NGHIÊN CỨU VÀ THỰC THI BỘ MÃ HÓA BẢO MẬT THEO THUẬT GIẢI COMET VỚI KHỐI 128BIT

Lê Văn Thanh Vũ*, Trương Minh Nhật

Khoa Điện, Điện tử & CNVL, Trường Đại học Khoa học, Đại học Huế

*Email: vulvt@hueuni.edu.vn

Ngày nhận bài: 21/8/2023; ngày hoàn thành phản biện: 28/8/2023; ngày duyệt đăng: 4/12/2023

TÓM TẮT

IoT là một xu thế phát triển vượt trội của lĩnh vực điện tử có phổ ứng dụng rộng rải trải khắp các lĩnh vực kinh tế - xã hội. Nghiên cứu bảo mật cho các hệ thống IoT sẽ góp phần gia tăng tính khả thi và thúc đẩy khả năng hiện thực hóa các hệ thống điện tử cỡ lớn đáp ứng tốt hơn các nhu cầu phát triển của xã hội. Giải thuật mã hóa COMET với trọng tâm là khối mã hóa xoắn theo chế độ đếm không dùng SBOX để tối ưu tài nguyên trong quá trình thực thi đồng thời nâng cao khả năng bảo mật thông tin. Trong bài báo này tập trung phân tích,thực thi giải thuật COMET và đã thu được kết quả đánh giá bước đầu đáng tin cậy. Đồng thời kết quả tổng hợp của thiết kế đã chứng minh được khả năng ứng dụng của giải thuật vào các thiết kế hệ thống IoT là hợp lý.

Từ khóa: Bảo mật, IoT, LWC – LightWeights Cryptographic.

1. MỞ ĐẦU

Xu thế IoT đã và đang là hướng phát triển được quan tâm hàng đầu của lĩnh vực điện tử và công nghệ hiện đại. Khả năng ứng dụng linh hoạt và hiệu quả trong đa lĩnh vực từ sản xuất nông nghiệp, công nghiệp đến y tế và cả quân sự. Đồng thời IoT cũng là điểm đầu của nguồn dữ liệu đa dạng và rất quan trọng trong xã hội hiện đại, nguồn dữ liệu này cần được bảo vệ và tăng tính cậy của tất cả các hệ thống IoT. Tuy nhiên, hệ thống IoT lại thường sử dụng các điểm nút có các vi xử lý hoặc vi điều khiển tối giản có nhiều hạn chế về tài nguyên. Điều này tạo nên ràng buộc khó giải quyết được trọn vẹn bài toán bảo mật trong các hệ thống IoT.

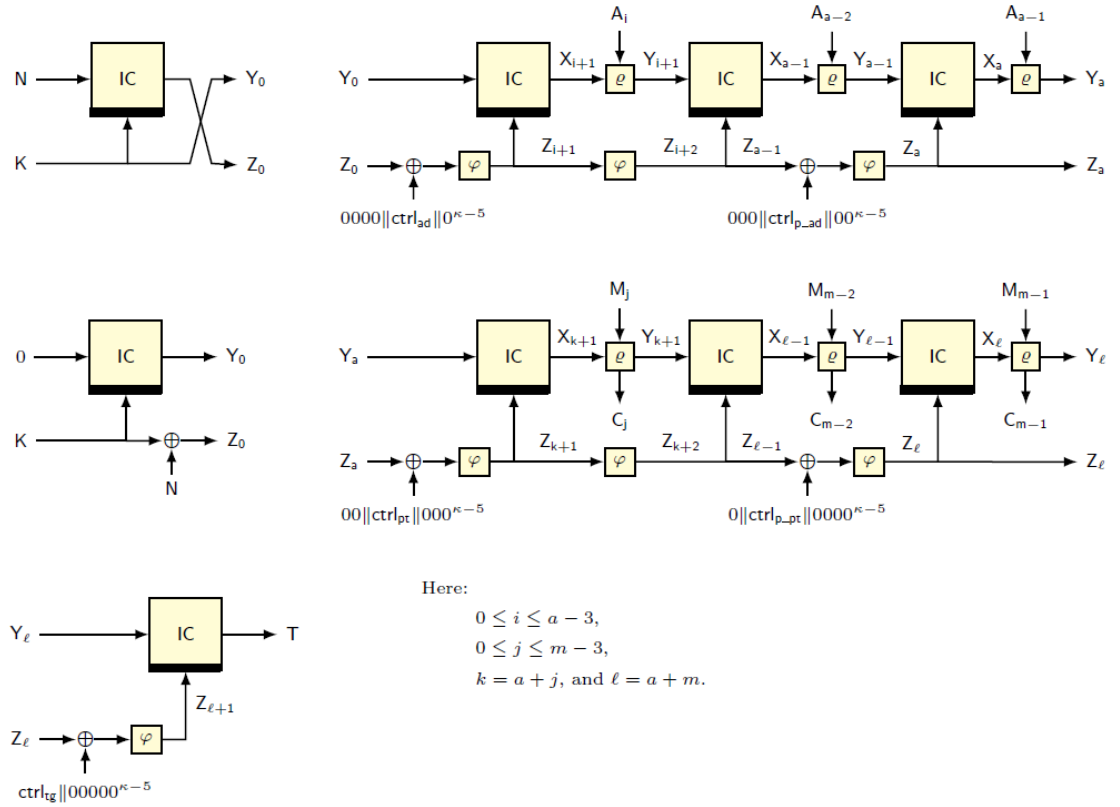
Công trình này được phát triển trong định hướng sử dụng các giải thuật mã hóa hiệu quả cao nhưng lại yêu cầu ít tài nguyên của hệ thống – LWC (Lightweight Cryptography) [1]. Giải thuật COMET được phát triển trên nền tảng xoắn trộn dữ liệu để tạo bản tin mã hóa giả ngẫu nhiên nhưng lại không sử dụng nguyên lý SBOX đã phổ

biến trong định hướng mã hóa PSA đã có.

Bài báo này tập trung vào khả năng chuyển đổi giải thuật COMET đã được phát triển trên nền mã nguồn C++ của NIST đã công bố thành kiến trúc khả thi trên nền công nghệ FPGA và có thể phát triển thành ASIC.

2. GIẢI THUẬT MÃ HÓA COMET

Giải thuật mã hóa COMET được đưa vào các vòng tuyển chọn tiêu chuẩn mã hóa cho các hệ thống IoT của NIST đã là một minh chứng sống động cho sự tin cậy và hiệu quả của thuật toán này. Thuật toán mã hóa COMET (*Counter Mode Encryption with authentication Tag*) là sự kết hợp giữa kỹ thuật xoắn dữ liệu với thẻ xác thực để tạo ra một cơ chế mã hóa an toàn bảo vệ các hoạt động truyền tin [2] [3] [3]. COMET sử dụng chế độ đếm để mã hóa thông qua việc xoắn khóa và dữ liệu liên kết tạo nên một chuỗi bit giả ngẫu nhiên và sau đó được XOR với luồng bit của bản tin để tạo nên bản tin mã hóa. Thẻ xác thực là một đột phá quan trọng của thuật toán COMET, thẻ xác thực sẽ có tính quyết định trong quá trình mã hóa và giải mã vì đây chính là tầng khóa cuối cùng để phía giải mã xác định độ tin cậy của thông tin được lan truyền. Toàn bộ quá trình thực hiện mã hóa và giải mã của thuật toán COMET được mô tả như trong Hình 1.



Hình 1: Nguyên lý mã hóa và giải mã COMET [4]

Các ưu điểm nổi trội của COMET:

- ✓ Bảo mật: COMET đảm bảo tính bảo mật của dữ liệu bằng cách mã hóa dữ liệu bằng kỹ thuật mã hóa Chế độ truy cập.
- ✓ Tính toàn vẹn: Các thẻ xác thực đảm bảo tính toàn vẹn của dữ liệu, vì bất kỳ sửa đổi nào trong quá trình truyền sẽ dẫn đến việc thẻ không khớp khi xác minh.
- ✓ Hiệu quả: Chế độ mã hóa Counter Mode của COMET hiệu quả đối với các tập dữ liệu lớn vì nó cho phép mã hóa và giải mã song song.
- ✓ Không từ chối: Cơ chế xác thực có thể cung cấp bằng chứng cho thấy dữ liệu có nguồn gốc từ người gửi.
- ✓ Giao tiếp an toàn: COMET phù hợp để liên lạc an toàn qua các mạng không đáng tin cậy, vì nó ngăn chặn việc nghe lén, giả mạo và hỏng dữ liệu.
- ✓ Điều quan trọng cần lưu ý là mặc dù COMET cung cấp các tính năng bảo mật mạnh mẽ, nhưng hiệu quả của nó phụ thuộc vào việc triển khai đúng cách, quản lý khóa và tuân thủ các phương pháp hay nhất về bảo mật.

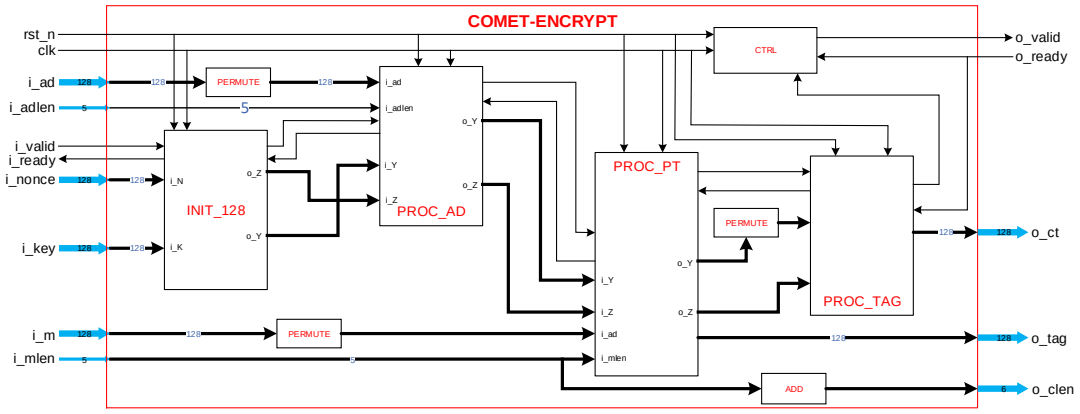
Từ nguyên lý mã hóa của giải thuật COMET, tại công trình [5] đã thực hiện được khối mã hóa trọng tâm trên nền tảng CHISEL, là một công cụ kết hợp với ngôn ngữ mô tả bậc cao. Trong bài báo này chúng tôi tiếp tục phát triển và hoàn thiện toàn bộ chức năng mã hóa của giải thuật COMET bằng cách sử dụng trực tiếp ngôn ngữ mô tả Verilog và công cụ Quartus hỗ trợ tổng hợp lên KIT DE2-115.

3. KIẾN TRÚC ĐỀ XUẤT CHO KHỐI MÃ HÓA

Giải thuật COMET là một hướng phát triển của nhóm các giải thuật mật mã hóa khóa công khai – PSA vốn rất được phổ biến trong lĩnh vực công nghệ thông tin, và nổi bật vẫn là thuật giải AES đã và đang được ứng dụng cho mạng toàn cầu Internet. Các giải thuật RSA vốn chủ yếu sử dụng các khối xáo trộn thông tin nhằm ngẫu nhiên hóa để bảo mật thông tin vốn cần rất nhiều tài nguyên tính toán. COMET được phát triển theo nguyên lý hạn chế tính toán mà tập trung vào hoạt động xoắn trộn để ngẫu nhiên hóa dữ liệu. Do vậy, giải thuật COMET sẽ không yêu cầu nhiều tài nguyên của hệ thống và phù hợp với các ứng dụng nhỏ gọn của xu thế IoT hiện đại.

3.1. Mô tả kiến trúc chung

Qua quá trình tìm hiểu và thử nghiệm cụ thể với bộ mã hóa COMET 128bit trên mã nguồn C++ đã được chuẩn hóa, giải thuật mã hóa COMET được chuyển hóa thành giải pháp cứng hóa thông qua ngôn ngữ mô tả phần cứng Verilog. Trong Hình 2 mô tả nguyên lý tổ chức kiến trúc đề xuất cho bộ mã hóa để thực hiện thuật giải COMET trên nền tảng FPGA và cũng có thể hướng đến khả năng tổng hợp khả thi trên ASIC.

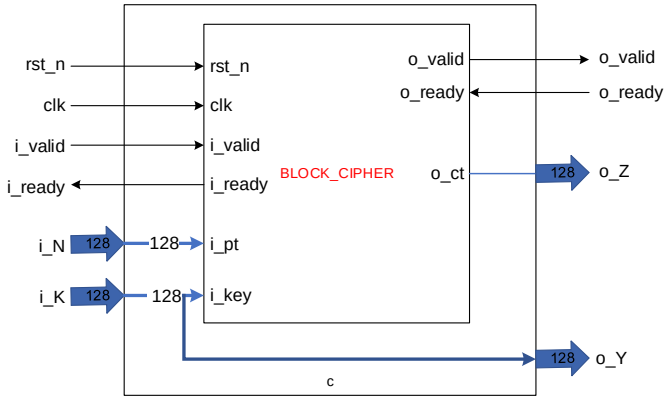


Hình 2: Kiến trúc đề xuất cho bộ mã hóa

Trong kiến trúc đề xuất này bộ mã hóa vẫn được chia thành bốn khối con cơ bản là khối thiết lập INIT128, khối xử lý dữ liệu liên kết PROC_AD, khối mã hóa bảng tin PROC_PT và khối tạo TAG. Tuy nhiên, trong quá trình cứng hóa giải thuật được đề xuất từ phần mềm không thể linh hoạt tương đồng hoàn toàn mà cần cải biến và thích ứng với nguyên lý thiết kế vi mạch. Do vậy, bài báo này chỉ tập trung vào hoạt động mã hóa với các khối tin không lớn hơn 128bit và được lượng hóa theo số lượng 1byte=8bit.

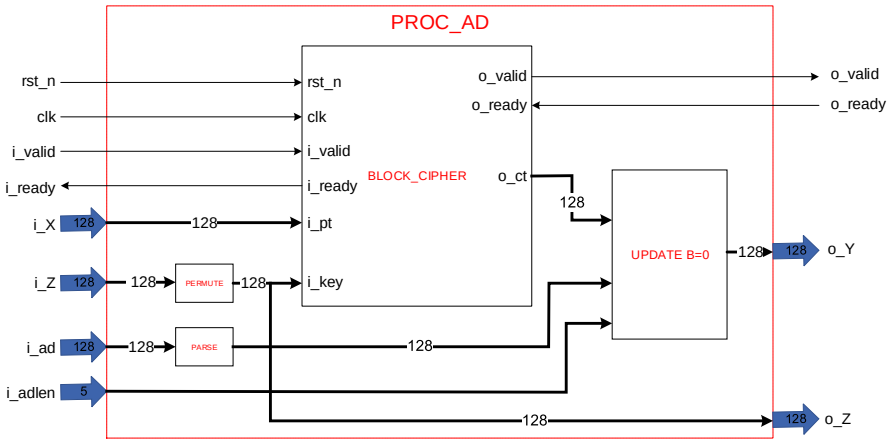
3.2. Mô tả chi tiết

Thuật toán mã hóa COMET lấy trọng tâm là khối mã hóa BLOCK_CIPHER có chức năng xoắn dữ liệu đầu vào để tạo khối dữ liệu ngẫu nhiên có cùng kích thước nhằm tăng tính bảo mật. Trong công trình [5] đã đề xuất chi tiết nhưng bằng ngôn ngữ CHISEL gần với các ngôn ngữ bậc cao nên chưa phù hợp với nền tảng FPGA cũng như khả năng tổng hợp và kiểm thực trên các công cụ dành cho lĩnh vực thiết kế vi mạch. Trong bài báo này chúng tôi phát triển lại khối mã hóa này và từ đó xây dựng đầy đủ các khối chức năng để tổng hợp thành một bộ mã hóa COMET hoàn chỉnh. Trong Hình 3 mô tả cụ thể kiến trúc chức năng thiết lập dữ liệu đầu vào từ khóa công khai KEY và khối NONCE để tạo các luồng bit đầu vào mã hóa.

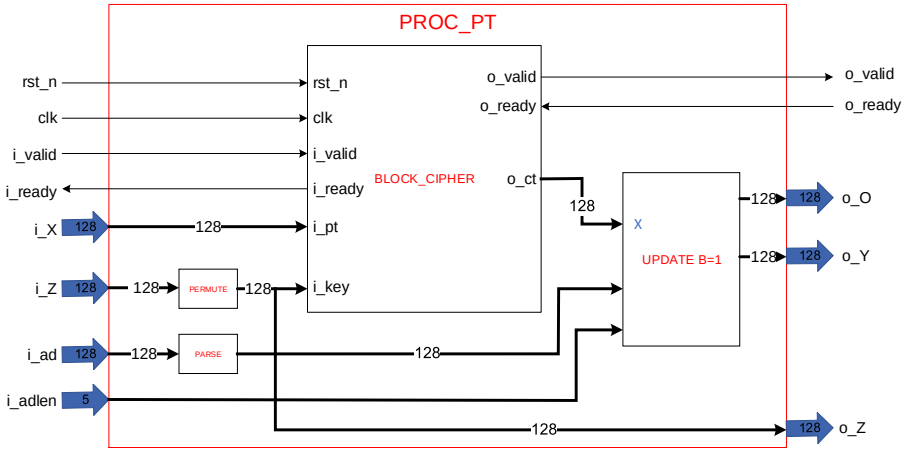


Hình 3: Kiến trúc thực hiện chức năng thiết lập chuỗi dữ liệu đầu vào bộ mã hóa

Từ luồng bit đầu vào của khối thiết lập sẽ được xoắn trộn tiếp với dữ liệu liên kết để tăng tính ngẫu nhiên hóa của dữ liệu thông qua chức năng xử lý dữ liệu liên kết PROC_AD như trong Hình 4.



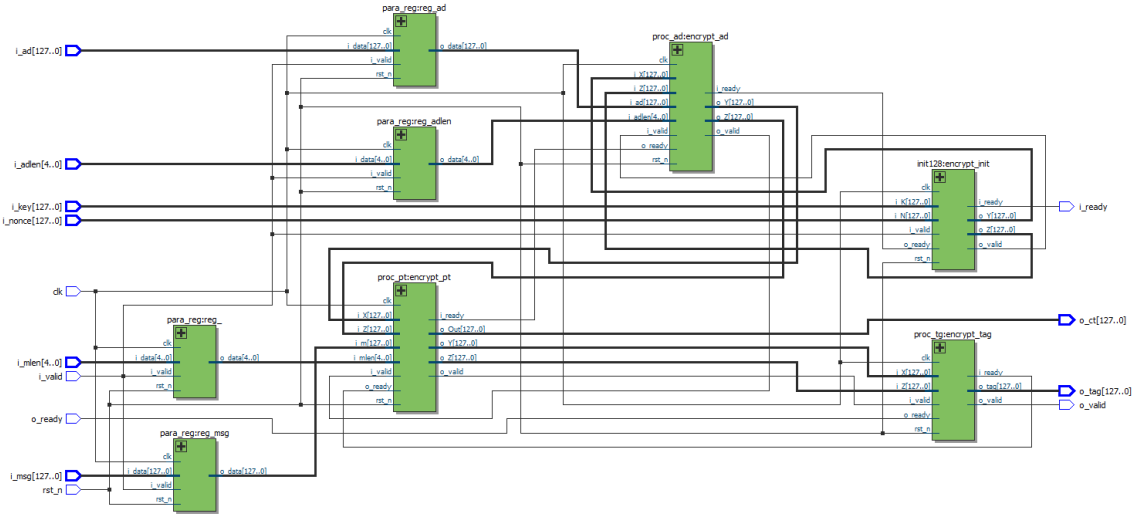
Hình 4: Kiến trúc đề xuất cho khối xử lý dữ liệu liên kết.



Hình 5: Kiến trúc chi tiết của khối chức năng xử lý dữ liệu bản tin.

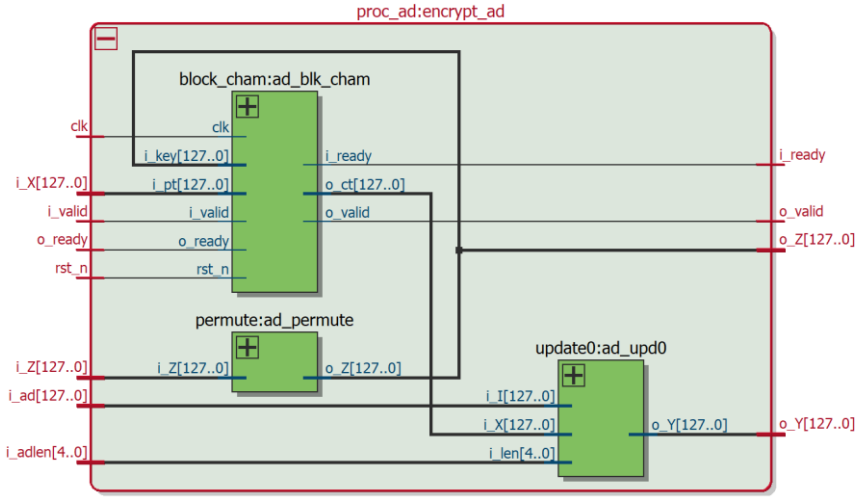
3.3. Kết quả tổng hợp bằng công cụ Quartus

Thông qua quá trình phân tích chức năng cụ thể bộ mã hóa được thực thi bằng ngôn ngữ thiết kế Verilog kết hợp với công cụ Quartus để tiến hành mô phỏng và kiểm thực cụ thể. Trong Hình 6 là kết quả tổng hợp thực tế của bộ mã hóa COMET 128bit từ công cụ RTL viewer.

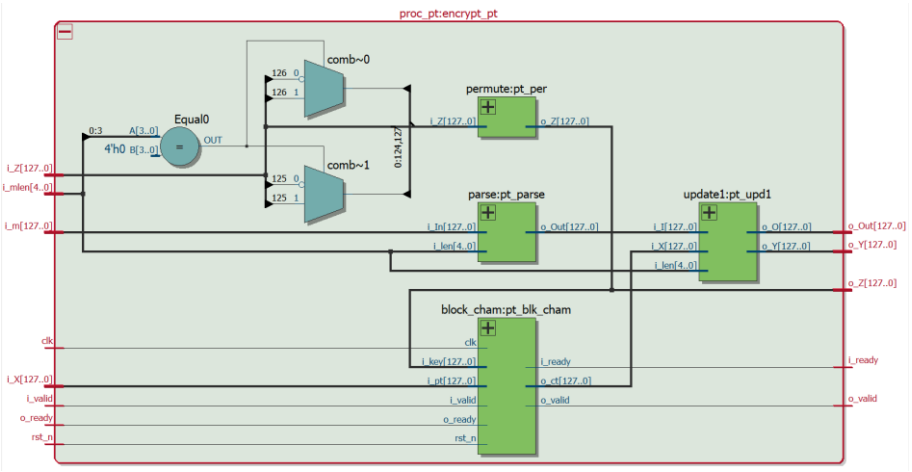


Hình 6: Kiến trúc chức năng của bộ mã hóa COMET tổng hợp được

Và trong các Hình 7 và Hình 8 là kiến trúc thực tế chúng tôi đã xây dựng tương ứng với các chức năng xử lý dữ liệu kết hợp với xử lý dữ liệu bản tin. Qua các kết quả tổng hợp đều cho thấy sự hợp lý và tin cậy của đề xuất kiến trúc đã trình bày trong các mục 3.1 và 3.2 của công trình này.



Hình 7: Kiến trúc chi tiết chức năng xử lý dữ liệu liên kết – AD

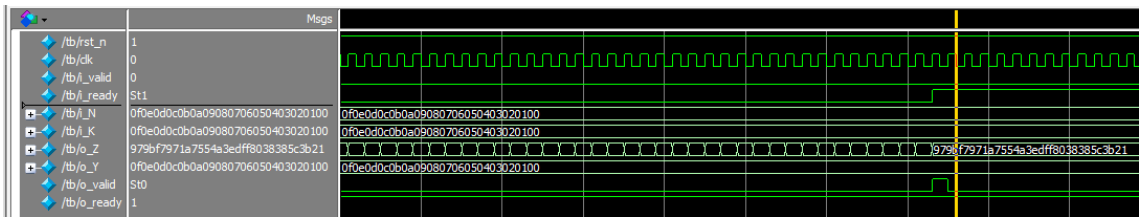


Hình 8: Kiến trúc chi tiết khối xử lý thông tin đầu vào

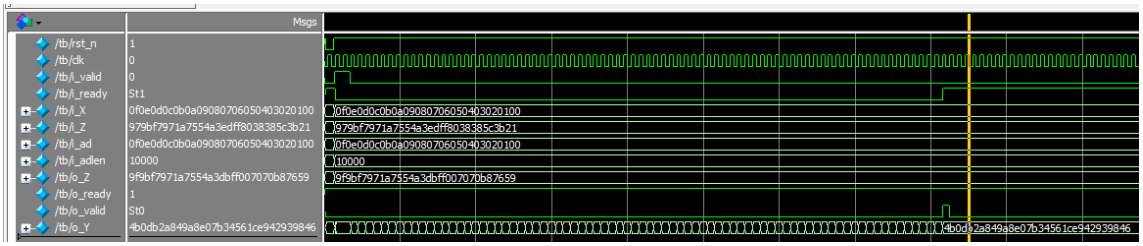
4. MÔ PHỎNG ĐỂ ĐÁNH GIÁ THỬ NGHIỆM

4.1. Mô phỏng khối chức năng

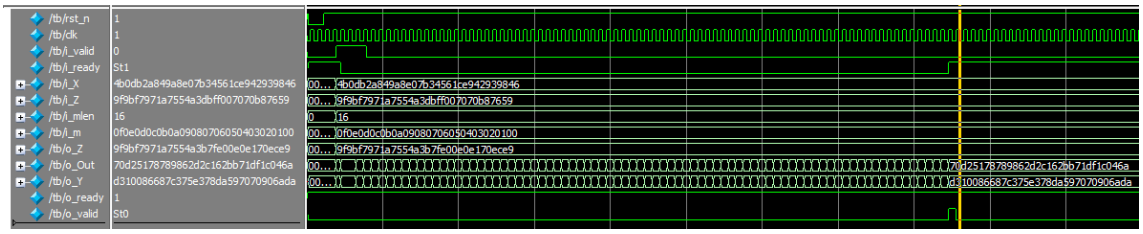
Bài báo này được thực hiện theo nguyên tắc thử nghiệm song song giữa quá trình tìm hiểu và sử dụng mã nguồn chuẩn hóa của giải thuật COMET để từng bước xây dựng các khối chức năng bên trong bộ mã hóa. Như trong Hình 9 là kết quả mô phỏng kiểm thực của khối chức năng thiết lập đầu vào với dữ liệu khóa KEY và NONCE đã thử nghiệm trên mã nguồn C++. Hình 10 thể hiện kết quả mô phỏng đánh giá với dữ liệu liên kết được xoắn trộn với dữ liệu thu được từ khối thiết lập đầu vào. Và Hình 11 là kết quả mô phỏng đánh giá quá trình xử lý dữ liệu bản tin với luồng bit đã được xoắn trộn từ hai khối chức năng trước đó là INIT và PROC_AD.



Hình 9: Kết quả mô phỏng kiểm thực với khối chức năng thiết lập INIT128



Hình 10: Kết quả đánh giá khối chức năng xoắn trộn dữ liệu liên kết

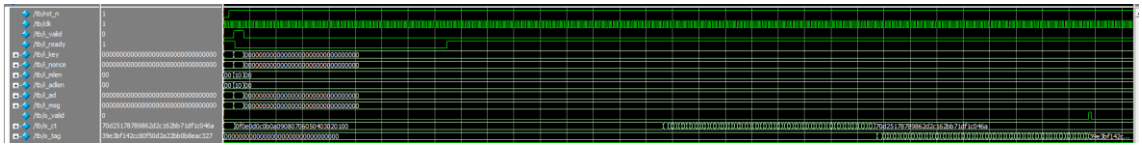


Hình 11: Kết quả mô phỏng đánh giá khối chức năng xử lý dữ liệu bản tin.

Các kết quả thu được từ quá trình mô phỏng đều được chúng tôi so sánh với nội dung thu được khi sử dụng mã nguồn chuẩn hóa từ các nhóm nghiên cứu tại NIST *[1]*. Kết quả thu được từ hoạt động mô phỏng đánh giá là tương đồng với kết quả thực hiện bằng ngôn ngữ C++ của giải thuật COMET đã cung cấp.

4.2. Đánh giá hoạt động trao đổi dữ liệu với đầu ra

Bộ mã hóa của giải thuật COMET được hoàn thiện sau khi đã được mô phỏng kiểm thực từng khối chức năng chi tiết. Hình 12 trình bày kết quả mô phỏng đánh giá bộ mã hóa với bốn khối dữ liệu đầu vào đồng thời là khối dữ liệu khóa KEY, khối khóa công khai NONCE và cả dữ liệu liên kết và dữ liệu bản tin cần truyền đi. Do đặc điểm của giải thuật mã hóa COMET sử dụng nguyên lý vòng lặp để xoắn trộn thông tin sẽ cần nhiều chu kỳ thực hiện. Do vậy, trong quá trình tổng hợp bộ mã hóa chúng tôi đã bổ sung thêm các thanh ghi dữ liệu đầu vào để luôn bảo đảm dữ liệu ổn định xuyên suốt quá trình mã hóa.



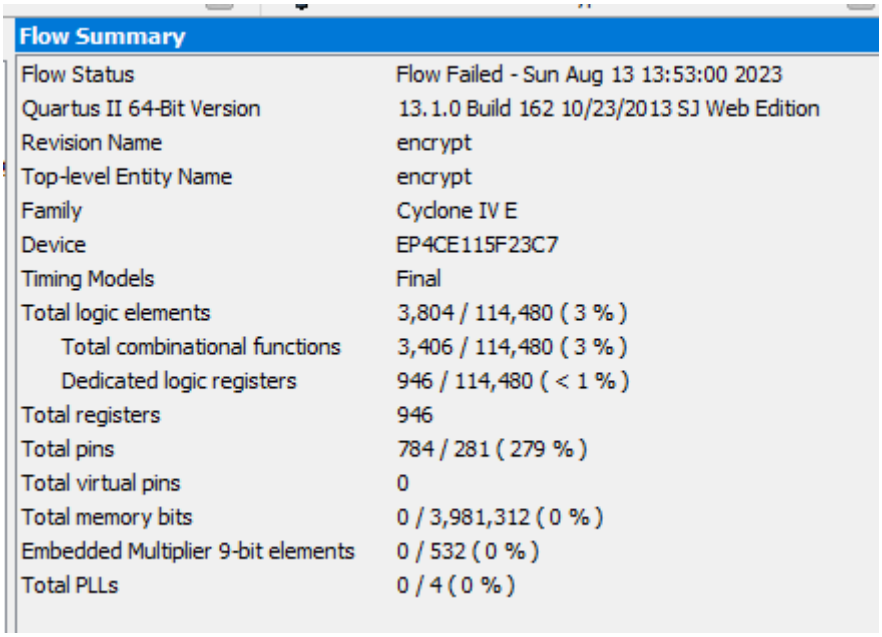
Hình 12: Kết quả mô phỏng toàn bộ hoạt động mã hóa COMET.

5. KẾT LUẬN

Bộ mã hóa COMET được đề xuất và thực thi hoàn thiện cho thấy khả năng triển khai giải thuật này cho hoạt động bảo mật trong quá trình truyền thông của các hệ thống IoT là hoàn toàn khả thi. Kết quả tổng hợp từ kiến trúc đề xuất trong công trình này được trình bày như trong Hình 13. Trong công trình này chúng tôi sử dụng kỹ thuật mô tả nối dây để xử lý các điểm nút tạo xoắn dữ liệu trong giải thuật COMET. Kỹ thuật này cho phép tối ưu tài nguyên sử dụng đồng thời bảo đảm khả năng thay đổi tức thời trong các bước xoắn trong quá trình thực hiện các chế độ đếm.

Do vậy, với KIT DE2 115 chỉ là một KIT FPGA dùng cho sinh viên chuyên ngành bước đầu tiếp cận với lĩnh vực thiết kế vi mạch, nên có tài nguyên rất hạn chế. Và trong kết quả tổng hợp lại càng cho thấy ưu điểm của giải thuật mã hóa COMET là cần rất ít tài nguyên; trong bảng kết quả thì toàn bộ mã hóa không chiếm quá 3% tài nguyên của

chip FPGA và hoàn toàn có thể kết hợp với các chức năng khác để hoàn thiện một con CHIP cho phép vừa xử lý thông tin (vi xử lý - μP) vừa có chức năng mã hóa bảo mật thông tin.



Flow Summary	
Flow Status	Flow Failed - Sun Aug 13 13:53:00 2023
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	EP4CE115F23C7
Timing Models	Final
Total logic elements	3,804 / 114,480 (3 %)
Total combinational functions	3,406 / 114,480 (3 %)
Dedicated logic registers	946 / 114,480 (< 1 %)
Total registers	946
Total pins	784 / 281 (279 %)
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 13: Chi phí thiết kế của bộ mã hóa COMET thu được.

Từ thành công của hoạt động nghiên cứu và thực thi bộ mã hóa COMET cũng tạo nên xu thế nghiên cứu để cứng hóa các giải thuật bảo mật LWC ứng dụng cho hoạt động truyền thông của các hệ thống IoT nói chung. Định hướng trong thời gian tới nhóm nghiên cứu sẽ tiếp tục hoàn thiện giải pháp bảo mật cho truyền thông IoT bằng giải thuật COMET gồm cả bộ mã hóa và giải mã.

TÀI LIỆU THAM KHẢO

[1] NIST, "https://csrc.nist.gov/projects/lightweight-cryptography," [Online].

[2] A. J. M. N. Shay Gueron, "https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/comet-spec-round2.pdf," 2022. [Online].

[3] B. Koo, Dongyoung and R. Kim, "Information Security and Cryptology – ICISC 2017," D. K. Howon Kim, Ed., Springer Cham, 2018, pp. 2-25.

[4] A. J. M. N. Shay Gueron, COMET: COunter Mode Encryption with authentication Tag, USA: National Institute of Standards and Technology, USA, 2019.

[5] T. H. T. Lê Văn Thanh Vũ, "Đề xuất kiến trúc và đánh giá thử nghiệm khối mã hóa không dùng SBOX cho hoạt động truyền thông của các hệ thống IoT," *Tạp chí Khoa học công nghệ - Trường ĐH Khoa học,* 2021.

[6] D. R. H. K. Y. J. D.-G. L. a. D. K. Bonwook Koo, "CHAM: A family of lightweight block ciphers for resource-constrained devices," in *ICISC 2017 - 20th International Conference*, Seoul, South Korea, 2017.

RESEARCH AND IMPLEMENTATION OF THE 128-BIT THE ENCRYPTOR FOR COMET ALGORITHM

Le Van Thanh Vu*, Nguyen Minh Nhat

Faculty of FEEMT, University of Sciences, Hue University

*Email: vulvt@hueuni.edu.vn

ABSTRACT

The Internet of Things (IoT) is a remarkable development trend in the electronic field, with a wide range of applications across numerous economic and social sectors. Security research for IoT systems contributes to increasing feasibility and promoting the realization of larger-scale electronic systems that better meet social development needs. The COMET encryption algorithm, focusing on counter mode encryption without using SBOX to optimize resources during execution, enhances information security. This research focuses on the analysis and implementation of the COMET algorithm, yielding promising initial assessment results. Additionally, the synthesized design outcomes demonstrate the rational application of the algorithm to IoT system designs.

Keywords: COMET, cryptography, blockcipher, IoT.

Lê Văn Thanh Vũ sinh ngày 20/05/1977 tại TP Huế. Ông nhận bằng cử nhân đại học ngành Vật lý tại Trường Đại học Khoa học, Đại học Huế. Năm 2004, ông nhận bằng thạc sỹ ngành Điện tử - Viễn thông tại Khoa Công nghệ thuộc Đại học Quốc gia Hà Nội. Năm 2017, ông nhận bằng tiến sĩ tại Trường ĐH Công nghệ - ĐHQG Hà Nội. Hiện đang là giảng viên tại Khoa Điện tử - Viễn thông, Trường Đại học Khoa học – Đại học Huế.

Lĩnh vực nghiên cứu: Thiết kế vi mạch, hệ thống nhúng – IoT.

Trương Minh Nhật sinh ngày 22/06/2002 tại TP Huế. Hiện tại đang là sinh viên ngành Điện tử - Viễn Thông thuộc khoa Điện, Điện tử và Công nghệ Vật liệu tại Trường Đại học Khoa học, Đại học Huế.

Lĩnh vực nghiên cứu: Thiết kế vi mạch, hệ thống nhúng.