SEQUENTIAL SAMPLING-BASED BIT-ALIASING PRESERVATION FOR MEMRISTOR-BASED PHYSICALLY UNCLONABLE FUNCTIONS WITH TEMPERATURE VARIABILITY

BẢO TỒN BIT-ALIASING DỰA TRÊN VIỆC LẤY MẪU TUẦN TỰ CHO CÁC CHỨC NĂNG KHÔNG THỂ SAO CHÉP VẬT LÝ VỚI SỰ BIẾN ĐỔI NHIỆT ĐỘ

Nguyễn Thị Hà Phương
Trường Đại học Quảng Bình

ABSTRACT: *The memristor devices are highly affected by the variability on the physical dimension, supply voltage, and temperature. The variability in thickness and area are translated to variations in read and write times of memristor when using the device as a memory cell. Those variability affect the resistance value and, in turn, the state of the device. The dependence between the write time and process variation of the memristor has been investigated as the candidate of physical unclonable function (or physically unclonable function, PUF). However, the effect from the other varability sources may degrade the quality of PUF device operation. In this work, we introduce a method to enhance the bit-aliasing of memristor-based PUF with write time variability while considering the effect of temperature and supply voltage variation. By exploiting the non-volatility of the memristor, the proposed method attempts to obtain multiple samples to generate the key with the maximum bit-aliasing whereas the conventional method attempt to stop the programming pulse when the measured bit-aliasing value meets the threshold. The experimental result shows that the proposed value achieves enhanced bit-aliasing by 17% even with the much lower operation frequency of the sampling unit.*

Keyword: *Bit-aliasing, PUF, physiclly unclonable function, memristor.*

TÓM TẮT: *Các thiết bị điện trở nhớ bị ảnh hưởng nhiều bởi sự thay đổi về kích thước vật lý, điện áp cung cấp và nhiệt độ. Sự thay đổi về độ dày và diện tích được chuyển thành các thay đổi về thời gian đọc và ghi của điện trở nhớ khi sử dụng thiết bị như một ô nhớ. Những sự biến đổi đó ảnh hưởng đến giá trị điện trở và trạng thái của thiết bị. Sự phụ thuộc giữa thời gian ghi và sự thay đổi quy trình của điện trở nhớ đã được nghiên cứu như là một ứng cử viên đắt giá của chức năng không thể sao chép vật lý (PUF- Physically Unclonable Function). Tuy nhiên, ảnh hưởng từ các nguồn khả biến khác có thể làm giảm chất lượng hoạt động của thiết bị PUF. Trong bài báo này, chúng tôi giới thiệu phương pháp tăng bit-aliasing của PUF dựa trên điện trở nhớ với sự biến đổi thời gian ghi trong khi xem xét sự ảnh hưởng của sự biến đổi nhiệt độ. Bằng cách khai thác tính bất biến của điện trở nhớ, phương pháp được đề xuất cố gắng lấy nhiều mẫu để tạo khóa với Bit-aliasing lớn nhất trong khi phương pháp thông thường cố gắng dừng xung lập trình khi giá trị Bit-aliasing được đo đáp ứng ngưỡng. Kết quả thử nghiệm cho thấy rằng giá trị được đề xuất tăng độ chính xác của Bit-aliasing lên 17% ngay cả với tần số hoạt động của đơn vị lấy mẫu thấp hơn nhiều.*

Từ khóa: *Bit-aliasing, PUF, chức năng vật lý không thể sao chép, điện trở nhớ.*

1. ĐẶT VẤN ĐỀ

Điện trở nhớ đã trở thành tiềm năng cho công nghệ thiết bị nhớ trong tương lai vì những lợi ích của chúng, chẳng hạn như mật độ cao, năng lượng thấp, tính bất biến và kích thước nano [1]. Điện trở nhớ có thể được coi là một phần tử điện có khả năng duy trì các trạng thái điện trở trong theo lịch sử của điện áp và dòng điện được áp dụng ngay cả khi nguồn điện bị ngắt [2]. Các trạng thái điện trở có thể được chuyển đổi giữa chúng bằng cách đặt điện áp với cường độ và thời lượng thích hợp. Do tính chất duy nhất này, điện trở nhớ là một lĩnh vực hứa hẹn cho nhiều ứng dụng cập nhật như bộ nhớ bất biến.

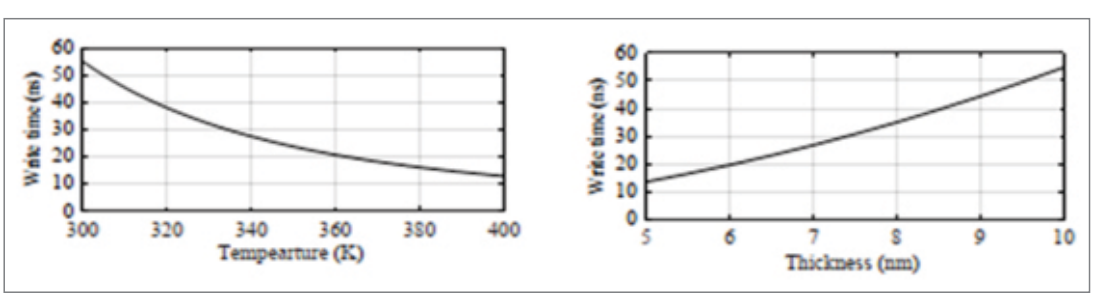
Nói chung, điện trở nhớ được sử dụng trong các hệ thống có kích thước nano. Do đó, một biến thể bình thường nhỏ có khả năng tác động đáng kể đến các tham số cũng như hoạt động của thiết bị. Cần phải xem xét cẩn thận khả năng biến thiên khi sử dụng điện trở nhớ trong thực tế. Sự thay đổi về độ dày và diện tích được chuyển thành các thay đổi về thời gian đọc và ghi của điện trở nhớ khi sử dụng thiết bị làm ô nhớ. Ảnh hưởng của sự thay đổi độ dày và diện tích ảnh hưởng đến giá trị điện trở liên quan đến điện áp và dòng điện được cung cấp trên thiết bị [3]. Hơn nữa, điện áp cung cấp cho từng thiết bị cũng thay đổi theo kết nối vật lý thông qua mạng phân phối điện. Sự phụ thuộc giữa tính di động của tường miền và nhiệt độ cũng là sự biến đổi nguồn phổ biến.

Đối với các ứng dụng bộ nhớ thông thường, ảnh hưởng của khả năng thay đổi phải được triệt tiêu thấp hơn một mức nhất định để đảm bảo yêu cầu về thời gian. Một số phương pháp đã cố gắng đo sự thay đổi của thời gian ghi để thu được nhiệt độ [4].

PUF là một thực thể vật lý với các tính năng thực tế không thể sao chép. Các tính năng như vậy thường bắt nguồn từ quy trình sản xuất của từng thiết bị. PUF phụ thuộc vào tính độc đáo của cấu trúc vi mô vật lý của chúng do các yếu tố vật lý ngẫu nhiên được đưa vào trong quá trình sản xuất. Những yếu tố này chính là không thể đoán trước và không thể kiểm soát tạo ra chức năng không thể sao chép.

Các thiết bị PUF thường được coi là nguồn ngẫu nhiên mong muốn cho các ứng dụng mật mã và bảo mật nhờ tính duy nhất của nó được kết nối với một thiết bị. PUF dựa trên sự biến đổi quá trình của mạch tích hợp như SRAM và bộ nhớ bất biến (NVM) đã được nghiên cứu cho đến nay. Tuy nhiên, dung lượng nhỏ hơn và độ tin cậy cao hơn của bộ nhớ cố định NVM khiến nó trở nên hấp dẫn đối với các ứng dụng nhỏ hơn với yêu cầu bảo mật thấp hơn [5].

Điện trở nhớ đã được các nhà nghiên cứu quan tâm vì những ưu điểm của chúng như mật độ nội tại cao, tốc độ truy cập



Hình 1. Sự thay đổi của thời gian ghi theo nhiệt độ và độ dày của ô nhớ.

nhanh và hiệu quả sử dụng năng lượng tốt [1]. Điện trở nhớ có thể được coi là một công tắc điện có khả năng duy trì các trạng thái điện trở bên trong theo lịch sử của điện áp và dòng điện được áp dụng ngay cả khi nguồn điện bị ngắt [2]. Sự thay đổi về độ dày và diện tích được chuyển thành các thay đổi về thời gian đọc và ghi của điện trở nhớ khi sử dụng thiết bị làm ô nhớ. Ảnh hưởng của độ dày và diện tích thay đổi phụ thuộc vào lịch sử của điện áp đặt trên thiết bị trong một thời gian nhất định và điều này được nghiên cứu trong [3].

Trong bài báo [5] đã đề xuất một phương pháp trong đó các nguồn entropy trong quy trình luồng của PUF, tức là cường độ của các biến thể tương tự, được mô phỏng và số hóa dưới dạng thông tin kỹ thuật số nhiều bit. Những thông tin bí mật này hỗ trợ cho các quy trình tái tạo và được lưu trữ trên bộ nhớ cố định chẳng hạn như điện trở nhớ đại diện cho một lỗ hổng và ngăn các NVM-PUF tạo ra ứng dụng bảo mật cao. Tuy nhiên, dấu chân nhỏ và độ tin cậy cao của việc lưu trữ thông tin trên bộ nhớ cố định khiến nó trở nên hấp dẫn hơn đối với các ứng dụng có hệ số dạng nhỏ và bảo mật thấp hơn.

PUF được áp dụng cho một số thiết bị để tăng tính bảo mật cho các thiết bị này, ví dụ: Arbiter PUF, ring oscillator PUF [6]… Một trong những phương pháp để chống lại hoặc hạn chế vi phạm bản quyền, làm giả và tấn công kênh phụ chính là PUF, nó cung cấp chữ ký hoặc nhận dạng duy nhất của phần cứng [7]. PUF có mối quan hệ với nguyên tắc bảo mật dựa trên phần cứng. Nó có một dấu vân tay duy nhất cho mỗi PUF có thể được sử dụng cho mục đích bảo mật [8]. Bit-aliasing là một trong những hiệu suất thống kê đối với hiệu suất APUF dựa trên điện trở nhớ được phân tích hoặc để điều tra tác động của việc có các chức năng cửa sổ điện trở nhớ khác nhau trên RO-PUF. Nhà nghiên cứu đã sử dụng các yếu tố Bit-aliasing, tính đồng nhất (Uniformity) và tính duy nhất (Uniqueness) để đánh giá PUF.

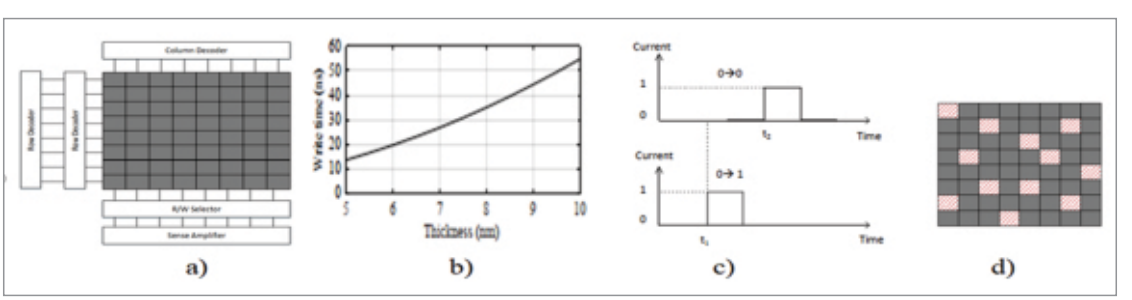
Chính vì vậy, trong bài báo này, chúng tôi tập trung việc bảo tồn Bit-aliasing dựa trên việc lấy mẫu tuần tự cho chức năng không thể sao chép (PUF) với sự thay đổi nhiệt độ để đánh giá PUF một cách chính xác hơn.

3. CHỨC NĂNG KHÔNG THỂ SAO CHÉP DỰA TRÊN ĐIỆN TRỞ NHỚ

3.1. Mô hình điện trở nhớ với sự biến thiên

Với mô hình mạch, hành vi tổng thể của điện trở nhớ có thể được tính theo công thức thời gian ghi của các ô điện trở nhớ [4]:

$$t_{ghi} = \frac{D^2}{\mu_I(T)v_w}\left(\frac{r_1-1}{2}\left(x_0^2 - x_f^2\right) + (r_1 + r_2)(x_f - x_0)\right) \quad (1)$$



Hình 2: Quy trình tạo ra PUF dựa trên điện trở nhớ

Trong đó các tham số r_1, r_2 phụ thuộc $R_{off}, R_{on}, R_{pulldown}$ và r_1 là tỷ lệ của R_{off} và R_{on}, r_2 là tỷ lệ của $R_{pulldown}$ và R_{on}, $\mu_I(T)$ là tính di động, D là độ dài của thiết bị, x_0, x_f là trạng thái ô nhớ lúc ban đầu và khi kết thúc. Theo như công thức thì thời gian ghi liên quan đến nhiệt độ, nếu nhiệt độ tăng thì thời gian ghi sẽ giảm, độ dày các ô nhớ tăng thì thời gian ghi sẽ tăng (Hình 1). Các tham số được sử dụng trong bài báo này với các thông số cụ thể trong Bảng 1.

Bảng 1. Hằng số và tham số trong mô hình

Tham số	**Giá trị**	**Mô tả (đơn vị tính)**
$\boldsymbol{\alpha}$	0.15	Hình học tinh thể (nm)
$\boldsymbol{E_a}$	0.18	Năng lượng hoạt động ion (eV)
$\boldsymbol{k_B}$	8.6173303×10^{-5}	Hàng số Boltzman (eV K^{-1})
$\boldsymbol{f}$	10	Tần số nhảy (THz)
$\boldsymbol{q_I}$	2	Cường độ ion
$\boldsymbol{v_w}$	10	Điện áp ghi (V)
Hằng số	**Giá trị**	**Mô tả (đơn vị tính)**
T	300 - 400	Nhiệt độ (K)
D	10	Độ dài (nm)
$\boldsymbol{R_{on}}$	100	Điện trở bật (ohm)
$\boldsymbol{R_{off}}$	16000	Điện trở tắt (ohm)
$\boldsymbol{R_{pulldown}}$	1000	Điện trở kéo xuống (ohm)
$\boldsymbol{x_0}$	0	Trạng thái bắt đầu
$\boldsymbol{x_f}$	1	Trạng thái kết thúc

3.2. Chức năng vật lý không thể sao chép (PUF) dựa trên điện trở nhớ

PUF là một chức năng vật lý mà không thể sao chép và thể dự đoán được. Trong hệ thống trả lời thử thách, khi một thử thách ảnh hưởng đến PUF thì một phản hồi được tạo ra và phản hồi này rất khó để dự đoán khi thử thách không được biết trước. Bộ nhớ của điện trở nhớ (Hình 2a) [9] có các hoạt động dựa vào thời gian truy cập và điện áp cung cấp. Nếu thời gian truy cập giảm, các ô điện trở nhớ không thể thay đổi trạng thái logic vì thời gian diễn ra quá nhanh. Bên cạnh đó, điện trường giảm cũng không có đủ thời gian để thay đổi trạng thái nếu điện áp được cung cấp giảm.

Cấu trúc của một mô hình PUF điện trở nhớ là xây dựng sự biến đổi quy trình bằng

cách xem xét sự biến đổi của điện trở nhớ và độ dày của ô nhớ. Công nghệ điện trở nhớ đạt lưu trữ sự biến đổi ngẫu nhiên và sự biến đổi của hệ thống. Sự biến đổi của hệ thống chỉ ra sự ngẫu nhiên của giá trị trong các tham số thiết bị cơ sở, sự biến đổi hệ thống diễn tả mối tương quan giữa mật độ và các hiệu ứng lân cận cũng như khoảng cách liên quan của các thiết bị.

PUF được sử dụng trong nhiều hệ thống để giúp chúng có độ bảo mật cao hơn bằng cách tạo ra các khóa bí mật từ các phản hồi của PUF. Để đánh giá chất lượng của PUF, chúng tôi có thể xem xét ba chỉ số hiệu suất của PUF là: Uniqueness, Uniformity và Bit-aliasing[10], [11].

Trong bài báo này, chúng tôi chỉ tập trung vào chỉ số hiệu suất Bit-aliasing để đánh giá và nâng cấp. Bit-aliasing tại mỗi vị trí chính là phần trăm của tổng các giá trị bit qua các phản hồi x. Trung bình của Bit-aliasing là trung bình của Bit-aliasing tại các vị trí của bit.

$$Bit - aliasing = \frac{1}{x}\sum_{i=1}^{x} r_{i,j} * 100\% \quad (2)$$

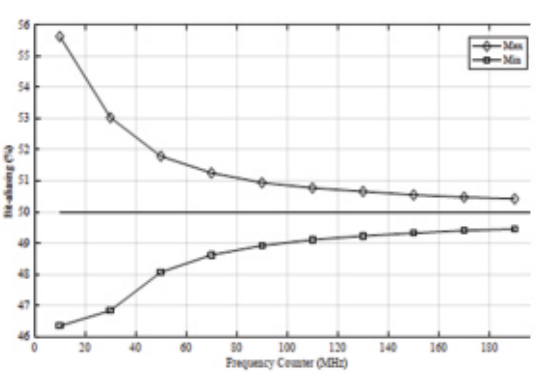
Trong đó x là số lượng các PUF, r_{ij} là giá trị của bit (0 hoặc 1) tại các vị trí thứ *j* của phản hồi thứ *i*. Giá trị lý tưởng của Bit-aliasing là 50%. Chúng tôi có thể xác định PUF được làm giả dễ dàng hay không dựa vào Bit-aliasing này. Vì vậy, khả năng làm giả PUF rất khó nếu Bit-aliasing gần với 50%.

Để tạo ra một PUF, ban đầu chúng ta có một điện trở nhớ với n x n ô nhớ đang ở trạng thái chưa được ghi (Hình 2.a), vì thời gian ghi của ô nhớ phụ thuộc vào độ dày ô nhớ (Hình 2.b) và nhiệt độ (Công thức 1) nên khi áp một xung điện lên điện trở nhớ và dừng lại tại một thời điểm nhất định thì một số các ô nhớ sẽ được ghi (trạng thái của ô nhớ sẽ chuyển từ 0 sang 1) một cách ngẫu nhiên mà người sử dụng không thể biết được (Hình 2.d) tức là người dùng sẽ không biết được ô nhớ nào được ghi và thứ tự ghi như thế nào vì không biết được độ dày của các ô nhớ. Chính vì vậy, để dự đoán được PUF như thế nào là một điều rất khó và cũng khó để làm giả PUF.

4. SỰ BẢO TỒN BIT-ALIASING VỚI SỰ BIẾN ĐỔI NHIỆT ĐỘ VÀ ĐIỆN ÁP

4.1. Bit-aliasing với lỗi thời gian

Bit-aliasing có thể được định nghĩa như tỷ lệ giữa bit 0 hoặc bit 1. Nếu giá trị của nó là 0% hoặc 100%, tất cả giá trị của các phản hồi tương ứng là 0 hoặc 1. Tuy nhiên, các trường hợp này không đưa ra độ bảo mật cao vì không có nhiều thông tin từ các phản hồi đó và nó dễ dàng để tạo ra PUF giả. Trong trường hợp Bit-aliasing đạt 75%, các phản hồi sẽ được tạo ra và đồng nghĩa với bit 0 đạt 25%. Việc dò tìm 25% số lượng các bit sẽ dễ dàng hơn là 50%. Vì vậy, giá trị Bit-aliasing càng gần với 50 càng tốt.

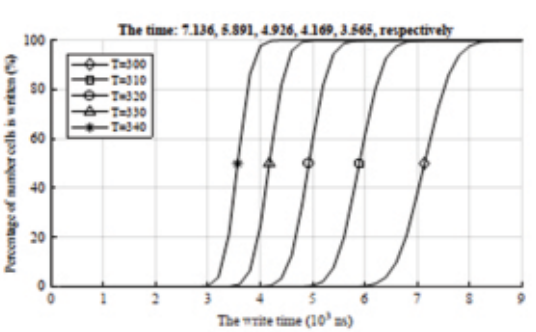


Hình 3. Sự thay đổi của Bit-aliasing theo bộ đếm tần số

Hình 3 mô phỏng Bit-aliasing theo bộ đếm tần số. Thời gian mà Bit-aliasing đạt được 50% trong thí nghiệm này là t=7.137μs tại nhiệt độ 300K.

Khi bộ đếm tần số tăng thì thời gian ghi giảm nghĩa là thời gian đó là độ lệch thời gian t. Với đường phía trên, thời gian trừ đi độ lệch thời gian, đường phía dưới là thời gian cộng với độ lệch. Từ đó, chúng tôi có Bit-aliasing theo tần số. Độ lệch là lỗi thời gian. Lỗi thời gian ảnh hưởng đến bit-aliasing và làm nó bị thay đổi theo giá trị lỗi thời gian lớn và nhỏ.

Chúng tôi xem xét trường hợp bộ đếm tần số là 10MHz, tương đương với 0.1 μs, giá trị lớn nhất của Bit-aliasing là 55.6370 (tại 7.2 μs) và giá trị nhỏ nhất là 46.3410% (tại 7.1 μs). Khả năng mà các phiên bản khác nhau của PUF sản xuất ra các phản hồi giống nhau là rất thấp nếu Bit-aliasing đạt gần giá trị lý tưởng. Theo Hình 3, bộ đếm tần số càng cao (thời gian lỗi càng nhỏ) thì Bit-aliasing càng đạt giá trị lý tưởng. Bộ đếm tần số là tỷ lệ nghịch với thời gian ghi của các ô điện trở nhớ. Để tăng độ chính xác của Bit-aliasing, lỗi Bit-aliasing phải giảm bởi nhiều mẫu tuần tự (phần 4.2).



Hình 4. Tỷ lệ phần trăm của số lượng các ô theo thời gian

Hình 4 diễn tả tỷ lệ phần trăm của số lượng các ô được ghi theo thời gian và thời gian để lấy được 50% số lượng các ô với sự thay đổi nhiệt độ. Khi nhiệt độ giảm, thời gian viết sẽ giảm, vì vậy thời gian lấy được 50% số các ô điện trở nhớ giảm. Trong bài báo này, tôi đề xuất tăng Bit-aliasing của PUF dựa trên điện trở nhớ với sự biến đổi thời gian, tuy nhiên tôi không trình diễn giảm tần số mà chỉ làm cho nhiệt độ hoặc điện áp cung cấp biến đổi theo hướng giảm (tại tần số thấp) và Bit-aliasing vẫn được bảo tồn. Do đó, với tần số hoạt động thấp hơn nhiều của các đơn vị mẫu, giá trị thực nghiệm của đề xuất của tôi sẽ tăng Bit-aliasing.

Trong công thức 1, nếu nhiệt độ hoặc điện áp cung cấp thay đổi (thay đổi theo hướng tăng) thì thời gian ghi sẽ thay đổi (theo hướng giảm).

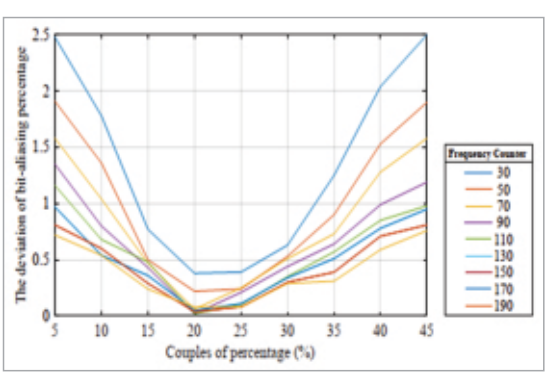
4.2. Giảm lỗi Bit-aliasing với nhiều mẫu

Sự thay đổi tỷ lệ của Bit-aliasing là lớn nhất tại điểm lấy 50% khi chúng ta giả sử phân bố bình thường trên sự biến đổi quá trình. Nó quyết định phản hồi r_i tại thời điểm t_i để lấy 50% trong CDF (Hàm phân phối tích lũy, các ô nhớ sẽ được ghi tại mỗi thời điểm sẽ được cộng dồn vào số lượng các ô nhớ được ghi trước đó). Khi giá trị Bit-aliasing được đo đạt ngưỡng, nó cố gắng để dừng xung chương trình và lỗi thời gian nhỏ tại 50% có thể dẫn đến kết quả lỗi lớn hơn nhiều trong Bit-aliasing.

Chúng ta có thể tăng độ chính xác bằng cách sử dụng tần số cao hơn của

mạch đếm giá trị ô hoặc logic chuyên dụng để tạo ra ký hiệu điều khiển của xung chương trình (có thể là bộ cộng tương tự,…). Tuy nhiên, nó lại dẫn đến chi phí đáng kể.

Với lỗi thời gian vừa phải, chúng ta có thể giảm lỗi Bit-aliasing bằng cách tạo giá trị cuối cùng như là sự kết hợp của nhiều mẫu từ phương pháp đề xuất. Phương pháp đề xuất là lấy ra 50% số lượng các bit 1 (hoặc 0) từ nhiều mẫu, có nghĩa là tổng số lượng các bit được ghi (bit 1) và không được ghi (bit 0) của các phản hồi từ phản hồi r_1 đến phản hồi r_i. Nếu số lượng các bit 1 và bit 0 bằng nhau thì chúng ta sẽ quyết định thời gian t_i. Ví dụ, nếu có 7 mẫu với 2%, 20%, 22%, 50%, 52%, 72% số lượng ô nhớ được ghi, chúng ta có thể tạo ra 50% Bit-aliasing bằng cách kết hợp 20% và 70% CDF hoặc 22% và 72% của số lượng ô nhớ được ghi (Hình 5) thay vì sử dụng một giá trị từ 54% bởi phương pháp truyền thống.



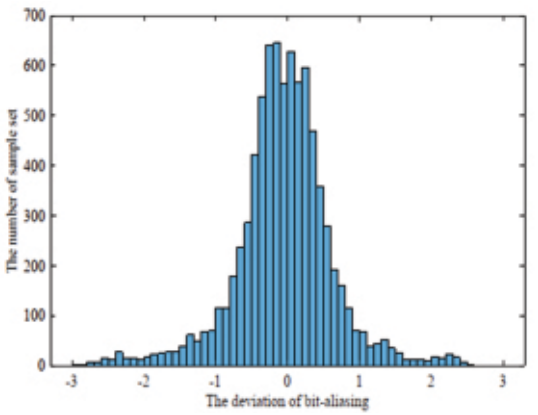
Hình 5. Độ lệch của Bit-aliasing của tập mẫu tại các bộ đếm tần số

Với phương pháp truyền thống, tại tỷ lệ 50%, t=7.137μs, khi lỗi thời gian xảy ra, độ lệch của thời gian là 0.063 μs, độ lệch phần trăm là 5.6370%. Ngược lại, với phương pháp đề xuất, tại lỗi thời gian tương tự, độ lệch phần trăm chưa đến 1% (nghĩa là Bit-aliasing nhỏ hơn 51%) và cặp phản hồi thử thách tốt nhất là 22%-72%. Nếu lựa chọn tại thời điểm lấy ra cặp CDF 50%-50%, khi có lỗi thời gian xảy ra thì việc lấy được 50% số lượng các ô nhớ được ghi cũng sẽ bị lệch, vì vậy chúng tôi chọn các cặp CDF sao cho tổng gần với 100% các ô được ghi để trừ hao trường hợp lỗi thời gian do nhiệt độ xảy ra.

Chương trình thực nghiệm sẽ xem xét sự thay đổi của Bit-aliasing tại các thời gian để lấy ra giá trị Bit-aliasing khác nhau và không phải tại 50%. Trong chương trình, tôi chọn các cặp 20-70%, 30-80%, 35-85%... Khi lỗi thời gian xảy ra, Bit-aliasing sẽ bị thay đổi tăng hoặc giảm, nếu Bit-aliasing không gần với 50% thì độ chính xác cũng giảm. Đề xuất của bài báo là lấy ra giá trị Bit-aliasing gần nhất với 50%, tuy nhiên, do lỗi thời gian nên tôi thực hiện việc kết hợp cặp CDF khác 50%-50% để cải thiện lỗi.

5. KẾT QUẢ THỰC NGHIỆM

Thí nghiệm được thực hiện với 8100 tập mẫu PUF dựa trên điện trở nhớ, mỗi tập mẫu biểu diễn tại các tần số khác nhau (có 9 tần số) và xem xét 9 cặp phần trăm tại CDF. Các tập mẫu mà tôi sử dụng có các ô nhớ mà độ dày của nó được tạo ra một cách ngẫu nhiên [4] để tránh trường hợp người dùng biết trước được PUF. Sự phân bố của độ lệch Bit-aliasing được mô phỏng trong Hình 6.



Hình 6. Sự phân bố độ lệch của Bit-aliasing

Chúng ta thấy rằng số lượng các tập mẫu dẫn đến độ lệch nhỏ nhất của Bit-aliasing là quanh điểm 0 là rất nhiều. Khi có sự thay đổi nhiệt độ thì thời gian ghi các ô nhớ sẽ thay đổi theo, đồng thời giá trị Bit-aliasing cũng sẽ xảy ra lỗi và xa với giá trị lý tưởng. Khi áp dụng phương pháp đề xuất thì độ lệch của Bit-aliasing nó sẽ giảm tới 17% so với phương pháp truyền thống.

Thuật toán phân tích lỗi Bit-aliasing và sự phân bố thời gian ghi khi lựa chọn tại các cặp CDF thay vì taị 50% như sau:

Input: Dữ liệu PUF;
Dữ liệu các cặp CDF;
Dữ liệu bộ đếm tần số;

Output: - Sự phân bố của độ lệch Bit-aliasing.

1. **for** mỗi mẫu PUF **do**
2. **for** mỗi tần số **do**
3. **for** mỗi cặp CDF **do**
4. Lấy ra số lượng các ô được ghi tại mỗi cặp CDF → num1, num2
5. Lấy ra số lượng các ô được ghi mà được thêm vào từ num1, num2
6. Tính tỷ lệ phần trăm của các ô thêm
7. **end for;**
8. **end for;**
9. **end for;**
10. Đưa ra kết quả độ lệch Bit-aliasing

5. KẾT LUẬN

Trong bài báo này, tôi đã đề xuất một phương pháp để bảo tồn Bit-aliasing dựa vào mẫu tuần tự với sự thay đổi nhiệt độ. Bit-alising là một trontg những hiệu suất của PUF để đánh giá khả năng độc nhất, khó dự đoán và làm giả của PUF, tuy nhiên các nhà nghiên cứu trước đó chỉ dừng lại ở việc phân tích và đánh giá hiệu suất của nó chứ chưa đi vào nghiên cứu các phương pháp để cải thiện hay giảm độ chênh lệch khi có tác động từ bên ngoài như sự thay đổi về nhiệt độ. Phương pháp đề xuất này làm giảm độ lệch của Bit-aliasing đến 17%, góp phần nâng cao độ bảo mật của thiết bị.

TÀI LIỆU THAM KHẢO

[1] J. J. Yang, D. B. Strukov, and D. R. Stewart (2013), "Memristive devices for computing", Nature nanotechnology, vol. 8, pp. 13--24.

[2] D. B. Strukov, G. S. Snider, D. R. Stewart, and R. S. Williams (2018), "The missing memristor found", Nature, vol. 453, pp. 80--83.

[3] J. Rajendran, H. Maenm, R. Karri, and G. S. Rose (2011), "An approach to tolerate process related variations in memristor-based applications", IEEE VLSI Design (VLSI Design), 24th International Conference on, 2011, pp. 18--23.

[4] C. Merkel (2011), "Thermal profiling in

CMOS/memristor hybrid architectures", Rochester Institute of Technology.

[5] W. Che, J. Plusquellic, and S. Bhunia (2014), "A non-volatile memory based physically unclonable function without helper data", Proceedings of the 2014 IEEE/ACM International Conference on Computer-Aided Design, pp. 148--153.

[6] R. Maes, and I. Verbauwhede (2010), "Physically unclonable functions: A study on the state of the art and future research directions", Towards Hardware-Intrinsic Security, Springer, Berlin, Heidelberg, pp. 3--37.

[7] G. S. Rose, N. McDonald, L. K. Yan, and B. Wysocki (2013), "A write-time based memristive PUF for hardware security applications", 2013 IEEE/ACM International Conference, pp. 830--833.

[8] J. T. H. Loong, N. A. N. Hashim, M. S. Hamid, and F. A. Hamid (2016), "Performance analysis of CMOS-memristor hybrid ring oscillator Physically Unclonable Function (RO-PUF)", IEEE Semiconductor Electronics (ICSE), 2016 IEEE International Conference, pp. 304-307.

[9] P. Koeberl, U. Kocabas, and A. R. Sadeghi (2013), "Memristor PUFs: a new generation of memory-based physically unclonable functions", Proceedings of the Conference on Design, Automation and Test in Europe, EDA Consortium, pp. 428--431.

[10] A. Maiti (2012), "A systematic approach to design an efficient physical unclonable function", Ph.D. dissertation, Virginia Tech.

[11] J. Rajendran, R. Karri, J. B. Wendt, M. Potkonjak, N. McDonald, G. S. Rose, and B. Wysocki (2015), "Nano meets security: Exploring nanoelectronic devices for security applications", Proceedings of the IEEE, vol. 103, pp. 829--849.

Liên hệ:

TS. Nguyễn Thị Hà Phương

Khoa Kỹ thuật - Công nghệ thông tin, Trường Đại học Quảng Bình.

Địa chỉ: 18 Nguyễn Văn Linh, Đồng Hới, Quảng Bình

Email: nguyenphuong18285@gmail.com

Ngày nhận bài: 05/6/2023

Ngày gửi phản biện: 05/6/2023

Ngày duyệt đăng: 01/8/2023