DOI: 10.64302/joshusc.v30n1e.1331

THIẾT KẾ VÀ THỰC THI GIẢI THUẬT MÃ HÓA ASCON TRÊN NỀN TẢNG FPGA CỦA KIT DE2 - 115

Lê Văn Thanh Vũ*, Hoàng Đại Long

Khoa Điện, Điện tử & Công nghệ vật liệu, Trường Đại học Khoa học, Đại học Huế

*Email: vulvt@hueuni.edu.vn

Ngày nhận bài: 9/5/2025; ngày hoàn thành phản biện: 11/5/2025; ngày duyệt đăng: 21/7/2025

TÓM TẮT

Phát triển các hệ thống IoT đã và đang là xu thế phát triển của lĩnh vực điện tử công nghệ hướng đến đa dạng các ứng dụng trong xã hội hiện đại. Giải pháp mã hóa trọng số nhẹ - LWC đang được chuẩn hóa để đáp ứng ngày càng tốt hơn cho các hệ thống IoT hiện đại. Giải pháp mã hóa ASCON đã được viện Tiêu chuẩn và công nghệ NIST của Mỹ là một trong các chuẩn mã hóa được khuyến nghị sử dụng ở vòng cuối. Trong bài báo này chúng tôi tập trung nghiên cứu thiết kế và đánh giá hoạt động mã hóa theo thuật toán này và hướng đến khả năng ứng dụng trong các hệ thống IoT thế hệ mới. Thiết kế cứng hóa cho giải thuật ASCON được mô tả chi tiết và mô phỏng đánh giá một cách toàn diện đã minh chứng được các ưu điểm về tính ổn định và tối ưu cả tốc độ và khả năng tích hợp vào hệ thống. Những kết quả thu được của thiết kế mạch mã hóa ASCON cho thấy khả năng ứng dụng của thuật toán này vào các hệ thống IoT hiện đại trong dãi rộng các ứng dụng.

Từ khóa: Hệ thống IC, IC design, LWC, ASCON.

1. MỞ ĐẦU

Xu hướng phát triển các hệ thống nhúng và IoT đã và đang thu hút sự quan tâm nghiên cứu phát triển cả trong nghiên cứu và triển khai công nghiệp. Các hệ thống IoT ngày càng mở rộng và đa dạng các ứng dụng [1]. Hệ thống IoT vừa có khả năng linh hoạt đáp ứng đa dạng các yêu cầu ứng dụng; vừa nâng cao khả năng tối ưu hiệu quả hoạt động thông qua xử lý phân tán. Cùng với sự phát triển vượt bậc thì thách thức đặt ra trong quá trình thiết kế và triển khai các hệ thống IoT cũng tạo nên các thách thức đa dạng mới [2]. Xu thế IoT càng phổ biến và được triển khai rộng khắp thì thách thức về bảo mật dữ liệu cũng càng lớn dần. Trong các ứng dụng nông nghiệp thông minh sẽ cần thu thập và quản lý thông tin đối tượng nuôi trồng chính xác và tin cậy. Các ứng dụng IoT trong gia đình cần phải tích hợp chức năng bảo vệ dữ liệu cá nhân. Các giải pháp

bảo mật hiện có trên mạng Internet thường dùng như DES và AES dù đã và đáp ứng tốt. Tuy nhiên, trong ràng buộc dặc trưng của IoT với các node mạng có tài nguyên (xử lý, bộ nhớ, năng lượng) hạn chế; giải pháp bảo mật cho các hệ thống IoT cần có lời giải phù hợp hơn với các giải thuật mã hóa cần ít tài nguyên tính toán, độ phức tạp cao.

Xu thế bảo mật cho các liên kết bên trong các hệ thống IoT đã tạo nên hướng nghiên cứu nổi bật, điều này thể hiện tại NIST cũng đã tiến hành chuẩn hóa giải thuật bảo mật cho IoT [3]. Hoạt động chuẩn hóa đã được triển khai từ năm 2015 đến gần đây (10/2025) với rất nhiều nhóm nghiên cứu chuyên môn tham gia. Trải qua các vòng đánh giá, NIST đã tạo nên danh sách các giải thuật vào vòng 3 cuối cùng gồm 10 giải thuật được chọn. Giải thuật ASCON là một giải pháp mật mã trọng số nhẹ - LWC (LightWeight Cryptography) vượt qua quá trình kiểm định vòng cuối của NIST [4]. Trong thời gian qua thuật toán ASCON cũng đã thu hút nhiều nhóm nghiên cứu để hướng đến khả năng triển khai ứng dụng trong một số điều kiện cụ thể khác nhau [5] [6]. Qua những nghiên cứu đã công bố cũng như quá trình triển khai hoạt động mã hóa của chúng tôi, khả năng bảo mật của thuật toán ASCON là đáng tin cậy, và tài nguyên cần có cho hoạt động mã hóa cũng phù hợp với xu thế triển khai các hệ thống IoT.

Trong bài báo này chúng tôi trình bày kết quả nghiên cứu giải thuật mã hóa ASCON trong hoạt động bảo mật cho các hoạt động truyền thông bên trong các hệ thống IoT. Phần 2 của bài báo sẽ trình bày tổng quan các hoạt động nghiên cứu về bảo mật định hướng cho lĩnh vực IoT trong thời gian qua. Phần 3 sẽ tập trung trình bày giải pháp cứng hóa giải thuật ASCON một chi tiết để tạo được một mạch mã hóa đầy đủ chức năng có khả năng bảo mật khối dữ liệu 128bit. Chúng tôi trình bày kết quả mô phỏng và tổng hợp thiết kế dựa trên phần mềm Quartus và bộ KIT DE2-115 trong phần 4, và kết luận nội dung công việc trong phần 5.

2. CÁC CÔNG TRÌNH LIÊN QUAN

Xu hướng nghiên cứu các hệ thống IoT đã và đang được quan tâm phát triển rộng khắp trên đa dạng các ứng dụng từ nhiều nguồn lực xã hội. Hệ thống IoT càng được phổ biến trên diện rộng với nhiều lĩnh vực ứng dụng và nhiều công nghệ được phát triển để hỗ trợ [3]. Khi lĩnh vực ứng dụng của IoT trải rộng, dữ liệu tạo ra từ các hệ thống IoT càng lớn và quan trọng thì nhu cầu bảo mật và an toàn trong hệ thống IoT càng là động lực và thách thức đối với tất cả các nghiên cứu triển khai hệ thống nhúng và IoT hiện đại. Tuy nhiên, hệ thống IoT hướng đến khả năng tối ưu tiết kiệm tài nguyên và sử dụng các thành phần sử dụng thường hạn chế hiệu năng tính toán. Vậy nên, việc sử dụng các giải thuật bảo mật tiên tiến như AES lại cần tài nguyên lớn, mức tiêu thụ năng lượng cao sẽ là rất khó để tối ưu các hệ thống IoT.

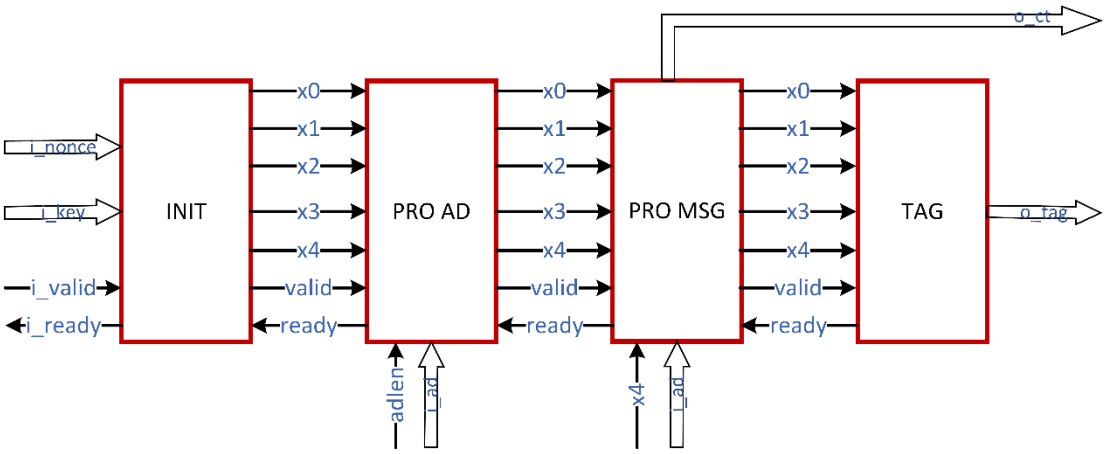
Giải thuật ASCON là giải thuật mã hóa trọng số nhẹ với hoạt động dựa trên nguyên lý xáo trộn dữ liệu và kỹ thuật hàm HASH đã được lựa chọn là một chuẩn hóa của NIST với khả năng tối ưu cho các hệ thống IoT [3]. Các nghiên cứu về giải thuật ASCON là rất đa dạng, từ các nghiên cứu chi tiết kỹ thuật bên trong đến các nghiên cứu đánh giá tổng thể giải thuật và so sánh với các giải thuật khác [4]. Tuy nhiên, giải thuật ASCON triển khai cụ thể trong xu thế cứng hóa các giải pháp bảo mật cho IoT lại còn rất hạn chế.

Các giải thuật mã hóa trọng số nhẹ tuy đã được NIST đề xuất thành chuẩn hóa nhưng vẫn chỉ đang ở giai đoạn đầu, phần lớn các giải thuật chỉ tập trung đề xuất ở dạng giải pháp phần mềm khả thi trên nền tảng nhúng với các vi xử lý và vi điều khiển [5]. Hiện có một số giải thuật cũng đã và đang được nghiên cứu và đề xuất thiết kế trên phần cứng như trong [6] sử dụng giải thuật COMET cho nền tảng FPGA và giải thuật AES theo định hướng ASIC như trong [7]. Nắm bắt xu hướng phát triển của các hệ thống IoT và truyền thông dữ liệu lớn trong các điều kiện rằng buộc là động lực để phát triển các giải pháp tích hợp cứng hóa các giải thuật mã hóa trọng số nhẹ lên vi mạch [6].

3. KIẾN TRÚC ĐỀ XUẤT CHO KHỐI MÃ HÓA

3.1. Hoạt động mã hóa

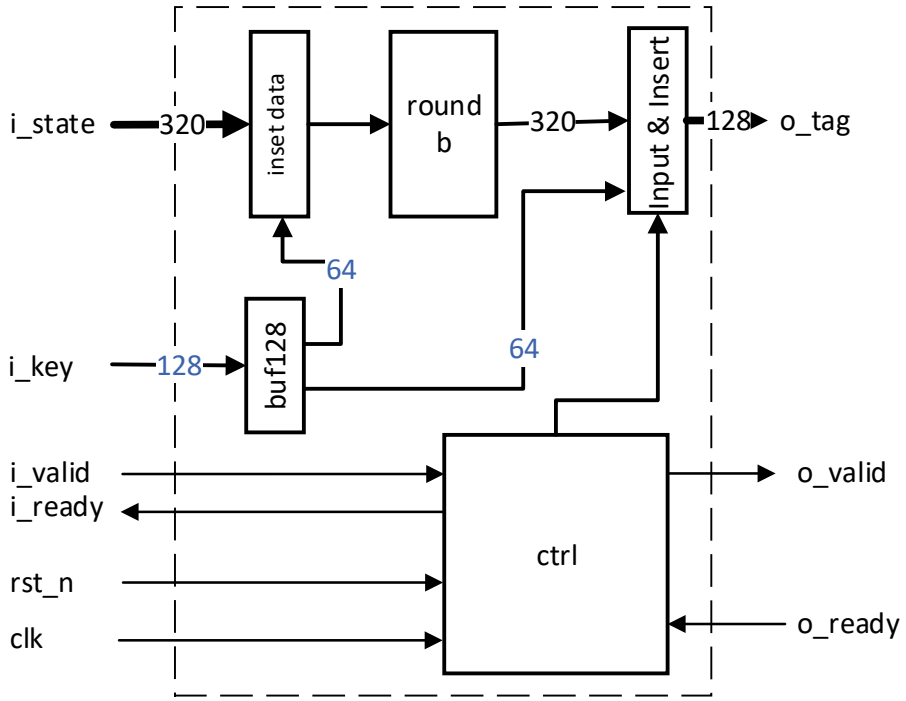
Giải thuật mã hóa ASCON được thực hiện qua bốn chức năng chính theo chuỗi nối tiếp cho mục tiêu ngẫu nhiên hóa chuỗi bản tin đầu vào. Hình 1 mô tả chuỗi chức năng mã hóa theo thuật toán ASCON. Trong giải thuật ASCON là tổ hợp các bước xáo trộn dữ liệu đầu vào và tổ hợp 5 vector trạng thái 64bit {x_0,x_1,x_2,x_3,x_4 }, qua mỗi quá trình xử lý sẽ nhận trạng thái vào để xáo trộn dữ liệu qua các hàm ROUND bậc phù hợp để tạo dữ liệu giả ngẫu nhiên đầu ra. Trừ quá trình khởi tạo sẽ sử dụng các khóa riêng tư KEY, dữ liệu công khai NONCE và thông tin mã hóa để tạo ra trạng thái khởi tạo.



Hình 1. Sơ đồ chức năng đề xuất cho mã hóa ASCON

Khởi động quá trình mã hóa là quá trình xáo trộn dữ liệu khóa công khai - NONCE và chìa khóa riêng bảo mật KEY để tạo được trạng thái khởi tạo. Từ trạng thái khởi tạo này sẽ được xáo trộn với dữ liệu liên kết ở khối xử lý dữ liệu liên kết PRO_AD. Khối xử lý bản tin sẽ xoắn dữ liệu bản tin đầu vào với trạng thái thu được từ khối xử lý dữ liệu liên kết, trong trường hợp bản tin có độ dài lớn hơn 128bit sẽ sử dụng thêm hàm xáo trộn ROUND 8 bước. Bản tin mã hóa thu được từ kết quả xáo trộn dữ liệu bản tin với trạng thái sau xử lý dữ liệu liên kết có độ dài tương ứng với bản tin đầu vào. Thẻ mã hóa đầu ra luôn có độ dài cố định là 128bit được tạo ra từ khối TAG bằng cách xoắn trạng thái ra của khối PRO_MSG.

Các khối chức năng chính của hoạt động mã hóa sẽ có chức năng xáo trộn dữ liệu từ các đầu vào. Dữ liệu vào sẽ được xử lý để tạo trạng thái gồm năm vector 64bit sau đó ngẫu nhiên hóa dữ liệu thông qua khối SBOX. Như trong Hình 2 trình bày chi tiết kiến trúc đề xuất cho khối tạo thẻ mã hóa – TAG. Khối TAG sử dụng dữ liệu đầu vào là khóa riêng tư KEY để trộn với hai vector đầu tiên của trạng thái là x0 và x1. Khối dữ liệu 320bit của trạng thái sau trộn sẽ được đưa vào hàm xáo trộn ROUND 12 bước rồi lại được trộn với khóa KEY một lần nữa mới tạo ra thể TAG đầu ra. Thẻ TAG đầu ra là tổ hợp của hai vector đầu tiên trong 5 vector của 320 bit trạng thái ra hàm xáo trộn.

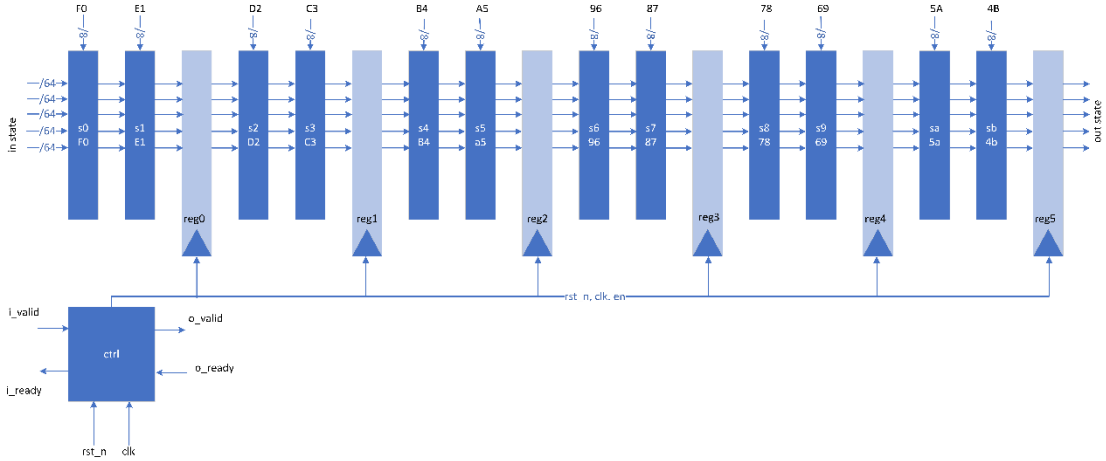


Hình 2. Khối chức năng đề xuất cho module tạo thẻ mã hóa - TAG

3.2. Kiến trúc đề xuất

Hoạt động xáo trộn dữ liệu trong các khối chức năng của quá trình mã hóa sử dụng hàm ROUND với số bước khác nhau, trong giải. Đầu vào hàm xáo trộn là trạng thái gồm 5 vector 64 và sử dụng hoạt động xáo trộn của SBOX cho mỗi bước bên trong

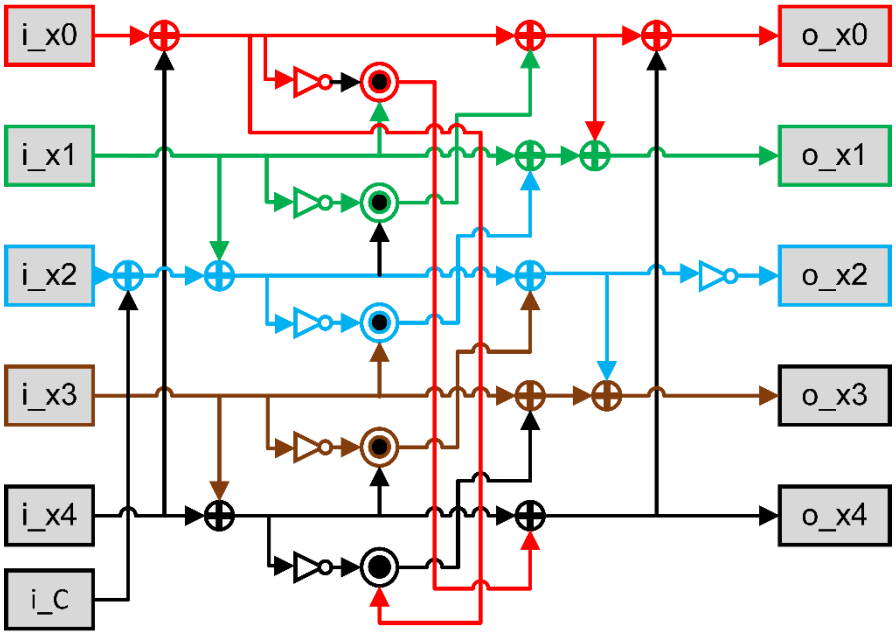
hàm ROUND. Thiết kếnày chúng tôi hướng đến khả năng tiết kiệm chi phí thời gian thực thi mã hóa nên kết hợp hai bước trong một chu kỳ xung. Do đó, hoạt động xáo trộn bên trong hàm ROUND 12 bước được mô tả như trong Hình 3, và khối ROUND này hoàn thành chỉ cần 6 chu kỳ nhịp – clk và đồng thời cũng giảm một nữa số thanh ghi cần dùng để lưu 320 bit trạng thái.



Hình 3. Khối xoắn trộn dữ liệu của Hàm ROUND 12 bước.

Tại mỗi bước xáo trộn dữ liệu chúng tôi sử dụng kỹ thuật thiết kế logic tổ hợp để thực hiện các hàm logic cơ bản như AND, XOR và kết nối các mạch trung gian để bảo đảm tính ổn định của thiết kế. Trong Hình 4 mô tả chi tiết kiến trúc thực thi khối mã hóa cơ bản SBOX của thuật toán ASCON. Kỹ thuật xáo trộn dữ liệu của thuật toán ASCON là sự kết hợp chia nhỏ nhóm dữ liệu và xoắn để tăng tính ngẫu nhiên hóa dữ liệu.

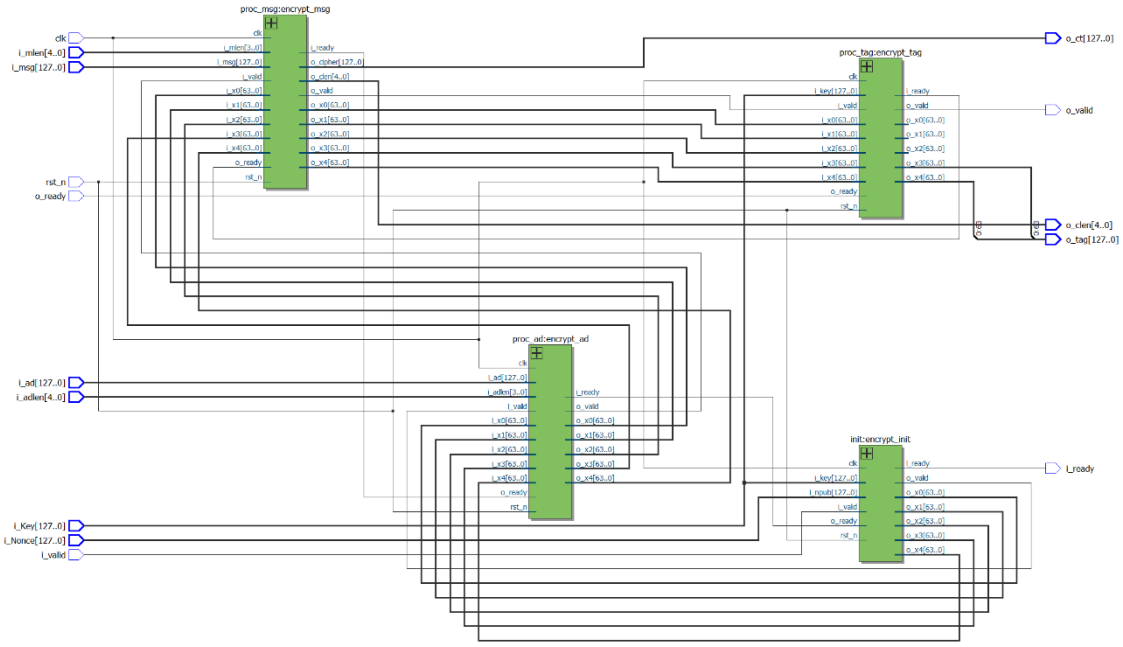
Hoạt động xáo trộn dữ liệu được thực hiện theo nhóm 320 bit với 5 vector độc lập 64 bit sẽ được kết hợp tại đầu vào, sau đó thực hiện phép đảo để kết hợp xoắn với nhánh đan chéo ở đầu ra. Đầu ra của mạch xáo trộn dữ liệu cũng là nhóm 320 bit trạng thái với 5 vector 64 bit đồng thời. Do đặc thù của hoạt động xáo trộn dữ liệu chỉ sử dụng các hàm logic cơ bản nên trong thiết kế này chúng tôi để xuất sử dụng kỹ thuật mạch tổ hợp.



Hình 4. Sơ đồ nguyên lý khối xoắn trộn SBOX

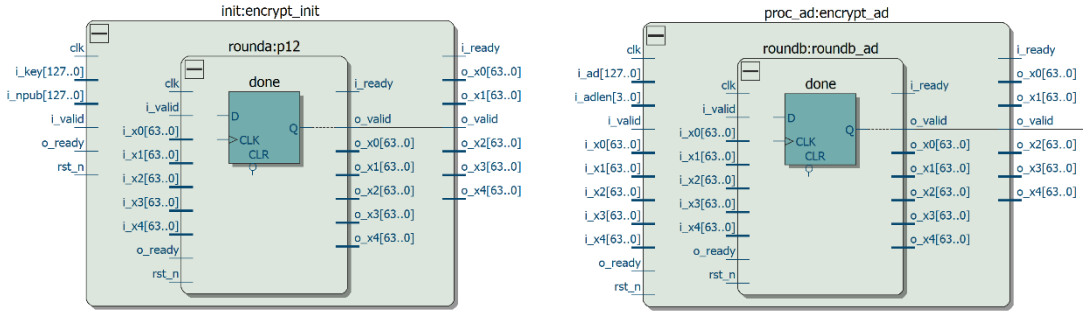
3.3. Kiến trúc tổng hợp của bộ mã hóa

Trên cơ sở tìm hiểu nguyên lý làm việc của giải thuật mã hóa ASCON được công bố tại NIST, chúng tôi đã tiến hành thiết kế lại giải thuật này phù hợp với xu thế thiết kế vi mạch. Thiết kế này đã sử dụng ngôn ngữ mô tả phần cứng Verilog kết hợp với công cụ tổng hợp Quartus để thực thi và thu được kiến trúc của bộ mã hóa theo thuật toán ASCON như trong Hình 5. Thiết kế đề xuất này sử dụng kỹ thuật đồng bộ theo xung nhịp và hoạt động trao đổi bắt tay đồng bộ bằng cặp tín hiệu valid/ready. Hoạt động chuyển dữ liệu bắt tay để bảo đảm thông tin trao đổi giữa các khối con là an toàn và tin cậy, điều này cho phép hệ thống hoạt động theo đúng nguyên lý mã hóa theo 4 nhóm chức năng đã được đề xuất trong Hình 1.



Hình 5. Kiến trúc bộ mã hóa tổng hợp ở mức RTL

Các khối chức năng bên trong bộ mã hóa sử dụng các hàm xáo trộn ROUND 8 bước hoặc 12 bước để ngẫu nhiên hóa dữ liệu. Dữ liệu đầu vào sẽ được trộn với 320 bit trạng thái vào bằng hàm logic XOR. Trong Hình 6 là kiến trúc tổng hợp thu được từ công cụ Quartus cho khối thiết lập đầu vào INIT và khối xử lý dữ liệu liên kết PROC_AD.



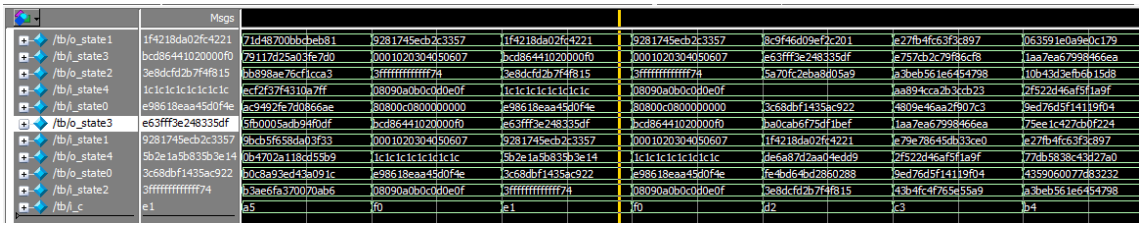
Hình 6. Kiến trúc tổng hợp mức RTL cho khối thiết lập INIT và PROC_AD

Trong công trình này chúng tôi tập trung thiết kế cho giải thuật mã hóa ASCON cho các khối bản tin đầu vào nhỏ hơn 128bit (16Byte). Khối xử lý bản tin sẽ không sử dụng hàm xáo trộn ROUND mà chỉ sử dụng chức năng trộn dữ liệu bằng hàm logic XOR. Đầu ra bản tin mã hóa Cipher được tổng hợp từ nhóm trạng thái ra của khối xử lý bản tin PROC_MSG và thẻ xác thực là kết hợp của hai vector 64bit $\{x_4, x_3\}$ tại đầu ra của khối tạo thẻ TAG.

4. MÔ PHỎNG ĐỂ ĐÁNH GIÁ THỬ NGHIỆM

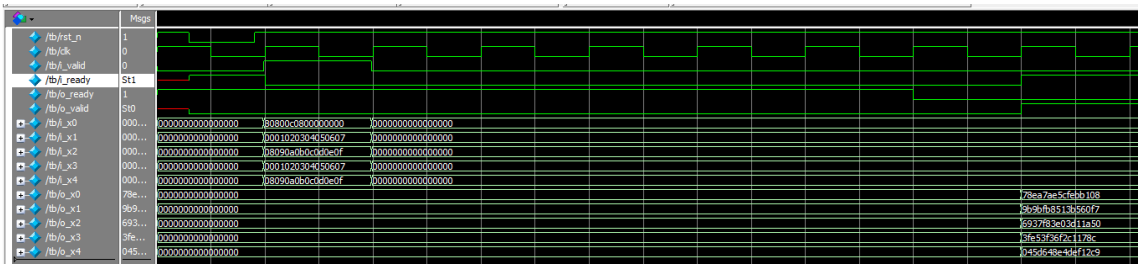
Quá trình tìm hiểu thuật toán ASCON được thi hiện dựa trên các công bố của NIST tại các vòng lựa chọn giải pháp chuẩn hóa cho hoạt động mã hóa bảo mật ứng dụng trong các hệ thống IoT. Các giải thuật bảo mật được NIST công bố bao gồm cả tài liệu và mã nguồn chuẩn hóa cho các dòng vi xử lý và vi điều khiển 8÷16bit, và có cả mã nguồn thực thi mã hóa và giải mã theo ngôn ngữ C. Vậy nên, chúng tôi lựa chọn phương pháp kiểm tra đánh giá song song kết hợp quá trình thực thi mã hóa trên mã nguồn C được công bố để có được dữ liệu đầu vào và đầu ra cho hoạt động kiểm thử thiết kế. Hoạt động kiểm thử được thực hiện theo nguyên lý từ khối nhỏ cơ bản đến các khối chức năng cụ thể của quá trình mã hóa.

Trong Hình 7 là kết quả mô phỏng đánh giá hoạt động xáo trộn dữ liệu tại khối SBOX mà chúng tôi đã thiết kế bằng công cụ ModelSim tích hợp trong Quartus. Khối mã hóa SBOX này được thiết kế theo nguyên lý mạch tổ hợp nên trong kết quả mô phỏng sẽ không thể hiện được độ trễ thời gian đáp ứng từ khi có dữ liệu vào đến lúc tín hiệu ra ổn định.

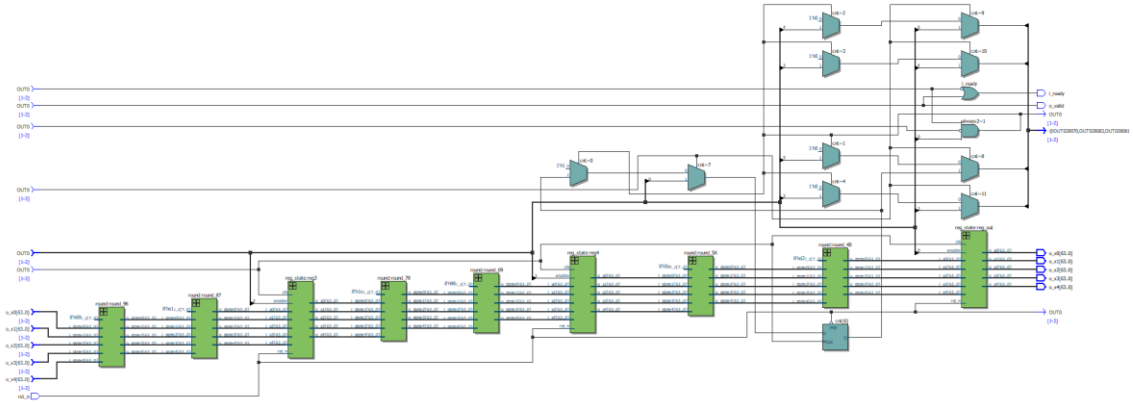


Hình 7. Kết quả kiểm thử khối mã hóa SBOX

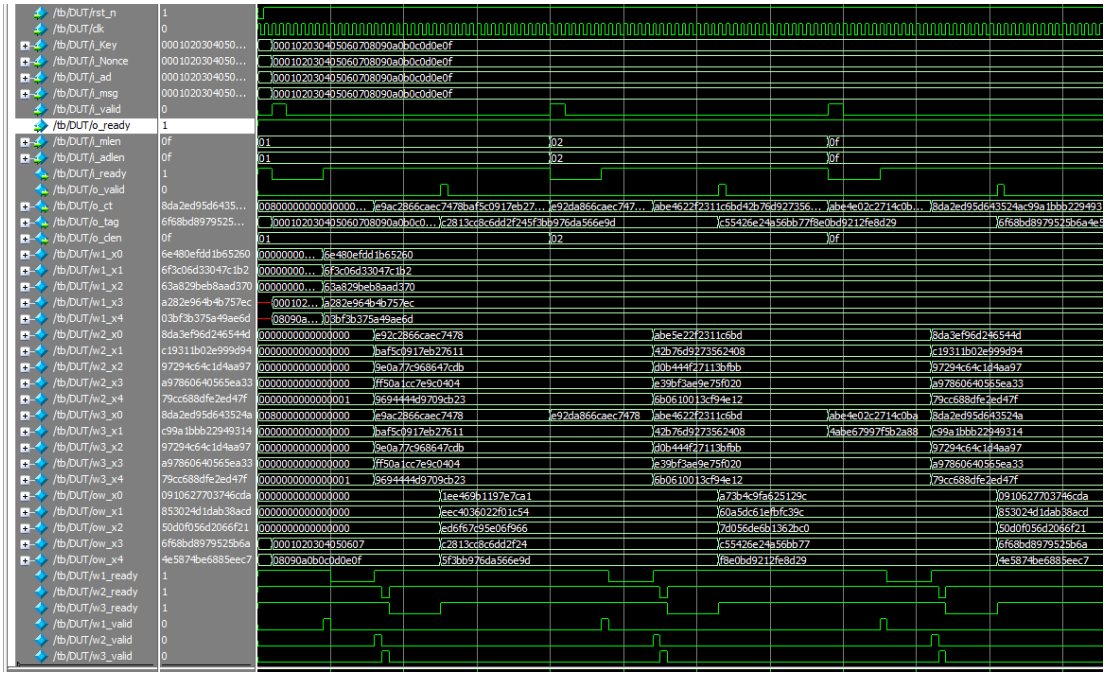
Kết quả mô phỏng đánh giá cho hàm xáo trộn ROUND với số bước là 12 được trình bày trong Hình 8. Ở khối con thực hiện chức năng hàm xáo trộn ROUND 12 bước thực hiện theo thiết kế động bộ gồm tín hiệu tái thiết lập rst_n và xung nhịp clk. Qua kết quả mô phỏng cho thấy độ trễ đáp ứng của hàm ROUND là 7 xung nhịp; điều này có thể giải thích là do thiết kế đề xuất trong Hình 3 cần thêm một xung nhịp để ghi dữ liệu đầu ra ổn định và sự bắt tay giữa đầu vào và mạch ghi tại đầu vào của khối xáo trộn này. Trong thiết kế này chúng tôi sử dụng một thanh ghi đệm để tạo trễ cho tín hiệu xác thực lối ra thay cho khối điều khiển phức tạp nhưng lại có tính ổn định cao (Hình 9). Nhưng thiết kế của chúng tôi hướng đến khả năng cân bằng giữa chi phí và hiệu năng nên chúng tôi kết hợp hai vòng mới sử dụng một thanh ghi đệm. Kỹ thuật thiết kế này cho phép chúng tôi tiết kiệm chi phí thời gian khi giảm được ½ số xung nhịp để thực hiện các khối bên trong bộ mã hóa.



Hình 8. Giản đồ xung mô tả hoạt động xáo trộn dữ liệu



Hình 9. Thiết kế chi tiết hàm ROUND



Hình 10. Giản đồ thời gian hoạt động mã hóa dữ liệu

Dựa trên các kết quả tổng hợp các thành phần chức năng ở trên, chúng tôi tổng hợp mạch mã hóa ASCON với kỹ thuật mã hóa 128bit. Khối mã hóa sẽ nhận thông tin đầu vào là các khối 128bit gồm: KEY, NONCE, AD và MSG cùng với các tín hiệu điều

khiển bắt tay. Đầu ra sẽ là kết quả mã hóa o_ct và thẻ xác thực ra o_tag. Kết quả mô phỏng kiểm thử được trình bày như trong Hình 11 và được so sánh đối chiếu với kết quả mã hóa thu được từ mã nguồn được cung cấp chính thức trên [8].

5. KẾT LUẬN

Trong bài báo này chúng tôi dã đề xuất một thiết kế cho bộ mã hóa ASCON khả thi trên nền tảng FPGA và cũng có thể hướng đến triển khai trên ASIC. Bộ mã hóa ASCON này có thể hoạt động ổn định với các khối tin nhỏ hơn 128bit. Quá trình mã hóa mất 15 xung để tạo được bản tin mã hóa và 9 xung để tạo nên thẻ mã hóa và kết thúc một quy trình mã hóa.

Kết quả tổng hợp các chi phí thiết kế cho bộ mã hóa ASCON được thể hiện như trong Hình 12. Thiết kế này sử dụng tài nguyên nhiều hơn các thiết kế của COMET [7], nhưng có ưu điểm nổi bật là tốc độ mã hóa dữ liệu lớn hơn nhiều. Kết quả chi phí thiết kế tăng cao trong kiến trúc đề xuất này hoàn toàn có thể giải thích từ nguyên lý làm việc của giải thuật ASCON sử dụng các khối xáo trộn lớn đến $5 \times 64 = 320(bit)$, đồng thời quá trình cần lặp lại nên cần sử dụng thanh ghi rất nhiều. Thiết kế này chỉ mất 15 chu kỳ để mã hóa 128bit thông tin thì hoàn toàn có thể triển khai trong các hệ thống IoT thời gian thực. Đây cũng là một nguyên nhân chính khi NIST đã lựa chọn giải thuật này cho vòng 3 của quá trình lựa chọn chuẩn hóa cho hoạt động bảo mật trọng số nhẹ trong các hệ thống IoT.

Flow Summary	
Flow Status	Flow Failed - Mon Jan 08 12:42:13 2024
Quartus II 64-Bit Version	13.1.0 Build 162 10/23/2013 SJ Web Edition
Revision Name	encrypt
Top-level Entity Name	encrypt
Family	Cyclone IV E
Device	EP4CE115F29C7
Timing Models	Final
Total logic elements	28,823 / 114,480 (25 %)
Total combinational functions	28,822 / 114,480 (25 %)
Dedicated logic registers	4,955 / 114,480 (4 %)
Total registers	4955
Total pins	789 / 529 (149 %)
Total virtual pins	0
Total memory bits	0 / 3,981,312 (0 %)
Embedded Multiplier 9-bit elements	0 / 532 (0 %)
Total PLLs	0 / 4 (0 %)

Hình 12. Kết quả thông tin tổng hợp thiết kế khối mã hóa trên KIT DE2-115

Từ kết quả thu được của kiến trúc đề xuất khối mã hóa cho giải thuật ASCON, chúng tôi sẽ hướng đến hoàn thiện cả khối giải mã dựa trên lõi giải thuật là khối SBOX đã hoàn thiện và sẽ tổng hợp trên cùng một kiến trúc hoàn chỉnh. Đồng thời thiết kế này cần được kiểm chứng cụ thể trên board FPGA hoàn chỉnh và có thể kết hợp với các vi xử lý tích hợp để phát triển thành một sản phẩm hoàn chính có khả năng ứng dụng cao.

TÀI LIỆU THAM KHẢO

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey," *Computer Networks,* vol. 54, p. 2787–2805, 2010.

[2] Q. Jing, A. Vasilakos, J. Wan, J. Lu and D. Qiu, "Security of the Internet of Things: Perspectives and challenges," *Wireless Networks,* vol. 20, pp. 2481-2501, November 2014.

[3] W. Anani, A. Ouda and A. Hamou, "A Survey Of Wireless Communications for IoT Echo-Systems," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)*, 2019.

[4] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schläffer, "Ascon v1.2: Lightweight Authenticated Encryption and Hashing," *J. Cryptol.,* vol. 34, p. 33, 2021.

[5] C. Dobraunig, M. Eichlseder, F. Mendel and M. Schläffer, *Ascon PRF, MAC, and Short-Input MAC,* 2021.

[6] I. K. Dutta, B. Ghosh and M. Bayoumi, "Lightweight Cryptography for Internet of Insecure Things: A Survey," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019.

[7] T. M. N. Lê Văn Thanh Vũ, "Nghiên cứu và thực thi bộ mã hóa bảo mật theo thuật giải Comet với khối 128bit," *Tạp chí Khoa học, Trường ĐH Khoa học,* 2023.

[8] NIST, "Lightweight Cryptography," [Online]. Available: https://csrc.nist.gov/ Projects/ Lightweight-Cryptography.

DESIGN AND IMPLEMENTATION OF THE ASCON ENCRYPTION ALGORITHM ON THE FPGA PLATFORM - DE2-115 KIT

Le Van Thanh Vu*, Hoang Dai Long

Faculty of Electronics, Electrical Engineering and Material Technology,
University of Sciences, Hue University

*Email: vulvt@hueuni.edu.vn

ABSTRACT

The development of IoT systems has been and remains a significant trend in the field of electronic technology, aiming toward a wide range of applications in modern society. A lightweight cryptography (LWC) solution is being standardized to meet the needs of modern IoT systems better. The ASCON encryption solution has been selected by the U.S. National Institute of Standards and Technology (NIST) as one of the recommended encryption standards in the final round. In this paper, we focus on the research, design, and evaluation of encryption operations based on this algorithm, to enable its application in next-generation IoT systems. The hardware implementation of the ASCON algorithm is described in detail, and its comprehensive simulation and evaluation have demonstrated advantages in stability as well as in optimization of speed and integration capability into systems. The obtained results from the ASCON encryption circuit design indicate the potential applicability of this algorithm to modern IoT systems across a wide range of applications.

Keywords: IC System, IC design, LWC, ASCON.