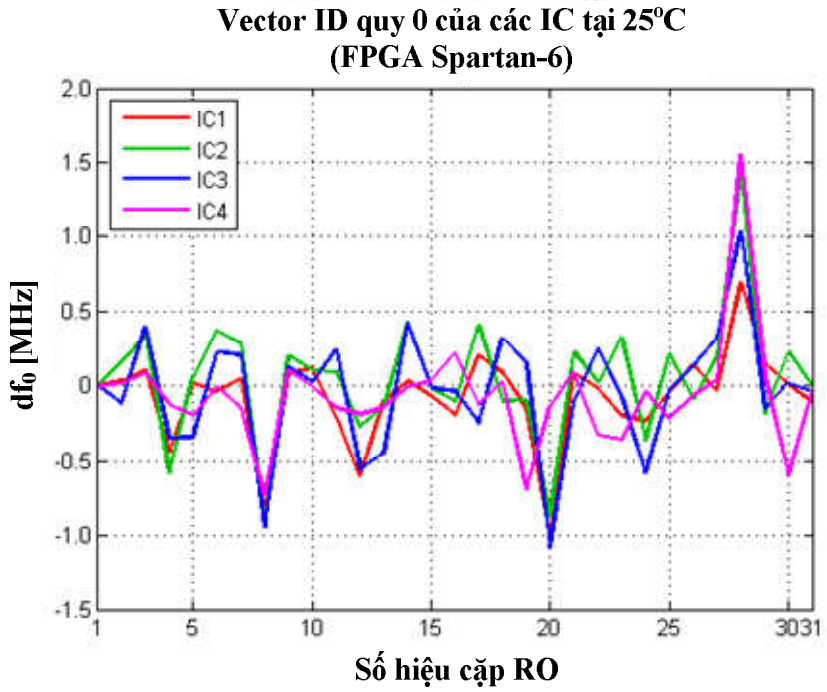
Tiếp theo, nghiên cứu sinh khảo sát hiệu quả của việc sử dụng tham số khoảng cách theo độ đo Hamming đến khả năng xác thực ID của thiết bị. Ở dạng tổng quát, ID của thiết bị là hàm của nhân tố biến thiên cục bộ, có thể được biểu diễn dưới dạng:

$$ID = F\left(\left\{\Delta f_{ij}\right\}\right) \tag{3.1}$$

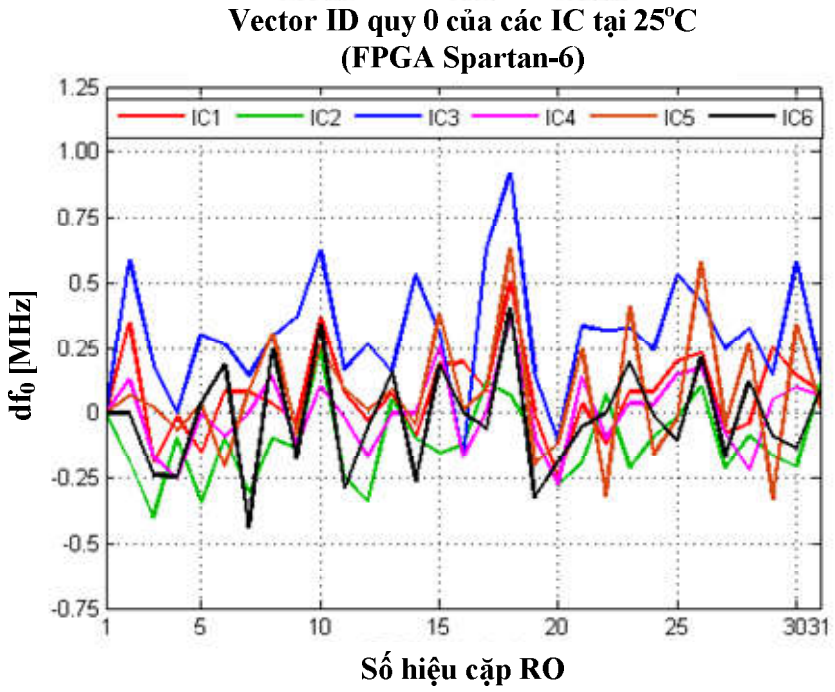
Trong đó $\Delta f_{ij} = f_i - f_j$ là sự khác biệt tần số gây ra bởi các nhân tố biến thiên cục bộ.

Số lượng và số hiệu (*index*) của các cặp tần số (*i, j*) tùy sơ đồ tách ID cụ thể. Đối với thiết kế tách ID bằng phương pháp ghép cặp liên tiếp [13], số cặp tần số là $(n-1)$ và F là hàm dấu. Vector ID có các tọa độ là các tần số hiệu giữa f_i và f_{i+1}, $i = \overline{1, n-1}$. Hình 3.4 biểu diễn đồ thị các vector ID tương ứng 4 IC FPGA Spartan-6 (6 IC FPGA Spartan-3E) quy chuẩn về điểm 0 tại 25^{o}C. Mỗi IC được biểu diễn chỉ bởi một dạng đường gấp khúc khác biệt nhau[11]. Phân tích định lượng chi tiết cho thấy có sự tương quan mạnh giữa các giữa các biến thiên cục bộ, và do vậy có sự tương quan giữa các bit đáp ứng. Cụ thể, cặp RO_{20} (RO_{28}) có xu hướng tạo tần số hiệu nhỏ nhất (lớn nhất) trong số các cặp RO đối với các IC FPGA Spartan-6 đang xét. Tiếp theo, bằng phương pháp ghép cặp liên tiếp và áp dụng hàm dấu, ta xác định các bit đáp ứng và khoảng cách Hamming tương đối. Hình 3.5 biểu diễn khoảng cách này theo số hiệu ghép cặp IC tương ứng các cấu hình mảng RO khác nhau về số RO trong mảng.

[11] Để thuận tiện trong so sánh dạng đường gấp khúc đặc trưng của các IC, tiến hành tịnh tiến các đường này sao cho điểm đầu các đường dịch về gốc tọa độ $(1,0)$, với "1" là chỉ số của cặp RO thứ nhất, tương ứng tần số hiệu df_1. Về mặt trị số, các tọa độ của ID $\left\{df_i \middle| i = \overline{1, n-1}\right\}$ được trừ cho df_1 để tạo tọa độ $\left\{df_j', j = \overline{1, n-1}\right\}$ của ID' đồng dạng với ID. Đồ thị ID' được gọi là đồ thị tần số hiệu quy chuẩn về điểm 0 (Hình 3.4).

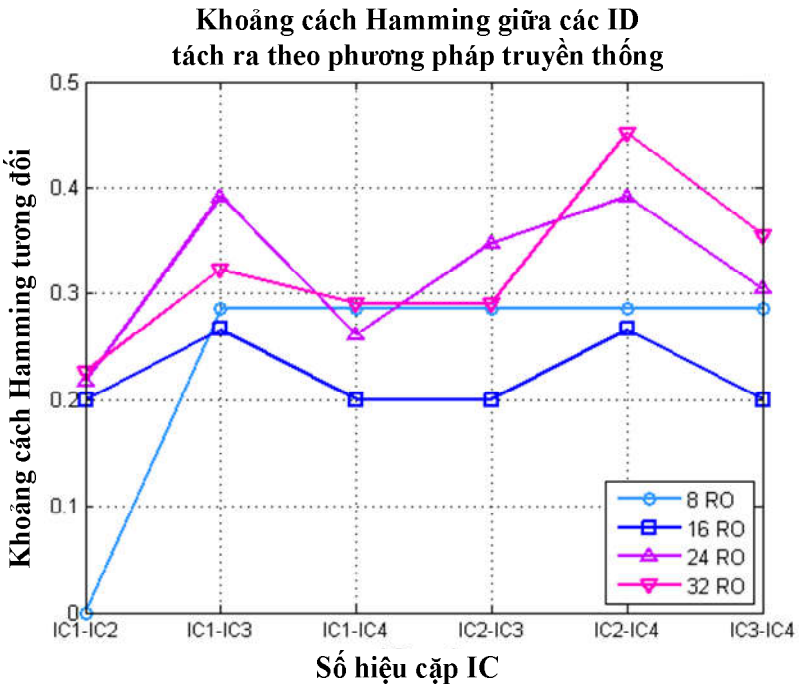


a)

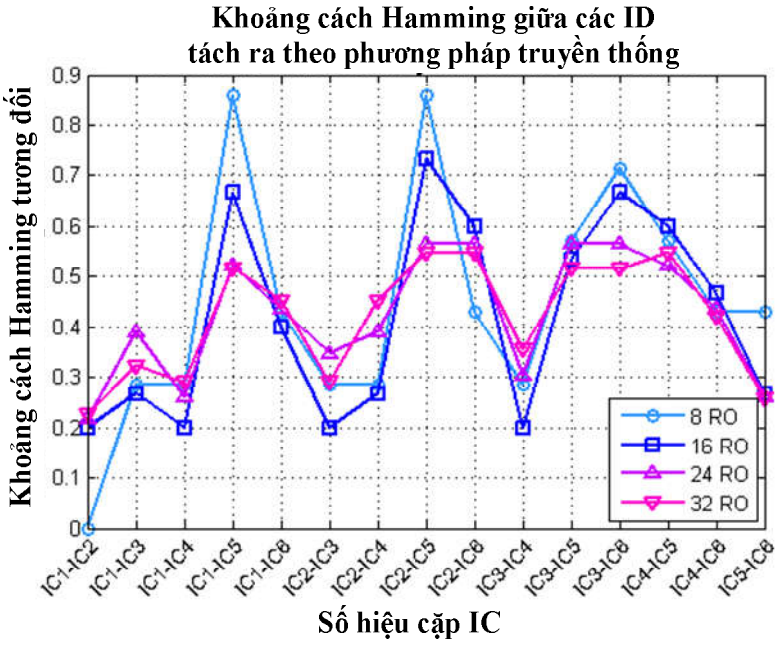


b)

Hình 3.4: Đồ thị các vector quy chuẩn về điểm 0 của 4 IC FPGA Spartan-6 (a) và 6 IC FPGA Spartan-3E (b) tại 25°C.



a)



b)

Hình 3.5: Khoảng cách Hamming tương đối giữa các ID tách ra theo phương pháp truyền thống, khảo sát đối với 4 FPGA Spartan-6 (a) và 6 FPGA Spartan-3E (b).

Từ các đồ thị được trình bày trên Hình 3.5(a) có thể thấy, với số RO lớn, $n_{RO} = 32(24)$, khoảng cách Hamming cực tiểu giữa các ID là 7 bit, tương ứng khoảng cách Hamming tương đối xấp xỉ $0,23$ (5 bit, $0,22$). Tuy nhiên, khi giảm số RO trong mảng, $n_{RO} = 16$, các cặp IC $IC_1 – IC_2$, $IC_1 – IC_4$, $IC_2 – IC_3$ và $IC_3 – IC_4$ chỉ khác nhau 3 bit ($0,20$). Với $n_{RO} = 8$, IC_1 và IC_2 còn không thể phân biệt được. Hiện tượng tương quan càng rõ ràng hơn đối với tập số lượng lớn các IC. Để đảm bảo độ tin cậy, cần thiết kế mảng RO có số RO lớn.

Phân tích trên đây cho thấy hạn chế của các phương pháp truyền thống (ghép cặp liên tiếp RO, tạo bit đáp ứng bằng hàm dấu và sử dụng khoảng cách Hamming) trong định danh và xác thực ID sử dụng mạch RO PUF. Theo đó, dữ liệu đáp ứng RO PUF có tính tương quan cao, cần số RO lớn để có độ dài dữ liệu đáp ứng đủ để tách ID và vì vậy không hiệu quả về phần cứng và năng lượng tiêu thụ. Tiếp theo, nghiên cứu sinh đề xuất giải pháp định danh và xác thực ID trên cơ sở tham khảo các công cụ lý thuyết [10-13] có bổ sung phương pháp ngưỡng dựa trên khoảng cách Euclid.

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

Về mặt toán học [89], không gian vector n chiều V có tích vô hướng được gọi là *không gian Euclid*.

Với $u = (u_1, u_2, ..., u_n), v = (v_1, v_2, ..., v_n) \in V$, chuẩn/độ dài của u là số không âm $\|u\|$ được xác định bởi:

$$\|u\| := \langle u, u \rangle^{1/2} = \sqrt{u_1^2 + u_2^2 + ... + u_n^2} \tag{3.2}$$

Khoảng cách Euclid giữa u và v được định nghĩa bởi:

$$d(u, v) := \|u - v\| = \sqrt{(u_1 - v_1)^2 + (u_2 - v_2)^2 + ... + (u_n - v_n)^2} \tag{3.3}$$

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:

$$df_i = f_i - f_{i+1} \tag{3.4}$$

là tần số hiệu của cặp tần số RO liên tiếp f_i, f_{i+1}, n là số RO có trong mảng RO.

Vector R đối với mỗi IC đặc trưng bởi một dạng đồ thị gấp khúc duy nhất như được trình bày trên Hình 3.4. Như đã trình bày trong thực nghiệm phần 2.3.3, dạng đường này rất ổn định đối với các nhân tố biến thiên toàn cục. Để định lượng phẩm chất của mạch RO PUF và làm cơ sở cho xác định mức ngưỡng cho quá trình xác thực, nghiên cứu sinh đề xuất các công thức tính khoảng cách dựa trên độ đo Euclid như sau.

Khoảng cách giữa hai vector R_i và R_j:

$$d\left(R_i, R_j\right) = \sqrt{\sum_{k=1}^{n-1}\left(df_{ik} - df_{jk}\right)^2} \tag{3.5}$$

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 (*normalized distance*) giữa R_i và R_j khi đó sẽ được xác định bởi:

$$d_{norm} = \frac{d\left(R_i, R_j\right)}{2^{k_{norm}}\sqrt{n-1}} \tag{3.6}$$

Trong đó, $2^{k_{norm}}\sqrt{n-1}$ là khoảng cách cực đại giữa hai vector $\left(n-1\right)$ chiều; k_{norm} là hệ số chuẩn hóa, dùng để chuẩn hóa khoảng cách $d\left(R_i, R_j\right)$

về giá trị nằm trong khoảng $(0,1)$. k_{norm} được tính từ giá trị tuyệt đối cực đại của tọa độ df_{ik} xác định từ thực nghiệm theo công thức:

$$k_{norm} = \left[\log_2 \left(\max \left\{ \left| df_{ik} \right|, i = \overline{1,N}, k = \overline{1,n-1} \right\} \right) \right] + 1 \qquad (3.7)$$

Khoảng cách nội chuẩn hóa (*normalized intra-distance*) giữa vector mẫu ID và vector ID danh định:

$$d_{intra}\left(R_l, R\right) = \frac{d\left(R_l, R\right)}{2^{k_{norm}} \sqrt{n-1}} \qquad (3.8)$$

Trong đó R_l là vectơ mẫu ID của lần đo thứ l, R là vectơ ID danh định của IC. R được xác định từ thống kê trên tập vector mẫu ID có số phần tử lớn, mỗi tọa độ của R là trung bình thống kê tập trị số tọa độ tương ứng của các vector mẫu ID. Trị số d_{intra} thể hiện biến thiên của df_i gây ra bởi thăng giáng của nhiệt độ môi trường và/hoặc điện áp nguồn nuôi. Giá trị mong muốn của d_{intra} là xấp xỉ bằng 0.

Khoảng cách tương quan chuẩn hóa (*normalized inter-distance*) giữa các vector ID danh định được xác định bởi:

$$d_{inter}\left(R_p, R_q\right) = \frac{d\left(R_p, R_q\right)}{2^{k_{norm}} \sqrt{n-1}} \qquad (3.9)$$

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 d_{inter} thể hiện mức độ phân bố về không gian (tính duy nhất) của các ID. Giá trị mong muốn của d_{inter} là:

$$\min\left\{ d_{inter}\left(R_p, R_q\right), \forall p,q = \overline{1,N}, p \neq q \right\} > d_{thr} \qquad (3.10)$$

Với d_{thr} là mức ngưỡng xác thực.

3.1.3. Đặc trưng thống kê của khoảng cách Euclid

Các thành phần df_i trong công thức (3.4) hay $\left(df_{ik} - df_{jk}\right)$ trong công thức (3.5) có thể coi là các biến ngẫu nhiên có phân bố chuẩn do tần số RO có phân bố chuẩn (khảo sát phần 2.3.1), với giá trị trung bình thống kê và phương sai xác định. Để khảo sát đặc trưng thống kê của các biến khoảng cách, không mất tính tổng quát, có thể 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.

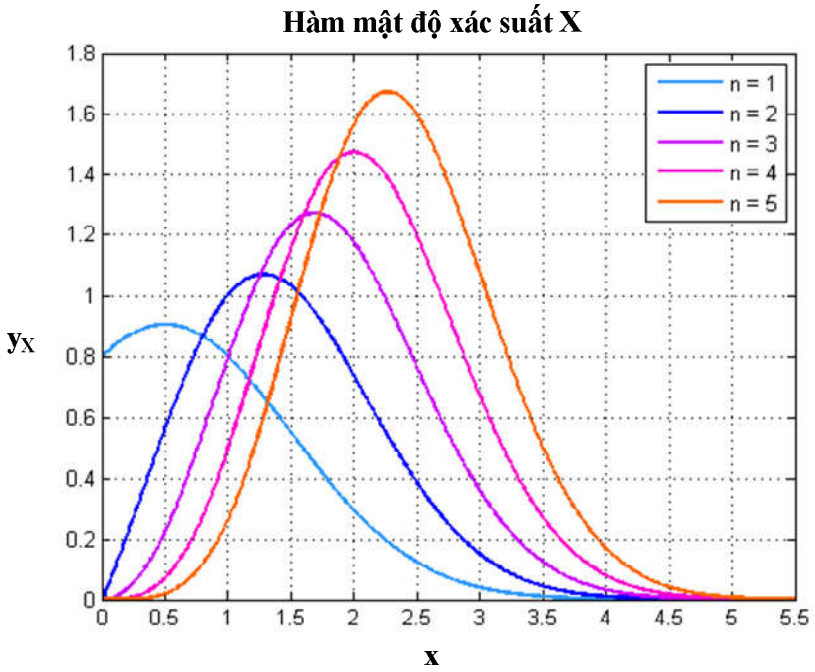
Xét n biến ngẫu nhiên X_i, $i = \overline{1,n}$, cùng tuân theo quy luật chuẩn hóa $\mathcal{N}(0,1)$. Khi đó, biến ngẫu nhiên $Y_i = \sqrt{\sum_{i=1}^{n} X_i^2}$ tuân theo quy luật phân bố $\mathcal{X}$ với n bậc tự do [90], có hàm mật độ xác suất được xác định bởi:

$$f_{\mathcal{X}}(x) = \frac{x^{n-1} e^{-\frac{x^2}{2}}}{2^{\frac{n}{2}-1}\Gamma\left(\frac{n}{2}\right)} \tag{3.11}$$

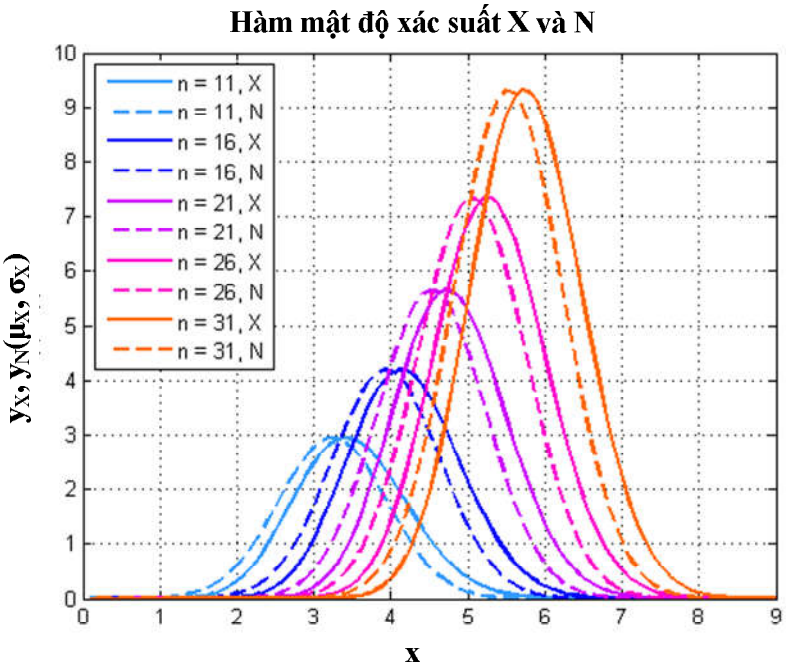
Trong đó $\Gamma(x) = \int_0^{\infty} t^{x-1} e^{-t} dt$ là hàm Gamma. Với đối số $x = n \in \mathbb{Z}, n \geq 0$, $\Gamma(n+1) = n\Gamma(n) = n!$. Đồ thị của hàm $f_{\mathcal{X}}(x)$ được trình bày trên Hình 3.6. Khi n lớn, giá trị trung bình và phương sai của phân phối $\mathcal{X}$ được xác định bởi [91]:

$$\mu_{\mathcal{X}} = \mu_k \Big|_{k=1} = 2^{\frac{k}{2}} \frac{\Gamma\left(\frac{n+k}{2}\right)}{\Gamma\left(\frac{n}{2}\right)}\Bigg|_{k=1} = 2^{\frac{1}{2}} \frac{\Gamma\left(\frac{n+1}{2}\right)}{\Gamma\left(\frac{n}{2}\right)} \approx \sqrt{n - \frac{1}{2}} \tag{3.12}$$

$$\sigma_{\mathcal{X}}^2 = n - \mu_{\mathcal{X}}^2 \approx n - \left(n - \frac{1}{2}\right) = \frac{1}{2} \tag{3.13}$$



Hình 3.6: Đồ thị hàm mật độ xác suất $\mathcal{X}$

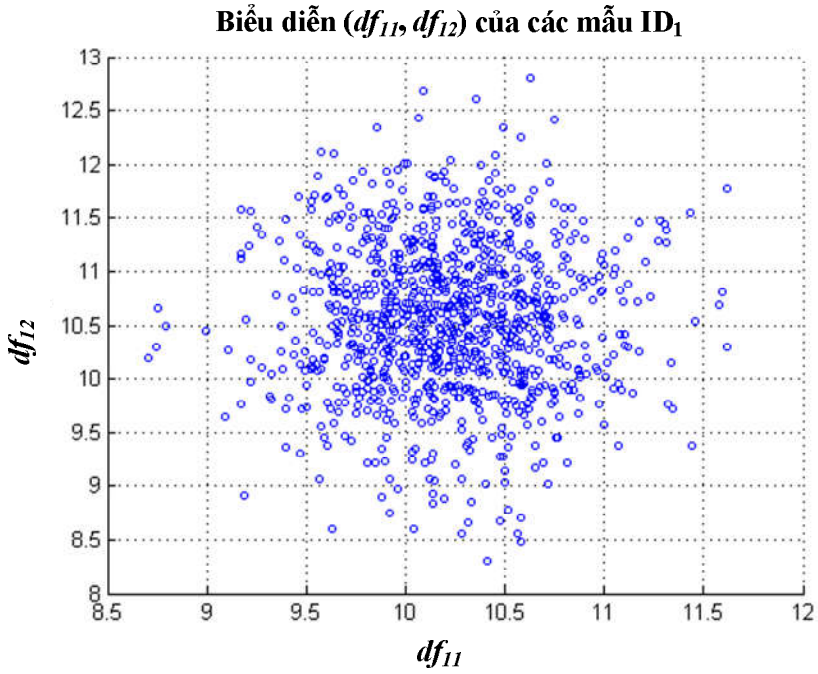


Hình 3.7: Đồ thị các hàm mật độ xác suất $\mathcal{X}$ và $\mathcal{N}(\mu_{\mathcal{X}}, \sigma_{\mathcal{X}})$

Hình 3.7 trình bày đồ thị các hàm mật độ xác suất $\mathcal{X}$ và $\mathcal{N}(\mu_{\mathcal{X}},\sigma_{\mathcal{X}})$ tương ứng khi n lớn. Như vậy, với n lớn (Trong thiết kế cụ thể, $n=31$), có thể coi các biến khoảng cách Euclid có phân bố chuẩn.

*** Mô phỏng đặc trưng thống kê khoảng cách Euclid**

Tạo hai tập vector ID mẫu tương ứng IC_1 và IC_2: $ID_1=\left\{df_{1i}\middle|i=\overline{1,n}\right\}$; $ID_2=\left\{df_{2i}\middle|i=\overline{1,n}\right\}$. Các tọa độ $df_{ij}, i=\overline{1,2}, j=\overline{1,n}$, có phân bố chuẩn $\mathcal{N}\left(\mu_{df_{ij}},\sigma^2_{df_{ij}}\right)$: $df_{ij}=\mu_{df_{ij}}+\sigma_{df_{ij}}$. Biểu diễn hai tọa độ đầu (df_{11},df_{12}) của ID_1 trên mặt phẳng được trình bày trên Hình 3.8.



Hình 3.8: Biểu diễn 2-D hai tọa độ đầu của ID_1

Từ tập n_{sample} mẫu ID_1, ID_2, xác định các vector ID danh định và hệ số chuẩn hóa:

$$ID_{i\_nom}=mean\left\{ID_{ijk}\middle|i=\overline{1,2},j=\overline{1,n},k=\overline{1,n_{sample}}\right\},$$

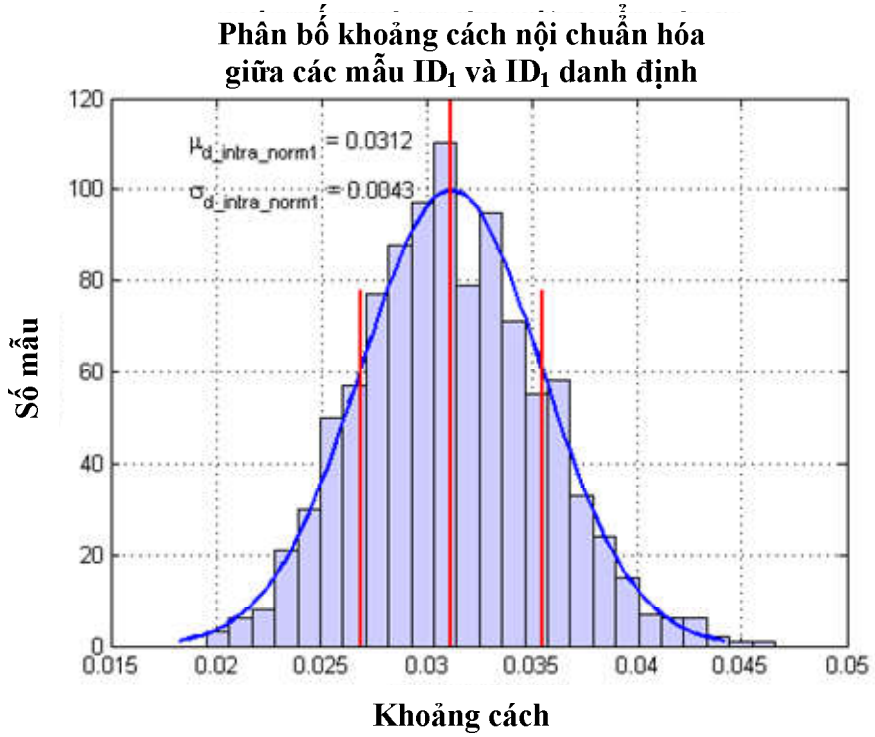
$$k_{norm} = \left[\log_2 \left(df_{max} \right) \right] + 1,$$

$$df_{max} = \max \left\{ \left| df_{ijk} \right| \middle| i = \overline{1,2}, j = \overline{1,n}, k = \overline{1,n_{sample}} \right\}$$

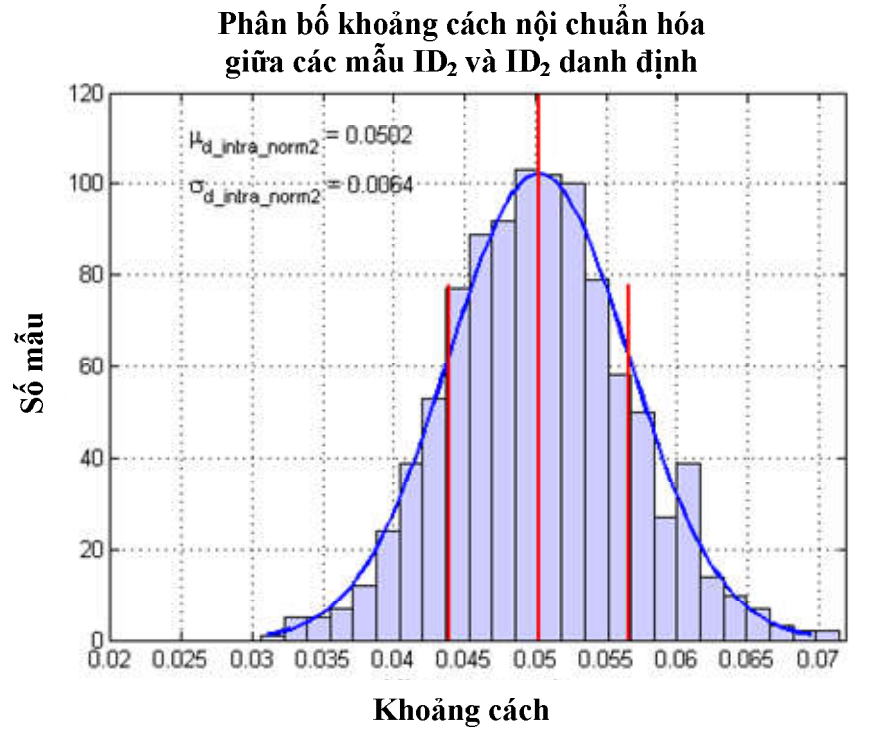
Từ đó xác định được khoảng cách nội chuẩn hóa từ các mẫu ID đến ID danh định theo công thức (3.8). Biểu diễn phân bố của các tập mẫu này được trình bày trên trên Hình 3.9. Có thể thấy các tập mẫu khoảng cách nội chuẩn hóa có phân bố chuẩn với giá trị trung bình và độ lệch chuẩn xác định.

Hình 3.10 là biểu đồ phân bố khoảng cách nội chuẩn hóa tính toán trên số liệu thực nghiệm của một IC FPGA Spartan-6/Spartan-3E tại 25^{o}C đối với 255 mẫu khảo sát. Biểu đồ có dạng phân bố chuẩn với các giá trị tập trung cao quanh giá trị trung bình thống kê, thể hiện ở độ lệch chuẩn nhỏ. Như vậy, số liệu thực nghiệm phù hợp với kết quả mô phỏng về đặc trưng thống kê khoảng cách nội chuẩn hóa.

Tiếp theo, tính khoảng cách tương quan chuẩn hóa từ các mẫu ID_1 đến ID_2 danh định theo công thức (3.6). Biểu diễn phân bố của tập mẫu này được trình bày trên Hình 3.11.

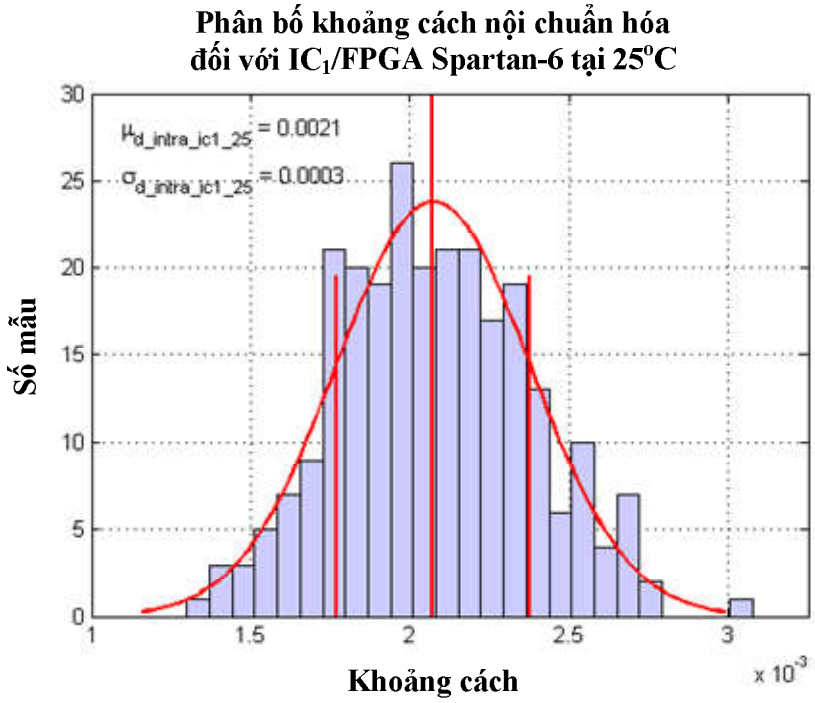


a)

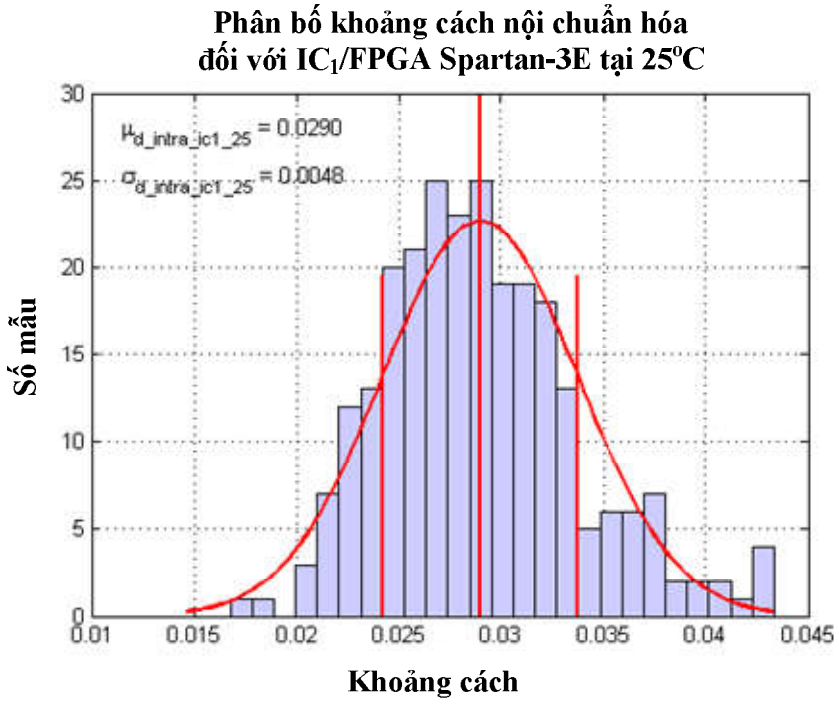


b)

Hình 3.9: Phân bố khoảng cách nội chuẩn hóa giữa các mẫu ID và ID danh định đối với ID_1 (a) và ID_2 (b).

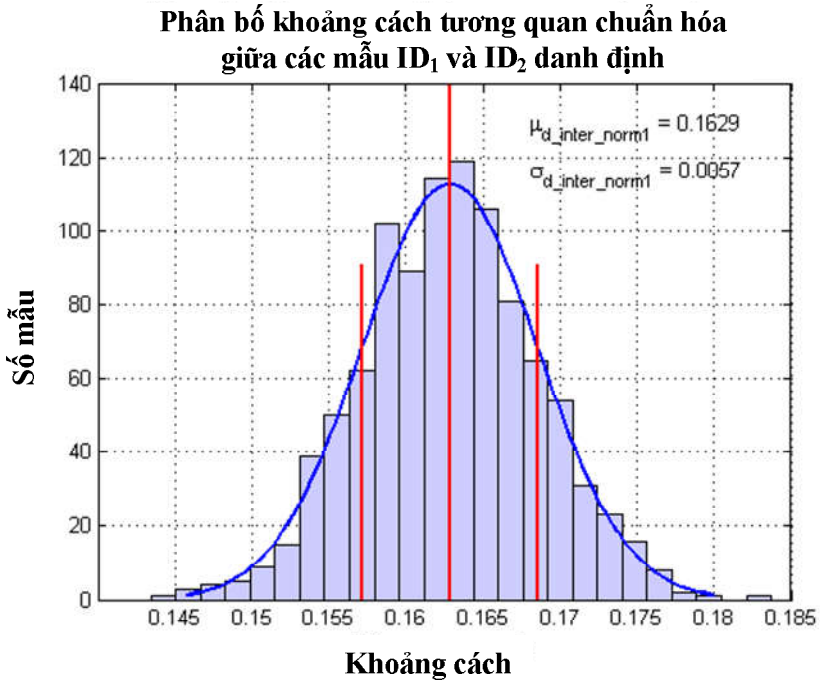


a)

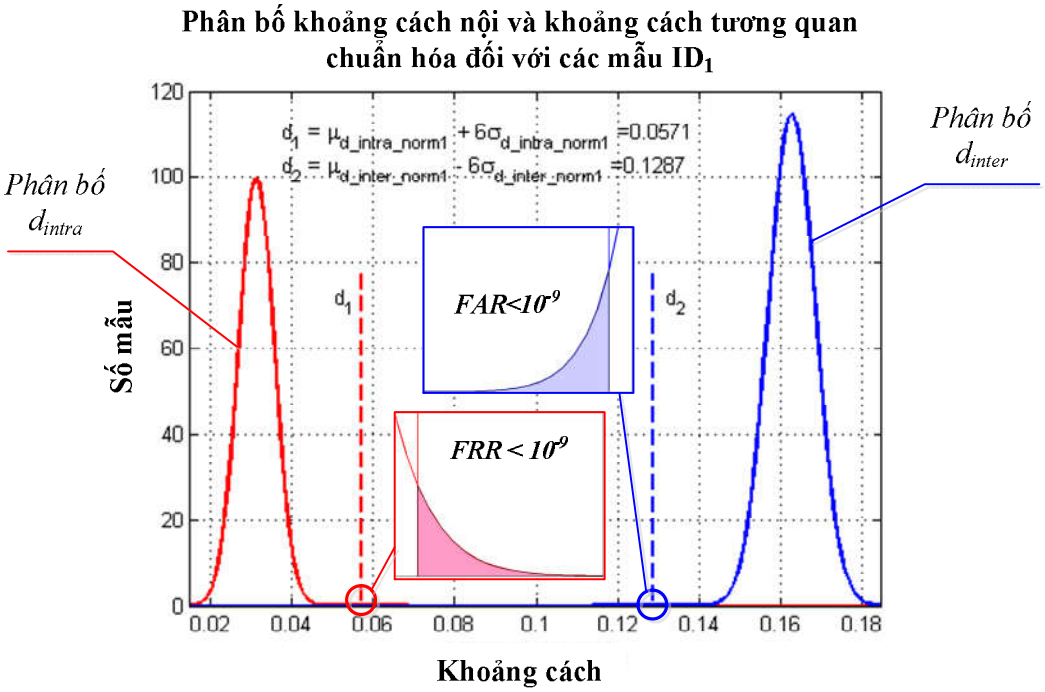


b)

Hình 3.10: Biểu đồ phân bố khoảng cách nội chuẩn hóa của một IC FPGA Spartan-6 (a) và Spartan-3E (b) tại 25°C



Hình 3.11: Phân bố khoảng cách tương quan chuẩn hóa giữa các mẫu ID_1 và ID_2 danh định.



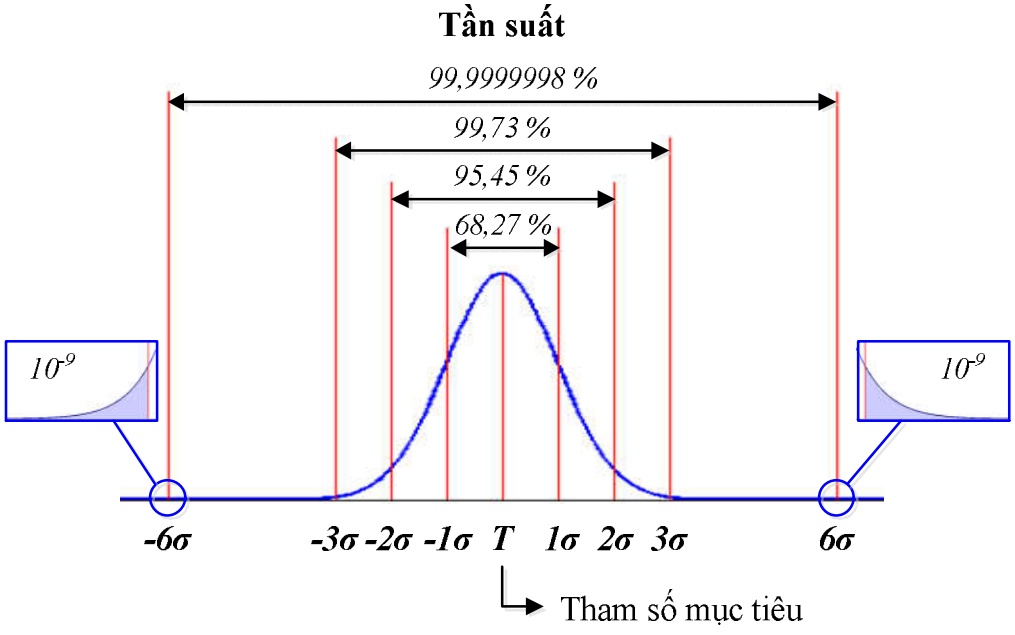
Hình 3.12: Phân bố khoảng cách nội và khoảng cách tương quan chuẩn hóa đối với các mẫu ID_1.

Kết hợp các đồ thị hàm mật độ xác suất trong Hình 3.9(a) và Hình 3.11 vào Hình 3.12, nhận được biểu diễn tương quan giữa phân bố khoảng cách nội chuẩn hóa và khoảng cách tương quan chuẩn hóa đối với ID_1. *FRR* và *FAR* được xác định từ các đường mức d_1, d_2 theo quy tắc 6σ:

$$d_1 = \mu_{d_{intra\_norm1}} + 6\sigma_{d_{intra\_norm1}} \quad (3.14)$$

$$d_2 = \mu_{d_{inter\_norm1}} - 6\sigma_{d_{inter\_norm1}} \quad (3.15)$$

Quy tắc 6σ là một tiêu chuẩn kiểm định chất lượng được ứng dụng rộng rãi trong kinh tế và công nghiệp từ đầu thập niên 2000. Mục đích của tiêu chuẩn này là tập trung vào giảm thiểu mức độ mất ổn định của các đặc tính chất lượng sản phẩm. Giả định các đặc tính chất lượng có mô hình phân bố chuẩn, quy tắc 6σ xác định giới hạn đảm bảo kiểm soát tính ổn định là 6 lần độ lệch chuẩn tính từ tham số mục tiêu. Ở mức 6σ, tỷ lệ bất định giảm xuống còn 2 phần tỷ [92]. Phân bố chuẩn và các giới hạn về độ lệch chuẩn được biểu diễn trên Hình 3.13, còn định lượng mức độ bất định trong kiểm soát đặc tính được trình bày trong Bảng 3.1 [93].



Hình 3.13: Phân bố chuẩn và các giới hạn về độ lệch chuẩn [93]

Bảng 3.1: Định lượng tỷ lệ lỗi tương ứng các giới hạn xác định mức ngưỡng [93]

Giới hạn	**Tỷ lệ chiếm lĩnh [%]**	**Tỷ lệ lỗi [phần triệu]**
±1 σ	*68,27*	*317300*
±2 σ	*95,45*	*45500*
±3 σ	*99,73*	*2700*
±4 σ	*99,9937*	*63*
±5 σ	*99,999943*	*0,57*
±6 σ	*99,9999998*	*0,002*

Từ Hình 3.12, có thể đề xuất một mức ngưỡng xác thực d_{thr}: Nếu mẫu ID có khoảng cách chuẩn hóa đến ID danh định nhỏ hơn d_{thr}, mẫu được coi là thuộc về IC có ID danh định đó; nếu khoảng cách chuẩn hóa đến ID danh định lớn hơn d_{thr}, mẫu được coi là thuộc về IC khác.

Có thể chọn $d_1 \le d_{thr} \le d_2$. Với $d_{thr} \ge d_1$, xác suất để một mẫu ID_1 có khoảng cách chuẩn hóa đến ID_1 danh định lớn hơn d_{thr} và bị loại bỏ (*FRR*) là nhỏ hơn 10^{-9}. Với $d_{thr} \le d_2$, xác suất để một mẫu ID lạ có khoảng cách chuẩn hóa đến ID_1 danh định nhỏ hơn d_{thr} và được coi là của IC_1 (*FAR*) là nhỏ hơn nhiều 10^{-9}. Như vậy, xác suất xác thực nhầm nhỏ hơn nhiều 2×10^{-9}.

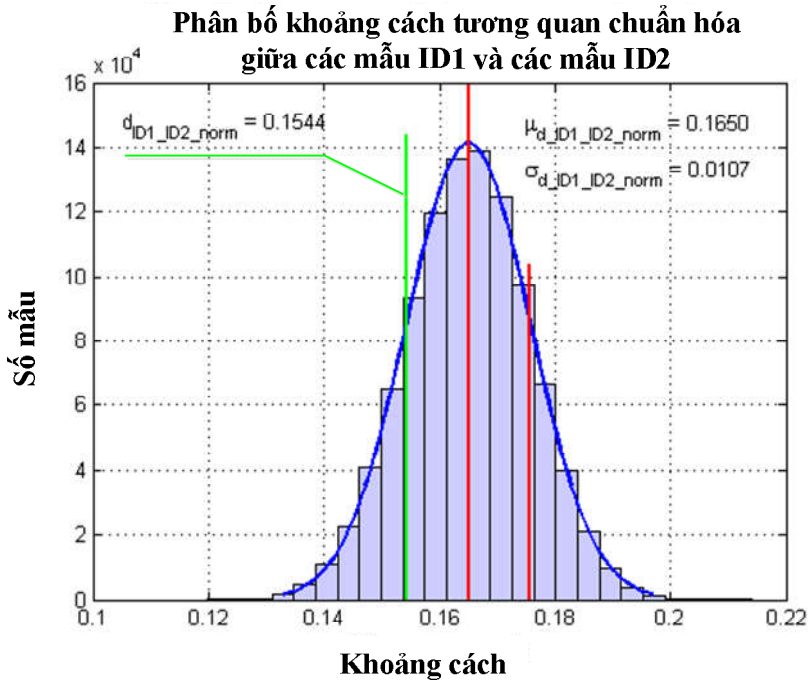
Xét tập số lượng lớn IC khảo sát. Giá trị cận dưới của d_{thr} có thể được xác định từ điều kiện:

$$d_{thr} \ge \max\left\{\mu_{d_{inntra\_i}}\right\} + 6\max\left\{\sigma_{d_{inntra\_i}}\right\},\ i = \overline{1,N}, \qquad (3.16)$$

Trong đó, $\mu_{d_{inntra\_i}}$ và $\sigma_{d_{inntra\_i}}$ tương ứng là giá trị trung bình và độ lệch chuẩn của phân bố các mẫu khoảng cách nội chuẩn hóa tương ứng IC_i trong

tập IC khảo sát.

Giá trị cận trên của d_{thr} cần nhỏ hơn khoảng cách chuẩn hóa cực tiểu giữa các ID danh định. Phân bố khoảng cách chuẩn hóa giữa hai mẫu ID bất kỳ thuộc IC_1 và IC_2 được trình bày trên Hình 3.14.



Hình 3.14: Phân bố khoảng cách tương quan chuẩn hóa giữa các mẫu ID_1 và các mẫu ID_2

Điều kiện chặt theo tiêu chuẩn 6σ là $d_{thr} \le \mu_{d_{i\_j\_norm}} - 6\sigma_{d_{i\_j\_norm}}$, $i, j \in \overline{I,N}, i \ne j$, với $\mu_{d_{i\_j\_norm}}$ và $\sigma_{d_{i\_j\_norm}}$ tương ứng là giá trị trung bình và độ lệch chuẩn của phân bố khoảng cách tương quan chuẩn hóa giữa ID_i và ID_j. Tuy nhiên, để giảm thiểu độ phức tạp tính toán mà không gây ra sai số xác thực đáng kể, có thể chọn:

$$d_{thr} \le \min\left\{ d_{inter\_i\_j\_norm} \middle| i, j \in \overline{I,N}, i \ne j \right\}, \qquad (3.17)$$

Với $d_{inter\_i\_j\_norm} \middle| i, j \in \overline{I,N}, i \ne j$ là khoảng cách tương quan chuẩn hóa

giữa các ID danh định trong tập N IC khảo sát. Sai số xác thực do việc chọn d_{thr} theo công thức (3.17) nếu có chỉ xuất hiện đối với cặp ID danh định có khoảng cách tương quan chuẩn hóa nhỏ nhất, đặc biệt có thể bỏ qua khi khoảng cách tương quan chuẩn hóa cực tiểu lớn hơn mức ngưỡng một số lần.

Như vậy, chọn d_{thr} từ các điều kiện (3.16) và (3.17) sẽ đảm bảo xác suất để một mẫu ID bị xác thực nhầm nhỏ hơn 2×10^{-9}. Như sẽ được trình bày trong thực nghiệm phần 3.3.3, khoảng cách tương quan chuẩn hóa nhỏ nhất giữa các ID danh định trong tập các IC khảo sát lớn hơn d_{thr}, đảm bảo độ tin cậy của sơ đồ xác thực.

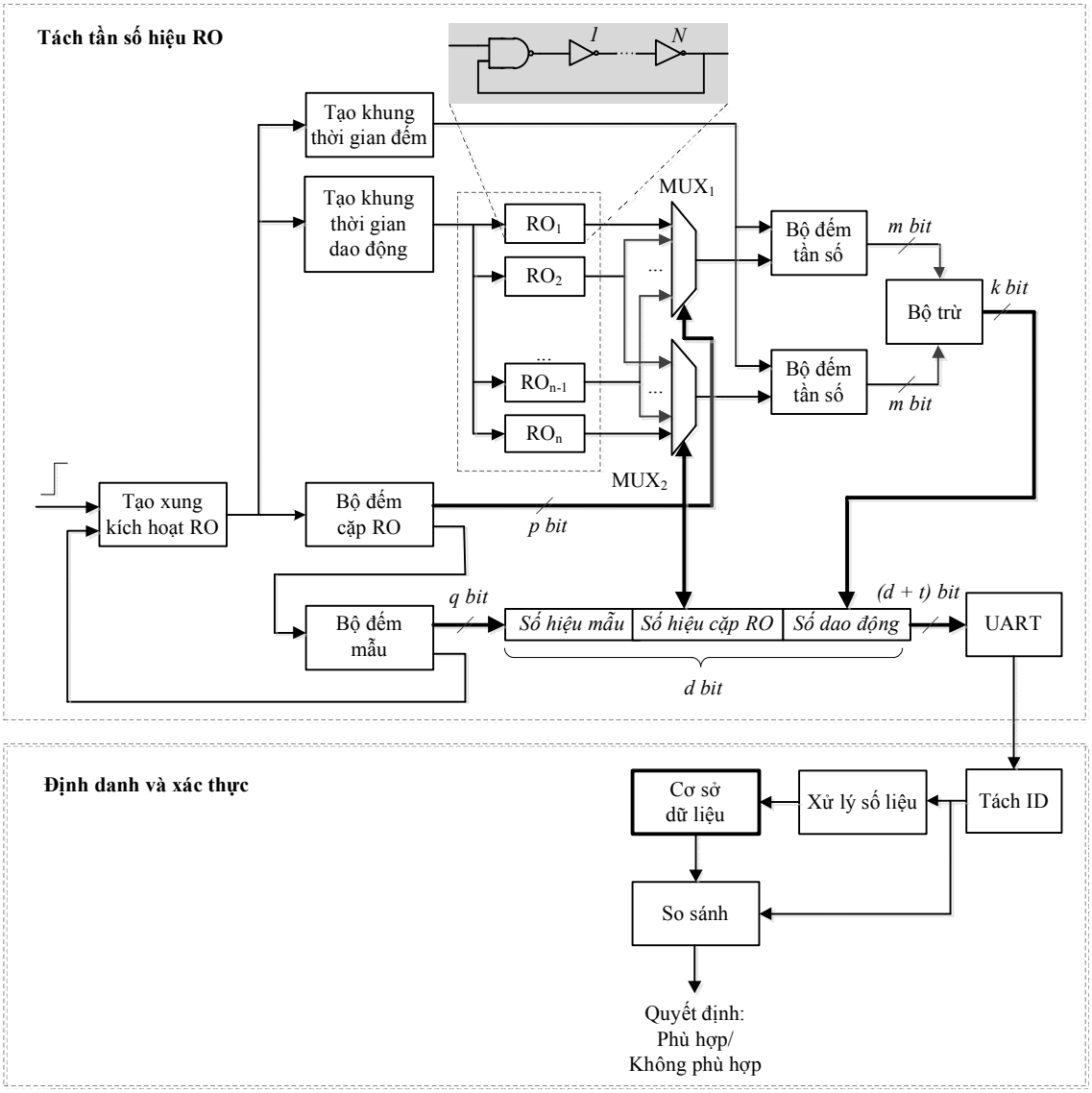
Việc sử dụng độ đo Euclid thay cho độ đo Hamming sẽ khắc phục được hạn chế của độ đo Hamming là độ phân giải xác định mức ngưỡng thấp, hiện tượng tương quan mạnh trong dữ liệu đáp ứng và yêu cầu tập RO lớn trong thiết kế RO PUF. Đồng thời, việc sử dụng các tham số khoảng cách dựa trên độ đo Euclid cũng thiết lập phương pháp xác thực tin cậy như trình bày dưới đây.

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

Hình 3.15 trình bày sơ đồ định danh và xác thực ID ứng dụng RO PUF. Sơ đồ gồm hai phần: i) Mạch tách tần số hiệu RO; ii) Giao thức định danh và xác thực ID.

* 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.



Hình 3.15: Sơ đồ định danh và xác thực ID ứng dụng RO PUF

So với sơ đồ Hình 2.5, mảng RO và các khối tạo xung kích hoạt RO, tạo khung thời gian dao động, tạo khung thời gian đếm, bộ đếm tần số, bộ đếm mẫu, UART có cấu trúc tương tự. Những điểm khác biệt là:

- Bộ đếm cặp RO có khoảng trị số đếm tương ứng từ 0 đến $(n-1)$;

- MUX_1 và MUX_2 là các bộ chọn kênh $(n-1):1$, khác nhau về điều kiện chọn. Với cùng p bit điều khiển, đầu ra MUX_1 là dao động tạo bởi RO_i,

đầu ra MUX_2 là dao động tạo bởi RO_{i+1}, $i = \overline{1,n-2}$.

- Bộ trừ xác định hiệu số dao động đếm được của cặp RO_i – RO_{i+1}. Vì giá trị này thường nhỏ hơn số dao động đếm được của mỗi RO nên dữ liệu ra bộ trừ có thể được định dạng với số bit nhỏ hơn ($k \le m$), nhằm đơn giản hóa thiết kế và tiết kiệm tài nguyên phần cứng.

*** Giao thức định danh và xác thực ID**

- 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 k bit dạng bù 2, sau đó chuyển các trị số này sang trị số thập phân và nhân với hệ số $1/\Delta T_{mea}$, với ΔT_{mea} là khoảng thời gian đếm. Kết quả, đầu ra bộ tách ID là mẫu vector ID $(n-1)$ chiều, mỗi chiều là giá trị tần số hiệu $df_i = f_i - f_{i+1}$, $i = \overline{1,n-1}$.

- Khối Xử lý số liệu tiến hành các 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 các cấu trúc dữ liệu này vào cơ sở dữ liệu.

- Trong pha xác thực, mẫu ID được kết hợp tuần tự với các ID 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.

Hình PL1.4 trình bày sơ đồ chức năng chi tiết mạch tách tần số hiệu trong sơ đồ định danh và xác thực ID sử dụng RO PUF xây dựng trên FPGA. Thiết kế này được thực thi trên vi mạch khả trình FPGA Xilinx Spartan 6, với $n = 32$, $m = 24$, $k = 24$.

Phương pháp xây dựng mảng RO của thiết kế tương tự như đối với sơ

đồ thực nghiệm dùng để khảo sát đặc tính RO đã được trình bày trong phần 2.1. Hai bộ chọn kênh 31:1 tuần tự chọn dao động của các cặp RO liên tiếp đưa tới hai bộ đếm 24 bit tương ứng. Dữ liệu đếm được đưa tới bộ trừ để tạo trị số hiệu dạng dữ liệu 24 bit. Trị số này được bổ sung các bit điều khiển – kiểm tra – báo hiệu để tạo khung dữ liệu 40 bit phù hợp để truyền đi. Việc truyền dữ liệu PUF từ mạch tới PC cũng như nhận tín hiệu *reset* từ máy tính được thực hiện qua giao diện UART.

Sơ đồ mạch vật lý của thiết kế được trình bày trên Hình PL1.5. Các thực thể RO được gán địa chỉ và kết nối thủ công, đảm bảo độ trễ đồng nhất cũng như tính đối xứng. Thiết kế có thể được thực thi linh hoạt trên các họ FPGA khác với chỉnh sửa phù hợp. Hình PL1.6 và Hình PL1.7 tương ứng là sơ đồ mạch vật lý của thiết kế trên các FPGA Spartan-3E, Artix-7. Quy trình định danh và xác thực ID cho thiết bị được trình bày trên Hình PL1.8.

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

3.3.1. Mô hình thực nghiệm

Mạch tách tần số hiệu trên Hình 3.15 được thực thi trên FPGA Xilinx Spartan-6, Xilinx Spartan-3E và Xilinx Artix-7:

- Trên FPGA Xilinx Spartan-6: $4\text{IC}\times 32\text{RO}$, đo 256 mẫu tần số hiệu đối với mỗi cặp RO của mỗi IC tại mỗi điểm nhiệt độ trong khoảng 25^{o}C – 80^{o}C, bước 5^{o}C.

- Trên FPGA Xilinx Spartan-3E: $6\text{IC}\times 32\text{RO}$, đo 256 mẫu tần số hiệu đối với mỗi cặp RO của mỗi IC tại mỗi điểm nhiệt độ trong khoảng 25^{o}C – 80^{o}C, bước 5^{o}C.

- Trên FPGA Xilinx Artix-7: $9\text{IC}\times 32\text{RO}$, đo 256 mẫu tần số hiệu đối với mỗi cặp RO của mỗi IC tại nhiệt độ phòng.

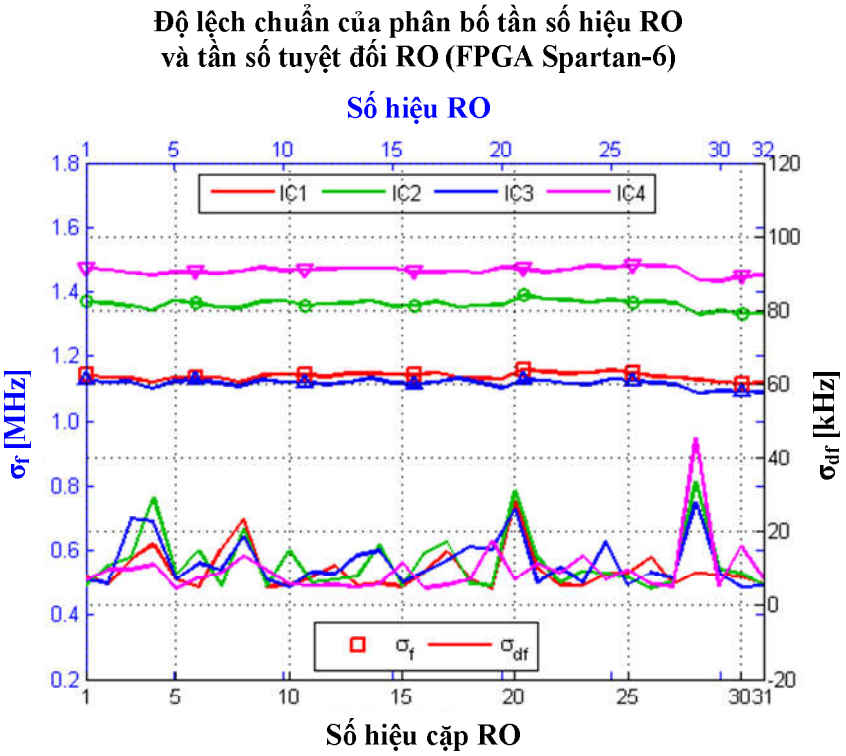
Nhiệt độ môi trường hoạt động được điều chỉnh bởi tủ sấy đa dụng Memmert UN110 với sai số 0,1^{o}C trong khoảng nhiệt độ khảo sát. Dữ liệu thu nhận từ mạch thí nghiệm FPGA được truyền tới máy tính qua giao diện UART. Dưới đây nghiên cứu sinh khảo sát tính ổn định và tính duy nhất của ID đối với mạch FPGA Spartan-6. Kết quả tương tự đối với các mạch FPGA Spartan-3E, Artix-7 sẽ được bổ sung sau đó.

3.3.2. Ước lượng tính ổn định của ID

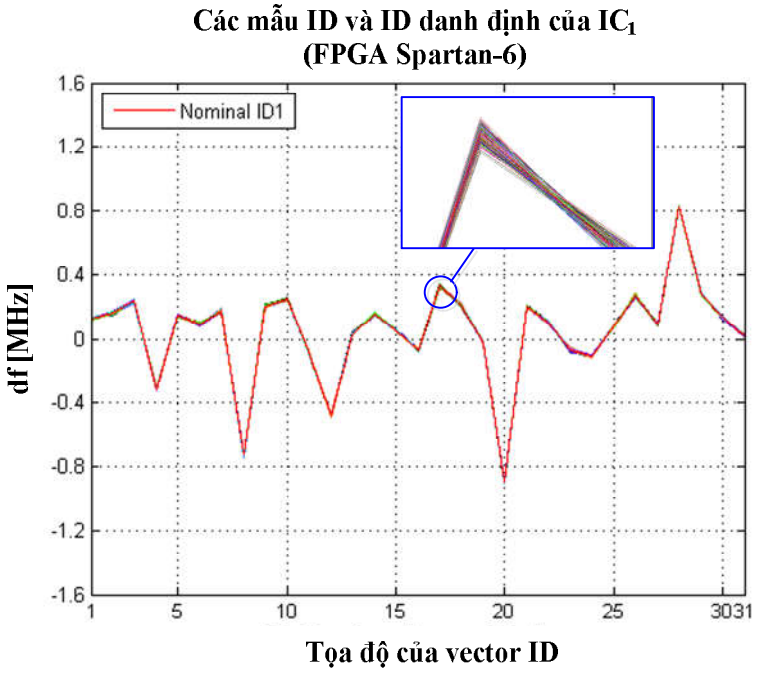
Sử dụng sơ đồ đề xuất, thu thập các mẫu dữ liệu tần số hiệu df cho mỗi IC tại mỗi điểm nhiệt độ với với 256 lần đo. Hình 3.16 biểu diễn đồ thị độ lệch chuẩn tần số hiệu RO (trục dưới – trục phải) và độ lệch chuẩn tần số tuyệt đối RO (trục trên – trục trái). Có thể thấy độ lệch chuẩn tần số hiệu RO nhỏ hơn nhiều độ lệch chuẩn tần số tuyệt đối RO trên toàn dải nhiệt độ khảo sát. Điều này thể hiện hiệu quả của phương pháp tần số hiệu, ghép cặp liên tiếp các RO đối với việc hạn chế tác động của các nhân tố biến thiên toàn cục (bao gồm nhiệt độ môi trường hoạt động) lên mạch RO PUF.

Với mỗi mẫu dữ liệu df, xác định mẫu ID có 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 (3.6).

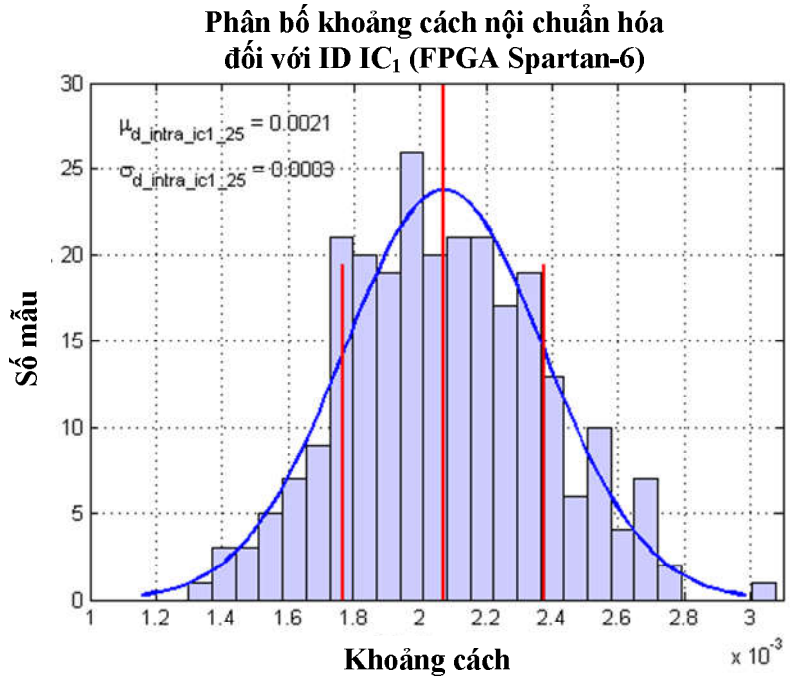
Hình 3.17 biểu diễn đồ thị của 256 mẫu vector ID và vector ID danh định (đường màu đỏ) của IC_1 tại 25^{o}C. Có thể thấy các mẫu vector ID của IC_1 duy trì dạng xác định, thăng giáng xung quanh vector ID danh định. Điều này được thể hiện qua định lượng tham số thống kê của các mẫu khoảng cách nội chuẩn hóa. Phân bố của các mẫu khoảng cách nội chuẩn hóa có dạng gần với phân bố chuẩn, được trình bày trên Hình 3.18.



Hình 3.16: Độ lệch chuẩn của tần số hiệu RO và tần số tuyệt đối RO của các IC FPGA Spartan-6, khảo sát trong dải nhiệt độ 25°C – 80°C.

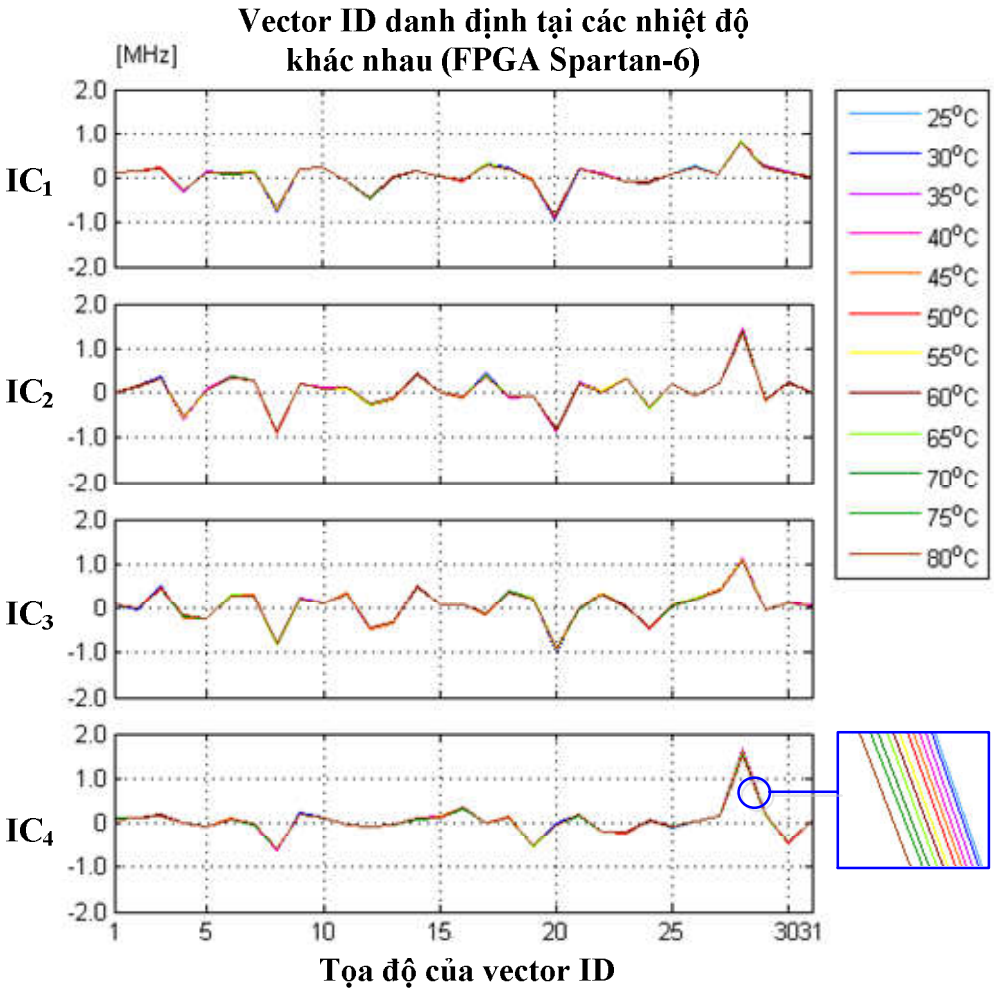


Hình 3.17: Tính ổn định của ID IC_1 (FPGA Spartan-6) đối với ảnh hưởng của thăng giáng tức thời.



Hình 3.18: Giản đồ phân bố khoảng cách nội chuẩn hóa tập mẫu ID của IC_1 (FPGA Spartan-6) tại 25°C.

Các vector ID danh định của 4 IC tại các nhiệt độ khác nhau (25°C – 80°C) có dạng tương tự được biểu diễn trên Hình 3.19. Bảng 3.2, Bảng 3.3 và Bảng 3.4 trình bày giá trị khoảng cách nội chuẩn hóa cực đại, giá trị trung bình và độ lệch chuẩn của khoảng cách nội chuẩn hóa đối với tập IC khảo sát FPGA Spartan-6), trên toàn dải nhiệt độ. Ước lượng sai số xác định khoảng cách chuẩn hóa gây ra bởi sai số đếm được trình bày trong Phụ lục 2:. Trị số này đối với FPGA Spartan-6 và FPGA Spartan-3E tương ứng là $1{,}38\times10^{-5}$ và $2{,}75\times10^{-5}$, nhỏ hơn nhiều độ lệch chuẩn khoảng cách chuẩn hóa và có thể bỏ qua.



Hình 3.19: Tính ổn định của ID tương ứng 4 IC FPGA Spartan-6 đối với sự thay đổi của nhiệt độ môi trường.

Bảng 3.2: Khoảng cách nội chuẩn hóa cực đại $\left[\times 10^{-3}\right]$ (FPGA Spartan-6)

	25°C	**30°C**	**35°C**	**40°C**	**45°C**	**50°C**	**55°C**	**60°C**	**65°C**	**70°C**	**75°C**	**80°C**
IC_1	*3,1*	*3,6*	*2,9*	*2,9*	*3,0*	*3,2*	*2,8*	*2,7*	*3,0*	*3,0*	*2,6*	*2,7*
IC_2	*3,0*	*3,3*	*3,1*	*2,9*	*3,3*	*3,3*	*3,2*	*3,1*	*2,8*	*2,7*	*3,1*	*2,9*
IC_3	*3,1*	*11,3*	*2,7*	*3,2*	*3,1*	*3,2*	*2,8*	*3,5*	*3,6*	*2,9*	*2,9*	*2,7*
IC_4	*10,6*	*2,8*	*2,9*	*2,8*	*3,3*	*3,3*	*3,3*	*3,2*	*2,8*	*2,8*	*2,7*	*2,9*

Bảng 3.3: Giá trị trung bình của khoảng cách nội chuẩn hóa $\left[\times 10^{-3}\right]$ (FPGA Spartan-6)

	25°C	**30°C**	**35°C**	**40°C**	**45°C**	**50°C**	**55°C**	**60°C**	**65°C**	**70°C**	**75°C**	**80°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 3.4: Độ lệch chuẩn của khoảng cách nội chuẩn hóa $\left[\times 10^{-4}\right]$ (FPGA Spartan-6)

	25°C	**30°C**	**35°C**	**40°C**	**45°C**	**50°C**	**55°C**	**60°C**	**65°C**	**70°C**	**75°C**	**80°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*

Đối với mỗi IC, tiến hành ghép cặp các ID danh định tương ứng các điểm nhiệt độ và tính khoảng cách chuẩn hóa giữa chúng. Kết quả đối với IC_1 (FPGA Spartan-6) được trình bày trên Bảng 3.5. Từ tập hợp các bảng dạng Bảng 3.5, xác định được khoảng cách chuẩn hóa cực đại chỉ là $18,5\times 10^{-3}$(Spartan-3E: $2,9\times 10^{-3}$). Các kết quả định lượng trên đây khẳng định kết luận chương 2 là các biến thiên cục bộ khá ổn định với sự thay đổi điều kiện hoạt động và thăng giáng nhiệt độ.

Bảng 3.5: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$ tương ứng các điểm nhiệt độ khảo sát đối với IC_1 (FPGA Spartan-6)

T_2	T_3	T_4	T_5	T_6	T_7	T_8	T_9	T_{10}	T_{11}	T_{12}	
2,3	*3,0*	*4,2*	*5,9*	*6,6*	*8,6*	*9,2*	*10,5*	*11,3*	*12,8*	*13,9*	T_1
	2,9	*3,9*	*5,8*	*6,6*	*8,5*	*9,2*	*10,5*	*11,3*	*12,7*	*13,8*	T_2
		2,6	*4,0*	*4,5*	*6,6*	*7,2*	*8,5*	*9,3*	*10,8*	*11,8*	T_3
			2,6	*3,4*	*5,3*	*6,1*	*7,2*	*8,0*	*9,6*	*10,6*	T_4
				2,1	*3,9*	*4,5*	*5,6*	*6,3*	*7,8*	*8,7*	T_5
					2,4	*3,5*	*4,5*	*5,3*	*6,7*	*7,7*	T_6
						2,6	*2,8*	*3,7*	*5,1*	*6,2*	T_7
							2,0	*2,7*	*4,3*	*5,5*	T_8
								1,2	*2,9*	*4,1*	T_9
									2,2	*3,3*	T_{10}
										1,8	T_{11}

T_1 – T_{12}: 25^oC – 80^oC, bước 5^oC

Mức ngưỡng được chọn bởi biểu thức:

$$d_{thr} = \max\left\{\mu_{d_{intra}}\right\} + 6 \times \max\left\{\sigma_{d_{intra}}\right\} \tag{3.18}$$

Khi tiến hành 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 tương ứng là các giá trị lớn nhất của Bảng 3.3 và Bảng 3.4. Trong trường hợp định danh và xác thực tại nhiệt độ bất kỳ, vector ID danh định, tập mẫu khoảng cách nội chuẩn hóa cùng các tham số thống kê được xác định từ tập dữ liệu tần số hiệu tổng hợp (Bảng 3.6), trên cơ sở đó xác định $\max\left\{\mu_{d_{intra}}\right\}$ và $\max\left\{\sigma_{d_{intra}}\right\}$ dùng để tính toán

mức ngưỡng. Mức ngưỡng xác thực khi này có thể lớn hơn so với trường hợp trước. Kết quả tính mức ngưỡng xác thực đối với các FPGA khác nhau được tổng hợp trong Bảng 3.7.

Bảng 3.6: Tham số thống kê khoảng cách nội chuẩn hóa 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**
$\mu_{d_{intra}}$	$4,9\times10^{-3}$	$6,2\times10^{-3}$	$5,9\times10^{-3}$	$5,3\times10^{-3}$
$\sigma_{d_{intra}}$	$1,8\times10^{-3}$	$2,5\times10^{-3}$	$2,3\times10^{-3}$	$2,2\times10^{-3}$

Bảng 3.7: Xác định mức ngưỡng xác thực

Điều kiện thực nghiệm	**Tham số**	**FPGA Spartan-6**	**FPGA Spartan-3E**	**FPGA Artix-7**
Tại nhiệt độ nhất định	$\max\left\{\mu_{d_{intra}}\right\}$	$2,3\times10^{-3}$	$8,0\times10^{-3}$	-
	$\max\left\{\sigma_{d_{intra}}\right\}$	$6,84\times10^{-4}$	$2,9\times10^{-3}$	-
	d_{thr}	$6,4\times10^{-3}$	$25,5\times10^{-3}$	-
Trên toàn dải nhiệt độ	$\max\left\{\mu_{d_{intra}}\right\}$	$6,2\times10^{-3}$	$10,0\times10^{-3}$	$0,99\times10^{-3}$
	$\max\left\{\sigma_{d_{intra}}\right\}$	$2,5\times10^{-3}$	$3,4\times10^{-3}$	$0,44\times10^{-3}$
	d_{thr}	$21,1\times10^{-3}$	$30,3\times10^{-3}$	$3,60\times10^{-3}$

3.3.3. Ước lượng tính duy nhất của ID

Tại mỗi điều kiện thực nghiệm, vector ID danh định của thiết bị được xác định từ tập mẫu dữ liệu tần số hiệu. Dữ liệu này là đáp ứng RO PUF, có đặc tính thăng giáng ngẫu nhiên do sự bất đồng nhất trong tham số mạch vật lý. Khi điều kiện thực nghiệm thay đổi, vector ID danh định của thiết bị sẽ có sự thay đổi nhỏ trong khi vẫn duy trì dạng đường gấp khúc đặc trưng cho thiết bị (Hình 3.19).

Tại điều kiện thực nghiệm xác định, 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 3.8). Trong Bảng 3.8, tại 25^{o}C, khoảng cách chuẩn hóa cực tiểu là $105,9\times10^{-3}$ (tương ứng cặp IC_1 – IC_2) lớn hơn mức ngưỡng $6,4\times10^{-3}$ (Bảng 3.7) $\sim16,5$ lần.

Để khẳng định tính duy nhất chặt của các ID danh định, tiến hành thực nghiệm trên toàn dải nhiệt độ, xác định các ID danh định và dữ liệu khoảng cách nội chuẩn hóa, khoảng cách tương quan chuẩn hóa. Bảng 3.9 trình bày khoảng cách chuẩn hóa giữa các ID danh định đối với tập 4 IC FPGA Spartan-6. Khoảng cách chuẩn hóa cực tiểu giữa các các ID danh định là $101,9\times10^{-3}$ (tương ứng cặp IC_1 – IC_2), lớn hơn các mức ngưỡng (Bảng 3.7) $\sim15,9$ và $\sim4,8$ lần tương ứng việc xác thực tiến hành tại cùng nhiệt độ và tại nhiệt độ hoạt động bất kỳ. Điều này tạo giới hạn đủ lớn cho việc phân biệt các thiết bị.

Tương tự, Bảng 3.10 trình bày khoảng cách chuẩn hóa giữa các ID của các IC FPGA Spartan-3E. Khoảng cách chuẩn hóa cực tiểu là $103,5\times10^{-3}$ giữa IC_1 và IC_4. Khoảng cách này lớn hơn các mức ngưỡng $\sim4,1$ và $\sim3,4$ lần tương ứng việc xác thực tiến hành tại cùng nhiệt độ và tại nhiệt độ hoạt động bất kỳ.

Bảng 3.11 trình bày khoảng cách chuẩn hóa giữa các ID của các IC FPGA Artix-7. Khoảng cách cực tiểu là $12,3\times10^{-3}$ giữa IC_1 và IC_2. Khoảng cách này lớn hơn các mức ngưỡng $\sim3,4$ lần (tại nhiệt độ hoạt động bất kỳ).

Bảng 3.8: 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 3.9: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$

(FPGA Spartan-6)

$\mathbf{IC_2}$	$\mathbf{IC_3}$	$\mathbf{IC_4}$	
101,9	*108,0*	*142,3*	$\mathbf{IC_1}$
	108,2	*154,7*	$\mathbf{IC_2}$
		169,2	$\mathbf{IC_3}$

Bảng 3.10: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$

(FPGA Spartan-3E)

$\mathbf{IC_2}$	$\mathbf{IC_3}$	$\mathbf{IC_4}$	$\mathbf{IC_5}$	$\mathbf{IC_6}$	
146,1	*176,5*	*103,5*	*187,2*	*162,5*	$\mathbf{IC_1}$
	203,9	*161,8*	*234,9*	*160,2*	$\mathbf{IC_2}$
		154,4	*207,0*	*209,5*	$\mathbf{IC_3}$
			161,8	*161,3*	$\mathbf{IC_4}$
				185,4	$\mathbf{IC_5}$

Bảng 3.11: Khoảng cách chuẩn hóa giữa các ID danh định $\left[\times 10^{-3}\right]$

(FPGA Artix-7)

$\mathbf{IC_2}$	$\mathbf{IC_3}$	$\mathbf{IC_4}$	$\mathbf{IC_5}$	$\mathbf{IC_6}$	$\mathbf{IC_7}$	$\mathbf{IC_8}$	
21,8	*13,3*	*17,0*	*16,2*	*22,6*	*17,5*	*16,7*	$\mathbf{IC_1}$
	20,0	*27,7*	*16,7*	*27,0*	*20,2*	*23,8*	$\mathbf{IC_2}$
		18,2	*12,3*	*20,6*	*16,5*	*16,8*	$\mathbf{IC_3}$
			19,9	*21,0*	*19,8*	*14,3*	$\mathbf{IC_4}$
				17,9	*16,2*	*15,7*	$\mathbf{IC_5}$
					21,4	*18,1*	$\mathbf{IC_6}$
						16,8	$\mathbf{IC_7}$

Như vậy, sơ đồ đề xuất thể hiện độ tin cậy và tính ổn định cao. Khi so sánh với độ tin cậy lớn nhất của các phương pháp hiện có được trình bày trên Hình 3.3, độ tin cậy đạt được của phương pháp lớn hơn vài bậc độ lớn.

3.3.4. So sánh mức tiêu thụ tài nguyên phần cứng

Mức tiêu thụ tài nguyên phần cứng khi thực thi mạch tách tần số hiệu trên các FPGA Xilinx Spartan-6, Spartan-3E, và Artix-7 (Công nghệ 45 nm, 90 nm, 28 nm tương ứng) được trình bày trong Bảng PL1.4, Bảng PL1.5 và Bảng PL1.6. Vì thiết kế đề xuất và thiết kế tham chiếu [10] được thực thi trên các nền 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 trong [10] dựa trên thiết kế cơ bản [42], thực thi trên ASIC Công nghệ CMOS 65 nm công suất thấp của TSMC[12]). Mỗi RO gồm 80 bộ đảo và một cổng NAND, tạo dao động có tần số trong khoảng $500-700$ MHz. Thiết kế gồm 4096 RO và các mạch điều khiển, giao tiếp. Các RO được phân vào 16 nhóm; mỗi nhóm gồm 256 RO, một bộ chọn kênh 256:1 để chọn dao động từ các RO đưa tới một bộ đếm. Các bit đáp ứng được tính trên cơ sở dữ liệu đếm được truyền tới máy tính từ mạch thí nghiệm. Thiết kế chiếm 0,241 mm^2 (10,7%) diện tích bán dẫn. 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 trong công trình [10].

3.4. Đánh giá hiệu quả của phương pháp

Việc định danh và xác thực ID cho thiết bị theo phương pháp đề xuất đạt được một số kết quả sau.

- RO PUF có độ đồng nhất trong cấu trúc vật lý cao.

[12] Taiwan Semiconductor Manufacturing Company – Công ty của Đài Loan, thành lập năm 1987, hoạt động trong lĩnh vực sản xuất linh kiện bán dẫn.

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

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

- Việc sử dụng khoảng cách Euclid thay cho khoảng cách Hamming trong định lượng các tham số khoảng cách mạch RO PUF giúp tận dụng toàn bộ dữ liệu tần số RO mà không phải loại bỏ các cặp RO có tần số gần nhau như trong các thiết kế truyền thống. Đồng thời, sơ đồ xác thực IC 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. Như được chỉ ra trong phần 3.1.1, đối với các phương pháp truyền thống, tính ổn định và tính duy nhất là những chỉ tiêu ràng buộc lẫn nhau bởi quan hệ giữa *FAR* và *FRR*, thể hiện bởi đặc tuyến hoạt động trên đồ thị Hình 3.3. Khi tăng tính ổn định, tính duy nhất giảm và ngược lại. Độ tin cậy xác thực được đánh giá qua *EER*. Theo [10], trị số *EER* nhỏ nhất có thể đạt được xấp xỉ 10^{-6} đối với mạch RO PUF sử dụng phương pháp ghép cặp RO liên tiếp. Với phương pháp đề xuất, bằng việc chọn mức ngưỡng xác thực dựa trên các trị số cực đại của giá trị trung bình và độ lệch chuẩn khoảng cách nội chuẩn hóa của các mẫu ID, xác suất xác thực nhầm sẽ nhỏ hơn 2×10^{-9}, giảm ít nhất 3 bậc độ lớn khi so với trị số *EER* nhỏ nhất trong [10]. Do đó, phương pháp đề xuất đã nâng cao độ tin cậy trong xác thực thiết bị.

Nghiên cứu ứng dụng này được trình bày chi tiết trong các công trình [J1, C1, P1, P2].

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. Mảng RO được thiết kế đặc biệt, sử dụng kỹ thuật *hard macro*, đảm bảo tính đồng nhất của các RO về mặt vật lý. Các tần số hiệu RO được thu nhận và xử lý cả về giá trị tuyệt đối và dấu, do vậy khai thác tốt hơn thông tin để tạo dữ liệu định danh so với các thiết kế truyền thống. Việc tính toán, xử lý số liệu sử dụng tham số khoảng cách Euclid có độ phân giải cao. Mức ngưỡng được xác định chặt chẽ từ tiêu chuẩn thống kê, đảm bảo xác thực chính xác. Các kết quả thực nghiệm khẳng định phương pháp đề xuất đạt được độ tin cậy 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 sang các nền tảng phần cứng khác.

CHƯƠNG 4: KỸ THUẬT ỔN ĐỊNH CHUỖI BIT TRÍCH XUẤT TỪ RO PUF

4.1. Khái quát về ổn định chuỗi bit ra RO PUF ứng dụng trong mã hóa bảo mật

Từ phân tích đặc trưng thống kê của tần số RO trong chương 2, có thể thấy các biến thiên cục bộ có tính đặc thù đối với thiết bị cụ thể, bền vững với sự thay đổi của điều kiện hoạt động cũng như các biến thiên toàn cục. Điều này gợi mở hướng ứng dụng RO PUF trong việc tạo chuỗi bit ổn định, phục vụ mã hóa bảo mật hay tạo các chuỗi giá trị ngẫu nhiên không thể dự đoán.

Để triển khai một thuật toán mã hóa, cần có khả năng tạo, lưu trữ và truy xuất khóa mã một cách an toàn. Yêu cầu chung đối với các khóa mã là phải đảm bảo tính ngẫu nhiên và khả năng không thể dự báo. Điều này phụ thuộc vào cơ chế tạo số ngẫu nhiên được sử dụng trong việc tạo khóa mã.

Các bộ tạo số giả ngẫu nhiên (*PRNG: Pseudo-Random Number Generator*) là các thuật toán được khởi tạo bởi một chuỗi bit (*seed*) và tạo ra chuỗi bit tương ứng có độ dài lớn hơn nhiều [94]. Các chuỗi bit ra thể hiện tính ngẫu nhiên qua số các bit trong chuỗi, sự cân bằng số bit $\{0\}$ và số bit $\{1\}$, nhưng cũng tương quan mạnh do có cùng nguyên lý hình thành. Do đó, việc tạo khóa mã dựa trên PRNG có một số hạn chế như sự phân bố không đều của số lượng lớn các mẫu, khả năng xuất hiện tính tương quan giữa các mẫu liên tiếp…, tạo ra nguy cơ suy giảm khả năng bảo mật của hệ thống mã hóa.

Các bộ tạo số ngẫu nhiên thực sự (*TRNG: True Random Number Generator*) khai thác tính ngẫu nhiên từ các quá trình vật lý vi mô như tạp

âm nhiệt tại mặt ghép bán dẫn [95], hiệu ứng quang điện [96], phân rã phóng xạ [97]… Đây là các hệ không nhớ, trong đó dữ liệu ra được xác định bởi các quá trình vật lý mà không phụ thuộc vào dữ liệu ra trước đó. Khóa mã được tạo ra bởi TRNG do vậy có tính ngẫu nhiên cao, số mẫu lớn, đáp ứng nhu cầu ứng dụng đa dạng của mã hóa bảo mật. Tuy nhiên, trở ngại trong việc tạo khóa bằng TRNG là các sơ đồ tạo khóa thường yêu cầu thủ tục xử lý bổ sung (*post-processing*) phức tạp [98-100].

Để giải quyết vấn đề này, các mô hình tạo khóa mã dựa trên PUF đã được nghiên cứu và phát triển. Mạch PUF khuếch đại các thăng giáng vi mô ở cấp vật lý xuất hiện trong quá trình chế tạo để tạo dữ liệu ra đảm bảo tính ngẫu nhiên, tính duy nhất và khả năng không thể dự báo. Do đó có thể sử dụng dữ liệu PUF để tạo khóa mã cho các tác vụ mã hóa mật. Có thể coi việc tạo khóa mã dựa trên PUF là giải pháp lai của các phương pháp tạo khóa dùng PRNG và TRNG: Dữ liệu PUF đảm bảo tính ngẫu nhiên được dùng làm chuỗi khởi tạo cho đầu vào hàm băm (*Hash function*) để tạo khóa mã có độ dài đủ lớn, đáp ứng các tác vụ mã hóa bảo mật.

Trên thế giới đã có nhiều công trình tạo lập cơ sở lý thuyết và đề xuất các sơ đồ tạo khóa mã ứng dụng PUF. Trong [16], các tác giả đề xuất mô hình gồm hai thành phần, khởi tạo và tái lập, trong đó các thủ tục mã hóa và giải mã sửa lỗi (*ECC*) duy trì sự ổn định cho dữ liệu ra mạch PUF ngay cả trong điều kiện hoạt động không ổn định. Các tác giả trong [17] tạo ra một biến thể mới của RO PUF dựa trên mã hóa Lehmer-Gray và một bộ giải mã BCH tối ưu hóa về tài nguyên tiêu thụ. Chúng được dùng như các thành phần chính của sơ đồ tạo dữ liệu bổ trợ (*helper data*) có nhiệm vụ tạo khóa mã thông qua một thủ tục được gọi là tích lũy entropy. Trong [18], các tác giả cải thiện hiệu năng của bộ tách dữ liệu mờ bằng cách thay thế đầu ra của hàm băm bởi một syndrome mã BCH. Do đó khoảng cách

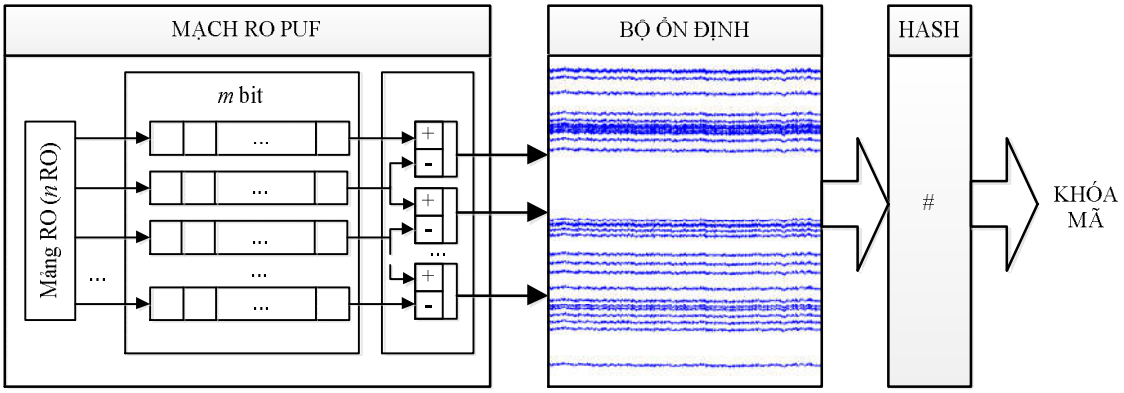
Hamming giữa các khóa mã biến thiên theo kích thước khóa mã, v.v… Hầu hết các nghiên cứu trên dựa trên sơ đồ RO PUF truyền thống, trong đó chuỗi bit ra được tạo từ hàm dấu. Cách tạo dữ liệu đáp ứng PUF này thiếu hiệu quả do hàm dấu loại bỏ nhiều thông tin quan trọng từ dữ liệu tần số RO. Ngoài ra, các sơ đồ tạo khóa mã đã đề xuất nhìn chung là phức tạp và tiêu tốn nhiều tài nguyên, gây trở ngại cho việc thực thi phần cứng.

Trong công trình [J1], các tác giả đã đề xuất sơ đồ định danh và xác thực ID ứng dụng mạch RO PUF và sử dụng tham số khoảng cách Euclid. ID tạo bởi phương pháp này có dạng vector đa chiều, khai thác sự khác biệt về độ lớn và dấu của các tần số hiệu RO gây ra bởi các nhân tố biến thiên cục bộ – Yếu tố bị bỏ qua trong các sơ đồ định danh và xác thực ứng dụng RO PUF truyền thống. Có thể sử dụng chuỗi tạo bởi việc ghép các tọa độ vector ID danh định làm chuỗi khởi tạo đầu vào hàm băm để tạo khóa mã, tuy nhiên điều này sẽ làm suy giảm tính bảo mật do các nguyên nhân sau.

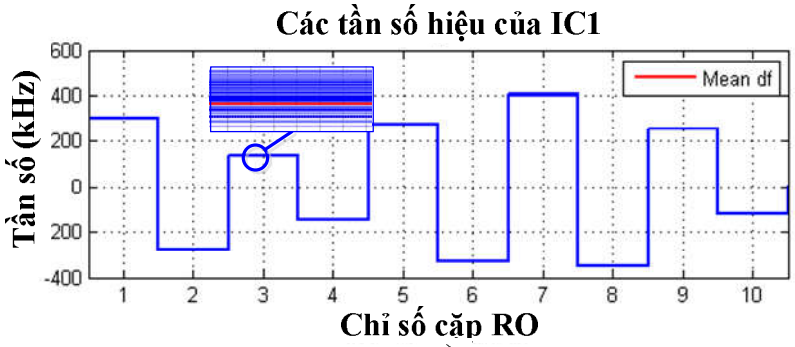
i) Vector ID được xác định bởi thiết kế đề xuất (Hình 3.15) là kết quả của việc xử lý thống kê số lượng lớn các mẫu tần số hiệu trên máy tính, yêu cầu một vùng nhớ vật lý để lưu cơ sở dữ liệu cũng như các công cụ tính toán và thuật toán nhất định. Vì vậy cần các giải pháp bảo mật chuỗi bit tạo bởi các tọa độ của vector ID danh định trước các hình thức tấn công phần cứng và phần mềm;

ii) Việc tính toán vector ID danh định và chuỗi bit đặc trưng cần một khoảng thời gian nhất định và thường lớn hơn nhiều thời gian yêu cầu đối với một số ứng dụng bảo mật.

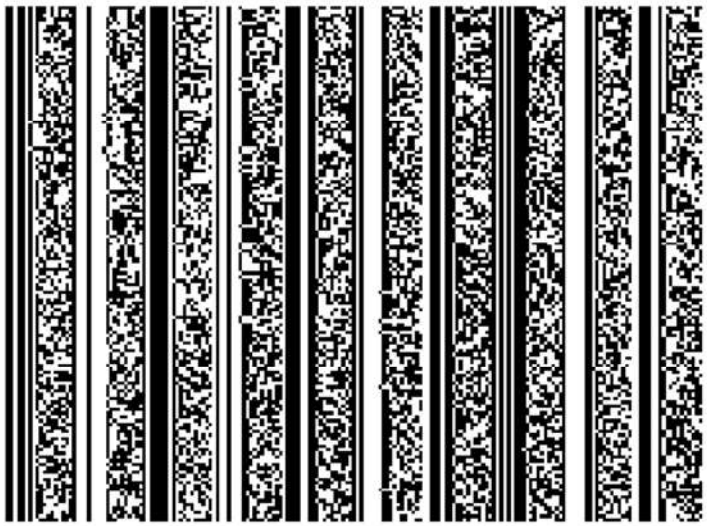
Do đó, cần tạo chuỗi bit ổn định trên chip từ các mẫu vector ID *tức thời* thu nhận được. Mô hình tổng quát quá trình tạo khóa mã ứng dụng RO PUF được trình bày trên Hình 4.1.



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



a)



b)

Hình 4.2: a) Đồ thị 140 mẫu, mỗi mẫu là kết hợp của 10 trị số *df* liên tiếp định dạng 19 bit, thu được từ thực nghiệm; b) Biểu diễn ảnh nhị phân của 140 mẫu hình a).

Các tần số RO tuyệt đối và các tần số hiệu (df) được đo, tính toán trên chip. Các chuỗi bit trong dữ liệu tần số hiệu (tọa độ của vector ID) thể hiện sự thăng giáng nhỏ qua mỗi lần kích hoạt mạch do bản chất không ổn định tuyệt đối của tần số RO. Từ đồ thị bậc thang các mẫu tần số hiệu trên Hình 4.2 có thể thấy, mặc dù các trị số mẫu xấp xỉ nhau và gần với giá trị trung bình của df, biểu diễn dạng dữ liệu nhị phân của chúng vẫn có thăng giáng lớn, đặc biệt tại các bit trọng số nhỏ. Do đó, cần một bộ ổn định (*Stabilizer*) để tạo chuỗi bit ra ổn định và duy nhất. Chuỗi bit này được đưa tới đầu vào hàm băm để tạo 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 RO PUF

Mô hình thực nghiệm: Dữ liệu vào được thu từ các phép đo trên 5 IC FPGA Artix-7 XC7A35T tại nhiệt độ phòng (25^oC). Thiết kế đối xứng và đồng nhất về vật lý với các RO được bố trí song song trên cùng vùng tần số xung nhịp hệ thống (*clock*). Dữ liệu ra đối với mỗi kênh RO là trị số đếm các dao động RO trong một khoảng thời gian. Sai số tuyệt đối cực đại của phép đo tỷ lệ nghịch với khoảng thời gian đo (Phụ lục 2). Trong thực nghiệm cụ thể này, sai số tuyệt đối đo tần số RO là 50 Hz tương ứng khoảng thời gian đo 20 ms. Sai số tương đối và độ chính xác của phép đo tương ứng là $0,002\%$ và $99,998\%$. Do các phép đo có độ chính xác cao, trong phần tiếp theo, nghiên cứu sinh sử dụng trị số đếm như giá trị tần số tuyệt đối của RO để thuận tiện cho việc trình bày.

4.2.1. Phương pháp trung bình mẫu

Các trị số df có tính ngẫu nhiên cao, biểu diễn nhị phân thường xuất hiện đột biến (*outlier*) tại các điểm chuyển trọng số (Ví dụ: $\{0111\}$,

$\{1000\}$), hạn chế hiệu quả của các thuật toán ổn định. Do đó, trong một số trường hợp (như điều kiện hoạt động không ổn định) có thể sử dụng trị số df trung bình thay cho các trị số mẫu df như một giải pháp kỹ thuật bổ trợ. Trị số df trung bình được tách ra từ số lượng lớn các mẫu df theo kỹ thuật trình bày dưới đây.

Giả sử tần số hiệu danh định của *cặp* RO_j (gồm RO_j và RO_{j+1}) là df_{j0}, $j = \overline{1, n_{ring} - 1}$, với n_{ring} là số RO trong mảng RO. Mẫu tần số hiệu thứ i của RO_j là:

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

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

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

Với n_{sample} là số mẫu tần số hiệu RO.

Giá trị 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.

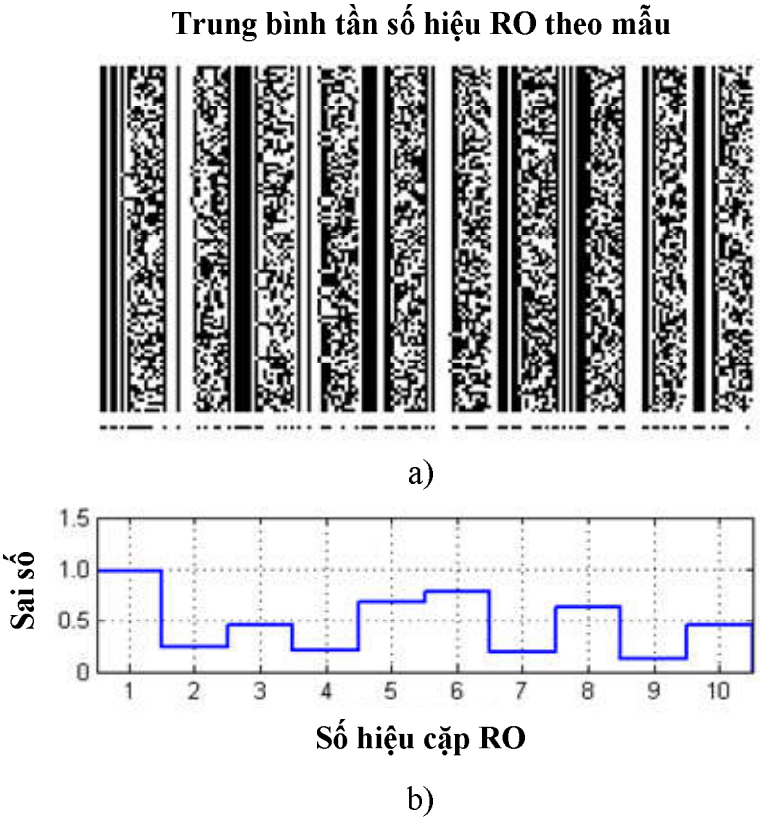
Để tránh hiện tượng tràn dữ liệu, thuật toán lấy trung bình mẫu tần số hiệu được trình bày trên Bảng 4.1. Số mẫu cần được chọn là lũy thừa của 2 để có thể thực hiện phép chia bằng cách dịch bit, giảm tiêu thụ tài nguyên phần cứng.

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

Kết quả mô phỏng với dữ liệu vào thu nhận từ thực nghiệm được trình bày trên Hình 4.3(a), trong đó dòng cuối của ảnh nhị phân là trị số df trung bình. Đồ thị Hình 4.3(b) biểu diễn sai số giữa các trị số df trung bình số học và các trị số df trung bình tách ra bởi thuật toán Bảng 4.1. Sai số này có giá trị tuyệt đối nhỏ hơn 1, khẳng định độ chính xác của kỹ thuật lấy trung bình.

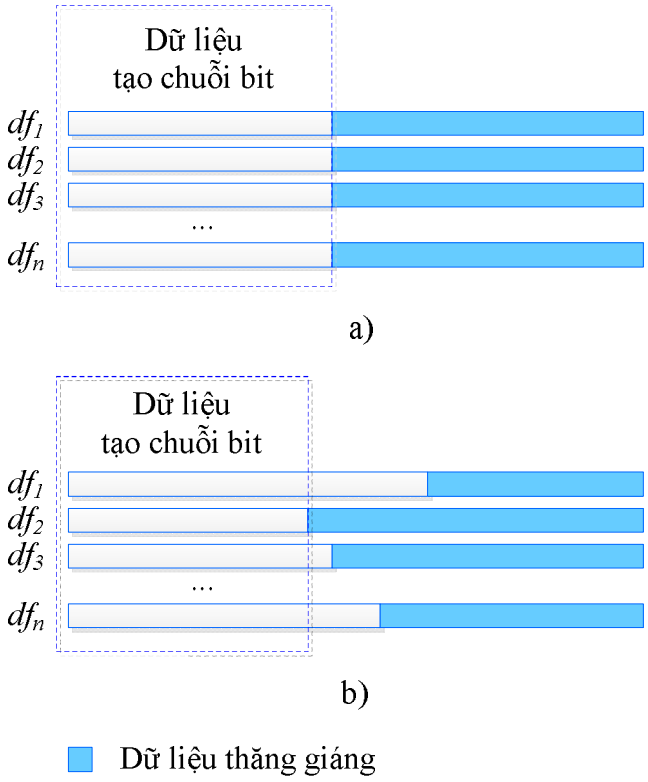
Kỹ thuật tính df trung bình yêu cầu nhiều tài nguyên phần cứng để thực thi các khối xử lý dữ liệu theo thuật toán trong Bảng 4.1. Ngoài ra, kỹ thuật này cũng yêu cầu một khoảng thời gian nhất định để tích lũy và xử lý dữ liệu, tạo điều kiện cho các nhân tố bên ngoài tác động lên hệ thống.



Hình 4.3: Ảnh nhị phân mô tả các mẫu df , df trung bình (a) và sai số tương ứng giữa trị số df_{mean} số học và df_{mean} tạo bởi thuật toán (b)

4.2.2. 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. Ở bước tiếp cận ban đầu, tiến hành xác định độ dài dữ liệu thăng giáng N_{EX} xét ở trường hợp xấu nhất và cắt đi đoạn dữ liệu có độ dài tương ứng giá trị cực đại của N_{EX} về phía các bit có trọng số nhỏ. Chuỗi bit được tạo thành bằng cách kết hợp các phần còn lại trong dữ liệu các df (Hình 4.4).



Hình 4.4: Minh họa phương pháp tạo chuỗi bit ổn định từ các phần không đổi của các df .

Thực nghiệm cho thấy, độ lệch chuẩn cực đại và cực tiểu đối với IC tương ứng là $1,37\times10^3$ và $0,15\times10^3$. Khi đó, phần không ổn định trong dữ liệu các df biến thiên trong khoảng 9 đến 13 bit. Giá trị này về lý thuyết có thể được ước lượng từ dữ liệu thống kê (Hình 4.5).

Để giữ lại phần không đổi trong chuỗi bit dữ liệu các df , N_{EX} được xác định từ điều kiện sau:

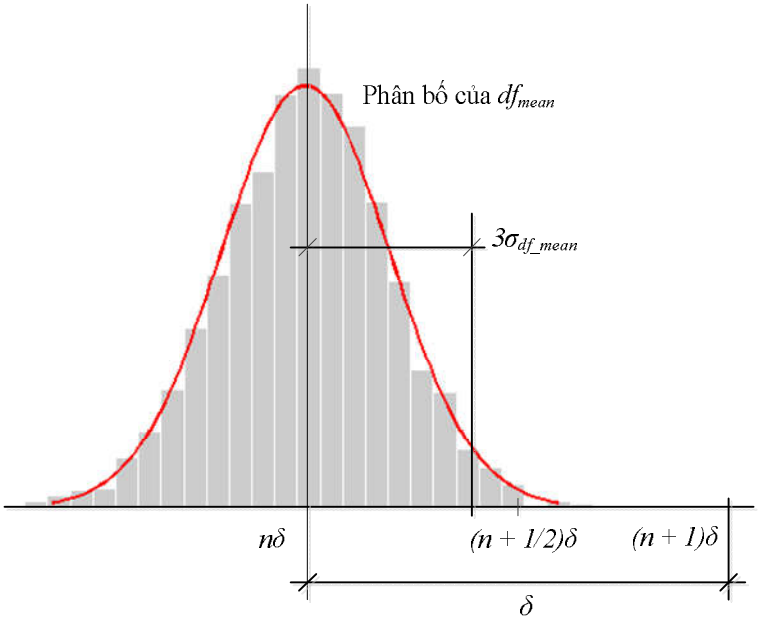
$$3\sigma_{df_{mean},\max} < \frac{\delta}{2} \tag{4.3}$$

Trong đó, $\sigma_{df_{mean},\max}$ là độ lệch chuẩn cực đại của trị số df trung bình. Từ thực nghiệm, ta có: $\sigma_{df_{mean},\max} = 1,37\times10^3$; δ là bước lượng tử tuyến tính của phép chuyển đổi tương tự – số khi coi các giá trị tuyệt đối của df

trước khi cắt là dữ liệu tương tự, chuỗi bit được giữ lại là dữ liệu số. Từ phương trình (4.1), ta có:

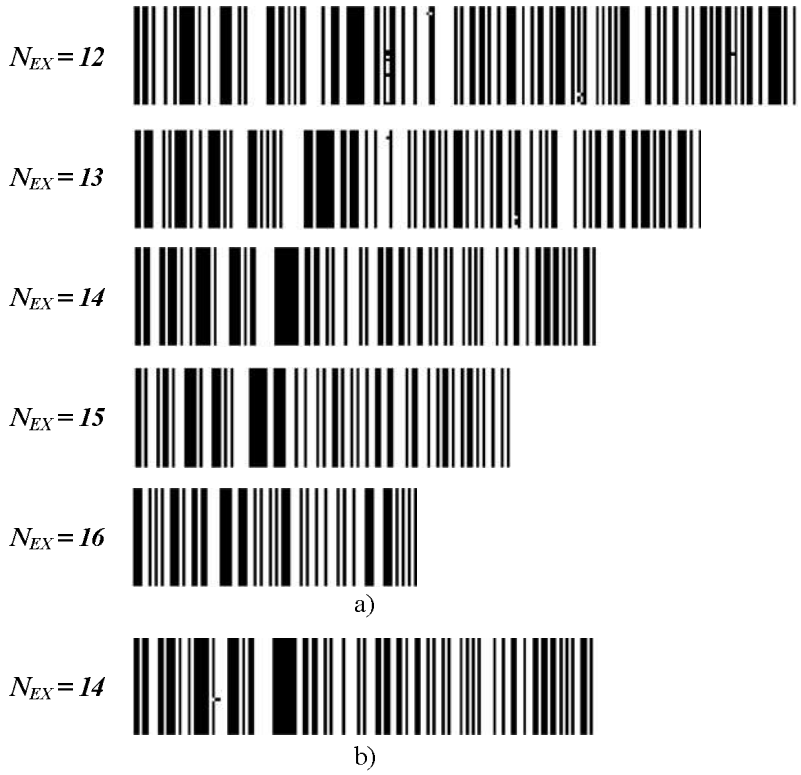
$$\delta > 6\sigma_{df_{mean},\max} \tag{4.4}$$

Cận dưới của giá trị N_{EX} được chọn bằng $\left\lceil \log_2\left(6\sigma_{df_{mean},\max}\right)\right\rceil = 13[bit]$.



Hình 4.5: Xác định số bit loại bỏ; n là trị số thập phân tương đương của df_{mean}

Mô phỏng MATLAB về tính ổn định của chuỗi bit với các giá trị khác nhau của N_{EX} dựa trên dữ liệu df thu được từ thực nghiệm được trình bày trên Hình 4.6(a), trong đó mỗi ảnh nhị phân tương ứng một giá trị của N_{EX} gồm 32 chu kỳ dữ liệu df, mỗi chu kỳ dữ liệu df tương ứng một hàng. Dữ liệu thu được khi thực thi thiết kế trên FPGA Artix-7 được trình bày trên Hình 4.6(b). Có thể thấy tại một trong 32 hàng xuất hiện hiện tượng đảo bit. Điều này có thể lý giải bởi: i) Sự xuất hiện của mẫu dữ liệu đột biến; ii) Trạng thái đảo bit của dữ liệu nhị phân tại biên biểu diễn dữ liệu df.



Hình 4.6: Ảnh nhị phân minh họa sự phụ thuộc của tính ổn định chuỗi bit ra vào số bit loại bỏ (a) và kiểm nghiệm độ ổn định với $N_{EX} = 14$ (b).

Có thể thấy, tính ổn định của chuỗi bit tăng lên khi tăng số bit loại bỏ, nghĩa là giảm độ rộng dữ liệu df còn lại và do đó làm giảm độ dài dữ liệu của chuỗi bit ra. Phương pháp này đơn giản và hiệu quả về thực thi phần cứng, nhưng có một số nhược điểm:

i) Từ phương diện khai thác thông tin, phương pháp không hiệu quả do trong thực tế, mức độ thăng giáng trong trị số của các df không đồng nhất. Đối với các cặp RO có trị số df ổn định cao, nghĩa là có thăng giáng nhỏ trong các chuỗi bit, số bit cắt bỏ có thể nhiều hơn độ rộng phần dữ liệu biến thiên. Ngược lại, với các trị số df ít ổn định, số bit cắt bỏ ước lượng có thể là không đủ, đặc biệt khi có sự xuất hiện của các điểm đột biến trong dữ liệu df làm tăng tính bất ổn định trong chuỗi bit.

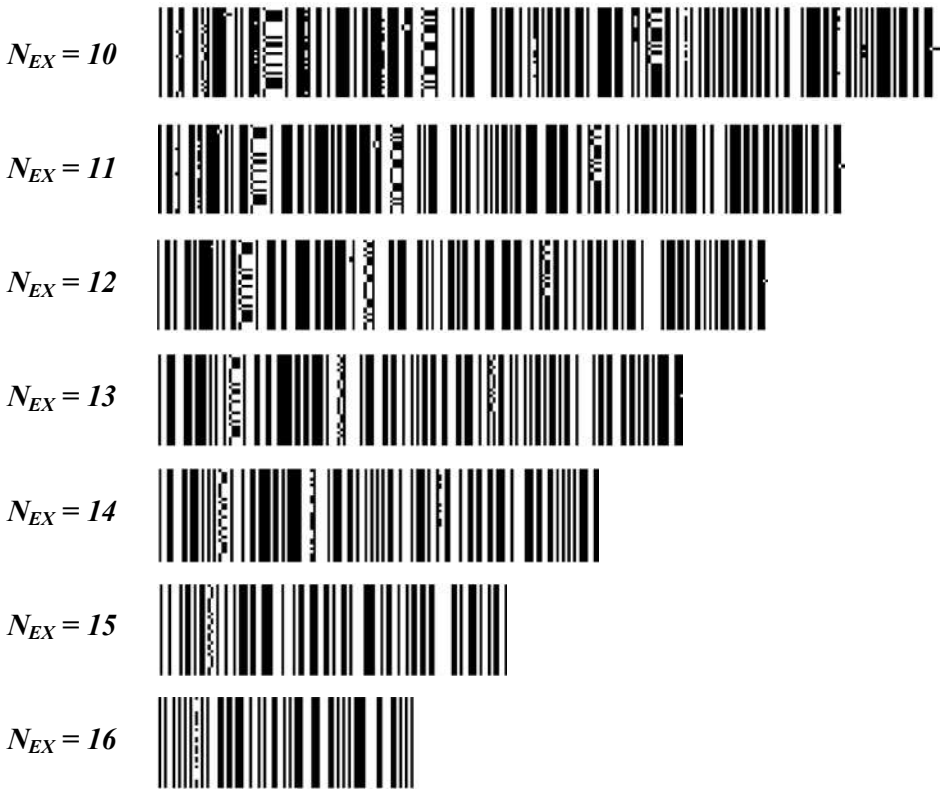
ii) Việc giới hạn các giá trị của df vào một tập các trị số lượng tử sẽ làm thay đổi các vector ID của cấu kiện, do đó làm thay đổi các tham số PUF quan trọng như khoảng cách nội và khoảng cách tương quan. Điều này ảnh hưởng đến khả năng phân biệt giữa các thiết bị. Bảng 4.2 mô phỏng hiện tượng này đối với 5 IC tại các giá trị khác nhau của số bit loại bỏ.

Bảng 4.2: Khoảng cách chuẩn hóa $\left[\times 10^{-3}\right]$ giữa các ID danh định của các thiết bị với các giá trị khác nhau của N_{EX}

	$N_{EX}=13$				$N_{EX}=14$			
	IC_2	**IC_3**	**IC_4**	**IC_5**	**IC_2**	**IC_3**	**IC_4**	**IC_5**
IC_1	*16,8*	*21,7*	*23,3*	*0,022,8*	*18,6*	*22,5*	*23,8*	*24,5*
IC_2		*23,1*	*25,9*	*21,7*		*25,7*	*28,1*	*21,0*
IC_3			*28,5*	*19,4*			*28,6*	*23,1*
IC_4				*23,3*				*25,7*
	$N_{EX}=15$				$N_{EX}=16$			
	IC_2	**IC_3**	**IC_4**	**IC_5**	**IC_2**	**IC_3**	**IC_4**	**IC_5**
IC_1	*27,5*	*33,7*	*27,5*	*27,5*	*31,8*	*22,5*	*38,9*	*22,5*
IC_2		*37,2*	*31,8*	*27,5*		*38,9*	*38,9*	*22,5*
IC_3			*33,7*	*29,7*			*44,9*	*31,8*
IC_4				*27,5*				*31,8*
	$N_{EX}=17$				$N_{EX}=18$			
	IC_2	**IC_3**	**IC_4**	**IC_5**	**IC_2**	**IC_3**	**IC_4**	**IC_5**
IC_1	*0*	*0*	*63,5*	*0*	*89,8*	*0*	*0*	*0*
IC_2		*44,9*	*77,8*	*44,9*		*89,8*	*89,8*	*89,8*
IC_3			*63,5*	*0*			*0*	*0*
IC_4				*63,5*				*0*

Từ Bảng 4.2 có thể thấy, khoảng cách Euclid cực tiểu giữa các ID danh định của IC đã giảm tới 0 khi tăng N_{EX} đến giá trị tới hạn $N_{EX} = 17$, nghĩa là các chuỗi bit tách ra không thể phân biệt lẫn nhau. Do đó giá trị N_{EX} có biên trên là $N_{EX} = 16$. Với $13 \le N_{EX} \le 16$, trị số cực tiểu của khoảng cách tương quan lớn hơn mức ngưỡng $d_{thr} = 1,4 \times 10^{-3}$ (được chọn bằng tổng của giá trị trung bình cực đại và sáu lần độ lệch chuẩn cực đại trong phân bố khoảng cách nội chuẩn hóa của các IC), đảm bảo xác thực chính xác thiết bị.

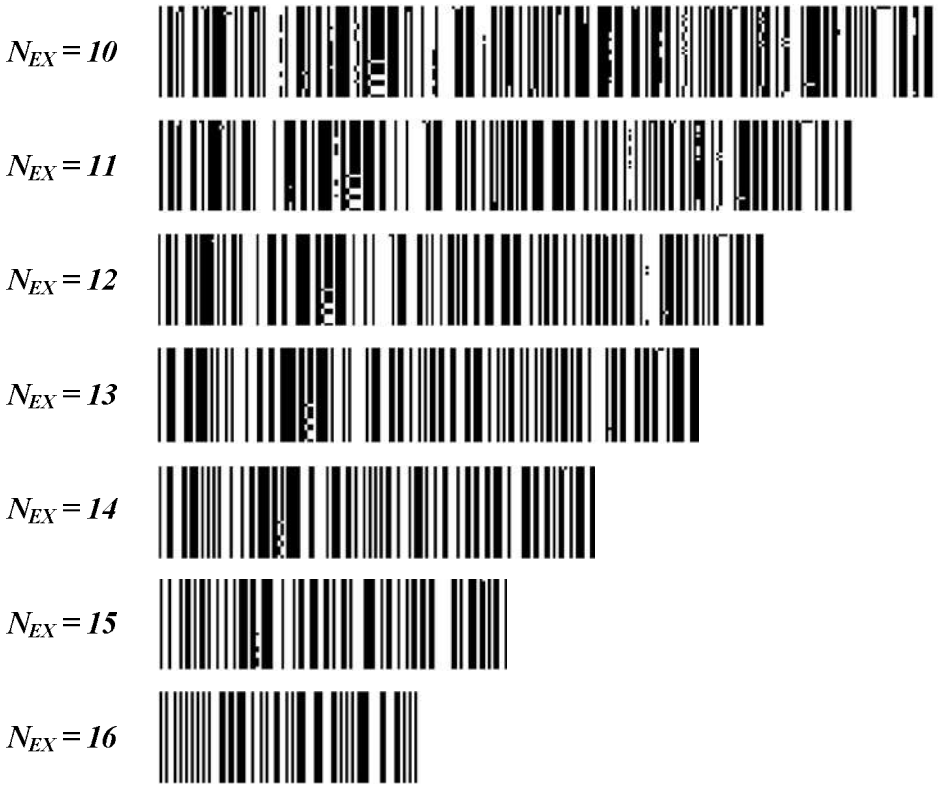
Giá trị của N_{EX} ảnh hưởng đến độ dài chuỗi bit ra. Khi chọn N_{EX} càng lớn, chuỗi bit ra thu được càng ngắn và ngược lại. Hình 4.7 trình bày mô phỏng thuật toán với các giá trị khác nhau của N_{EX}.



Hình 4.7: Ảnh nhị phân mô tả sự phụ thuộc của tính ổn định chuỗi bit ra vào N_{EX}

*** Ổn định chuỗi bit ra bằng phương pháp cắt bit kết hợp kỹ thuật trung bình mẫu**

Trong thực tế, hiệu quả của phương pháp cắt bit không cao do sự xuất hiện các mẫu dữ liệu df đột biến. Để đồng thời duy trì tính ổn định của chuỗi bit ra mà không tăng N_{EX} lên quá lớn, đảm bảo chuỗi bit ra có độ dài đủ lớn, có thể kết hợp phương pháp cắt bit với việc lấy trung bình mẫu df. Đặt tầng lấy trung bình mẫu df vào trước thuật toán Bảng 4.1, dữ liệu vào của thuật toán là trị số df trung bình thay cho giá trị tuyệt đối của df. Mô phỏng phương pháp được trình bày trên Hình 4.8. So sánh với kết quả Hình 4.7, có thể thấy chuỗi bit ra ổn định hơn nhiều.



Hình 4.8: Ảnh nhị phân mô tả việc tạo chuỗi bit ra bằng cách kết hợp phương pháp cắt bit và kỹ thuật trung bình mẫu df

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

Từ biểu diễn dữ liệu df trên Hình 4.2 có thể thấy, các giá trị mẫu df khác biệt nhau một số bit trọng số nhỏ, do đó 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 4.3.

Bảng 4.3: 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 $mask\_temp1_j$[13]
6	Đảo bit $mask\_temp1_j$ để nhận được mặt nạ cần tạo ($mask$)

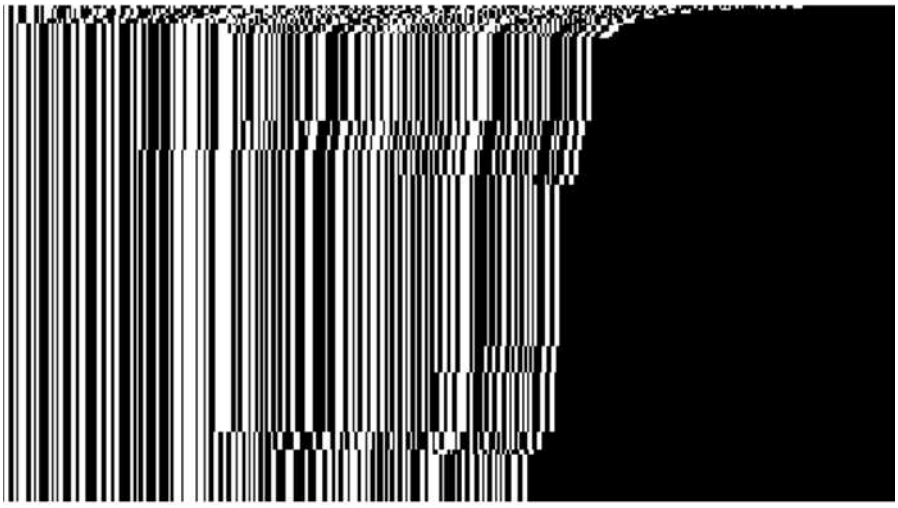
[13] Các trị số trung gian trong khoảng dữ liệu biến thiên sẽ bị loại bỏ.

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:

$$key0_{ij,k} = \begin{cases} df_{j0,k} & : mask_{ij,k} = 1 \\ 0 & : mask_{ij,k} = 0 \end{cases} \quad (4.5)$$

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.

a) $n_{sample} = 32$



b) $n_{sample} = 200$

Hình 4.9: Ảnh nhị phân mô tả sự hội tụ của các mẫu chuỗi bit về chuỗi bit ổn định sử dụng phương pháp mặt nạ dữ liệu với số mẫu df khác nhau.

Kết quả mô phỏng thuật toán được trình bày trên Hình 4.9. Trong đó, mỗi chu kỳ cập nhật mặt nạ và tạo chuỗi bit tương ứng với một hàng. Sau một số chu kỳ, chuỗi bit tạo bởi việc kết hợp các phần ổn định tạm thời của

các df sẽ hội tụ về một chuỗi bit duy nhất, được gọi là chuỗi sơ bộ (Dòng cuối trong ảnh nhị phân). Chuỗi sơ bộ chứa chuỗi bit $\{0\}$ phía phải cùng tạo ra từ quá trình tạo mặt nạ, do đó cần gắn chuỗi sơ bộ với dữ liệu chỉ ra số bit có nghĩa nhằm tách ra chuỗi bit ổn định.

Từ quá trình trích xuất chuỗi bit ổn định được trình bày trên Hình 4.9, có thể rút ra một số nhận xét:

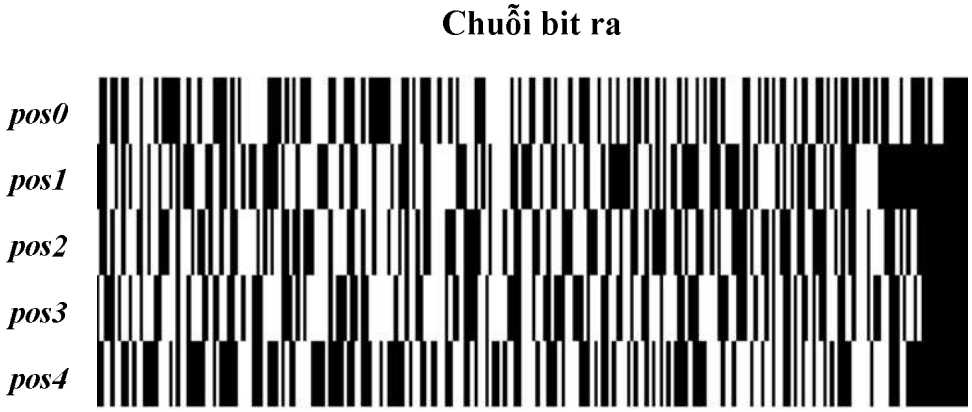
i) Thuật toán tạo mặt nạ thích ứng với sự khác biệt về số bit thăng giáng của các df, do đó khai thác được nhiều thông tin hơn so với phương pháp cắt bit với các cặp RO được giả định là có số bit thăng giáng bằng nhau.

ii) Sơ đồ tạo chuỗi bit ổn định và duy nhất bằng phương pháp mặt nạ dữ liệu khá nhạy đối với dữ liệu đột biến. Bất kỳ sự khác biệt nào trong dữ liệu df gây ra sự biến đổi giá trị chỉ một bit cũng có thể ảnh hưởng đến chuỗi bit mẫu khóa mã cuối cùng. Có thể được khắc phục nhược điểm này bằng việc kết hợp thuật toán tạo mặt nạ dữ liệu với kỹ thuật lấy trung bình mẫu và phương pháp cắt bit.

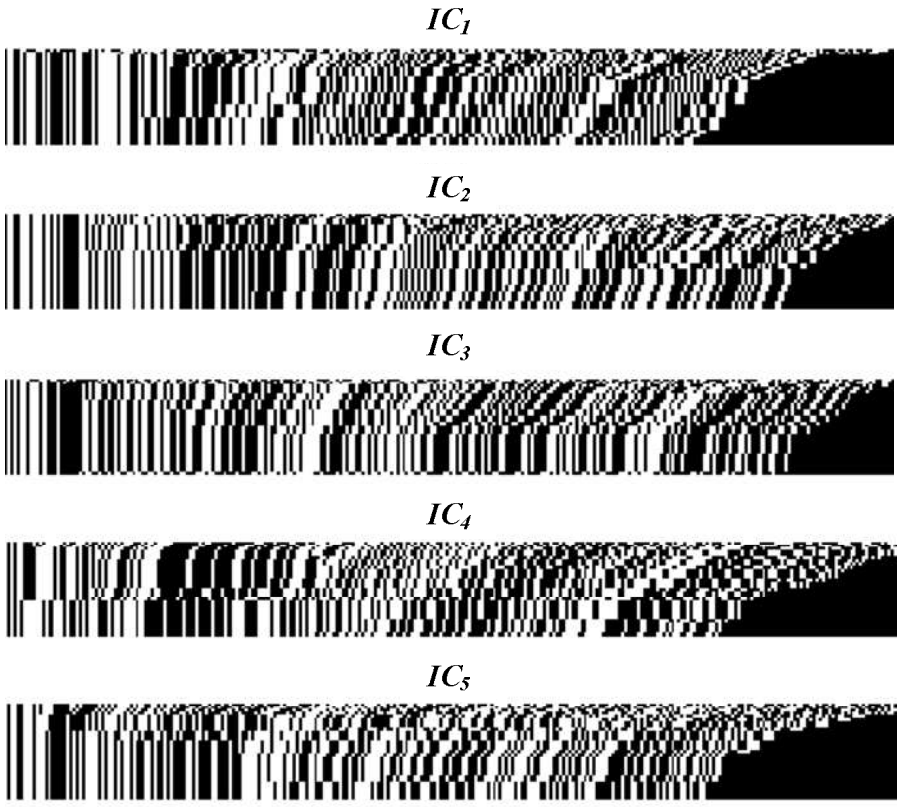
Tính ổn định của phương pháp mặt nạ dữ liệu được kiểm định bằng cách thực thi thiết kế tại 5 vị trí khác nhau trên chip (*pos0*,…, *pos4*). Kết quả mô phỏng phương pháp tạo chuỗi bit ra ổn định bằng thuật toán mặt nạ dữ liệu dựa trên dữ liệu df thực nghiệm được trình bày trên Hình 4.10. Trong đó, ảnh nhị phân tại mỗi vị trí tương ứng chuỗi bit ra đối với 18 chu kỳ tạo mặt nạ dữ liệu cuối.

Từ Hình 4.10 có thể thấy, các chuỗi bit tạo nên từ các vị trí khác nhau là không đồng nhất. Điều này có nghĩa là khi thực thi thiết kế trên các chip FPGA, chuỗi bit ra là duy nhất đối với mỗi vị trí thực thi cũng như đối với mỗi IC. Thuật toán kết hợp kỹ thuật lấy trung bình vào thuật toán trong

Bảng 4.3 nhằm ổn định dữ liệu vào được trình bày trong Bảng 4.4. Chuỗi bit được tạo ra từ thuật toán này sẽ ổn định hơn nhiều, như kết quả mô phỏng trên Hình 4.11.



Hình 4.10: Mô phỏng các chuỗi bit ra đối với các vị trí khác nhau khi áp dụng thuật toán mặt nạ dữ liệu lên dữ liệu *df* thực nghiệm.



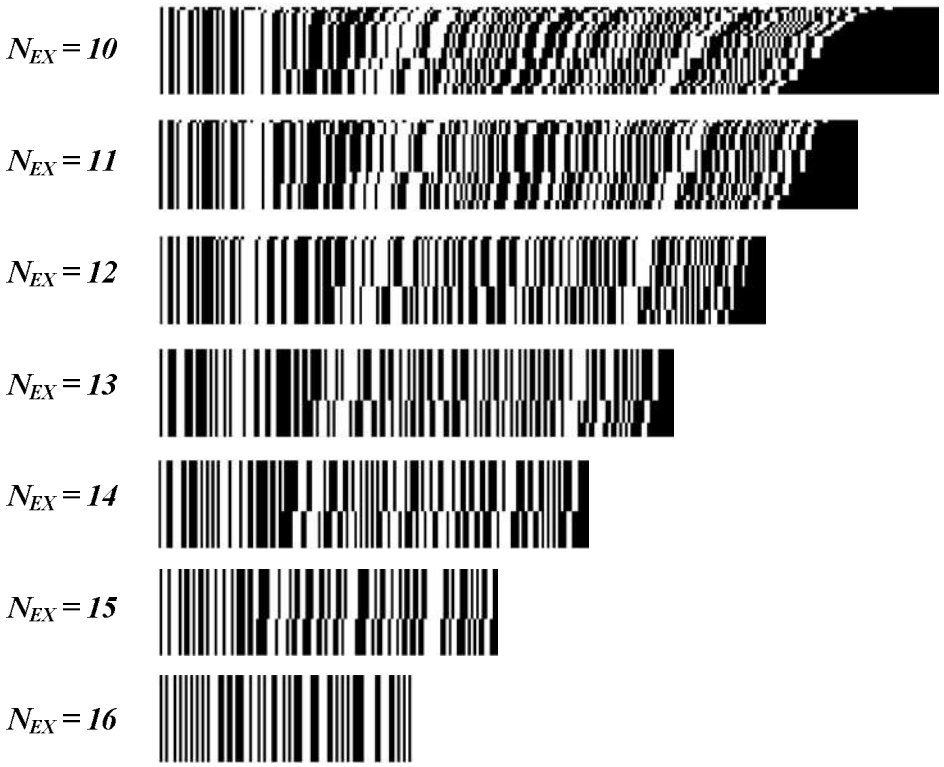
Hình 4.11: Kết quả mô phỏng tạo chuỗi bit ổn định bằng thuật toán tạo mặt nạ dữ liệu kết hợp kỹ thuật lấy trung bình mẫu.

Bảng 4.4: Thuật toán kết hợp kỹ thuật lấy trung bình mẫu và tạo mặt nạ thích nghi

Bước	**Tác vụ**
1	Khởi tạo mảng RO.
2	Thu nhận dữ liệu df : $(df)_{n_{key\_sample}\times(n_{ring}-1)\times n_{sample}}$
3	Tính df_{mean} đối với tất cả các cặp RO và với mọi mẫu khóa mã.
4	Với mỗi RO_j, đặt mẫu $df_{1,mean,j}$ đầu tiên (tương ứng với mẫu khóa mã đầu tiên) làm giá trị tham chiếu (dạng chuỗi bit): $df_{mean\_0,j} = df_{1,mean,j}$
5	Đối với mỗi mẫu $df_{k,mean,j}$, $k = \overline{1, n_{key\_sample}}$ tính: $df_{k,mean_{xor},j} = df_{k,mean,j} \oplus df_{mean\_0,j}$
6	Tính các mặt nạ trung gian: $mask\_temp_j = \bigcup_{i=1}^{n} df_{k,mean_{xor},j}$ Lọc bỏ tất cả các bit {0} trong khoảng giới hạn bởi các bit {1} của $mask\_temp_j$ để nhận được $mask\_temp1_j$
7	Đảo bit $mask\_temp1_j$ để nhận được mặt nạ thành phần tương ứng với RO_j cần tạo ($mask$)

Để tiếp tục nâng cao hiệu quả của thuật toán tạo mặt nạ dữ liệu thích nghi, tiến hành tích hợp vào thuật toán kỹ thuật lấy trung bình mẫu và phương pháp cắt bit. Thuật toán kết hợp này như sau: Sau bước 3 của thuật

toán trong Bảng 4.4 bổ sung bước 3a: Cắt N_{EX} bit phải cùng của chuỗi bit dữ liệu df_{mean}. Các bước tiếp theo như trình bày trong Bảng 4.4. Kết quả mô phỏng phương án kết hợp này được trình bày trên Hình 4.12, theo đó có thể thấy quá trình hội tụ về chuỗi bit duy nhất nhanh hơn và ổn định hơn. Tuy nhiên, phương pháp này cũng làm cho thiết kế trở nên phức tạp hơn và tiêu thụ tài nguyên phần cứng nhiều hơn.



Hình 4.12: Mô phỏng quá trình tạo chuỗi bit ra ổn định bằng cách kết hợp thuật toán mặt nạ dữ liệu, kỹ thuật lấy trung bình mẫu và cắt bit.

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

Hiện tượng đột biến trong dữ liệu nhị phân của df thường xảy ra tại các biên của trị số thập phân tương đương bằng lũy thừa 2, đặc biệt khi số bit dữ liệu df cần cắt bỏ (tương ứng đoạn dữ liệu thăng giáng) không đủ lớn. Giải pháp đề xuất nhằm khắc phục hiện tượng này là trích xuất phần

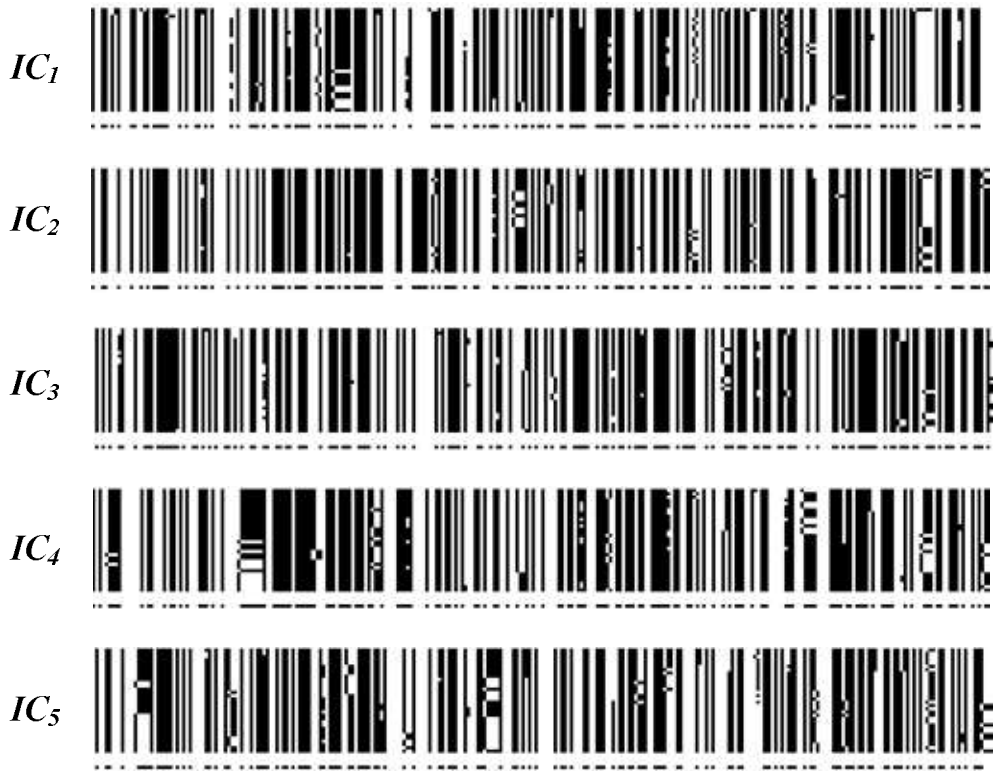
dữ liệu lặp lại nhiều nhất từ phân bố thống kê các mẫu dữ liệu df sau cắt bit. Phương pháp này không phù hợp để áp dụng với các mẫu dữ liệu tương ứng trị số tuyệt đối của df vì chúng là các giá trị rời rạc và thường là khác nhau. Thay vào đó, phương pháp áp dụng đối với các trị số tương đối ổn định của df sau cắt bit. N_{EX} được xác định từ thực nghiệm là dữ liệu bổ trợ quan trọng, đặc biệt đối với các df có mức thăng giáng thấp. Các trị số này được phân phối vào tập hữu hạn các mẫu trị số ổn định tạm thời. Mẫu lặp lại nhiều nhất sẽ được xác định bằng cách phân tích tần suất của các phần tử. Thuật toán của phương pháp được trình bày trong Bảng 4.5.

Bảng 4.5: 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

Các mẫu *df* tương ứng các RO xác định được sẽ được kết hợp để tạo chuỗi bit duy nhất và ổn định. Kết quả mô phỏng thuật toán với dữ liệu thực nghiệm của 5 IC được trình bày trên Hình 4.13, với hàng cuối tương ứng chuỗi bit ra sau 32 chu kỳ mẫu *df* . Có thể thấy dữ liệu hội tụ về trị số xuất hiện thường xuyên nhất.



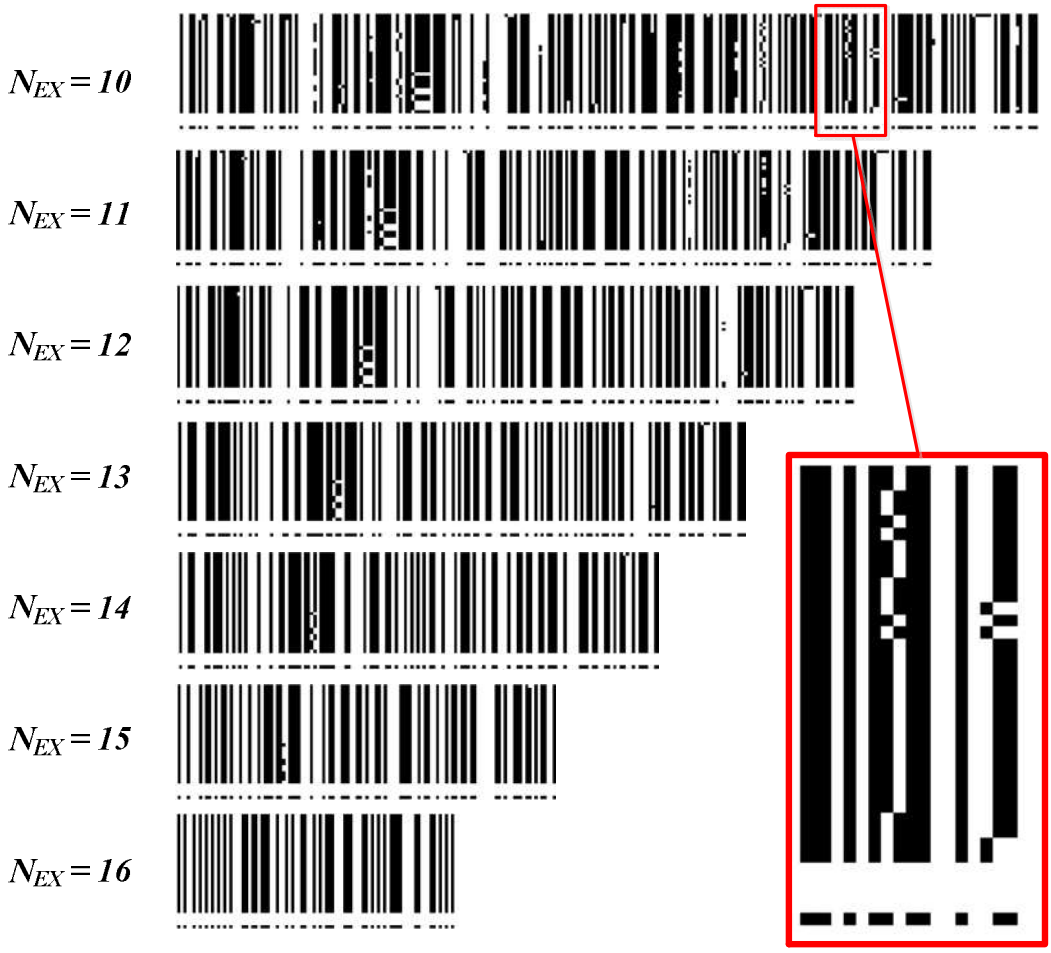
Hình 4.13: Tách chuỗi bit bằng cách kết hợp dữ liệu tương ứng các trị số trung bình của *df* phổ biến nhất

Phương pháp này có một số đặc điểm sau:

i) Số các phần tử dữ liệu (*bin*) trong giản đồ phân bố sẽ tăng khi số bit không ổn định (giả thiết) giảm và ngược lại. Điều này dẫn đến cần phải có số mẫu *df* lớn để xác định chính xác trị số phổ biến nhất.

ii) Khi giới hạn số phần tử dữ liệu để đạt được phân bố tần suất chính xác hơn, thông tin có thể bị mất, làm giảm hiệu quả của phương pháp. Do đó,

số bit không ổn định giả thiết được xác định từ điều kiện cân đối các yêu cầu: 1) Độ bảo mật của chuỗi bit ra, thể hiện ở độ dài chuỗi bit đủ lớn, đặc trưng cho thiết bị; 2) Thời gian tạo chuỗi bit, mức tiêu thụ tài nguyên phần cứng và độ phức tạp trong thực thi phần cứng. Hình 4.14 trình bày kết quả mô phỏng thuật toán với các giá trị khác nhau của N_{EX}.



Hình 4.14: Mô phỏng thuật toán cực đại tần suất với các giá trị khác nhau của N_{EX}

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. Mạch vật lý của các thiết kế được trình bày trên Hình PL1.9 và Hình PL1.10, mức tiêu thụ phần cứng được trình bày trong Bảng PL1.7 và Bảng PL1.8. Nghiên cứu ứng dụng này được trình bày chi tiết trong các công trình [J2, C2, C3].

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, chương 4 đề xuất 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

PUF là hướng nghiên cứu mới trong lĩnh vực bảo mật phần cứng, khuếch đại sự bất đồng nhất/thăng giáng của các tham số thiết bị ở thang vi mô nhằm tách ra dữ liệu đặc trưng cho thiết bị. Dữ liệu này có tính ngẫu nhiên, không thể dự đoán, có các tham số thống kê ổn định và duy nhất, do đó phù hợp với các ứng dụng bảo mật phần cứng. Luận án trình bày kết quả nghiên cứu thiết kế RO PUF trên FPGA, ứng dụng trong tách và xác thực ID cho thiết bị, ổn định dữ liệu đáp ứng mạch RO PUF. Các thực nghiệm được tiến hành trong điều kiện phòng thí nghiệm, đáp ứng tốt các yêu cầu đề ra đối với mỗi ứng dụng.

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, luận án chỉ ra rằng, 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 thông tin định danh (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, so với các kết quả nghiên cứu đã có, 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. Thực nghiệm cho thấy 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. Các chuỗi bit này có thể được sử dụng làm chuỗi khởi tạo trong các ứng dụng mã hóa mật như tạo số ngẫu nhiên, tạo khóa mã…

II. Hướng phát triển tiếp theo

Cùng với những kết quả đạt được, luận án còn tồn tại một số hạn chế như số IC dùng trong khảo sát còn nhỏ, khoảng nhiệt độ môi trường khảo sát còn hẹp, hiệu suất truyền dữ liệu thấp, thời gian thu dữ liệu đáp ứng RO PUF lớn. Trong các nghiên cứu tiếp theo về RO PUF, nghiên cứu sinh dự kiến sẽ khắc phục những hạn chế và đề xuất một số nội dung phát triển nghiên cứu mới như sau:

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 vi mạch khả trình FPGA.

- Nghiên cứu khả năng thay thế khoảng cách Euclid bằng bình phương khoảng cách Euclid nhằm giảm độ phức tạp tính toán.
- Thực thi thiết kế tại các vị trí khác nhau trên chip, mở rộng khoảng nhiệt độ khảo sát.
- Nghiên cứu các giải pháp chống tấn công phần cứng đối với thiết kế.

- Nghiên cứu khả năng áp dụng các tiêu chuẩn kiểm tra ngẫu nhiên đối với chuỗi bit ổn định tạo ra bởi các kỹ thuật trình bày trong chương 4.

- Ứng dụng giao thức truyền số liệu tốc độ cao thay cho giao thức UART nhằm tăng hiệu suất thu dữ liệu đáp ứng RO PUF.

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 vi mạch chuyên dụng (ASIC) nhằm nâng cao hơn nữa hiệu năng RO PUF, khắc phục hạn chế của công nghệ FPGA trong tạo cấu hình đồng nhất về độ trễ đường truyền tín hiệu.

4. Thực thi các hình thức tấn công khác nhau 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.

DANH MỤC CÔNG TRÌNH ĐÃ CÔNG BỐ

*** Bài báo khoa học**

J1. Tran, V. T., Trinh, Q. K., & Hoang, V. P. (2022). A robust Euclidean metric based ID extraction method using RO-PUFs in FPGA. *Integration*, *82*, 37-47 (*Thuộc danh mục SCIE, Q3, CiteScore: 3.1, Impact Factor: 1.345*). ISSN: 0167-9260.

J2. Hoang, V. P., Tran, V. T., & Trinh, Q. K. (2022). Stabilizing Techniques for Secure On-chip Key Generation Based on RO-PUF. *VNU Journal of Science: Computer Science and Communication Engineering*. ISSN: 2588-1086.

C1. V. -T. Tran, Q. -K. Trinh and V. -P. Hoang, "Enhanced ID Authentication Scheme Using FPGA-Based Ring Oscillator PUF," *2019 IEEE 13th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoC)*, 2019, pp. 320-327, doi: 10.1109/MCSoC.2019.00052. ISBN-13: 978-1-7281-4882-3.

C2. V. -T. Tran, Q. -K. Trinh and V. -P. Hoang, "Stabilizing On-chip Secure Key Generation Using RO-PUF," *2021 International Conference on Information and Communication Technology Convergence (ICTC)*, 2021, pp. 805-809, doi: 10.1109/ICTC52510.2021.9621147. ISSN: 2162-1233.

C3. V. -T. Tran, Q. -K. Trinh, T. -H. Le, T. -L. Nguyen and V. -P. Hoang, "Highly Secure Data Encryption Devices Using Unique Physically Unclonable Key," *2021 8th NAFOSTED Conference on*

Information and Computer Science (NICS), 2021, pp. 414-419, doi: 10.1109/NICS54270.2021.9701548. ISBN: 978-1-6654-1001-4.

*** Đăng ký sở hữu trí tuệ**

P1. Bằng độc quyền sáng chế: *Quy trình xác thực định danh (ID) cho mạch tích hợp (IC) ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF).*

Số đơn:	1-2020-05234
Ngày nộp đơn:	11/09/2020
Ngày công bố đơn:	26/07/2021
Số bằng:	34677
Ngày công bố bằng:	25/01/2023
Vai trò:	Đồng tác giả

P2. Giải pháp hữu ích: *Mạch tạo hàm không thể sao chép về vật lý (PUF) sử dụng bộ dao động vòng và tham số khoảng cách Euclid.*

Số đơn:	2-2022-00218
Ngày nộp đơn:	11/09/2020
Ngày công bố đơn:	25/07/2022
Vai trò:	Đồng tác giả

TÀI LIỆU THAM KHẢO

[1] Shamsoshoara, A., Korenda, A., Afghah, F., & Zeadally, S. (2020). A survey on physical unclonable function (PUF)-based security solutions for Internet of Things. *Computer Networks*, *183*, 107593.

[2] Alam, T. (2018). A reliable communication framework and its use in internet of things (IoT). *CSEIT1835111| Received*, *10*, 450-456.

[3] Z. Doffman, "Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims", Sep 14, 2019, https://www.forbes.com/sites/zakdoffman/2019/09/14/dangerous-cyberattacks-on-iot-devices-up-300-in-2019-now-rampant-report-claims/.

[4] Brewer, R. (2016). Ransomware attacks: detection, prevention and cure. *Network Security*, *2016*(9), 5-9.

[5] Lowry, R. K. (2007). Counterfeit electronic components-an overview. In *Military, Aerospace, Spaceborne and Homeland Security Workshop (MASH)*.

[6] H. Livingston, "Avoiding Counterfeit Electronic Components," in *IEEE Transactions on Components and Packaging Technologies*, vol. 30, no. 1, pp. 187-189, March 2007, doi: 10.1109/TCAPT.2007.893682.

[7] Guin, U., DiMase, D., & Tehranipoor, M. (2014). Counterfeit integrated circuits: Detection, avoidance, and the challenges ahead. *Journal of Electronic Testing*, *30*(1), 9-23.

[8] B. Daniel, Counterfeit Electronic Parts: A Multibillion-Dollar Black Market, https://www.trentonsystems.com/blog/counterfeit-electronic-parts. Trenton Systems (2020).

[9] Prinetto, P., & Roascio, G. (2020, August). Hardware Security, Vulnerabilities, and Attacks: A Comprehensive Taxonomy. In *ITASEC* (pp. 177-189).

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

[11] Maes, R., & Verbauwhede, I. (2010). Physically unclonable functions: A study on the state of the art and future research directions. In *Towards hardware-intrinsic security* (pp. 3-37). Springer, Berlin, Heidelberg.

[12] Maiti, A., Kim, I., & Schaumont, P. (2011). A robust physical unclonable function with enhanced challenge-response set. *IEEE Transactions on Information Forensics and Security*, *7*(1), 333-345.

[13] Kim, I., Maiti, A., Nazhandali, L., Schaumont, P., Vivekraja, V., & Zhang, H. (2010). From statistics to circuits: Foundations for future physical unclonable functions. In *Towards Hardware-Intrinsic Security* (pp. 55-78). Springer, Berlin, Heidelberg.

[14] Berger, V. W., & Zhou, Y. (2014). Kolmogorov–smirnov test: Overview. *Wiley statsref: Statistics reference online*.

[15] S. Eiroa and I. Baturone, "Circuit authentication based on Ring-Oscillator PUFs," *2011 18th IEEE International Conference on Electronics, Circuits, and Systems*, 2011, pp. 691-694, doi: 10.1109/ICECS.2011.6122368.

[16] Maes, R., Herrewege, A. V., & Verbauwhede, I. (2012, September). PUFKY: A fully functional PUF-based cryptographic key generator. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 302-319). Springer, Berlin, Heidelberg.

[17] J. Delvaux, D. Gu, D. Schellekens and I. Verbauwhede, "Helper Data Algorithms for PUF-Based Key Generation: Overview and Analysis," in *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 6, pp. 889-902, June 2015, doi: 10.1109/TCAD.2014.2370531.

[18] Delvaux, J. (2017). Security analysis of PUF-based key generation and entity authentication.

[19] Hoang, V. P., Nguyen, Q. P., Nguyen, V. T., Nguyen, T. T., & Tran, X. N. (2021, April). A Design of CMOS PUF Based on Ring Oscillator and Time-to-Digital Converter. In *International Conference on Industrial Networks and Intelligent Systems* (pp. 233-242). Springer, Cham.

[20] T. T. K. Hue, T. M. Hoang and S. A. Assad, "Design and implementation of a Chaotic Cipher block chaining mode for image encryption," *2013 International Conference on Advanced Technologies for Communications (ATC 2013)*, 2013, pp. 185-190, doi: 10.1109/ATC.2013.6698102.

[21] D. Bui, D. Puschini, S. Bacles-Min, E. Beigné and X. Tran, "AES Datapath Optimization Strategies for Low-Power Low-Energy Multisecurity-Level Internet-of-Things Applications," in *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 25, no. 12, pp. 3281-3290, Dec. 2017, doi: 10.1109/TVLSI.2017.2716386.

[22] M. Dao, V. Hoang, V. Dao and X. Tran, "An Energy Efficient AES Encryption Core for Hardware Security Implementation in IoT Systems," *2018 International Conference on Advanced Technologies for Communications (ATC)*, 2018, pp. 301-304, doi: 10.1109/ATC.2018.8587500.

[23] V. -N. Ho, K. -M. Ma, H. -H. Thai and D. -H. Le, "Implementation of a Dual-core 64-bit RISC-V on 7nm FinFET Process," *2021 International Conference on Advanced Technologies for Communications (ATC)*, 2021, pp. 28-32, doi: 10.1109/ATC52653.2021.9598283.

[24] Gassend, B., Clarke, D., Van Dijk, M., & Devadas, S. (2002, November). Silicon physical random functions. In *Proceedings of the 9th ACM Conference on Computer and Communications Security* (pp. 148-160).

[25] Anandakumar, N. N., Hashmi, M. S., & Tehranipoor, M. (2021). FPGA-based Physical Unclonable Functions: A comprehensive overview of theory and architectures. *Integration*, *81*, 175-194.

[26] Zhang, J. L., Qu, G., Lv, Y. Q., & Zhou, Q. (2014). A survey on silicon PUFs and recent advances in ring oscillator PUFs. *Journal of computer science and technology*, *29*(4), 664-678.

[27] Pappu, R., Recht, B., Taylor, J., & Gershenfeld, N. (2002). Physical one-way functions. *Science*, *297*(5589), 2026-2030.

[28] Bulens, P., Standaert, F. X., & Quisquater, J. J. (2010). How to strongly link data and its medium: the paper case. *IET Information Security*, *4*(3), 125-136.

[29] Hammouri, G., Dana, A., & Sunar, B. (2009, September). CDs have fingerprints too. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 348-362). Springer, Berlin, Heidelberg.

[30] Vrijaldenhoven, S. (2004). Acoustical physical uncloneable functions. *Philips internal publication PR-TN-2004-300300*.

[31] J. Das, K. Scott, S. Rajaram, D. Burgett and S. Bhanja, "MRAM PUF: A Novel Geometry Based Magnetic PUF With Integrated CMOS," in *IEEE Transactions on Nanotechnology*, vol. 14, no. 3, pp. 436-443, May 2015, doi: 10.1109/TNANO.2015.2397951.

[32] DeJean, G., & Kirovski, D. (2007, September). RF-DNA: Radio-frequency certificates of authenticity. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 346-363). Springer, Berlin, Heidelberg.

[33] Willers, O. (2019). MEMS sensors as physical unclonable functions.

[34] Hwang, K. M., Park, J. Y., Bae, H., Lee, S. W., Kim, C. K., Seo, M., ... & Choi, Y. K. (2017). Nano-electromechanical switch based on a physical unclonable function for highly robust and stable performance in harsh environments. *ACS nano*, *11*(12), 12547-12552.

[35] Guajardo, J., Škorić, B., Tuyls, P., Kumar, S. S., Bel, T., Blom, A. H., & Schrijen, G. J. (2009). Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. *Information Systems Frontiers*, *11*(1), 19-41.

[36] Mazady, A., Rahman, M. T., Forte, D., & Anwar, M. (2015). Memristor PUF—A security primitive: Theory and experiment. *IEEE*

Journal on Emerging and Selected Topics in Circuits and Systems, *5*(2), 222-229.

[37] Jiang, D., & Chong, C. N. (2008, August). Anti-counterfeiting using phosphor puf. In *2008 2nd International Conference on Anti-counterfeiting, Security and Identification* (pp. 59-62). IEEE.

[38] Sehwag, V., & Saha, T. (2016, December). TV-PUF: a fast lightweight analog physical unclonable function. In *2016 IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)* (pp. 182-186). IEEE.

[39] Morehouse, T., & Zhou, R. (2020, August). RF device identification using CNN based PUF. In *2020 IEEE 63rd International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 217-220). IEEE.

[40] Bojesomo, A., Elfadel, I. A. M., & Sinanoglu, O. (2019, May). Piezo-PUF: Physical Unclonable Functions for Vacuum-Packaged, Piezoelectric MEMS. In *2019 Symposium on Design, Test, Integration & Packaging of MEMS and MOEMS (DTIP)* (pp. 1-4). IEEE.

[41] Lee, J. W., Lim, D., Gassend, B., Suh, G. E., Van Dijk, M., & Devadas, S. (2004, June). A technique to build a secret key in integrated circuits for identification and authentication applications. In *2004 Symposium on VLSI Circuits. Digest of Technical Papers (IEEE Cat. No. 04CH37525)* (pp. 176-179). IEEE.

[42] Suh, G. E., & Devadas, S. (2007, June). Physical unclonable functions for device authentication and secret key generation. In *2007 44th ACM/IEEE Design Automation Conference* (pp. 9-14). IEEE.

[43] Chen, Q., Csaba, G., Lugli, P., Schlichtmann, U., & Rührmair, U. (2011, June). The bistable ring PUF: A new architecture for strong physical unclonable functions. In *2011 IEEE International Symposium on Hardware-Oriented Security and Trust* (pp. 134-141). IEEE.

[44] Guajardo, J., Kumar, S. S., Schrijen, G. J., & Tuyls, P. (2007, August). Physical unclonable functions and public-key crypto for FPGA IP protection. In *2007 International Conference on Field Programmable Logic and Applications* (pp. 189-195). IEEE.

[45] Guajardo, J., Kumar, S. S., Schrijen, G. J., & Tuyls, P. (2007, September). FPGA intrinsic PUFs and their use for IP protection. In *International workshop on cryptographic hardware and embedded systems* (pp. 63-80). Springer, Berlin, Heidelberg.

[46] Kumar, S. S., Guajardo, J., Maes, R., Schrijen, G. J., & Tuyls, P. (2008, June). The butterfly PUF protecting IP on every FPGA. In *2008 IEEE International Workshop on Hardware-Oriented Security and Trust* (pp. 67-70). IEEE.

[47] Yamamoto, D., Sakiyama, K., Iwamoto, M., Ohta, K., Takenaka, M., & Itoh, K. (2013). Variety enhancement of PUF responses using the locations of random outputting RS latches. *Journal of Cryptographic Engineering*, *3*(4), 197-211.

[48] Rührmair, U., & Holcomb, D. E. (2014, March). PUFs at a glance. In *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)* (pp. 1-6). IEEE.

[49] Gu, C., Hanley, N., & O'neill, M. (2017). Improved reliability of FPGA-based PUF identification generator design. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, *10*(3), 1-23.

[50] Yu, M. D., Hiller, M., Delvaux, J., Sowell, R., Devadas, S., & Verbauwhede, I. (2016). A lockdown technique to prevent machine learning on PUFs for lightweight authentication. *IEEE Transactions on Multi-Scale Computing Systems*, *2*(3), 146-159.

[51] Tehranipoor, F., Karimian, N., Yan, W., & Chandy, J. A. (2016). DRAM-based intrinsic physically unclonable functions for system-level security and authentication. *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, *25*(3), 1085-1097.

[52] Yu, H., Leong, P. H., & Xu, Q. (2011). An FPGA chip identification generator using configurable ring oscillators. *IEEE transactions on very* large *scale integration (VLSI) systems*, *20*(12), 2198-2207.

[53] Rostami, M., Majzoobi, M., Koushanfar, F., Wallach, D. S., & Devadas, S. (2014). Robust and reverse-engineering resilient PUF authentication and key-exchange by substring matching. *IEEE Transactions on Emerging Topics in Computing*, *2*(1), 37-49.

[54] Aysu, A., Gulcan, E., Moriyama, D., Schaumont, P., & Yung, M. (2015, September). End-to-end design of a PUF-based privacy preserving authentication protocol. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 556-576). Springer, Berlin, Heidelberg.

[55] Kalanadhabhatta, S., Kumar, D., Anumandla, K. K., Reddy, S. A., & Acharyya, A. (2020). PUF-based secure chaotic random number generator design methodology. *IEEE transactions on very large scale integration (VLSI) systems*, *28*(7), 1740-1744.

[56] Li, D., Lu, Z., Zou, X., & Liu, Z. (2015). PUFKEY: A high-security and high-throughput hardware true random number generator for sensor networks. *Sensors*, *15*(10), 26251-26266.

[57] Leest, V. V. D., Sluis, E. V. D., Schrijen, G. J., Tuyls, P., & Handschuh, H. (2012). Efficient implementation of true random number generator based on sram pufs. In *Cryptography and security: from theory to applications* (pp. 300-318). Springer, Berlin, Heidelberg.

[58] Chen, S., Li, B., & Zhou, C. (2018). FPGA implementation of SRAM PUFs based cryptographically secure pseudo-random number generator. *Microprocessors and Microsystems*, *59*, 57-68.

[59] Kean, T. (2002, February). Cryptographic rights management of FPGA intellectual property cores. In *Proceedings of the 2002 ACM/SIGDA tenth international symposium on Field-programmable gate arrays* (pp. 113-118).

[60] Simpson, E., & Schaumont, P. (2006, October). Offline hardware/software authentication for reconfigurable platforms. In *International Workshop on Cryptographic Hardware and Embedded Systems* (pp. 311-323). Springer, Berlin, Heidelberg.

[61] Kokila, J., & Ramasubramanian, N. (2019). Enhanced authentication using hybrid puf with fsm for protecting ips of soc fpgas. *Journal of Electronic Testing*, *35*(4), 543-558.

[62] Mukhopadhyay, D., & Chakraborty, R. S. (2014). *Hardware security: design, threats, and safeguards*. CRC Press.

[63] Joost, R., & Salomon, R. (2005, November). Advantages of FPGA-based multiprocessor systems in industrial applications. In *31st Annual*

Conference of IEEE Industrial Electronics Society, 2005. IECON 2005. (pp. 6-pp). IEEE.

[64] Zhang, J., & Qu, G. (2019). Recent attacks and defenses on FPGA-based systems. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, *12*(3), 1-24.

[65] Anandakumar, N. N., Sanadhya, S. K., & Hashmi, M. S. (2019). FPGA-based true random number generation using programmable delays in oscillator-rings. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *67*(3), 570-574.

[66] Bakiri, M., Guyeux, C., Couchot, J. F., & Oudjida, A. K. (2018). Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses. *Computer Science Review*, *27*, 135-153.

[67] Anandakumar, N. N., Das, M. P. L., Sanadhya, S. K., & Hashmi, M. S. (2018). Reconfigurable hardware architecture for authenticated key agreement protocol over binary edwards curve. *ACM Transactions on Reconfigurable Technology and Systems (TRETS)*, *11*(2), 1-19.

[68] Menhorn, N. (2018). External secure storage using the PUF. *Xilinx, San Jose, CA, USA, Application Note XAPP1333 (v1. 0) June 26*.

[69] Horovitz, K., & Kenny, R. (2018). *Intel FPGA secure device manager*. Intel Corporation, Programmable Solutions Group (formerly Altera) San Jose United States.

[70] T. Speers, Polarfire non-volatile FPGA family delivers ground breaking value: Best-in-class security, 2018,

https://www.microsemi.com/blog/2018/04/10/ polarfire-non-volatile-fpga-family-delivers-ground-breaking-value-best-in-class-security/.

[71] Maiti, A., & Schaumont, P. (2011). Improved ring oscillator PUF: An FPGA-friendly secure primitive. *Journal of cryptology*, *24*(2), 375-397.

[72] Xin, X., Kaps, J. P., & Gaj, K. (2011, August). A configurable ring-oscillator-based PUF for Xilinx FPGAs. In *2011 14th Euromicro conference on digital system design* (pp. 651-657). IEEE.

[73] Yu, H., Leong, P. H., & Xu, Q. (2011). An FPGA chip identification generator using configurable ring oscillators. *IEEE transactions on very large scale integration (VLSI) systems*, *20*(12), 2198-2207.

[74] Choudhury, M., Pundir, N., Niamat, M., & Mustapa, M. (2017, August). Analysis of a novel stage configurable ROPUF design. In *2017 IEEE 60th International Midwest Symposium on Circuits and Systems (MWSCAS)* (pp. 942-945). IEEE.

[75] Gao, M., Lai, K., & Qu, G. (2014, June). A highly flexible ring oscillator PUF. In *Proceedings of the 51st annual design automation conference* (pp. 1-6).

[76] Pang, Z., Zhang, J., Zhou, Q., Gong, S., Qian, X., & Tang, B. (2017, March). Crossover ring oscillator PUF. In *2017 18th International Symposium on Quality Electronic Design (ISQED)* (pp. 237-243). IEEE.

[77] Habib, B., Gaj, K., & Kaps, J. P. (2013, September). FPGA PUF based on programmable LUT delays. In *2013 Euromicro Conference on Digital System Design* (pp. 697-704). IEEE.

[78] Anandakumar, N. N., Hashmi, M. S., & Sanadhya, S. K. (2017, January). Compact implementations of FPGA-based PUFs with enhanced performance. In *2017 30th International Conference on VLSI Design and 2017 16th International Conference on Embedded Systems (VLSID)* (pp. 161-166). IEEE.

[79] Cherif, Z., Danger, J. L., Guilley, S., & Bossuet, L. (2012, September). An easy-to-design PUF based on a single oscillator: the loop PUF. In *2012 15th Euromicro Conference on Digital System Design* (pp. 156-162). IEEE.

[80] Liu, W., Zhang, L., Zhang, Z., Gu, C., Wang, C., O'neill, M., & Lombardi, F. (2019). XOR-based low-cost reconfigurable PUFs for IoT security. *ACM Transactions on Embedded Computing Systems (TECS)*, *18*(3), 1-21.

[81] Merli, D., Stumpf, F., & Eckert, C. (2010, October). Improving the quality of ring oscillator PUFs on FPGAs. In *Proceedings of the 5th workshop on embedded systems security* (pp. 1-9).

[82] Yu, M. D., & Devadas, S. (2010). Secure and robust error correction for physical unclonable functions. *IEEE Design & Test of Computers*, *27*(1), 48-65.

[83] Yin, C. E. (2011). *Kendall Syndrome Coding (KSC) for Group-Based Ring-Oscillator Physical Unclonable Functions*.

[84] Yin, C. E., & Qu, G. (2013, May). Improving PUF security with regression-based distiller. In *Proceedings of the 50th Annual Design Automation Conference* (pp. 1-6).

[85] Pelgrom, M.J.M. (2010). Technology. In: Analog-to-Digital Conversion. Springer, Dordrecht. https://doi.org/10.1007/978-90-481-8888-8_11

[86] Boning, D., & Nassif, S. (2000). Models of process variations in device and interconnect. *Design of high performance microprocessor circuits*, 6.

[87] VLSIFacts. "The mystery of Monte Carlo Simulation". *https://www.vlsifacts.com/mystery-monte-carlo-simulation/*

[88] Bernstein, K., Frank, D. J., Gattiker, A. E., Haensch, W., Ji, B. L., Nassif, S. R., ... & Rohrer, N. J. (2006). High-performance CMOS variability in the 65-nm regime and beyond. *IBM journal of research and development*, *50*(4.5), 433-449.

[89] Boyd, S., & Vandenberghe, L. (2018). *Introduction to applied linear algebra: vectors, matrices, and least squares*. Cambridge university press.

[90] Evans, M., Hastings, N., Peacock, B., & Forbes, C. (2011). *Statistical distributions*. John Wiley & Sons.

[91] Gooch, J. W. (Ed.). (2010). *Encyclopedic dictionary of polymers* (Vol. 1). Springer Science & Business Media.

[92] Montgomery, D. C., & Woodall, W. H. (2008). An overview of six sigma. *International Statistical Review/Revue Internationale de Statistique*, 329-346.

[93] BPI. Six Sigma. *https://www.leansixsigmadefinition.com/glossary/six-sigma/*

[94] Kohlbrenner, P., & Gaj, K. (2004, February). An embedded true random number generator for FPGAs. In *Proceedings of the 2004 ACM/SIGDA 12th international symposium on Field programmable gate arrays* (pp. 71-78).

[95] Yang, K., Fick, D., Henry, M. B., Lee, Y., Blaauw, D., & Sylvester, D. (2014, February). 16.3 A 23Mb/s 23pJ/b fully synthesized true-random-number generator in 28nm and 65nm CMOS. In *2014 IEEE International Solid-State Circuits Conference Digest of Technical Papers (ISSCC)* (pp. 280-281). IEEE.

[96] López-Leyva, J. A., & Arvizu-Mondragón, A. (2016). Simultaneous dual true random numbers generator. *Dyna*, *83*(195), 93-98.

[97] Figotin, A., Vitebskiy, I., Popovich, V., Stetsenko, G., Molchanov, S., Gordon, A., ... & Stavrakas, N. (2004). *U.S. Patent No. 6,745,217*. Washington, DC: U.S. Patent and Trademark Office.

[98] Rožić, V., & Verbauwhede, I. (2018). Hardware-efficient post-processing architectures for true random number generators. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *66*(7), 1242-1246.

[99] Schellekens, D., Preneel, B., & Verbauwhede, I. (2006, August). FPGA vendor agnostic true random number generator. In *2006 International conference on field programmable logic and applications* (pp. 1-6). IEEE.

[100] Teh, J. S., Teng, W., Samsudin, A., & Chen, J. (2020). A post-processing method for true random number generators based on hyperchaos with applications in audio-based generators. *Frontiers of Computer Science*, *14*(6), 1-11.

[101] Gu, C., Liu, W., Cui, Y., Hanley, N., O'Neill, M., & Lombardi, F. (2019). A flip-flop based arbiter physical unclonable function (APUF) design with high entropy and uniqueness for FPGA implementation. *IEEE Transactions on Emerging Topics in Computing*, *9*(4), 1853-1866.

[102] Sahoo, D. P., Chakraborty, R. S., & Mukhopadhyay, D. (2015, August). Towards ideal arbiter PUF design on Xilinx FPGA: A practitioner's perspective. In *2015 Euromicro Conference on Digital System Design* (pp. 559-562). IEEE.

[103] Maiti, A., Gunreddy, V., & Schaumont, P. (2013). A systematic method to evaluate and compare the performance of physical unclonable functions. In *Embedded systems design with FPGAs* (pp. 245-267). Springer, New York, NY.

[104] Machida, T., Yamamoto, D., Iwamoto, M., & Sakiyama, K. (2015). A new arbiter PUF for enhancing unpredictability on FPGA. *The Scientific World Journal*, *2015*.

[105] Hori, Y., Yoshida, T., Katashita, T., & Satoh, A. (2010, December). Quantitative and statistical performance evaluation of arbiter physical unclonable functions on FPGAs. In *2010 International conference on reconfigurable computing and FPGAs* (pp. 298-303). IEEE.

[106] Avvaru, S. S., Zeng, Z., & Parhi, K. K. (2020). Homogeneous and heterogeneous feed-forward XOR physical unclonable functions. *IEEE Transactions on Information Forensics and Security*, *15*, 2485-2498.

[107] Nguyen, P. H., Sahoo, D. P., Jin, C., Mahmood, K., Rührmair, U., & van Dijk, M. (2018). The interpose PUF: Secure PUF design against state-of-the-art machine learning attacks. *Cryptology ePrint Archive*.

[108] Katzenbeisser, S., Kocabaş, Ü., Van Der Leest, V., Sadeghi, A. R., Schrijen, G. J., & Wachsmann, C. (2011). Recyclable pufs: Logically reconfigurable pufs. *Journal of Cryptographic Engineering*, *1*(3), 177-186.

[109] Yu, H., Leong, P. H., & Xu, Q. (2011). An FPGA chip identification generator using configurable ring oscillators. *IEEE transactions on very large scale integration (VLSI) systems*, *20*(12), 2198-2207.

[110] Günlü, O., Kernetzky, T., İşcan, O., Sidorenko, V., Kramer, G., & Schaefer, R. F. (2018). Secure and reliable key agreement with physical unclonable functions. *Entropy*, *20*(5), 340.

[111] Zhang, J., Tan, X., Zhang, Y., Wang, W., & Qin, Z. (2018). Frequency offset-based ring oscillator physical unclonable function. *IEEE Transactions on Multi-Scale Computing Systems*, *4*(4), 711-721.

[112] Tanamoto, T., Yasuda, S., Takaya, S., & Fujita, S. (2016). Physically unclonable function using an initial waveform of ring oscillators. *IEEE Transactions on Circuits and Systems II: Express Briefs*, *64*(7), 827-831.

[113] Stanciu, A., Cirstea, M. N., & Moldoveanu, F. D. (2016). Analysis and evaluation of PUF-based SoC designs for security applications. *IEEE Transactions on Industrial Electronics*, *63*(9), 5699-5708.

[114] Marchand, C., Bossuet, L., Mureddu, U., Bochard, N., Cherkaoui, A., & Fischer, V. (2017). Implementation and characterization of a physical unclonable function for IoT: a case study with the TERO-PUF. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *37*(1), 97-109.

[115] Cui, Y., Wang, C., Liu, W., Yu, Y., O'Neill, M., & Lombardi, F. (2016, May). Low-cost configurable ring oscillator PUF with improved uniqueness. In *2016 IEEE International symposium on circuits and systems (ISCAS)* (pp. 558-561). IEEE.

[116] Chauhan, A. S., Sahula, V., & Mandal, A. S. (2019, January). Novel randomized & biased placement for FPGA based robust random number generator with enhanced uniqueness. In *2019 32nd International Conference on VLSI Design and 2019 18th International Conference on Embedded Systems (VLSID)* (pp. 353-358). IEEE.

[117] Yan, W., Jin, C., Tehranipoor, F., & Chandy, J. A. (2017, September). Phase calibrated ring oscillator PUF design and implementation on FPGAs. In *2017 27th International Conference on Field Programmable Logic and Applications (FPL)* (pp. 1-8). IEEE.

[118] Srinivasu, B., Vikramkumar, P., Chattopadhyay, A., & Lam, K. Y. (2018, October). CoLPUF: a novel configurable LFSR-based PUF. In *2018 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (pp. 358-361). IEEE.

[119] Bossuet, L., Ngo, X. T., Cherif, Z., & Fischer, V. (2013). A PUF based on a transient effect ring oscillator and insensitive to locking phenomenon. *IEEE Transactions on Emerging Topics in Computing*, *2*(1), 30-36.

[120] Maes, R., Tuyls, P., & Verbauwhede, I. (2008, November). Intrinsic PUFs from flip-flops on reconfigurable devices. In *3rd Benelux workshop on information and system security (WISSec 2008)* (Vol. 17, p. 2008).

[121] Ardakani, A., Shokouhi, S. B., & Reyhani-Masoleh, A. (2018). Improving performance of FPGA-based SR-latch PUF using Transient Effect Ring Oscillator and programmable delay lines. *Integration*, *62*, 371-381.

[122] Habib, B., Kaps, J. P., & Gaj, K. (2015, April). Efficient sr-latch PUF. In *International symposium on applied reconfigurable computing* (pp. 205-216). Springer, Cham.

[123] Gubner, J. A. (2006). *Probability and random processes for electrical and computer engineers*. Cambridge University Press.

PHỤ LỤC

Phụ lục 1: Thiết kế RO PUF trên FPGA

PL1.1. Thiết kế PUF trên FPGA

Bảng PL1.1: So sánh hiệu năng và mức tiêu thụ phần cứng của một số thiết kế PUF trên FPGA [25]

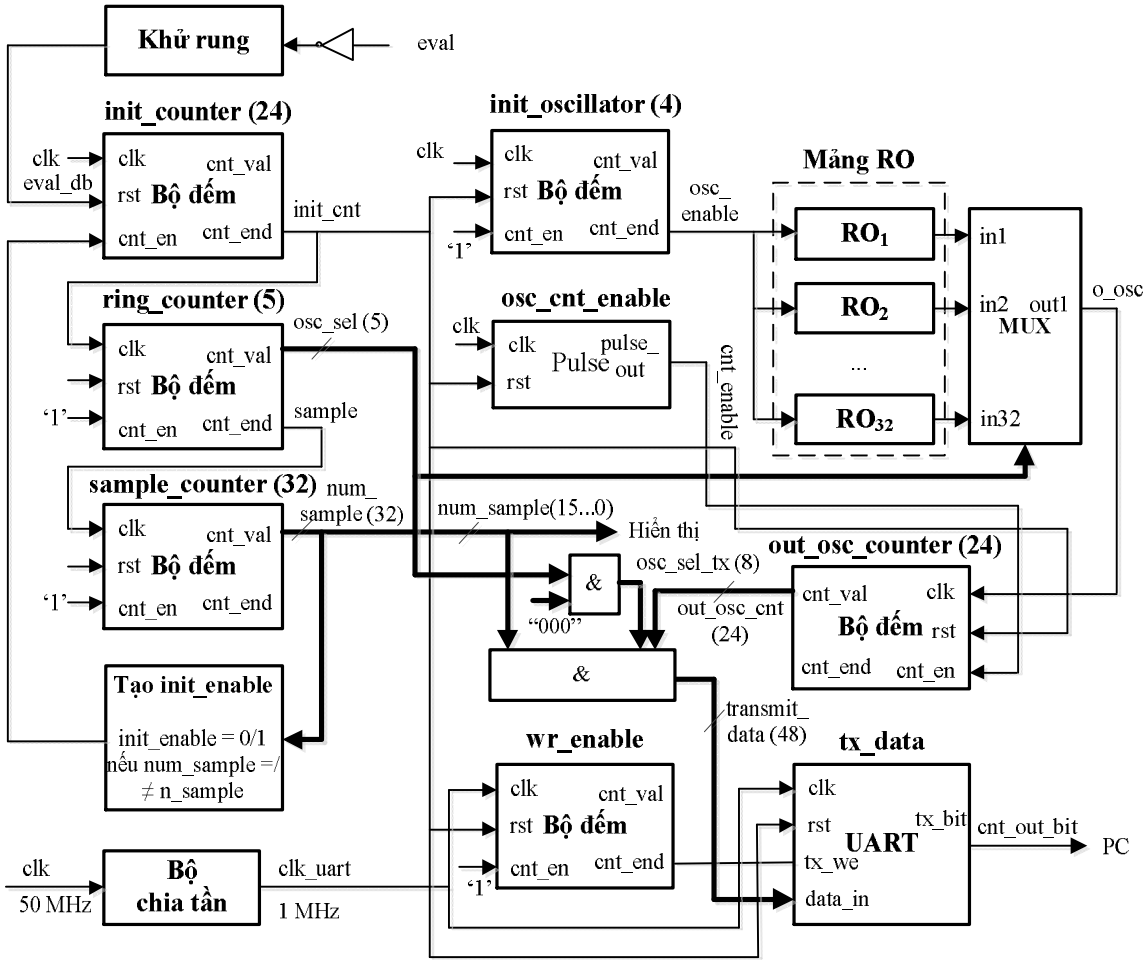
Kiểu	Thiết kế	Nhóm nghiên cứu	Tính duy nhất [%]	Độ ổn định [%]	Diện tích (Tổng số slice)	Loại phần cứng FPGA
PUF dựa trên độ giữ chậm	APUF	Gu [101]	41,53	95,50	2816	Artix-7
		Sahoo [102]	45,25	95,93	-	Spartan-3
		Maiti [103]	18,37	99,76	-	Virtex-5
		Machida [104]	04,70	99,32	177	Virtex-5
		Hori [105]	36,75	98,48	-	Virtex-5
		Anandakumar[78]	44,30	96,00	234	Spartan-6
	FFXORPUF	Avvaru [106]	49,20	89,50	-	Artix-7
	IPUF	Nguyen [107]	49,25	89,50	-	Artix-7
	LRPUF	Katzenbeisser [108]	-	62,36	425	Spartan-6
	RO PUF	Maiti [103]	47,24	99,14	-	Spartan-3E
		Merli [81]	48,51	98,28	512	Spartan-3E
		Yu [109]	47,00	-	420	Spartan-3E
		Maiti [71]	44,10	99,00	-	Spartan-3
		Gao [75]	47,31	95,95	-	Spartan-3
		Xin [72]	40,00	98,98	-	Spartan-3
		Habib [77]	48,30	97,88	747	Spartan-3
		Gunlu [110]	-	-	849	Zinq-7000
		Suh [42]	46,15	99,52	-	Virtex-4

Bảng PL1.1 (tiếp)

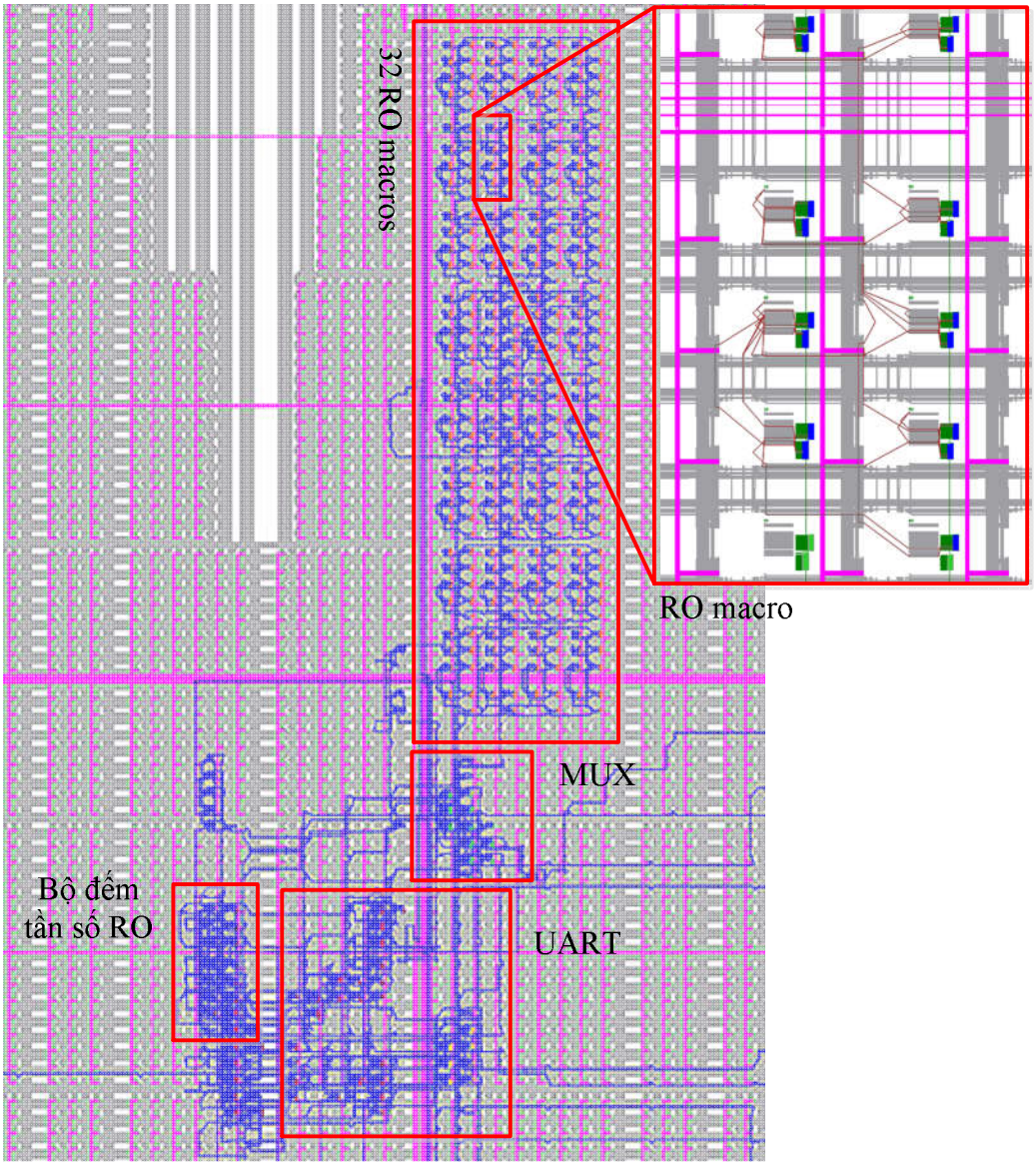
Kiểu	Thiết kế	Nhóm nghiên cứu	Tính duy nhất [%]	Độ ổn định [%]	Diện tích (Tổng số slice)	Loại phần cứng FPGA
PUF dựa trên độ giữ chậm	RO PUF	Zhang [111]	49,33	95,45	186	Virtex-5
		Maes [10]	48,40	90,31	952	Spartan-6
		Tanamoto [112]	32,52	96,96	-	Spartan-6
		Stanciu [113]	58,58	94,00	-	Spartan-6
		Marchand [114]	55,00	94,50	-	Spartan-6
		Cui [115]	49,97	98,41	-	Spartan-6
		Anandakumar[78]	47,13	99,16	82	Spartan-6
		Liu [80]	48,76	97,72	-	Spartan-6
		Chauhan [116]	49,83	99,35	-	Artix-7
		Choudhury [74]	47,40	-	-	Artix-7
		Yan [117]	-	99,33	-	Kintex-7
	Loop PUF	Cherif [79]	49,94	95,00	-	Cyclone II
	CoLPUF	Srinivasu [118]	49,20	99,99	572	Artix-7
	BR PUF	Chen [43]	14,80	99,20	-	Virtex-II
		Liu [80]	40,67	98,22	-	Spartan-6
	TERO PUF	Bossuet [119]	48,00	98,30	-	Cyclone II
		Marchand [114]	48,50	85,00	-	Spartan-6
PUF dựa trên trạng thái phần tử nhớ	SRAM PUF	Guajardo [45]	49,97	88,00	-	-
	FF PUF	Maes [120]	≈50	95,00	-	Virtex-II
	Butterfly PUF	Kumar [46]	43,16	96,20	130	Virtex-5
	Latch PUF	Ardakani [121]	49,32	98,80	128	Spartan-3
		Yamamoto [47]	49,00	96,34	256	Spartan-6
		Habib [122]	49,24	98,87	324	Spartan-6
		Stanciu [113]	34,73	92,00	-	Spartan-6
		Anandakumar[78]	48,10	99,19	54	Spartan-6

PL1.2. Mạch RO PUF tách tần số tuyệt đối RO

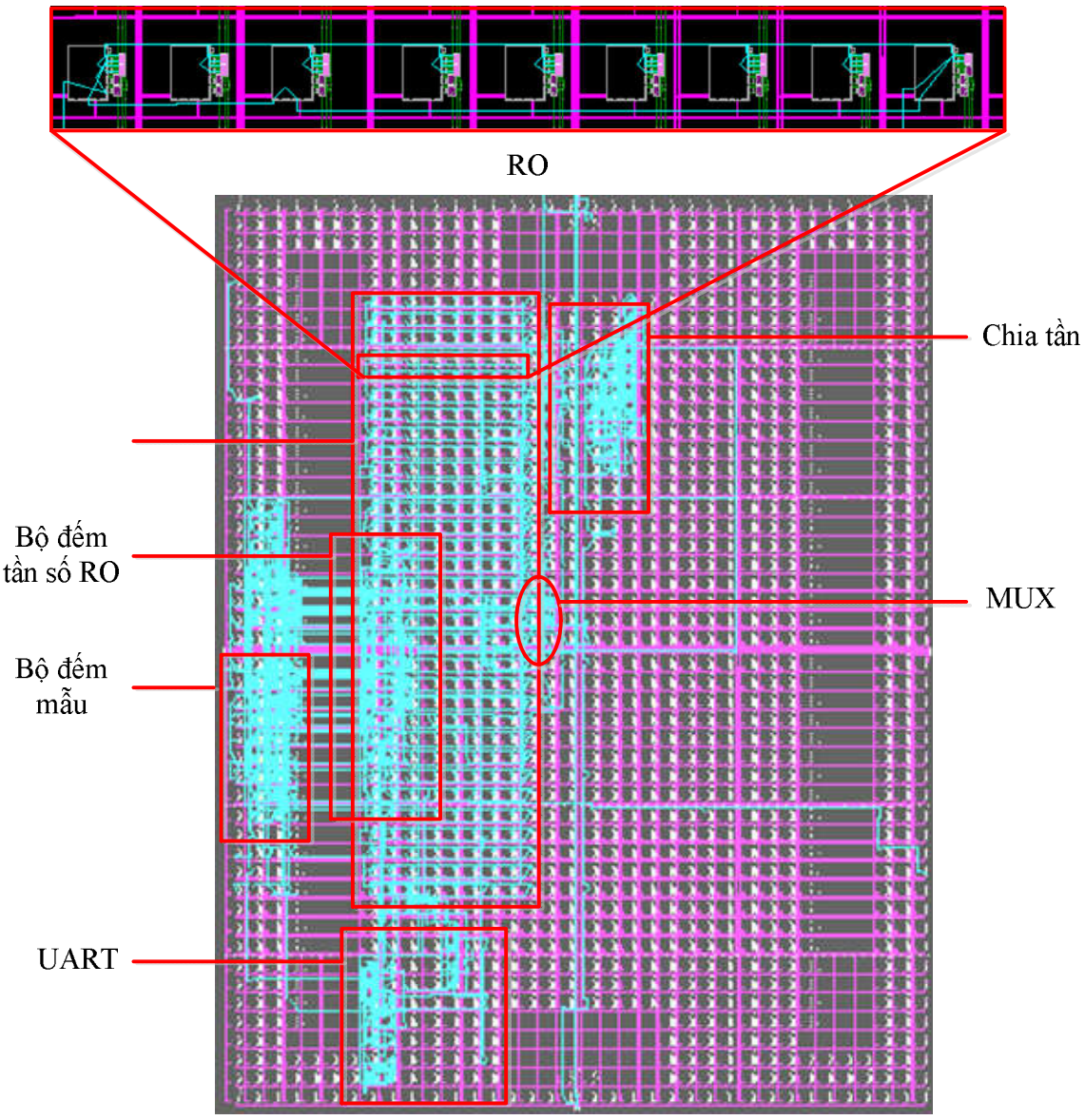
Sơ đồ chức năng của mạch được trình bày trên Hình PL1.1, sơ đồ mạch vật lý của thiết kế thực thi trên FPGA Xilinx Spartan-6, Spartan-3E tương ứng được trình bày trên Hình PL1.2 và Hình PL1.3. Mức tiêu thụ phần cứng của các thiết kế được liệt kê trong Bảng PL1.2 và Bảng PL1.3.



Hình PL 1.1: Sơ đồ chức năng mạch tách tần số tuyệt đối RO thực thi trên FPGA



Hình PL1.2: Mạch vật lý của thiết kế RO PUF đề xuất trên FPGA Xilinx Spartan-6



Hình PL1.3: Mạch vật lý của thiết kế RO PUF đề xuất trên FPGA Xilinx Spartan-3E

Bảng PL1.2: Mức tiêu thụ phần cứng của thiết kế tách tần số tuyệt đối RO thực thi trên FPGA Xilinx Spartan-6 XC6SLX25

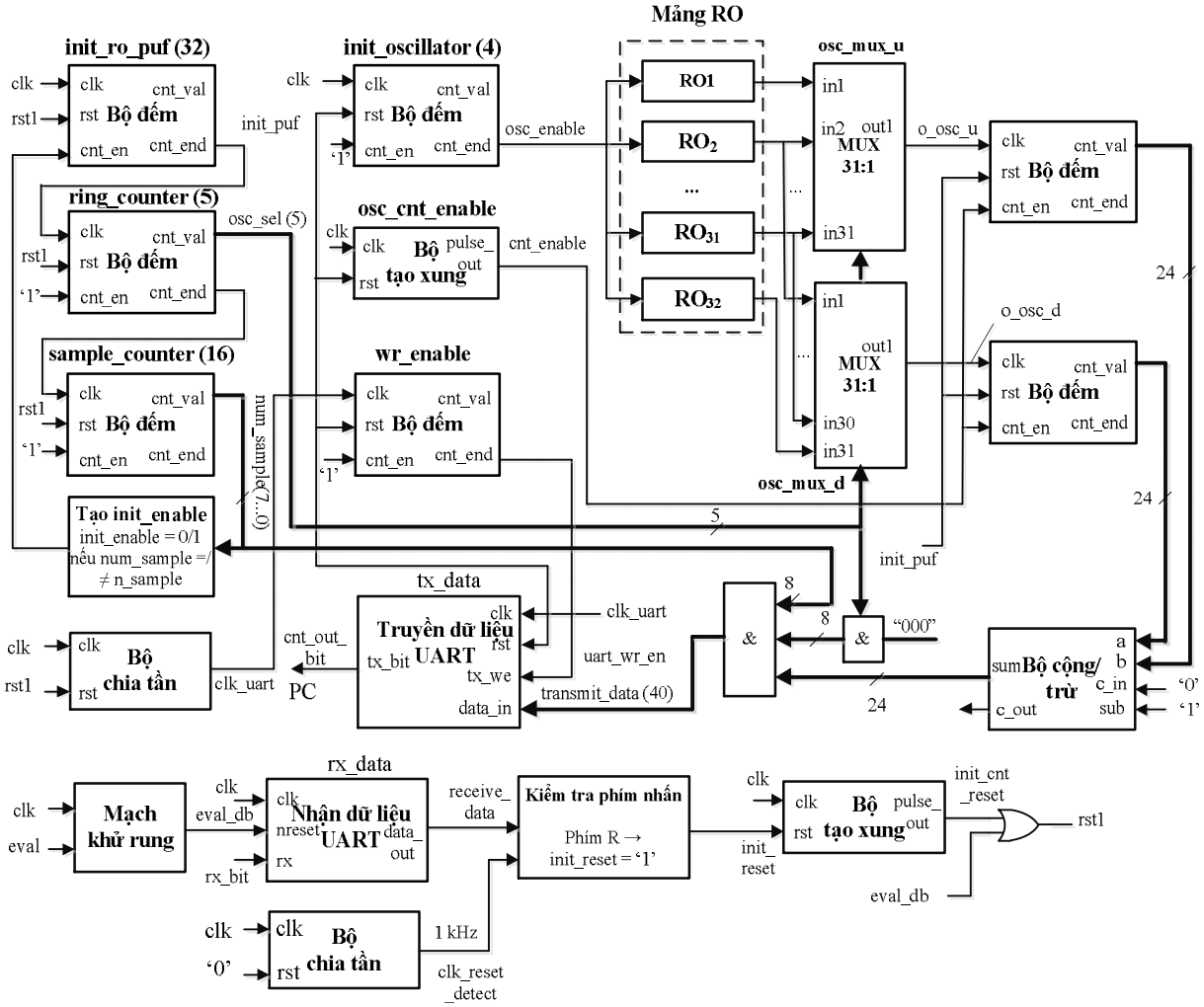
Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
Thanh ghi	309	30.064	1
LUT	956	15.032	6
Slice	704	3.758	18
MUXCY	196	7.516	2
Cặp LUT-FF	247	979	25
IOB	12	186	6
RAMB8BWER	2	104	1
BUFG/ BUFGMUX	4	16	25

Bảng PL1.3: Mức tiêu thụ phần cứng của thiết kế tách tần số tuyệt đối RO thực thi trên FPGA Xilinx Spartan-3E XC3S500E

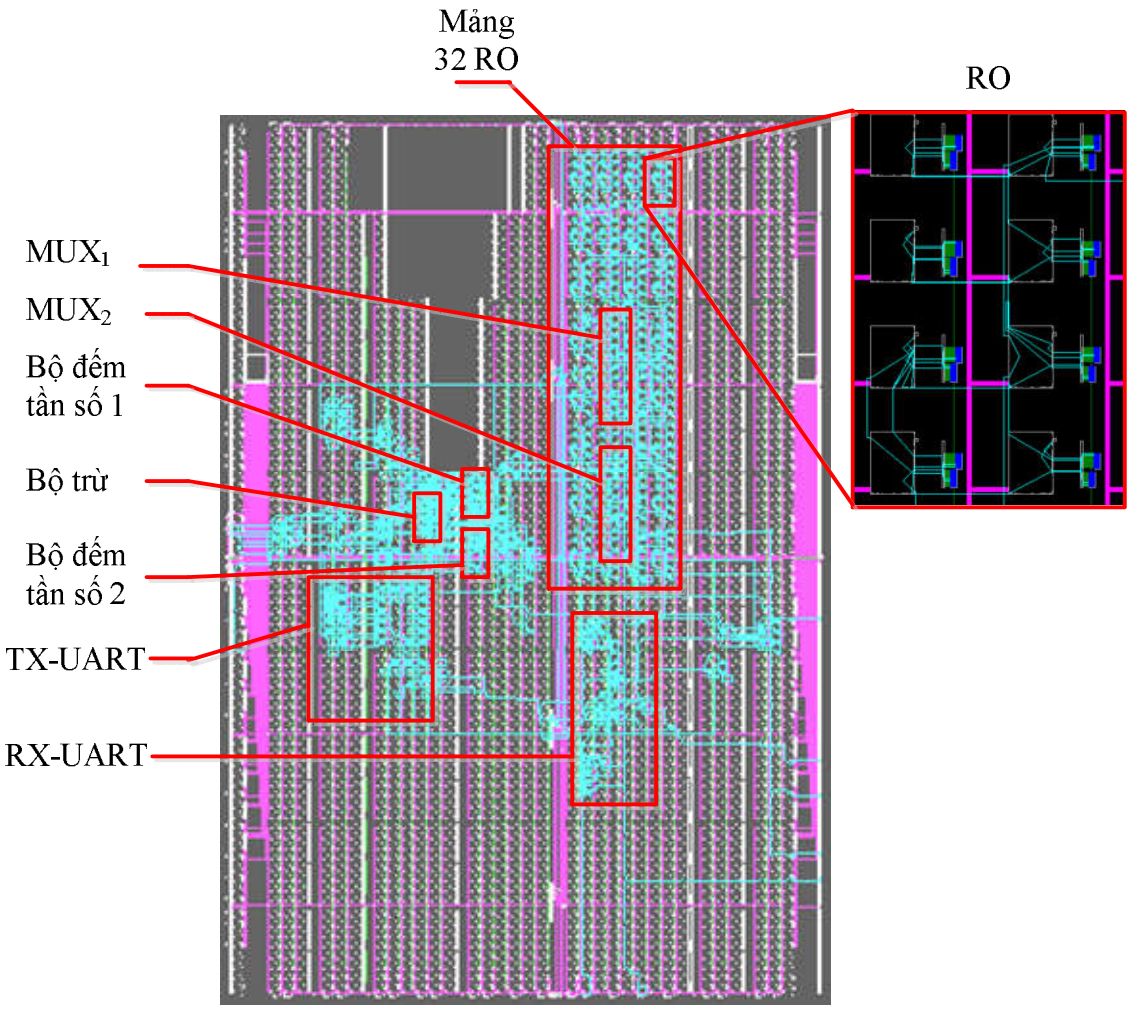
Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
FF	306	9.312	3
LUT 4 đầu vào	1.029	9.312	11
Slice	807	4.656	17
IOB	11	158	6
RAMB 16	2	20	10
BUFGMUX	3	24	12

PL1.3. Mạch RO PUF tách tần số hiệu RO

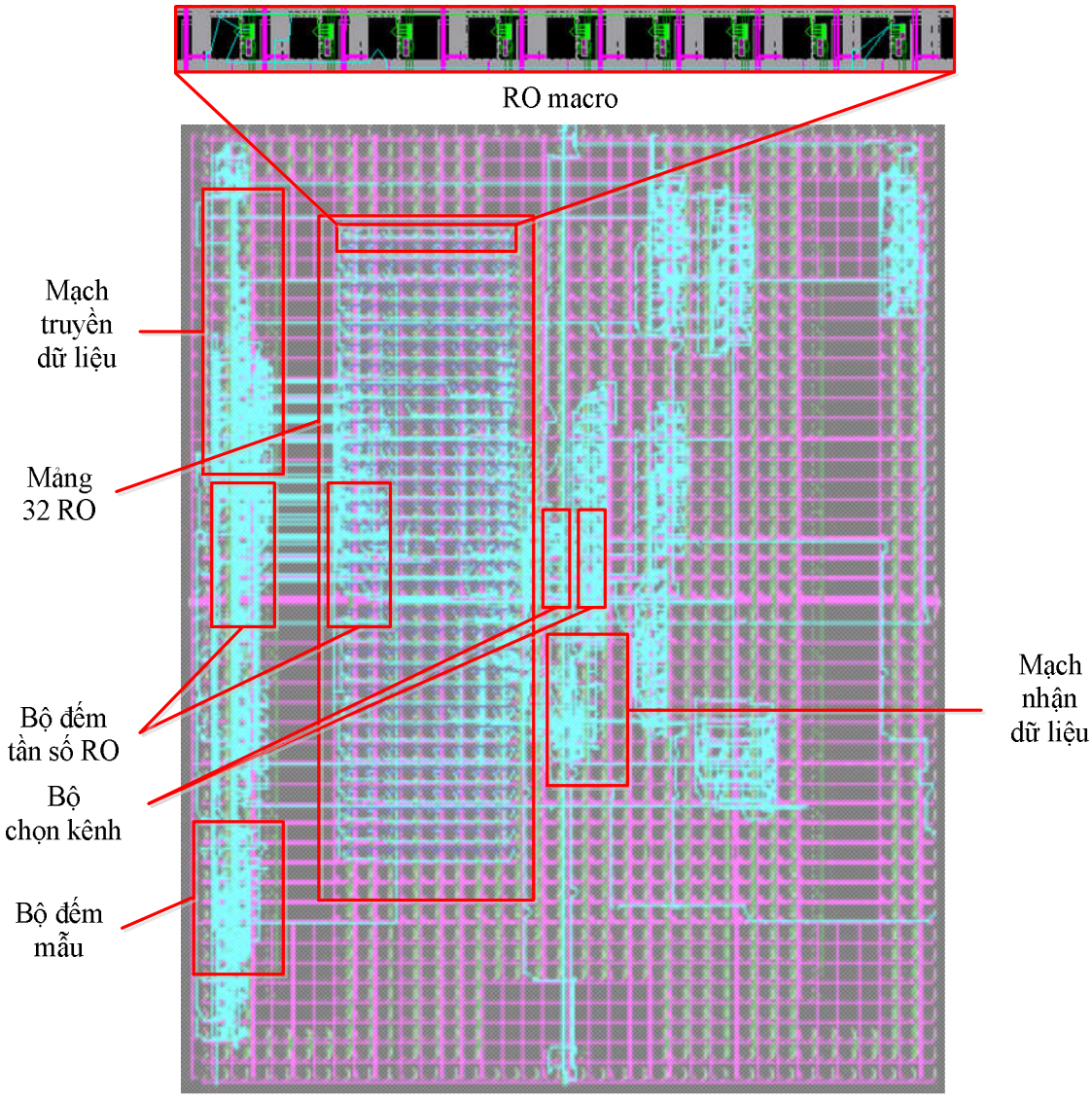
Sơ đồ chức năng của mạch được trình bày trên Hình PL1.4, sơ đồ mạch vật lý của thiết kế thực thi trên FPGA Xilinx Spartan-6, Spartan-3E, Artix-7 tương ứng được trình bày trên Hình PL1.5, Hình PL1.6 và Hình PL1.7. Mức tiêu thụ phần cứng của các thiết kế được liệt kê trong Bảng PL1.4, Bảng PL1.5 và Bảng PL1.6. Quy trình định danh và xác thực ID cho thiết bị ứng dụng RO PUF và tham số khoảng cách Euclid được trình bày trên Hình PL1.8.



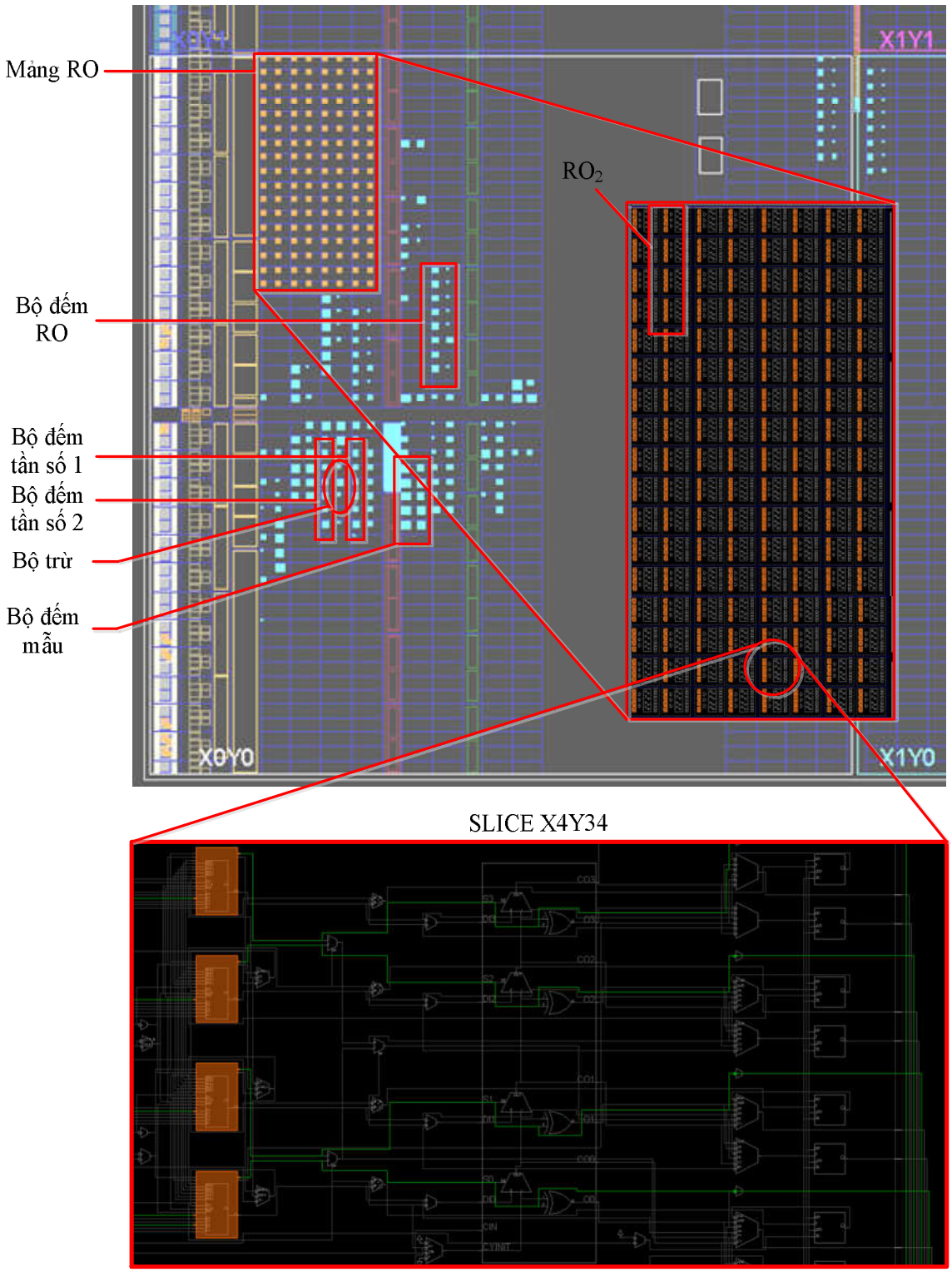
Hình PL1.4: Sơ đồ chức năng mạch tách tần số hiệu RO trong sơ đồ định danh và xác thực ID ứng dụng RO PUF thực thi trên FPGA



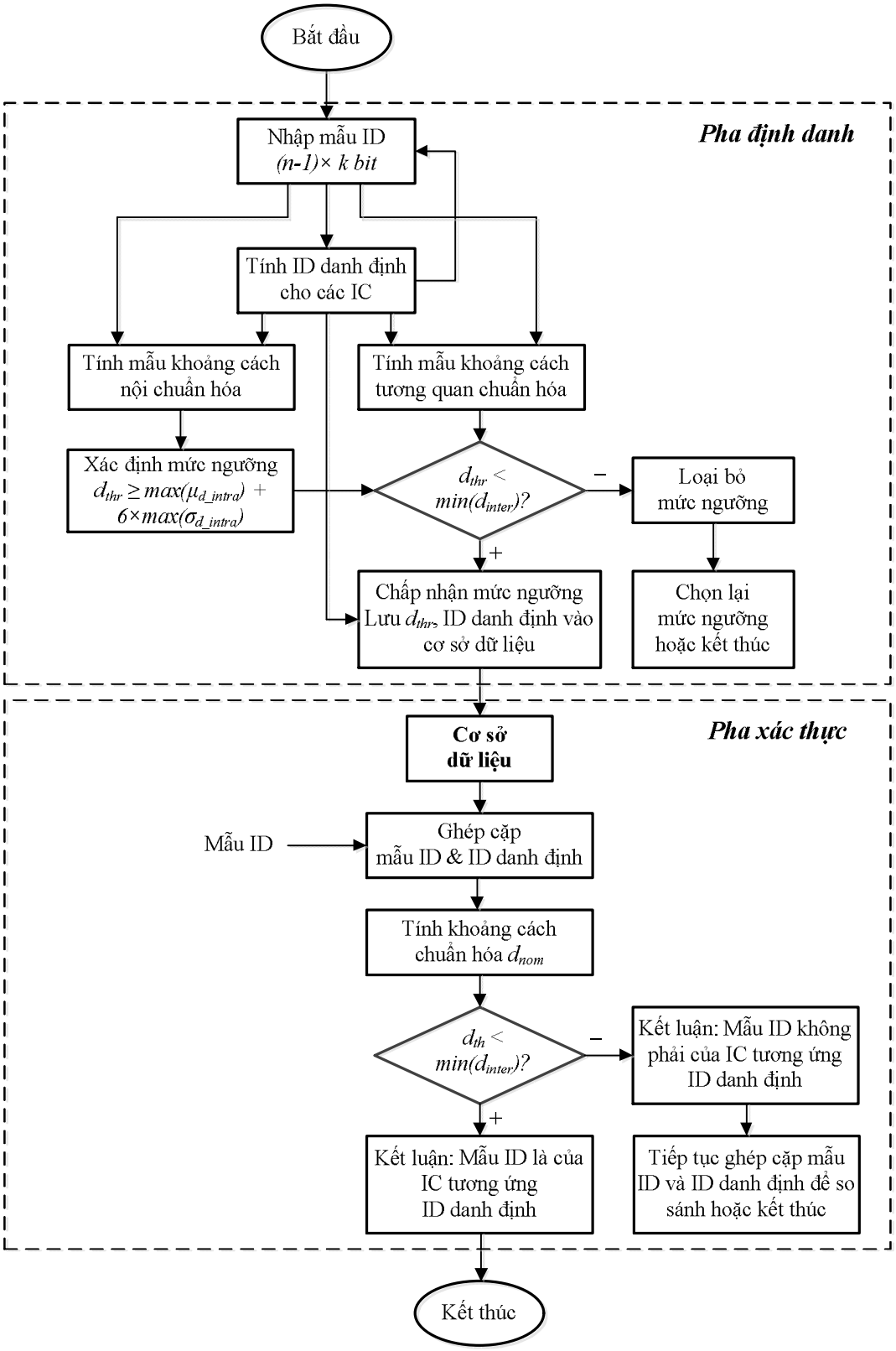
Hình PL1.5: Sơ đồ mạch vật lý của mạch tách tần số hiệu RO trên FPGA Spartan-6



Hình PL1.6: Sơ đồ mạch vật lý của mạch tách tần số hiệu RO trên FPGA Spartan-3E



Hình PL1.7: Sơ đồ mạch vật lý của mạch tách tần số hiệu RO trên FPGA Artix-7



Hình PL1.8: Quy trình định danh và xác thực ID cho thiết bị ứng dụng RO PUF và tham số khoảng cách Euclid

Bảng PL1.4: Mức tiêu thụ phần cứng của thiết kế tách tần số hiệu RO thực thi trên FPGA Xilinx Spartan-6 XC6SLX25

Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
Thanh ghi	779	30.064	2
LUT	1.198	15.032	7
Slice	785	3.758	20
MUXCY	228	7.516	3
Cặp LUT-FF	469	1.260	37
IOB	9	186	4
RAMB8BWER	1	104	1
BUFG/ BUFGMUX	6	16	37

Bảng PL1.5: Mức tiêu thụ phần cứng của thiết kế tách tần số hiệu RO thực thi trên FPGA Xilinx Spartan-3E XC3S500E

Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
FF	498	9.312	5
LUT 4 đầu vào	1312	9.312	14
Slice	963	4.656	20
IOB	12	158	7
RAMB 16	2	20	10
BUFGMUX	5	24	20

Bảng PL1.6: Mức tiêu thụ phần cứng của thiết kế tách tần số hiệu RO thực thi trên FPGA Xilinx Artix-7 XC7A35T

Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
LUT	889	20.800	4,27
FF	473	41.600	1,14
BRAM	1	50	2,00
IO	9	170	5,29

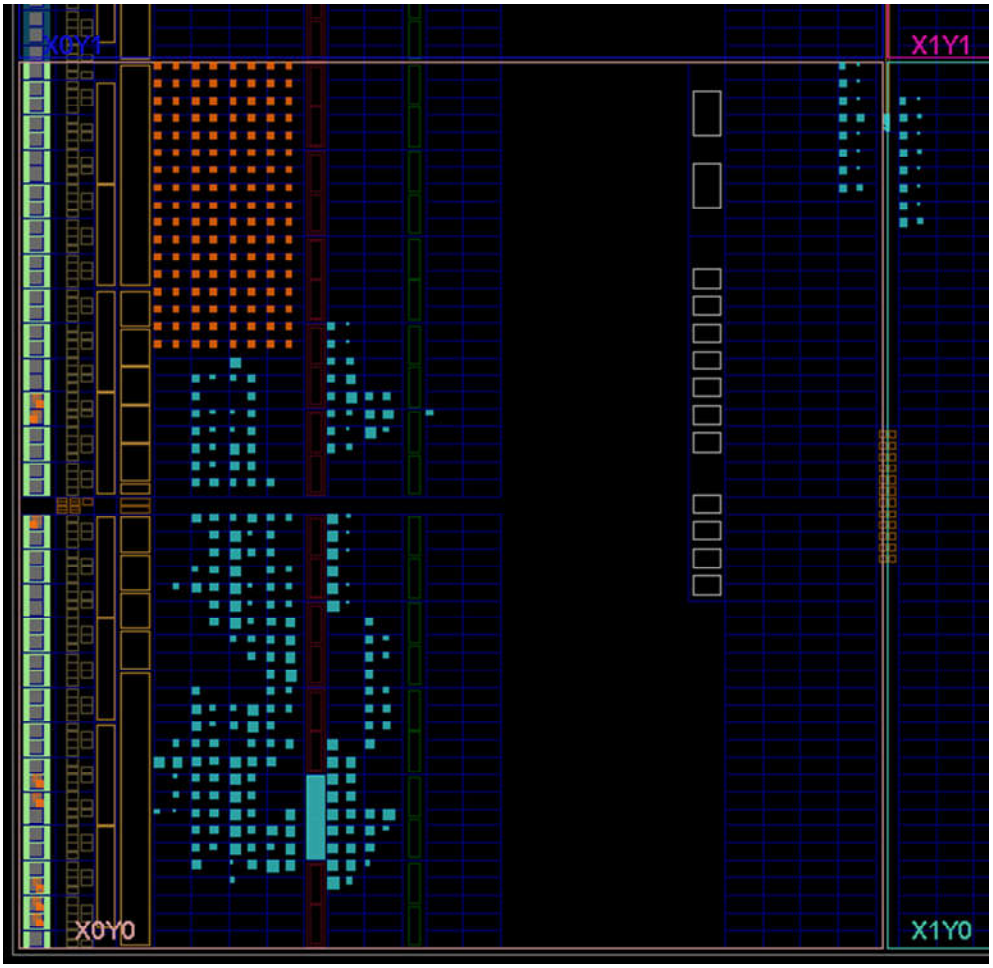
PL1.4. Mạch ổn định chuỗi bit ra RO PUF

Bảng PL1.7: Mức tiêu thụ phần cứng của thiết kế ổn định chuỗi bit ra RO PUF bằng phương pháp cắt bit kết hợp lấy trung bình mẫu tần số hiệu RO thực thi trên FPGA Xilinx Artix-7 XC7A35T

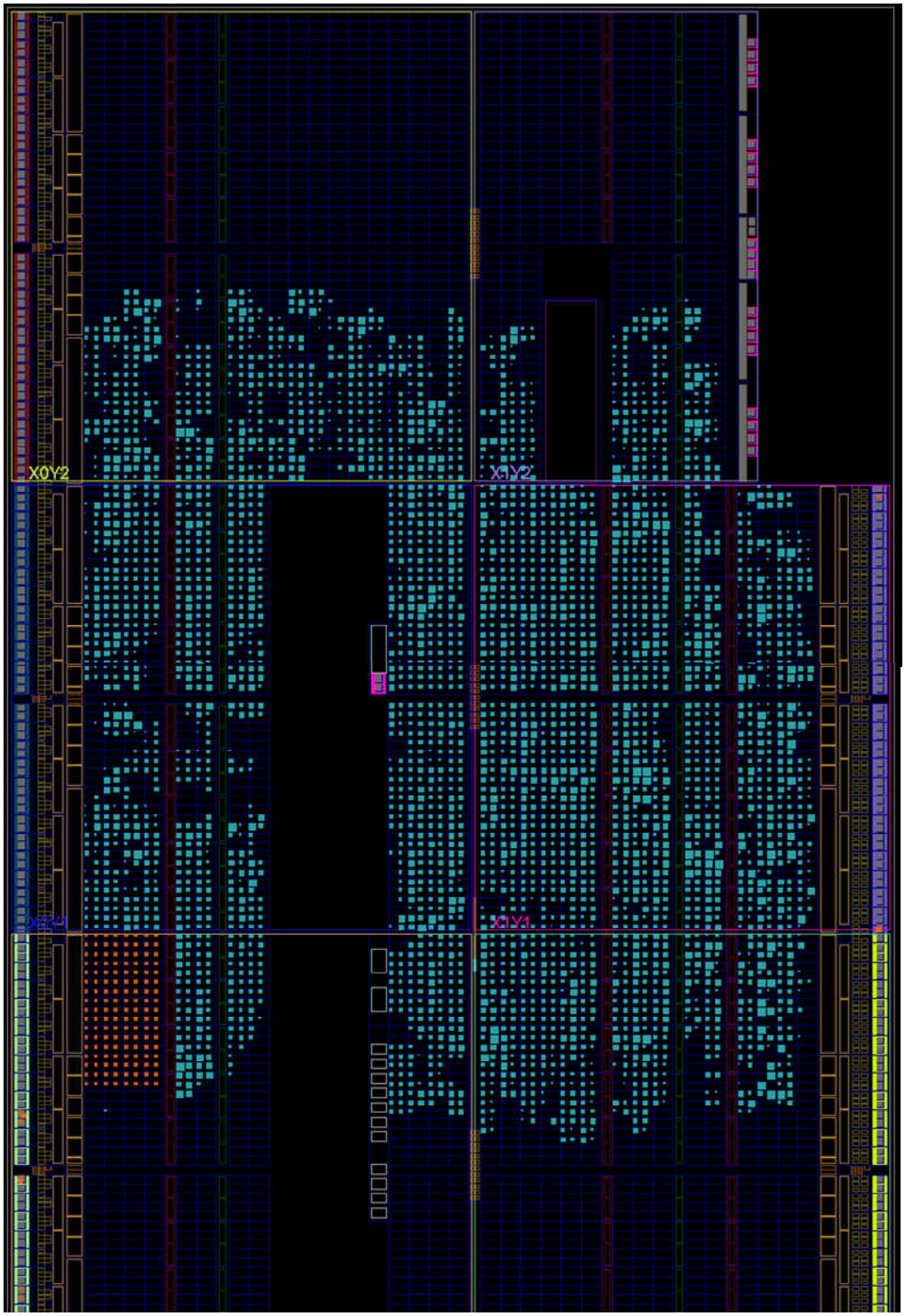
Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
LUT	980	20.800	4,71
FF	630	41.600	1,51
BRAM	1	50	2,00
IO	9	170	5,29

Bảng PL1.8: Mức tiêu thụ phần cứng của thiết kế ổn định chuỗi bit ra RO PUF bằng phương pháp mặt nạ dữ liệu thực thi trên FPGA Xilinx Artix-7 XC7A35T

Tài nguyên	Sử dụng	Khả năng cung cấp	Phần trăm sử dụng [%]
LUT	10.608	20.800	51,00
FF	10.480	41.600	25,19
LUTRAM	256	9.600	2,67
IO	8	170	4,71



Hình PL1.9: Mạch vật lý của thiết kế ổn định chuỗi bit ra RO PUF bằng phương pháp cắt bit kết hợp trung bình mẫu trên FPGA Artix-7



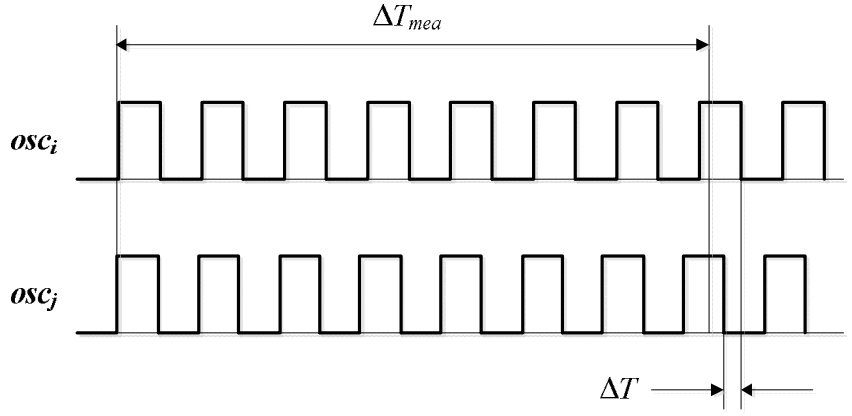
Hình PL1.10: Mạch vật lý của thiết kế ổn định chuỗi bit ra RO PUF bằng phương pháp mặt nạ dữ liệu trên FPGA Artix-7

Phụ lục 2: Ước lượng sai số xác định tần số RO

Gọi f_{i_mea} là tần số đo được của tần số RO_i f_i. f_{i_mea} được xác định bằng cách nhân trị số đếm trong một khoảng thời gian ΔT_{mea} với một hệ số k_{mea} để xác định số chu kỳ dao động tạo bởi mạch RO trong 1 s:

$$f_{i\_mea} = n_{cycle} \times k_{mea} = n_{cycle} \times \frac{1}{\Delta T_{mea}} \quad \text{(PL2.1)}$$

Với n_{cycle} là số chu kỳ dao động RO đếm được trong khoảng ΔT_{mea}.



Hình PL2.1: Giản đồ thời gian mô tả hoạt động của bộ đếm tần số RO

Như được trình bày trên Hình PL2.1, sai số xuất hiện khi hai dao động có tần số khác nhau nhưng lại có cùng trị số đếm gây ra bởi khoảng thời gian ΔT. Giả sử ΔT là biến ngẫu nhiên có phân bố đều trong khoảng $[0, T_i]$, với T_i là chu kỳ của dao động RO tần số f_i. Khi đó, trị số cực đại của sai số đo tần số RO là:

$$\Delta f_{i\_mea\_\max} = \frac{n_{cycle}+1}{\Delta T_{mea}} - \frac{n_{cycle}}{\Delta T_{mea}} = \frac{1}{\Delta T_{mea}} = k_{mea} \quad \text{(PL2.2)}$$

Giả sử sai số tần số đo Δf_{i_mea} có phân bố đều trong khoảng

$\left[0, \Delta f_{i\_mea\_\max}\right]$. Từ [123], có thể ước lượng độ lệch chuẩn của Δf_{i_mea} bởi công thức:

$$\sigma_{\Delta f_{i\_mea}} = \sqrt{\frac{\left(\Delta f_{i\_mea\_\max}\right)^2}{12}} = \frac{\Delta f_{i\_mea\_\max}}{2\sqrt{3}} = \frac{k_{mea}}{2\sqrt{3}} \qquad \text{(PL2.3)}$$

Trong thiết kế cụ thể, chọn $\Delta T_{mea} = 20ms$, $k_{mea} = 50$, xác định được trị số Δf_{i_mea}:

$$\sigma_{\Delta f_{i\_mea}} = \frac{k_{mea}}{2\sqrt{3}} = 14,4\left[Hz\right]$$

Đối với sơ đồ tách ID đề xuất (Hình 3.15), trị số đếm tỷ lệ với tần số hiệu, độ lệch chuẩn của $df_i = f_i - f_{i+1}$ là $\sqrt{2}\sigma_{\Delta f_{i\_mea}}$. Từ các công thức (3.8) và (3.9) có thể thấy khoảng cách Euclid chuẩn hóa tỷ lệ với $\sqrt{n-1}\left(df_i - df_j\right)$. Do đó:

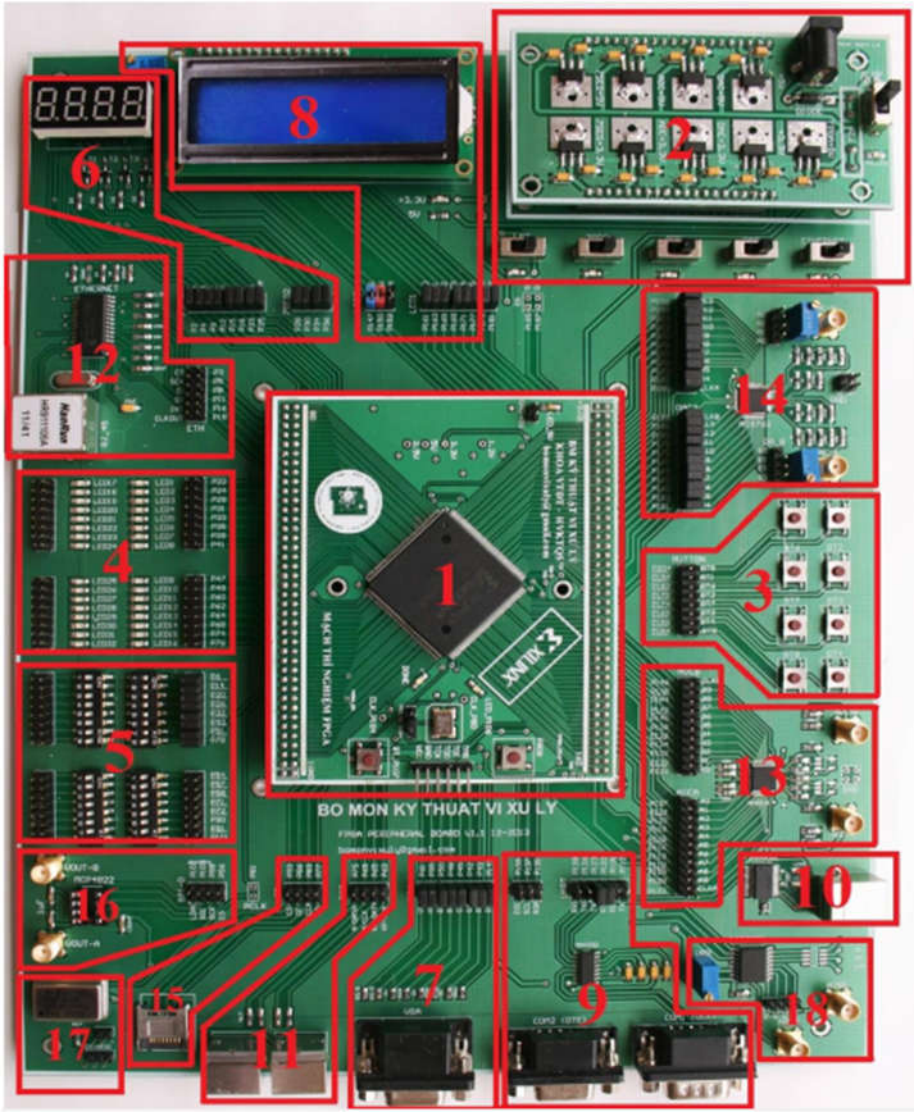
$$\sigma_{\Delta d_{inter}} = \sigma_{\Delta d_{intra}} = \sqrt{n-1}.\sqrt{2}.\frac{\sqrt{2}\sigma_{\Delta f_{i\_mea}}}{2^{k_{norm}}\sqrt{n-1}} = \frac{\sigma_{\Delta f_{i\_mea}}}{2^{k_{norm}-1}} \qquad \text{(PL2.4)}$$

Từ đây xác định được trị số của $\sigma_{\Delta d_{inter}}$ và $\sigma_{\Delta d_{inter}}$ là $1,38\times10^{-5}$ ($k_{norm} = 21$) đối với FPGA Spartan-6 và $2,75\times10^{-5}$ ($k_{norm} = 20$) đối với FPGA Spartan-3E.

Phụ lục 3: Một số thiết bị phục vụ đo đạc, thực nghiệm

PL3.1. Mạch thí nghiệm FPGA Xilinx Spartan-3E

Mạch thí nghiệm FPGA Xilinx Spartan-3E phục vụ việc học tập, nghiên cứu, thực hành và phát triển các ứng dụng trên chip Xilinx Spartan-3E. Mạch gồm ba khối chính: bo mạch chủ, nguồn DC và ngoại vi (Hình PL3.1), trong đó bo mạch chủ có thể tháo rời, thuận tiện cho thay thế, sửa chữa.



Hình PL3.1: Mạch thí nghiệm FPGA Xilinx Spartan-3E

**** Bo mạch chủ (1)***

Bo mạch chủ chứa chip FPGA Xilinx XC3S500E, chip hỗ trợ vào ra XC3S500-5PQG208C, ROM XCF04S (4Mb), bộ tạo dao động 50 MHz.

Tài nguyên chip FPGA Xilinx XC3S500E được trình bày trên Bảng PL3.1.

Bảng PL3.1: Tài nguyên FPGA Xilinx XC3S500E

Số lượng cổng		500.000
Cổng logic tương đương		10476
Ma trận CLB	Hàng	46
	Cột	34
	Tổng số CLB	1164
	Tổng số Slice	4656
RAM phân tán		73KB
RAM khối		360KB
Khối nhân chuyên dụng		20
DCM		4
Cổng vào ra		232
Cổng vào ra vi sai		92

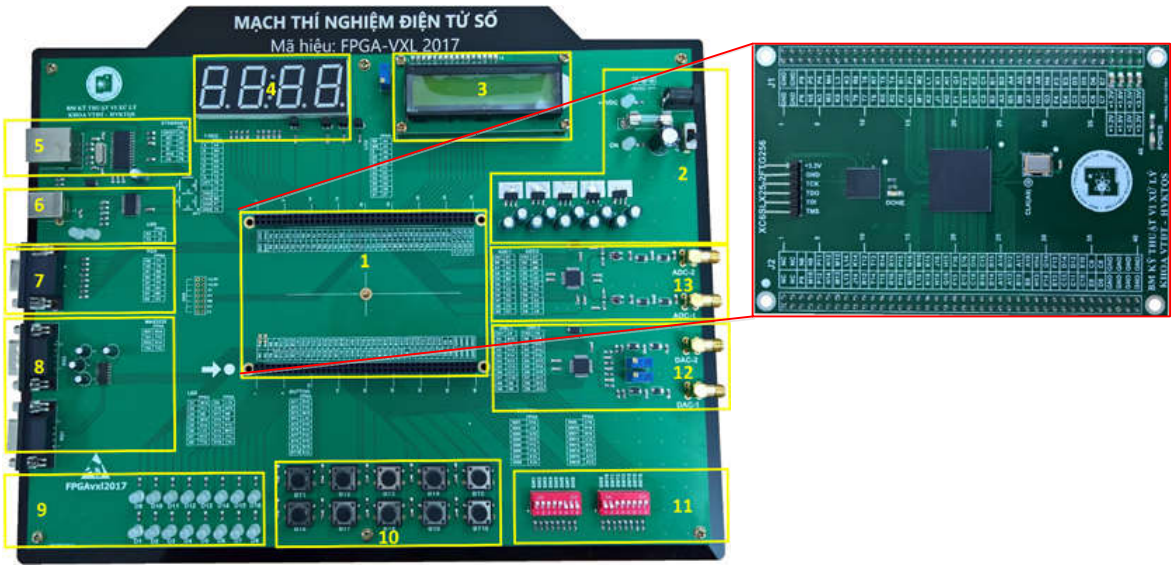
**** Khối nguồn DC (2):*** Được cấp điện áp vào 6-9V DC, tạo các điện áp ra 5V cho bo mạch chủ, 3,3V cho các mạch ngoại vi: LED, 7SEG, Switch, Ethernet, ADC, DAC,…

**** Khối ngoại vi***

Gồm các mạch chức năng phục vụ điều khiển, hiển thị, kiểm tra, truyền số liệu, giao tiếp với mạch ngoài: Bàn phím (8 phím) (3), 4×8 LED (4); Chuyển mạch 4×8 SWITCH (5), 4×7SEG (6), VGA (7), LCD 1602A (8), RS232 (9), PS2 (10), USB-RS232 (11), Ethernet (12), ADC (13), DAC (14), MMC/SD Card (15), I2C (16), 1-Wire (17).

PL3.2. Mạch thí nghiệm FPGA Xilinx Spartan-6

Mạch thí nghiệm FPGA Xilinx Spartan-6 gồm hai mô-đun: FPGA và bo mạch chủ (Hình PL3.2).



Hình PL3.2: Mạch thí nghiệm FPGA Xilinx Spartan-6

**** Mô-đun FPGA (1)***

Mô-đun FPGA là mạch in 8 lớp với chip FPGA Spartan 6 XC6SLX25-2FTG256, Flash ROM XCF08S (8Mb), SMD, khối tạo dao động 50 MHz SMD, sử dụng giao tiếp JTAG 6×1 để nạp cấu hình cho FPGA.

Chip FPGA XC6SLX25-2FTG256 có 24.061 phần tử logic khả trình (logic cells), 38 khối xử lý tín hiệu số (DSP) và 52×18Kb RAM khối (Block RAM); đóng gói 256 chân với 184 chân có thể lập trình; sử dụng nguồn DC 3,3V, 2,5V, 1,8V, 1,2V.

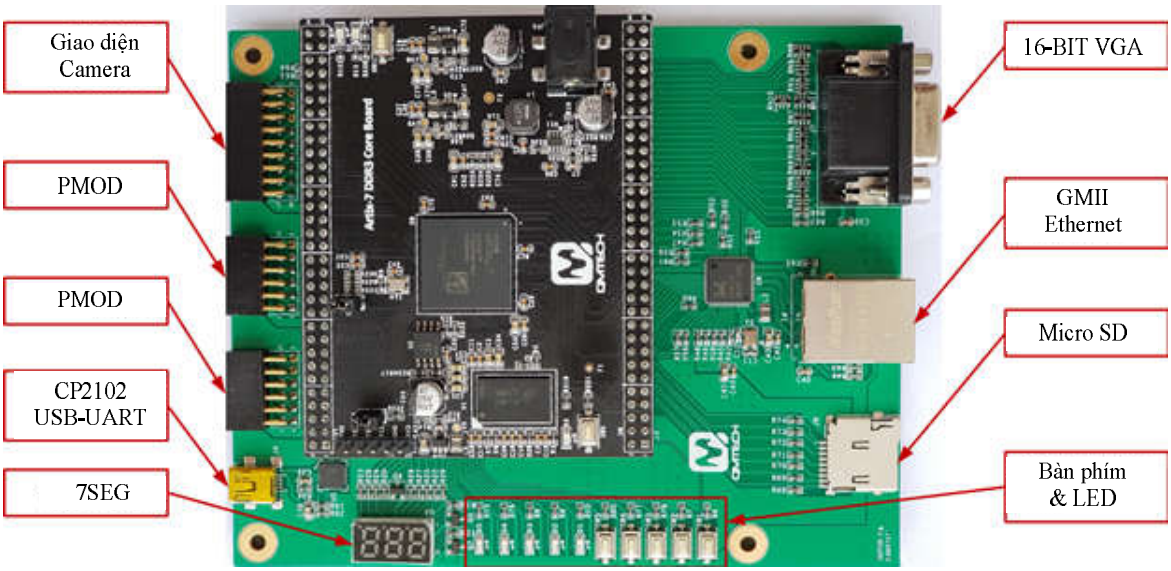
**** Mô-đun bo mạch chủ***

Gồm khối nguồn (2) và các khối chức năng phục vụ điều khiển, hiển thị, giao tiếp: TEXT-LCD (3), 4×7SEG (4), Ethernet (5), USB-RS232 (6), VGA

(7), RS232 (8), 16 LED (9), 10 nút ấn (10), 2×8 chuyển mạch (11), DAC (12), ADC (13).

PL3.3. Mạch thí nghiệm FPGA Xilinx Artix-7

Mạch thí nghiệm FPGA Xilinx Artix-7 (QMTECH ARTIX-7 XC7A35T) phục vụ việc học tập, nghiên cứu, thực hành và phát triển các ứng dụng trên chip Xilinx Artix-7. Mạch gồm bo mạch lõi và bo mạch chủ (Hình PL3.3).



Hình PL3.3: Mạch thí nghiệm FPGA Xilinx Artix-7

**** Bo mạch lõi***

Bo mạch lõi sử dụng chip FPGA Xilinx Artix-7 XC7A35T với bộ xử lý mềm MicroBlaze, 108 chân vào/ra, sử dụng nguồn 3,3V DC, xung nhịp hệ thống 50 MHz, có 2 phím bấm, 3 LED, giao diện JTAG . Chip XC7A35T có tài nguyên phong phú, gồm 33.280 phần tử logic khả trình, RAM khối 1.800 Kb, phù hợp cho việc phát triển các ứng dụng tốc độ cao, tiêu thụ ít năng lượng.

**** Bo mạch chủ***

Bo mạch chủ cung cấp một số giao diện ngoại vi, đáp ứng các yêu cầu khác nhau về kết nối và ứng dụng: Cổng chuyển đổi nối tiếp USB-UART, VGA 16 bit, Ethernet GMII, thẻ nhớ, camera,...

PL3.4. Tủ sấy công nghiệp Memmert UN110

Tủ sấy công nghiệp Memmert UN110 được sử dụng trong nghiên cứu và công nghiệp nhằm sấy khô các mạch điện tử, khử khí trong nhựa epoxy, chuẩn bị mẫu thử,… (Hình PL3.4)

Hình PL3.4: Tủ sấy công nghiệp Memmert UN110

Một số thông số chính của tủ:

- Thể tích: 108 lít;
- Kích thước trong: Rộng 560 × Cao 480 × Sâu 400 mm;
- Kích thước ngoài: Rộng 745 × Cao 864 × Sâu 584 mm;

- Số khay: 5;

- Khoảng nhiệt độ hoạt động: 5^{o}C trên nhiệt độ môi trường đến 300^{o}C;

- Độ chính xác cài đặt: 0,1^{o}C đối với nhiệt độ ≤ 99,9^{o}C, 0,5^{o}C đối với nhiệt độ ≥ 100^{o}C;

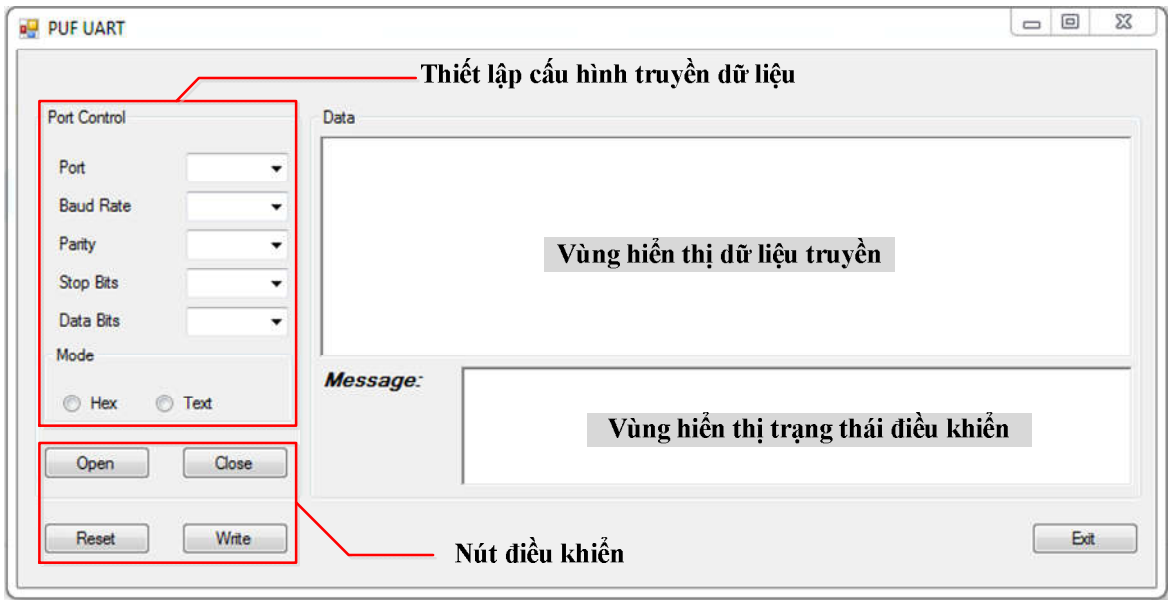
- Sử dụng đầu dò nhiệt Pt100 DIN Class A;

- Đối lưu không khí tự nhiên.

Phụ lục 4: Chương trình truyền số liệu UART

PL4.1. Giới thiệu

Chương trình dùng để giao tiếp với mạch FPGA qua giao diện UART, thu thập dữ liệu và lưu có định kiểu cho xử lý về sau. Chương trình được viết trên Visual Studio 2017, có giao diện như Hình PL4.1.



Hình PL4.1: Giao diện chương trình truyền số liệu UART

PL4.2. Hoạt động

- Kết nối cáp truyền số liệu giữa mạch FPGA và cổng USB của máy tính.

- Cài đặt cổng (*Port*), tốc độ truyền (*Baud Rate*), số bit chẵn lẻ (*Parity*), số bit Stop (*Stop Bits*), định dạng dữ liệu (*Data Bits*)…

- Nhấn *Open* để mở kết nối cổng.

- Kích hoạt mạch FPGA.

- Nhấn *Write* để ghi dữ liệu dưới dạng file **.txt* sau khi việc truyền số liệu hoàn thành.

- Nhấn *Reset* khi cần reset mềm mạch FPGA.