



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN)
CỤC SỞ HỮU TRÍ TUỆ

(11)



1-0034677

(51)^{2020.01} G06F 21/30; G06F 21/44

(13) B

(21) 1-2020-05234

(22) 11/09/2020

(45) 25/01/2023 418

(43) 26/07/2021 400

(76) 1. Trịnh Quang Kiên (VN)

Khoa Vô tuyến Điện tử - Học viện Kỹ thuật Quân Sự, 236 Hoàng Quốc Việt, Quận Bắc Từ Liêm, Hà Nội

2. Trần Văn Toàn (VN)

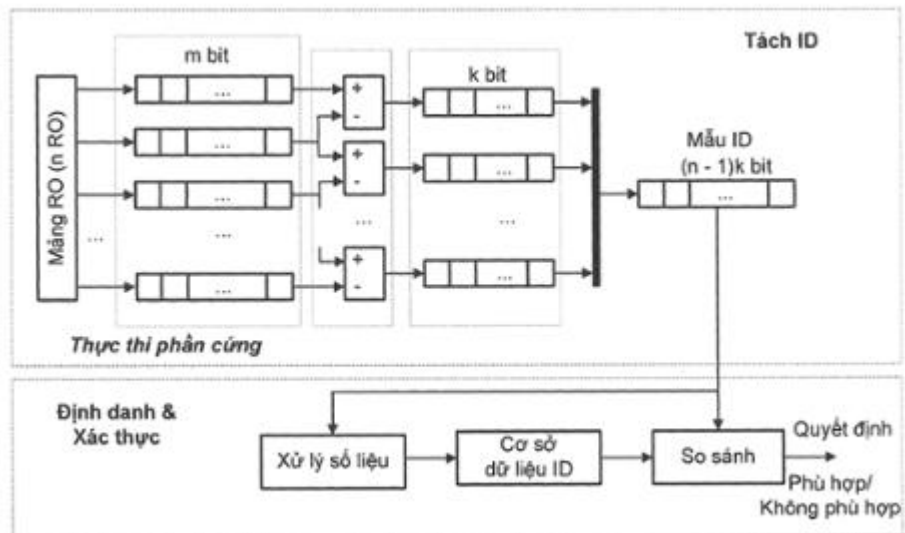
Khoa Vô tuyến Điện tử-Học viện Kỹ thuật Quân sự, 236 Hoàng Quốc Việt, Hà Nội

3. Hoàng Văn Phúc (VN)

Viện Tích hợp hệ thống-Học viện Kỹ thuật Quân sự, 236 Hoàng Quốc Việt, Hà Nội.

(54) 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)

(57) Sáng chế đề xuất mạch tạo hàm không thể sao chép về vật lý (PUF) trên FPGA (Field Programmable Gate Array - Mảng cổng logic lập trình được ở cấp độ người dùng) sử dụng bộ dao động vòng và tham số khoảng cách Euclid và ứng dụng trong xác thực vi mạch, chống giả mạo IC và bảo mật các thiết bị điện tử. Cấu tạo của PUF bao gồm: khối các hard macro (thiết kế mẫu) dao động vòng đồng nhất, bộ ghép kênh (MUX) được điều khiển bởi các tín hiệu định thời, mạch đo tần số dao động vòng dựa trên bộ đếm, mạch truyền/nhận dữ liệu *UART* (Giao diện truyền dữ liệu nối tiếp không đồng bộ), mạch tạo tín hiệu điều khiển. Sáng chế cũng đề xuất phương pháp tách và xác thực ID cho vi mạch ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF) trên FPGA sử dụng bộ dao động vòng và tham số khoảng cách Euclid nêu trên. Trong đó, từ kết quả phân tích định lượng ảnh hưởng của các biến thiên cục bộ, tiến hành trích xuất ID cho IC dựa trên độ đo khoảng cách Euclid và xác định mức ngưỡng dùng để xác thực vi mạch. Hai mẫu ID có khoảng cách chuẩn hóa nhỏ hơn mức ngưỡng sẽ được xem là thuộc về cùng một vi mạch. Ngược lại, nếu khoảng cách chuẩn hóa giữa hai mẫu ID lớn hơn mức ngưỡng, chúng sẽ được coi là thuộc về hai vi mạch khác nhau. Sáng chế cũng đề xuất quy trình xác thực định danh (ID - Identification) cho mạch tích hợp (IC - integrated circuit) ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF) này. Thực nghiệm phương pháp xác thực trên nhiều vi mạch thể hiện tính ổn định cao.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới quy trình xác thực định danh (ID) cho mạch tích hợp sử dụng mạch tạo hàm không thể sao chép về vật lý (PUF - *Physically Unclonable Functions*), ứng dụng trong định danh và xác thực vi mạch, chống giả mạo chip và bảo mật các thiết bị điện tử.

Tình trạng kỹ thuật của sáng chế

Sự phát triển nhanh chóng của công nghệ vi điện tử, bán dẫn và chế tạo mạch tích hợp (IC - *Integrated Circuit*) trong những năm gần đây đặt ra vấn đề bảo vệ bản quyền và xác thực cho các IC, cũng như bảo vệ an ninh, an toàn cho thiết bị và dữ liệu. Các mạch tạo hàm không thể sao chép về vật lý (PUF - *Physically Unclonable Functions*) là một kỹ thuật hiệu quả của bảo mật phần cứng, có triển vọng ứng dụng rộng rãi trong định danh (ID - *Identification*), xác thực (*Authentication*) cũng như chống các hình thức tấn công nhằm vào thiết bị trong môi trường số. Thiết kế PUF được thực thi trên thiết bị bởi các thực thể PUF (*PUF instances*). Thực thể PUF cho phép tạo ra giá trị phụ thuộc vào cấu trúc vật lý cụ thể gây ra bởi các thăng giáng ngẫu nhiên xuất hiện trong quá trình chế tạo. PUF vì vậy có thể xem là duy nhất, đặc trưng cho thiết bị, được coi như vân tay của chip. Khi tác động một kích thích (*challenge*) ở đầu vào, thực thể PUF sẽ tạo dữ liệu đáp ứng (*respond*) ở đầu ra có dạng ngẫu nhiên với các tham số thống kê đặc trưng. Do đó ID tạo ra trên cơ sở PUF có tính duy nhất, đảm bảo tính khách quan, độc lập ngay cả với nhà sản xuất và khó có thể làm giả.

Các sơ đồ PUF dạng dao động vòng (RO-PUF) trên FPGA (Field Programmable Gate Array - Mảng cổng logic lập trình được ở cấp độ người dùng) được sử dụng phổ biến bởi độ tin cậy (*reliability*) và tính duy nhất (*uniqueness*) cao, dễ dàng trong thực thi phần cứng. Tuy nhiên, các thiết kế truyền thống sử dụng RO-PUF thường tiêu tốn nhiều tài nguyên phần cứng, tần số mạch dao động vòng (RO) nhạy với điều kiện hoạt động cũng như các biến thiên toàn cục khác. Ngoài ra, các biến thiên cục bộ có tính tương quan cao, dẫn đến yêu cầu phải có các thuật toán phức tạp nhằm tách ra thông tin định danh thiết bị cũng như phải sử dụng số lượng lớn các RO.

Các sơ đồ truyền thống dựa trên thiết kế RO-PUF cơ bản được đề xuất năm 2007 bởi Suh và Devadas với một số biến đổi nhằm tăng tính linh hoạt trong việc điều chỉnh tham số mạch giữ chậm trong RO. Tuy nhiên, các thay đổi này làm phức tạp đáng kể thiết kế do việc sử dụng các bộ ghép kênh (MUX - *Multiplexer*) bổ sung, trong khi không cải thiện về căn bản đặc tính đáp ứng đầu ra cũng như phương pháp ước lượng phẩm chất của mạch và

phương pháp xác thực thiết bị. Về phương pháp tạo ID (phương pháp xử lý số liệu), các thiết kế RO-PUF truyền thống sử dụng phương pháp so sánh ghép cặp hoặc so sánh ghép cặp liên tiếp, tương ứng số bit ID tạo ra là $n/2$ hoặc $n - 1$, với n là số lượng RO trong thiết kế. Các cách tiếp cận này ngoài ưu thế về tính đơn giản thì không khai thác đầy đủ các thông tin cũng như tách ra toàn bộ đặc tính của tập n tần số ngẫu nhiên. Về phương pháp xác thực ID, các thiết kế truyền thống sử dụng tham số độ đo khoảng cách Hamming, hiệu quả xác thực không cao, thể hiện ở việc xuất hiện các trường hợp không thể phân biệt được thiết bị và yêu cầu phải có số lượng lớn các RO trong thiết kế.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là khắc phục những hạn chế của các giải pháp trước đây. Do đó, sáng chế đề xuất một thiết kế PUF thực thi trên FPGA gọn nhẹ và phương pháp tách, xác thực ID cho IC hiệu quả.

Ở mức mạch vật lý, sáng chế đề xuất việc sử dụng thiết kế RO đơn giản, có tính đồng nhất cao dựa trên kỹ thuật sử dụng hard macro (các thiết kế mẫu) và các mạch hỗ trợ (ước lượng tần số, truyền dữ liệu...). Kỹ thuật hard macro được hỗ trợ bởi trình thiết kế FPGA Editor/Xilinx ISE. Thiết kế vì vậy có tính gọn nhẹ, dễ dàng thực thi trên bất kỳ linh kiện FPGA từ bất kỳ nhà cung cấp nào chỉ với những điều chỉnh nhỏ. Dựa trên việc phân tích thống kê các số liệu thực nghiệm, nhóm tác giả đã chứng minh tần số các RO chịu ảnh hưởng lớn từ các nhân tố biến thiên toàn cục và do đó không thể được sử dụng trực tiếp để tách ID cho cấu kiện. Ngược lại, các thành phần tần số gây nên bởi các biến thiên cục bộ từ quá trình chế tạo bên trong một chip lại khá ổn định với mọi điều kiện hoạt động và có thể được sử dụng để tách ra ID duy nhất.

Ngoài ra, sáng chế còn đề xuất sơ đồ xác thực ID sử dụng RO-PUF phù hợp cho cả việc xử lý trực tiếp (*on-chip processing*) và xử lý hậu kỳ (*off-chip post processing*), trong đó tác động của các biến thiên toàn cục và điều kiện hoạt động bị loại trừ. Sơ đồ này cho phép khai thác đầy đủ các đặc tính biến thiên cục bộ bằng việc sử dụng mạch PUF độc lập với công nghệ và nhà cung cấp. Thêm vào đó, mạch tách ID được giữ đơn giản và nhỏ gọn, thiết kế tổng thể hiệu quả về diện tích và năng lượng. Đặc biệt, việc định lượng sự khác biệt giữa các ID không sử dụng khoảng cách nhị phân (Hamming) mà sử dụng khoảng cách vector đa chiều Euclid. Từ n RO tách ra $n - 1$ trị số tần số hiệu giữa các cặp tần số RO liên tiếp $\delta_i = f_i - f_{i+1}$, $i = \overline{1, n-1}$. Thông tin tách ra có tính đầy đủ hơn do mỗi ID được biểu diễn bởi một vector $n - 1$ chiều, mỗi tọa độ là một trị số k bit dạng bù 2. Sơ đồ đề xuất thể hiện phương pháp xác thực tin cậy ngay với một số lượng RO nhỏ, do đó đạt hiệu quả cao về diện tích và công suất tiêu thụ của mạch. Các kết quả thực nghiệm thể hiện tính ổn định cao (99,94%) với thiết kế 32 RO trên các chip FPGA khác nhau.

Theo một phương án, sáng chế đề xuất mạch tạo hàm không thể sao chép về vật lý (PUF - *Physically Unclonable Functions*) sử dụng bộ dao động vòng và tham số khoảng cách Euclid, mạch PUF này có cấu tạo bao gồm:

mảng RO gồm n RO có cấu trúc vật lý đồng nhất được xây dựng trên FPGA (Field Programmable Gate Array - *Mảng cổng logic lập trình được ở cấp độ người dùng*), trong đó:

phần tử giữ chậm (bộ đảo) của RO được xây dựng trên một LUT nguyên mẫu (LUT primitive). LUT (Look-Up Table) là cấu trúc phần cứng của FPGA dùng để tạo các hàm logic dựa trên kỹ thuật bảng tra, việc sử dụng LUT nguyên mẫu đảm bảo độ tin cậy và đồng nhất của các bộ đảo, nhờ đó đảm bảo độ trễ đồng nhất và có thể kiểm soát;

mỗi RO gồm 2^N bộ đảo và một cổng NAND, để đảm bảo cấu trúc mạch vật lý đồng nhất của các RO, các bộ đảo và cổng NAND được kết nối thủ công sử dụng phần mềm FPGA Editor, sau đó được đóng gói thành một khối thiết kế sẵn (Hard macro);

mỗi mảng RO khi được kích hoạt tạo ra n dao động dạng xung nhịp (clock), trị số đếm mỗi dao động này trong một khoảng thời gian có dạng dữ liệu m bit, tỷ lệ với tần số RO, n trị số m bit được ghép cặp liên tiếp, tạo ra $n - 1$ cặp số m bit;

(hai) bộ ghép kênh $(2^N - 1):1$ tuần tự chọn dao động của các cặp RO liên tiếp đưa tới hai bộ đếm m bit tương ứng;

(hai) bộ đếm tần số RO m bit đếm số chu kỳ dao động RO trong một đơn vị thời gian;

bộ cộng/trừ m bit tạo trị số hiệu dạng dữ liệu k bit từ dữ liệu đếm các bộ đếm tần số RO;

mạch truyền/nhận dữ liệu UART (Giao diện truyền dữ liệu nối tiếp không đồng bộ) truyền dữ liệu PUF từ mạch tới PC cũng như nhận tín hiệu tái lập (Reset) từ PC, dữ liệu truyền $(k + p)$ bit gồm k bit trị số hiệu và p bit điều khiển – báo hiệu – kiểm tra;

mạch tạo tín hiệu điều khiển tạo tín hiệu điều khiển, đồng bộ, báo hiệu phục vụ hoạt động chức năng của hệ thống theo chương trình đã lập, mạch tạo tín hiệu điều khiển gồm các bộ chia tần, bộ tạo xung vuông, bộ đếm tạo xung, mạch khử rung phím bấm.

Theo một phương án khác, sáng chế đề xuất quy trình xác thực ID cho IC ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF) sử dụng bộ dao động vòng và tham số khoảng cách Euclid theo điểm 1, quy trình này gồm hai pha: pha định danh (Identification) và pha xác thực (Authentication), trong đó:

pha định danh gồm các bước:

tạo ID danh định: trên PC, thực hiện tách ra k bit trị số tần số hiệu từ dữ liệu truyền ($k + p$) bit, tập $(n - 1)$ trị số k bit tương ứng $(n - 1)$ cặp RO được ghép liên tiếp nhau, tạo mẫu ID có dạng $(n - 1)k$ bit, mỗi lần kích hoạt mạch tách ID tạo ra một mẫu ID, tập các mẫu ID được lưu trữ trong bộ nhớ máy tính, ID danh định của IC có dạng $(n - 1)k$ bit, là một vector $(n - 1)$ chiều, mỗi chiều/tọa độ là một trị số k bit được tính trung bình thống kê từ tập các giá trị k bit của tọa độ tương ứng của vector ID mẫu, các ID danh định được lưu trong cơ sở dữ liệu ID (ID Database);

tạo mức ngưỡng, trong đó:

với mỗi tập dữ liệu tương ứng một IC, tiến hành tính khoảng cách Euclid chuẩn hóa (khoảng cách nội chuẩn hóa - *normalized intra-distance*) theo công thức (2) dưới đây giữa vector ID mẫu và vector ID danh định, từ đó xác định độ lệch chuẩn trong phân bố của tập khoảng cách này, mức ngưỡng dùng cho xác thực IC này được chọn bằng 06 lần độ lệch chuẩn trong phân bố khoảng cách nội đã tính,

$$d_{intra} = \frac{d(\mathbf{R}_I, \mathbf{R})}{2^{k_{norm}} \sqrt{n - 1}} \quad (2)$$

trong đó $d(\mathbf{R}_I, \mathbf{R}_j) = \sqrt{\sum_{k=1}^{n-1} (\delta_{ik} - \delta_{jk})^2}$ là khoảng cách Euclid giữa hai vector $\mathbf{R}_I$, $\mathbf{R}_j$ trong giải tích cổ điển; $\mathbf{R}_I$ là vector mẫu ID của lần đo thứ 1, $\mathbf{R}$ là vector ID danh định của IC; k_{norm} là hệ số chuẩn hóa,

từ tập các mức ngưỡng riêng tương ứng các IC được khảo sát, xác định giá trị cực đại và chọn làm mức ngưỡng chung,

tính khoảng cách giữa các ID danh định và so sánh với mức ngưỡng chung đã tính, nếu khoảng cách nhỏ nhất giữa các ID danh định lớn hơn mức ngưỡng chung, mức ngưỡng này được chấp nhận trong xác thực IC và được lưu vào cơ sở dữ liệu ID,

pha xác thực gồm bước:

kết hợp mẫu ID của một IC bất kỳ một cách tuần tự với các ID danh định trong cơ sở dữ liệu ID và tạo dữ liệu khoảng cách Euclid theo công thức (2), sau đó, bộ so sánh (Comparator) 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 được đăng ký.

Mục đích của sáng chế được thực hiện nhờ cấu trúc PUF và phương pháp tách, xác thực ID hiệu quả.

Mô tả vắn tắt các hình vẽ

Hình 1: Sơ đồ chức năng của mạch tách và xác thực ID sử dụng RO-PUF.

Hình 2: Sơ đồ chức năng chi tiết của mạch tách và xác thực ID sử dụng RO-PUF.

Hình 3: Sơ đồ mạch vật lý của thiết kế.

Hình 4: Biểu đồ phân bố tần số hiệu của một cặp RO cụ thể tại một nhiệt độ cố định và trên toàn dải nhiệt độ khảo sát.

Hình 5: Đồ thị thể hiện đặc tính ổn định của ID tương ứng 6 IC đối với sự thay đổi của nhiệt độ môi trường.

Hình 6: Biểu đồ phân bố khoảng cách nội chuẩn hóa của IC1 cho 255 mẫu.

Hình 7: Minh họa tính ổn định của sơ đồ xác thực

Mô tả chi tiết sáng chế

Hình 1 thể hiện sơ đồ chức năng mạch tách và xác thực ID sử dụng RO-PUF. Mảng RO gồm n RO có cấu trúc vật lý đồng nhất, khi được kích hoạt tạo ra n dao động dạng xung nhịp (clock). Trị số đếm các dao động này trong một khoảng thời gian xác định (trong thiết kế cụ thể là 20 ms) là số m bit, tỷ lệ với tần số RO. n số m bit được ghép cặp liên tiếp, tạo ra $n - 1$ cặp số m bit. Mỗi cặp số này được đưa tới đầu vào bộ trừ tương ứng, tạo dữ liệu hiệu k bit. Dữ liệu ra các bộ trừ được ghép liên tiếp nhau, tạo ID có dạng $(n - 1)k$ bit. Mỗi lần kích hoạt mạch tách ID tạo ra một mẫu ID. Tập các mẫu ID được lưu trữ và tách ra ID danh định cho IC. Pha định danh (Identification) tạo các ID danh định cho các IC cũng như xác định mức ngưỡng và lưu trong cơ sở dữ liệu ID (ID Database). Trong pha xác thực (Authentication), 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 (Comparator) 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 2 thể hiện sơ đồ chức năng chi tiết mạch tách và xác thực ID sử dụng RO-PUF xây dựng trên FPGA. Sáng chế có thể áp dụng cho thiết kế vi mạch trên nền tảng bất kỳ. Tuy nhiên, thiết kế cụ thể của sáng chế được thực thi trên vi mạch khả trình FPGA loại Xilinx Spartan 3, với $n = 32$, $m = 24$, $k = 24$. FPGA (Field Programmable Gate Array) là công nghệ vi mạch khả trình cho phép thiết kế logic số từ cấp độ người dùng, tạo sự linh hoạt với các ứng dụng cụ thể. Phần tử giữ chậm (bộ đảo) của RO được xây dựng trên một LUT nguyên mẫu (LUT primitive). LUT (Look-Up Table) là cấu trúc phần cứng của FPGA dùng để tạo các hàm logic dựa trên kỹ thuật bảng tra. Việc sử dụng LUT nguyên mẫu đảm

bảo độ tin cậy và đồng nhất của các bộ đảo, nhờ đó đảm bảo độ trễ đồng nhất và có thể kiểm soát. RO gồm 2^N bộ đảo ($N = 4$) và một cổng NAND. Theo trình tự thiết kế thông thường, việc kết nối vật lý bên trong IC (routing) được thực hiện tự động trong quá trình tối ưu hóa (optimization), theo đó các RO có thể khác nhau về độ trễ và do đó vi phạm thiết kế PUF về ý tưởng. Để đảm bảo cấu trúc mạch vật lý đồng nhất của các RO, các bộ đảo và cổng NAND được kết nối thủ công sử dụng FPGA Editor, sau đó được đóng gói thành một khối hard macro (tương ứng với một RO) trên FPGA. 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 PC được thực hiện bằng giao diện truyền dữ liệu nối tiếp không đồng bộ UART (Universal Asynchronous Receiver-Transmitter).

Hình 3 là sơ đồ mạch vật lý (layout) của thiết kế. Các RO macro được gán địa chỉ và kết nối thủ công, đảm bảo độ trễ đồng nhất. Thiết kế có thể thực thi linh hoạt trên các họ FPGA với chỉnh sửa phù hợp.

Hình 4 là biểu đồ phân bố tần số hiệu của một cặp RO cụ thể tại một nhiệt độ cố định và trên toàn dải nhiệt độ khảo sát. Tần số hiệu của các cặp RO liên tiếp được sử dụng để tách ID đặc trưng cho IC dựa trên khảo sát dưới đây.

Vấn đề chính trong việc sử dụng các sơ đồ RO-PUF vào định danh và xác thực là tính nhạy của chúng đối với sự thay đổi của nhiệt độ môi trường. Điều này làm cho các đáp ứng của RO-PUF không ổn định và do đó không thể sử dụng chúng trực tiếp. Tần số RO có thể được mô hình hóa bởi biểu thức:

$$f_{RO} = f_{nominal} + \Delta f_{proc,global} + \Delta f_{proc,local} + \Delta f_{OP} \quad (1)$$

Trong đó, $f_{nominal}$ là tần số RO danh định (là tần số đo được khi thiết bị danh định vận hành ở điều kiện danh định, trong trường hợp này tương ứng nhiệt độ môi trường 25°C và điện áp lõi FPGA 1V). 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 (1) là các biến ngẫu nhiên; $\Delta f_{proc,global}$ và $\Delta f_{proc,local}$ tương ứng là các biến thiên tần số tương ứng gây ra bởi biến thiên toàn cục (thay đổi giữa các IC) và biến thiên cục bộ (thay đổi bên trong một IC); Δf_{OP} là là thăng giáng ngẫu nhiên của tần số RO xung quanh giá trị danh định ở điều kiện hoạt động cố định (temporal variation). Khi ổn định điện áp lõi FPGA, biến thiên toàn cục chủ yếu là nhiệt độ môi trường. Biến thiên cục bộ là những khác biệt trong các tham số vật lý cấu kiện bán dẫn, gây ra bởi những thăng giáng ngẫu nhiên xuất hiện trong quá trình chế tạo.

Kết quả thực nghiệm cho thấy:

- i) Δf_{OP} nhỏ và có thể bỏ qua;
- ii) $\Delta f_{proc,global}$ thay đổi đáng kể khi nhiệt độ môi trường thay đổi, làm f_{RO} giảm khi nhiệt độ tăng và ngược lại.
- iii) $\Delta f_{proc,local}$ tương đối ổn định khi nhiệt độ môi trường thay đổi.

Do đó, chỉ có thể tạo ID cho thiết bị từ $\Delta f_{proc,local}$, trong thiết kế cụ thể ứng dụng RO-PUF này là các hiệu tần số của các cặp RO liên tiếp.

Tính ổn định (reliability) tần số hiệu của cặp RO (ROp – RO pair) được xác định bởi hệ thức $1 - \sigma/\mu$ [%], với μ là giá trị trung bình thống kê (trung bình theo trọng số), σ là độ lệch chuẩn. Tính ổn định càng cao khi σ/μ càng nhỏ và ngược lại. Số liệu thực nghiệm cho thấy mạch RO-PUF có tính ổn định cao (lớn hơn 95%) trong cả hai trường hợp, khi hoạt động trong điều kiện nhiệt độ môi trường không đổi và trên toàn dải nhiệt độ làm việc thông thường của thiết bị (Từ nhiệt độ phòng đến dưới 100°C). Hình 4 (a) tương ứng tính ổn định $\approx 98,2626$ %, hình 4 (b) – 97,1192%. Tập mẫu khảo sát tương ứng là 255 mẫu và 3060 mẫu.

Hình 5 là đồ thị thể hiện đặc tính ổn định của ID tương ứng 6 IC đối với sự thay đổi của nhiệt độ môi trường. Ở dạng dữ liệu tần số, ID của thiết bị là một vector $n - 1$ chiều $R(\{\delta_i | i = \overline{1, n - 1}\})$, trong đó $\delta_i = f_i - f_{i+1}$ là độ lớn của gia số tần số thứ i , là trị số k bit dạng bù 2. Mỗi vector ID được biểu diễn bằng một đường zig-zag có hoành độ rời rạc là chỉ số cặp RO (1 – 31). Tập hợp các mẫu ID trung bình (của 255 lần đo) tại các điểm nhiệt độ môi trường (25°C – 80°C, bước nhảy 5°C) tương ứng một IC được thể hiện trên cùng một đồ thị thành phần (subplot) của đồ thị hình 5. Có thể thấy các đường này rất gần nhau và có dạng xác định. Các nhóm đường zig-zag tương ứng các IC khác nhau có dạng khác nhau và đặc trưng cho thiết bị.

Để định lượng sự tương đồng/khác biệt giữa các vector mẫu ID, nhóm tác giả đưa vào các tham số khoảng cách dựa trên độ đo Euclid sau. Với mỗi tập dữ liệu tương ứng một IC, tiến hành tính khoảng cách Euclid chuẩn hóa (khoảng cách nội chuẩn hóa - normalized intra-distance) theo công thức (2) dưới đây giữa vector ID mẫu và vector ID danh định.

Khoảng cách nội chuẩn hóa (*normalized intra-distance*):

$$d_{intra} = \frac{d(R_i, R)}{2^{k_{norm}} \sqrt{n - 1}} \quad (2)$$

Trong đó $d(R_i, R_j) = \sqrt{\sum_{k=1}^{n-1} (\delta_{ik} - \delta_{jk})^2}$ là khoảng cách Euclid giữa hai vector R_i , R_j trong giải tích cô điển;

n là số RO trong mảng RO,

δ_{ik} , $k = \overline{1, n - 1}$, là tọa độ thứ k của vector R_i ,

R_l là vectơ mẫu ID của lần đo thứ l ,

R là vectơ ID danh định của IC,

k_{norm} là hệ số chuẩn hóa, dùng để chuẩn hóa khoảng cách $d(R_l, R)$ về trị số nằm trong khoảng $(0, 1)$;

từ đó xác định độ lệch chuẩn trong phân bố của tập khoảng cách này, mức ngưỡng dùng cho xác thực IC này được chọn bằng 06 lần độ lệch chuẩn trong phân bố khoảng cách nội chuẩn hóa đã tính,

Khoảng cách tương quan chuẩn hóa (*normalized inter-distance*):

$$d_{inter} = 1 - \sum_{i,j} \frac{2d(R_i, R_j)}{N(N-1)2^{k_{norm}}\sqrt{n-1}} \quad (3)$$

Với N là số các IC trong tập các IC được khảo sát.

Hình 6 là biểu đồ phân bố khoảng cách nội chuẩn hóa của một IC cho 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.

Phân tích thống kê khoảng cách nội chuẩn hóa của các mẫu ID so với các ID danh định tương ứng cho phép xác định mức ngưỡng chung d_{thr} , phục vụ xác thực IC. Nếu một mẫu ID có khoảng cách tới ID danh định tính theo công thức (2) nhỏ hơn d_{thr} , mẫu ID này sẽ được coi là thuộc về IC hoặc phần cứng đã được đăng ký. Nếu khoảng cách này lớn hơn d_{thr} , IC sẽ được xem là chưa được đăng ký.

Khoảng cách d_{inter} và d_{intra} được sử dụng để tính toán mức ngưỡng d_{thr} . d_{thr} cần bao trùm khoảng phân bố chính của d_{intra} mỗi ID danh định, nhưng cần nhỏ hơn d_{inter} giữa các ID danh định. Do đó, d_{thr} được chọn bằng 6 lần độ lệch chuẩn cực đại trong phân bố của d_{intra} . Điều này đảm bảo xác suất để 1 mẫu ID bị xác thực nhầm xấp xỉ $1/(0,5 \times 10^9)$ hay 2×10^{-9} . Phân tích thống kê d_{inter} giữa các cặp IC trong tập các IC khảo sát cho thấy, khoảng cách nhỏ nhất giữa các ID danh định lớn hơn khoảng 6 lần d_{thr} , đảm bảo tính ổn định của sơ đồ xác thực.

Hình 7 minh họa độ tin cậy xác thực PUF. Xác suất xác thực nhầm được đặc trưng bởi diện tích hình giới hạn bởi đường PUF1, đường ngưỡng $d_{thr} = 6\sigma_{intra1}$ và trục hoành. Giá trị này xấp xỉ 2×10^{-9} .

Nguyên lý tách và xác thực ID trên cùng kết quả thực nghiệm được trình bày chi tiết trong báo cáo "Enhanced ID Authentication Scheme Using FPGA-Based Ring Oscillator PUF." - *IEEE 13th International Symposium on Embedded Multicore/Many-core Systems-on-Chip (MCSoc)* 01-04/10/2019 (DOI: [10.1109/MCSoc.2019.00052](https://doi.org/10.1109/MCSoc.2019.00052)).

Hiệu quả đạt được bởi sáng chế

- Nhờ sử dụng kỹ thuật LUT nên có thể thực thi được thiết kế RO-PUF có độ đồng nhất trong cấu trúc vật lý cao.
- Nhờ sử dụng tần số hiệu nên loại trừ được ảnh hưởng biến thiên nhiệt độ lên đáp ứng đầu ra của RO-PUF.
- Nhờ sử dụng biên độ thay cho hàm dấu trong xử lý dữ liệu PUF trước đây nên khai thác được nhiều thông tin hơn trong dữ liệu PUF với cùng số lượng các RO được sử dụng, giữ cho thiết kế nhỏ gọn với số lượng hạn chế các RO cần dùng, đạt hiệu quả về năng lượng tiêu thụ và diện tích silicon.
- Nhờ sử dụng khoảng cách Euclid thay cho khoảng cách Hamming nhị phân để định lượng các độ đo ID nên có thể sử dụng toàn bộ các 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.

YÊU CẦU BẢO HỘ

1. Quy trình xác thực định danh (ID - Identification) cho mạch tích hợp (IC - integrated circuit) ứng dụng mạch tạo hàm không thể sao chép về vật lý (PUF - *Physically Unclonable Functions*) sử dụng bộ dao động vòng và tham số khoảng cách Euclid, mạch PUF này có cấu tạo bao gồm:

mảng RO gồm n RO có cấu trúc vật lý đồng nhất được xây dựng trên FPGA (Field Programmable Gate Array - Mảng cổng logic lập trình được ở cấp độ người dùng), trong đó:

phần tử giữ chậm (bộ đảo) của RO được xây dựng trên một LUT nguyên mẫu (LUT primitive). LUT (Look-Up Table) là cấu trúc phần cứng của FPGA dùng để tạo các hàm logic dựa trên kỹ thuật bảng tra, việc sử dụng LUT nguyên mẫu đảm bảo độ tin cậy và đồng nhất của các bộ đảo, nhờ đó đảm bảo độ trễ đồng nhất và có thể kiểm soát;

mỗi RO gồm 2^N bộ đảo và một cổng NAND, để đảm bảo cấu trúc mạch vật lý đồng nhất của các RO, các bộ đảo và cổng NAND được kết nối thủ công sử dụng phần mềm FPGA Editor, sau đó được đóng gói thành một khối thiết kế sẵn (Hard macro);

mỗi mảng RO khi được kích hoạt tạo ra n dao động dạng xung nhịp (clock), trị số đếm mỗi dao động này trong một khoảng thời gian có dạng dữ liệu m bit, tỷ lệ với tần số RO, n trị số m bit được ghép cặp liên tiếp, tạo ra $n - 1$ cặp số m bit;

(hai) bộ ghép kênh $(2^N - 1):1$ tuần tự chọn dao động của các cặp RO liên tiếp đưa tới hai bộ đếm m bit tương ứng;

(hai) bộ đếm tần số RO m bit đếm số chu kỳ dao động RO trong một đơn vị thời gian;

bộ cộng/trừ m bit tạo trị số hiệu dạng dữ liệu k bit từ dữ liệu đếm các bộ đếm tần số RO;

mạch truyền/nhận dữ liệu UART (Giao diện truyền dữ liệu nối tiếp không đồng bộ) truyền dữ liệu PUF từ mạch tới PC cũng như nhận tín hiệu tái lập (Reset) từ PC, dữ liệu truyền $(k + p)$ bit gồm k bit trị số hiệu và p bit điều khiển – báo hiệu – kiểm tra;

mạch tạo tín hiệu điều khiển tạo tín hiệu điều khiển, đồng bộ, báo hiệu phục vụ hoạt động chức năng của hệ thống theo chương trình đã lập, mạch tạo tín hiệu điều khiển gồm các bộ chia tần, bộ tạo xung vuông, bộ đếm tạo xung, mạch khử rung phím bấm.

trong đó, quy trình xác thực ID cho IC này gồm hai pha: pha định danh (Identification) và pha xác thực (Authentication), trong đó:

pha định danh gồm các bước:

tạo ID danh định: trên PC, thực hiện tách ra k bit trị số tần số hiệu từ dữ liệu truyền ($k + p$) bit, tập $(n - 1)$ trị số k bit tương ứng $(n - 1)$ cặp RO được ghép liên tiếp nhau, tạo mẫu ID có dạng $(n - 1)k$ bit, mỗi lần kích hoạt mạch tách ID tạo ra một mẫu ID, tập các mẫu ID được lưu trữ trong bộ nhớ máy tính, ID danh định của IC có dạng $(n - 1)k$ bit, là một vector $(n - 1)$ chiều, mỗi chiều/tọa độ là một trị số k bit được tính trung bình thống kê từ tập các giá trị k bit của tọa độ tương ứng của vector ID mẫu, các ID danh định được lưu trong cơ sở dữ liệu ID (ID Database);

tạo mức ngưỡng, trong đó:

với mỗi tập dữ liệu tương ứng một IC, tiến hành tính khoảng cách Euclid chuẩn hóa (khoảng cách nội chuẩn hóa - *normalized intra-distance*) theo công thức (2) dưới đây giữa vector ID mẫu và vector ID danh định,

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

trong đó $d(R_i, R_j) = \sqrt{\sum_{k=1}^{n-1} (\delta_{ik} - \delta_{jk})^2}$ là khoảng cách Euclid giữa hai vector R_i, R_j

trong giải tích cổ điển;

n là số RO trong mảng RO,

$\delta_{ik}, k = \overline{1, n-1}$, là tọa độ thứ k của vector R_i ,

R_l là vector mẫu ID của lần đo thứ l ,

R là vector ID danh định của IC,

k_{norm} là hệ số chuẩn hóa, dùng để chuẩn hóa khoảng cách $d(R_l, R)$ về trị số nằm trong khoảng $(0, 1)$;

từ đó xác định độ lệch chuẩn trong phân bố của tập khoảng cách này, mức ngưỡng dùng cho xác thực IC này được chọn bằng 06 lần độ lệch chuẩn trong phân bố khoảng cách nội chuẩn hóa đã tính,

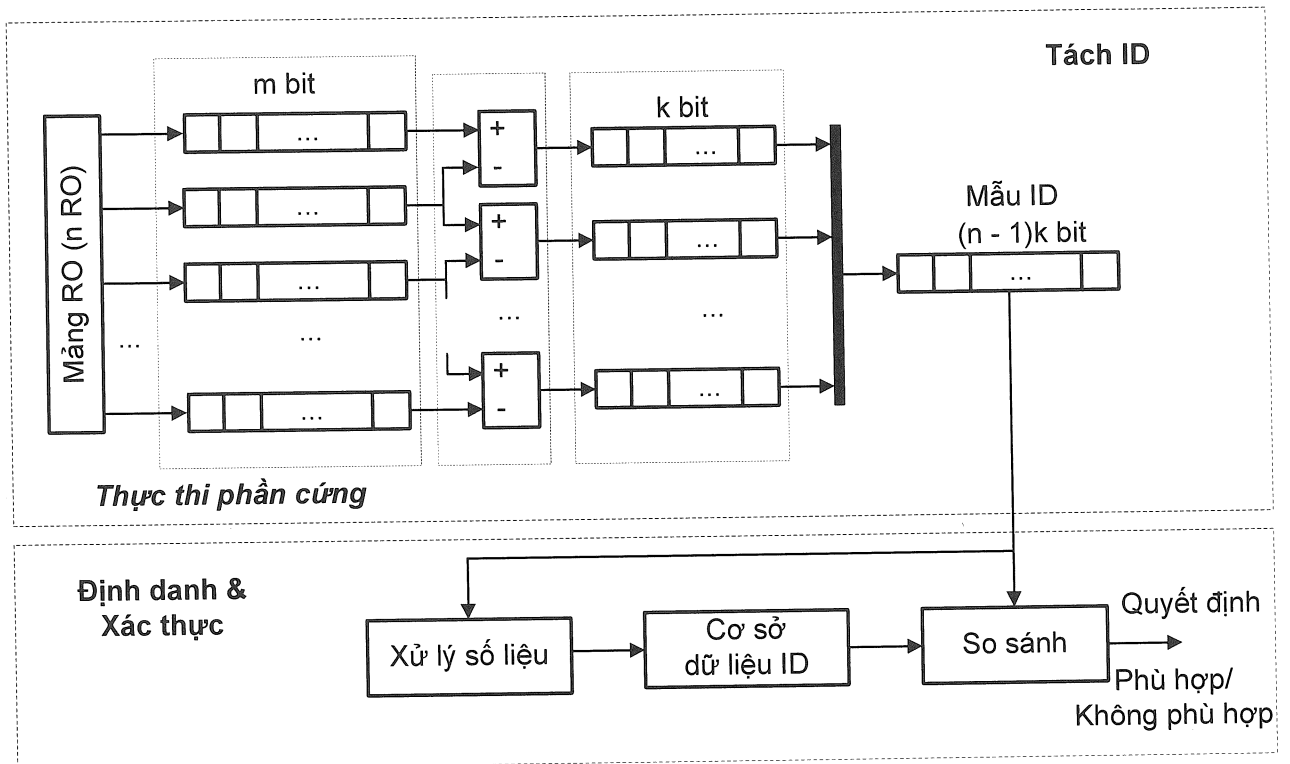
từ tập các mức ngưỡng riêng tương ứng các IC được khảo sát, xác định giá trị cực đại và chọn làm mức ngưỡng chung,

tính khoảng cách giữa các ID danh định và so sánh với mức ngưỡng chung đã tính, nếu khoảng cách nhỏ nhất giữa các ID danh định lớn hơn mức ngưỡng chung, mức ngưỡng này được chấp nhận trong xác thực IC và được lưu vào cơ sở dữ liệu ID,

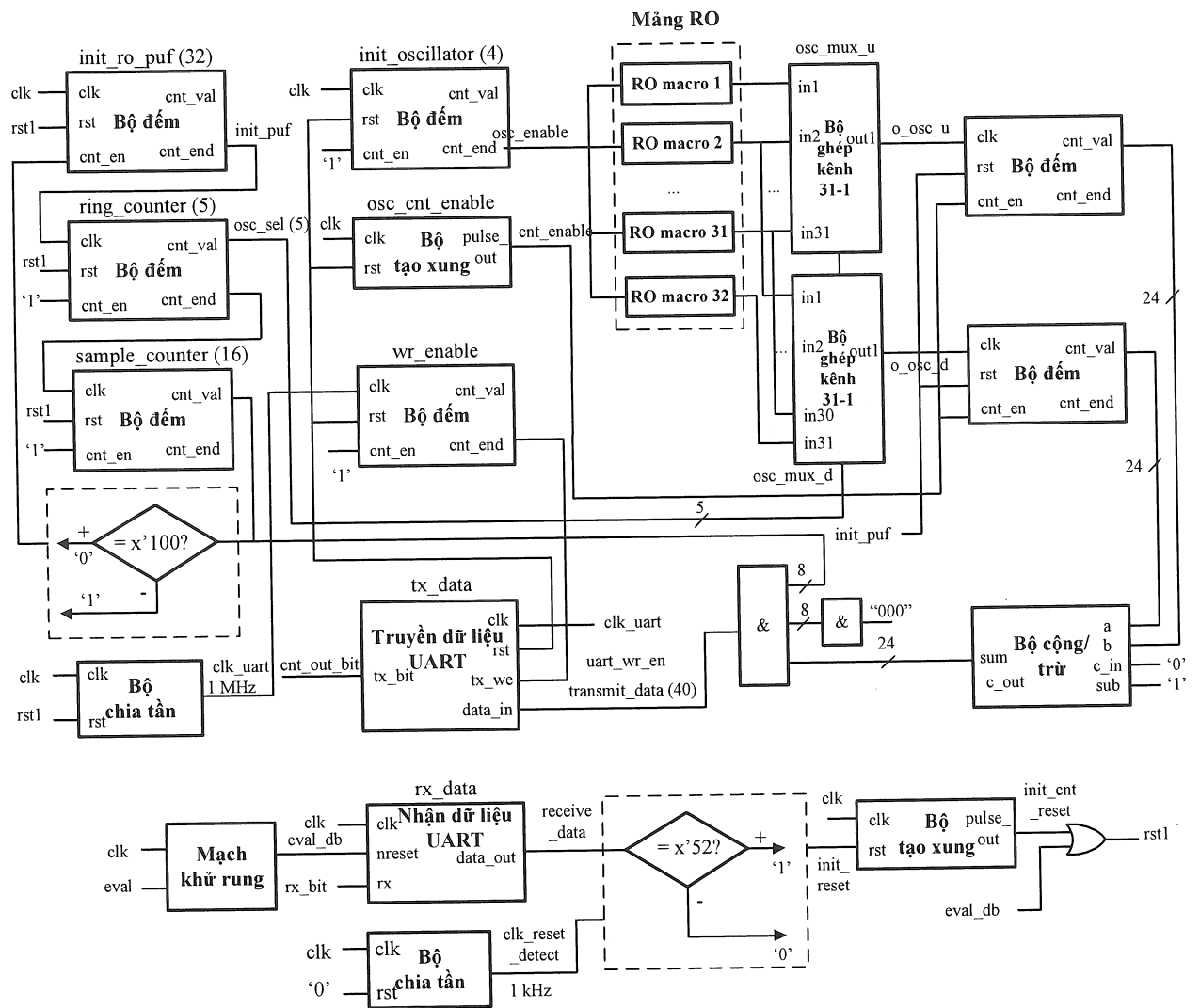
pha xác thực gồm bước:

kết hợp mẫu ID của một IC bất kỳ một cách tuần tự với các ID danh định trong cơ sở dữ liệu ID và tạo dữ liệu khoảng cách Euclid theo công thức (2), sau đó, bộ so sánh (Comparator) so sánh khoảng cách này với mức ngưỡng, nếu khoảng cách nhỏ hơn mức

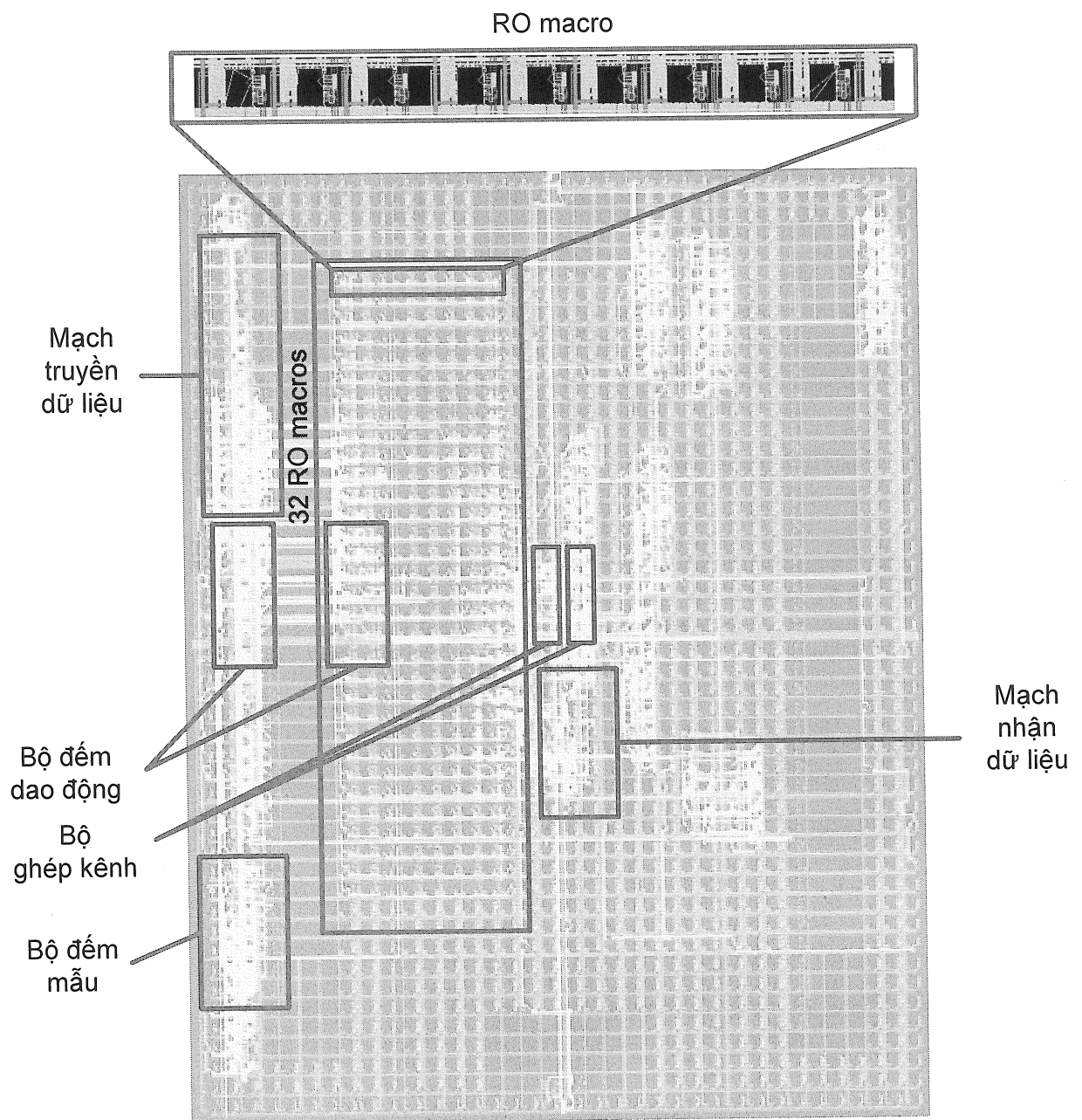
ngưỡng, mẫu ID được coi là tạo bởi IC đã được đăng ký, nếu khoảng cách lớn hơn mức ngưỡng, mẫu ID được coi là tạo bởi IC chưa được đăng ký.



Hình 1

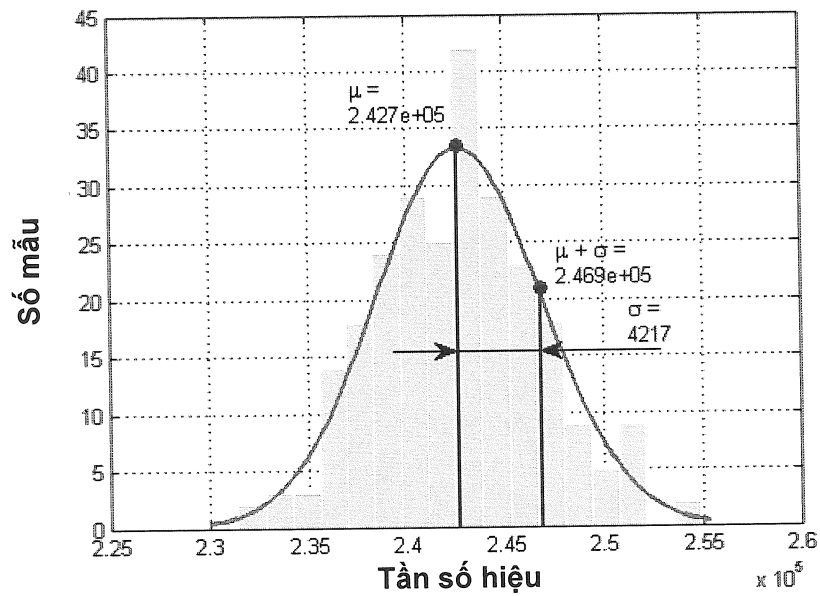


Hình 2



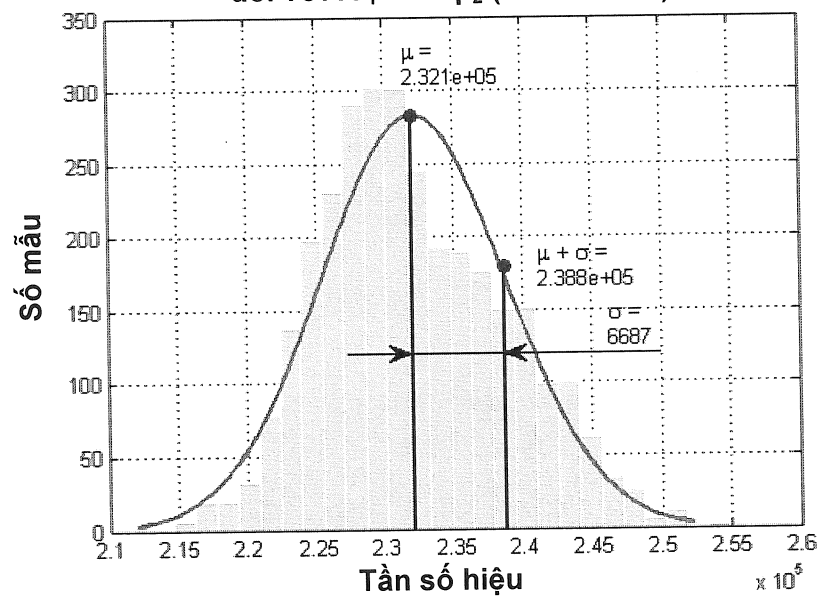
Hình 3

**Biểu đồ phân bố tần số hiệu
đối với IC₁ – ROP₂/25°C**



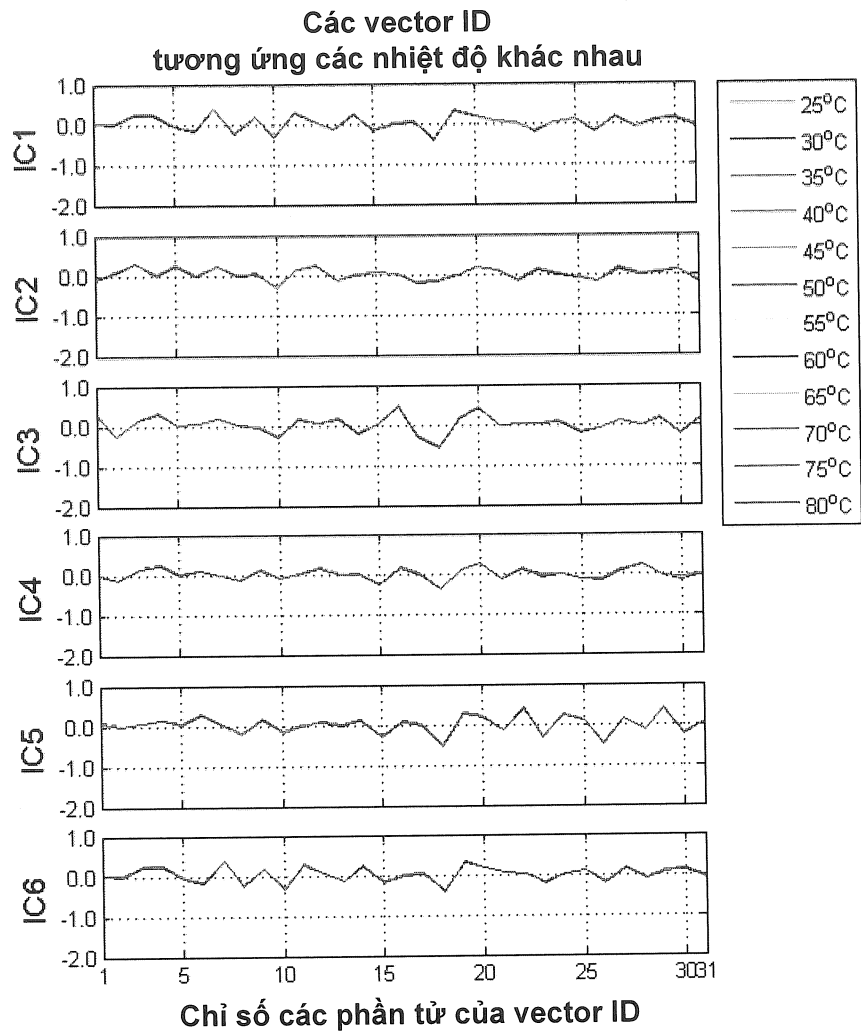
a)

**Biểu đồ phân bố tần số hiệu
đối với IC₁ – ROP₂/(25°C - 85°C)**

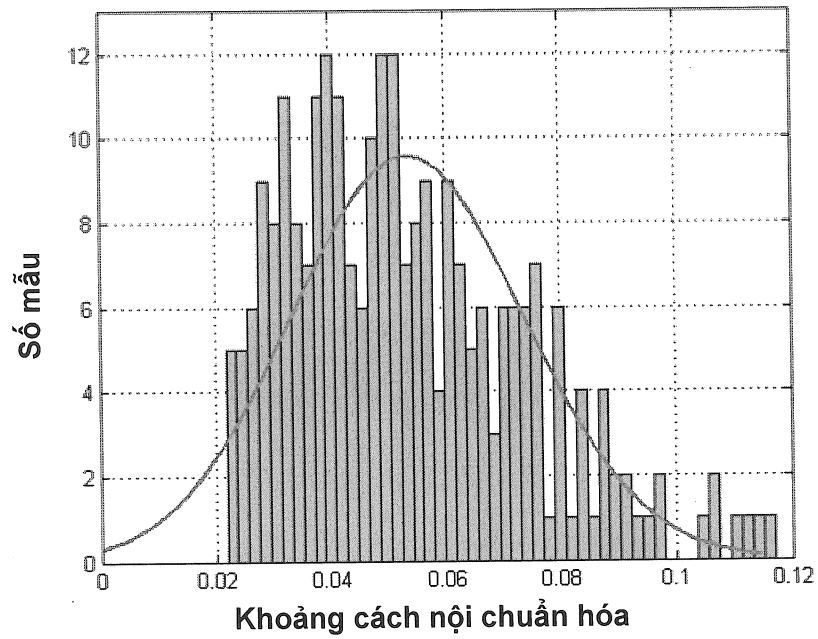


b)

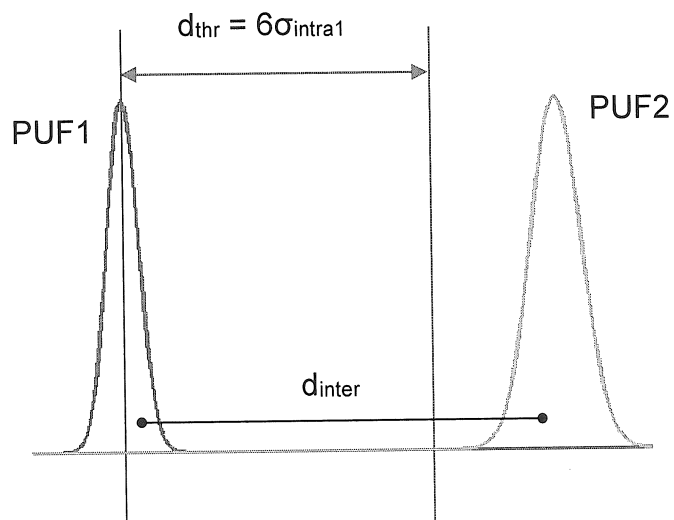
Hình 4

**Hình 5**

**Biểu đồ phân bố
khoảng cách nội chuẩn hóa đối với IC1**



Hình 6



Hình 7