DOI: 10.64302/joshusc.v32n1e.1345

THIẾT KẾ VÀ KIỂM THỬ BỘ MÃ HÓA GIFT-COFB 128BIT

Lê Văn Thanh Vũ

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

Email: vulvt@hueuni.edu.vn

Ngày nhận bài: 13/9/2025; ngày hoàn thành phản biện: 19/9/2025; ngày duyệt đăng: 01/12/2025

TÓM TẮT

Hệ thống IoT là xu thế phát triển tất yếu của các hệ thống nhúng theo xu hướng mở rộng và đa dạng hóa cả theo hướng ứng dụng và triển khai công nghệ. Nhóm giải thuật mã hóa trọng số nhẹ là giải pháp tối ưu góp phần giải quyết bài toán bảo mật bên trong các hệ thống IoT. Bài báo này tập trung phân tích thuật toán GIFT-COFB để thực thi và kiểm thử bộ mã hóa và giải mã 128bit từ đó góp phần giải quyết một cách triệt để thách thức bảo mật trong các hệ thống IoT. Trong bài báo này chúng tôi đưa ra một thiết kế chi tiết và triển khai thực tiễn giải thuật mã hóa GIFT 128bit trên nền tảng công nghệ FPGA đồng thời kết hợp với giải pháp kiểm thử đa năng UVM để nâng cao độ tin cậy của thiết kế được đề xuất.

Từ khóa: GIFT-COFB, LWC, Mã hóa, UVM.

1. MỞ ĐẦU

Những năm gần đây xu thế phát triển các hệ thống IoT ngày càng phát triển sâu rộng, các ứng dụng trải rộng khắp từ những thiết bị cá nhân, hệ thống đô thị thông minh hay thiết bị phục vụ an ninh quốc phòng [1]. Ưu điểm nổi trội của hệ thống IoT là tính đa dạng và khả năng mở rộng linh hoạt dựa vào đặc điểm của các hệ nhúng và khả năng truyền thông linh hoạt [2]. Tuy nhiên, hệ thống IoT ngày càng mở rộng thì thách thức đặt ra ngày càng lớn đó chính là nhu cầu bảo mật thông tin trong điều kiện tài nguyên hạn chế [3]. Giải quyết bài toán truyền thông trong các hệ thống IoT cần giải pháp toàn diện kết hợp hợp lý hiệu quả truyền thông và nâng cao tính bảo mật trong điều kiện ràng buộc của tài nguyên hạn chế [4]. Giải pháp mã hóa trọng số nhẹ tập trung vào các giải thuật mã hóa tận dụng các phép toán logic đơn giản và phép dịch bit để xáo trộn thông tin tạo hiệu ứng giả ngẫu nhiên. Nhóm giải pháp LWC được pháp triển giải thuật DES và AES đã được nghiên cứu và triển khai một cách hợp lý và tối ưu cho các hệ thống IoT được xét đến [5]. Do vậy, một giải pháp truyền thông toàn diện cho các hệ thống IoT

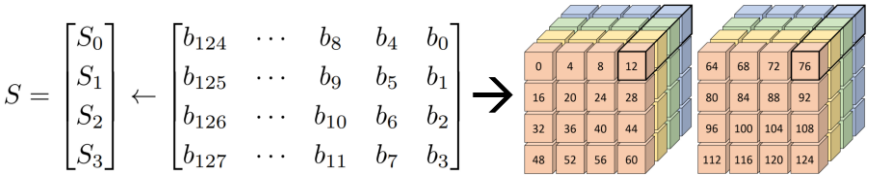
sẽ là tập các giao thức truyền thông và bảo mật được tối ưu trong điều kiện ràng buộc cụ thể của thực tiễn triển khai [6]. Từ nhu cầu và thách thức của hệ thống IoT mà viện tiêu chuẩn và công nghệ - NIST đã tổ chức thành công việc tìm được một chuẩn hóa cho hoạt động bảo mật thông qua quy trình lựa chọn nhiều vòng với nhiều giải thuật đa dạng [7]. Mặc dù, giải pháp ASCON đã được lựa chọn là giải thuật tiêu chuẩn thì vẫn còn đa dạng các giải thuật khác phù hợp với từ nhóm ứng dụng cụ thể dựa vào các đặc điểm riêng có.

Trong thời gian dài triển khai chuẩn hóa giải thuật mã hóa cho các hệ thống IoT; các giải thuật mã hóa được nghiên cứu chi tiết hơn và đa dạng hơn các phương pháp tiếp cận. Giải thuật ASCON được tập trung nghiên cứu triển khai với nhiều cấp độ nhúng trong hệ thống; từ hoạt động mã hóa bằng phần mềm tiêu chuẩn [8] đến mức cứng hóa tích hợp vào hệ thống cụ thể [9].

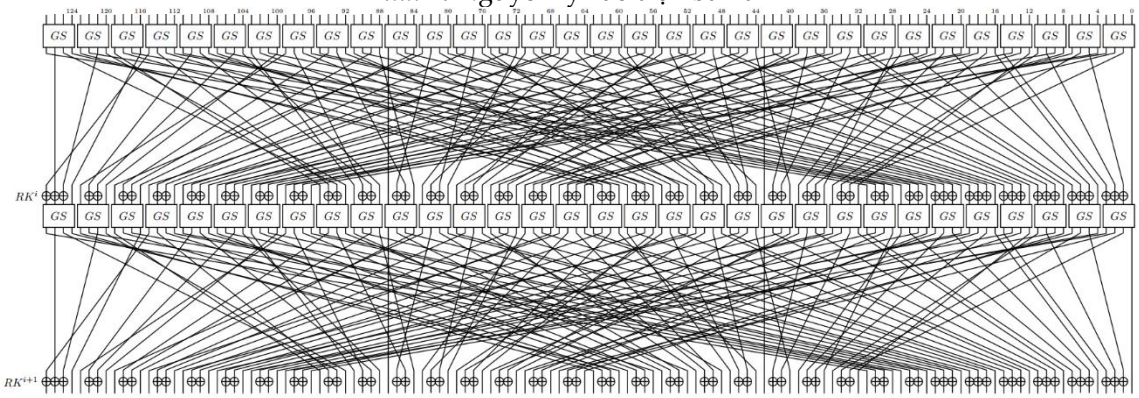
Tuy nhiên, các giải thuật khác tham gia trong các vòng đánh giá lại có nhiều đặc điểm riêng có và có thể phù hợp với những yêu cầu của từng loại.

2. CÔNG VIỆC LIÊN QUAN

Thuật toán GIFT-COFB thuộc dạng mã hóa khối dựa trên nguyên lý xáo trộn từ các khối dữ liệu đầu vào thành các từ nhỏ hơn và xoắn trộn để ngẫu nhiên hóa thông tin. Các thành phần thông tin trong các từ được xoắn trộn và lặp lại với số vòng lặp được tối ưu tăng tối đa khả năng bảo mật thông tin và tiết giảm chi phí thực hiện mã hóa. Nguyên lý xoắn trộn các từ bên trong thuật toán GIFT chỉ sử dụng các phép toán logic cơ bản và dịch bit để tăng tốc xử lý và sự ổn định của quá trình mã hóa như trong Hình 1. Hình 2 trình bày chi tiết hoạt động xoắn trộn thông tin bên trong các hàm lặp của thuật toán GIFT-COFB [10].



Hình 1. Nguyên lý xáo trộn bản tin



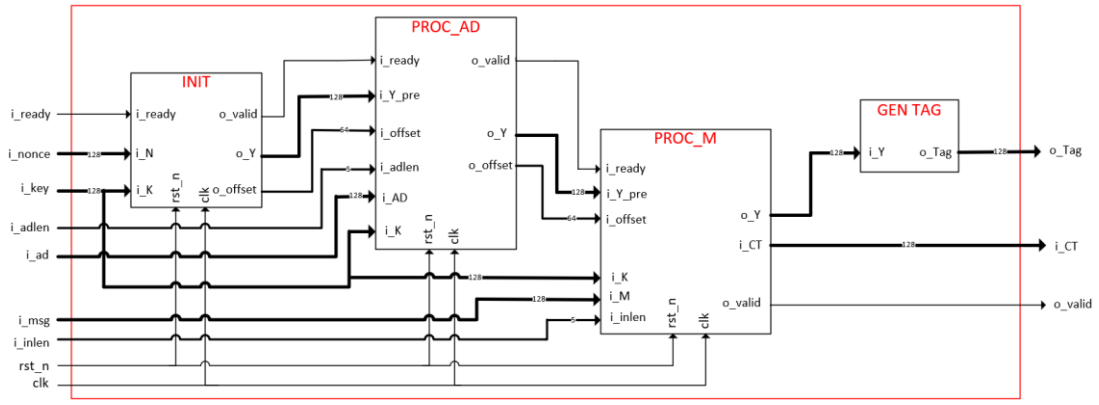
Hình 2. Sơ đồ xáo trộn hai vòng GIFT-COFB

Hoạt động mã hóa GIFT-COFB được chia làm 4 pha: Khởi tạo (INIT); xử lý dữ liệu (PROC_AD); xử lý bản tin (PROC_M) và khối tạo TAG (GEN_TAG). Mỗi pha sẽ sử dụng SBOX làm trọng tâm mã hóa kết hợp với các phép toán sinh khối và nhồi dữ liệu để tối ưu hoạt động trao đổi bên trong hoạt động mã hóa. Nguyên lý chính của thuật toán GIFT vẫn tập trung vào phép XOR và xoắn trộn để tiết kiệm chi phí lập và giải mã nhưng vẫn bảo đảm tối ưu khả năng bảo mật thông tin đầu vào.

3. KIẾN TRÚC ĐỀ XUẤT CHO KHỐI MÃ HÓA

3.1. Mô tả kiến trúc chung

Dựa trên việc nghiên cứu các giải thuật LWC từ NIST đưa ra và tập trung cho giải thuật GIFT-COFB chúng tôi nhận thấy toàn bộ hoạt động mã hóa được chia làm 4 pha nối tiếp gồm pha INIT (khởi tạo), pha PROC_AD (xử lý dữ liệu liên kết), pha PROC_M (xử lý bản tin) và pha GEN_TAG (tạo TAG). Khác với mã nguồn chuẩn dựa trên ngôn ngữ C++ các lệnh được thực hiện một cách lần lượt; các khối con của bộ mã hóa được thực thi đồng thời nên cần có cơ chế bắt tay đồng bộ. Hình 3 mô tả tổng thể kiến trúc chia pha được đề xuất cho bộ mã hóa GIFT-COFB 128bit.

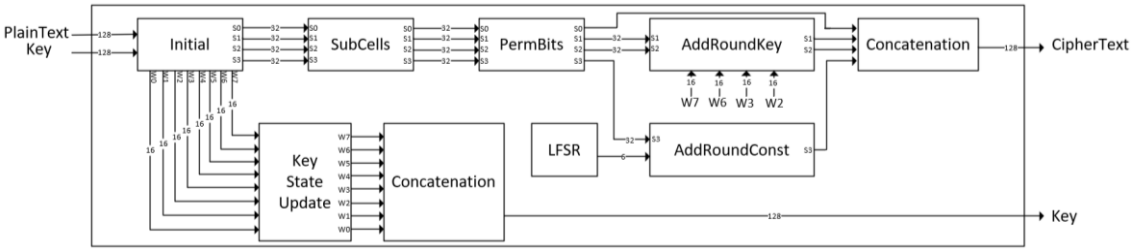


Hình 3. Nguyên lý thực hiện mã hóa của GIFT-COFB

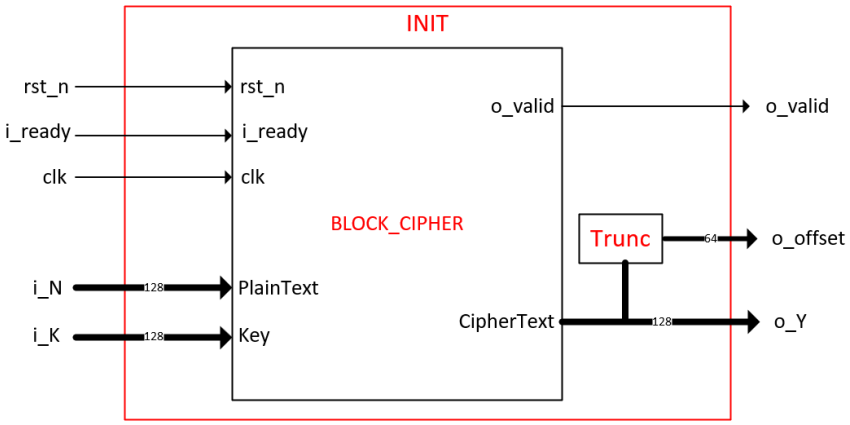
Khối INIT thực hiện chức năng khởi tạo dữ liệu dựa trên hai khóa bảo mật và công khai để khối dữ liệu tiền đề cho hoạt động xáo trộn với dữ liệu liên kết có kích thước tối đa là 16 từ 8bit (*tổng là 128bit*). Đặc điểm riêng có của thuật toán GIFT là luôn sử dụng khóa riêng tư KEY để xáo trộn với dữ liệu liên kết cũng như nội dung bản tin ở các khối PROC_AD và PROC_M. Nguyên lý này thể hiện rõ trong các kiến trúc chi tiết đề xuất ở các phần sau.

3.2. Mô tả chi tiết

Giải thuật mã hóa GIFT được thực hiện với lõi là khối mã hóa bằng các kỹ thuật xáo ngẫu nhiên hai khối dữ liệu vào bằng các phép toán logic cơ bản và dịch bit. Dựa trên thuật toán được đề xuất chúng tôi đề xuất kiến trúc khối mã hóa GIFT 128bit như được mô tả chi tiết trong Hình 4. Khối mã hóa được xây dựng dựa vào kỹ thuật xây dựng mạch điện tổ hợp, điều này cho phép tối ưu chi phí và nâng cao tốc độ xử lý phép mã hóa. Tuy nhiên, tổng thể hoạt động mã hóa được xây dựng dựa trên kỹ thuật thiết kế đồng bộ; các khối chức năng hoạt động đồng bộ vào xung đồng hồ chung. Đồng thời, chúng tôi bổ sung các tín hiệu bắt tay để đồng bộ quá trình trao đổi thông tin giữa các khối con. Do vậy, kiến trúc trong Hình 5 trình bày chi tiết các tín hiệu vào ra của khối INIT (thiết lập) bằng cách sử dụng lõi là khối mã hóa ở Hình 4.

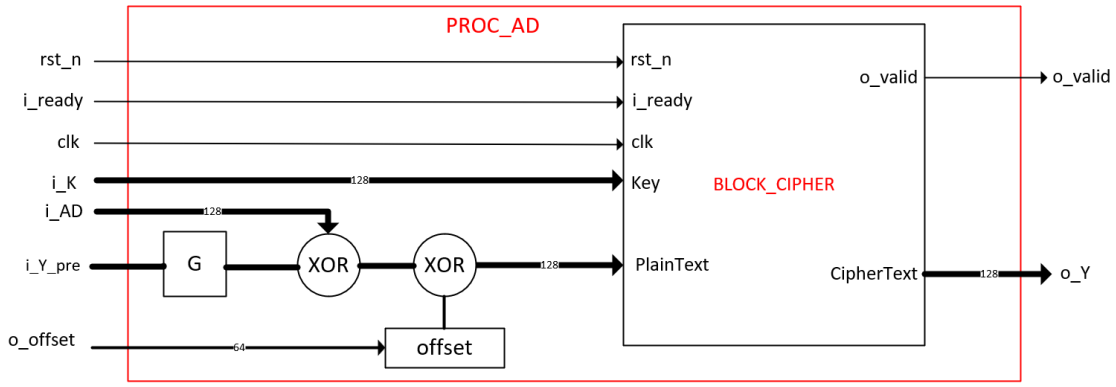


Hình 4. Kiến trúc chi tiết khối mã hóa GIFT 128bit



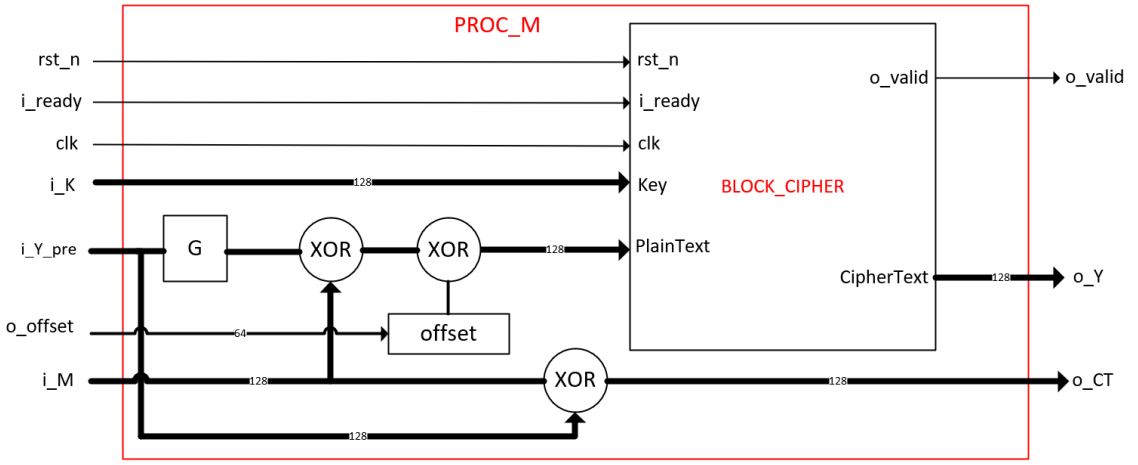
Hình 5. Kiến trúc đề xuất cho khối INIT khởi tạo mã hóa

Nguyên lý bắt tay trao đổi thông tin dựa theo kỹ thuật xác thực thông qua tín hiệu trạng thái từ khối nhận. Từ khối phát sẽ tích cực tín hiệu xác thực (*valid*) để báo với khối nhận thông tin sẵn sàng; khối nhận tin sẽ lập cờ bận (ready = un_active) bằng tín hiệu trạng thái (*ready*).



Hình 6. Kiến trúc đề xuất cho khối xử lý dữ liệu liên kết – PROC_AD

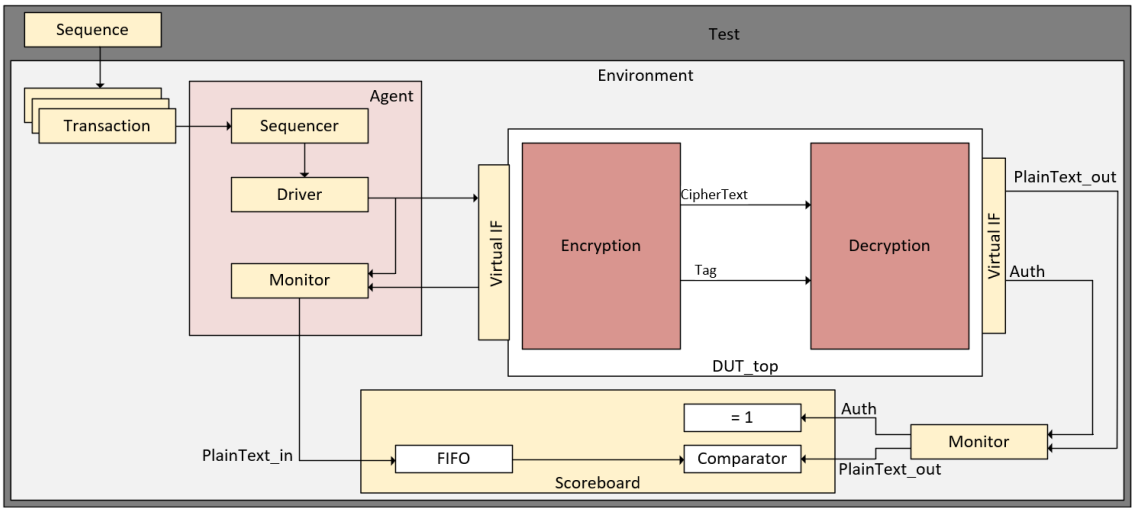
Các khối xử lý dữ liệu PROC_AD và PROC_M cũng đều dùng lại khối mã hóa kết hợp với các khối xử lý thông tin bằng các phép toán logic (XOR, OR và AND) kết hợp với kỹ thuật ghép dữ liệu cơ bản. Chi tiết kiến trúc cho các khối xử lý dữ liệu và xử lý bản tin được trình bày chi tiết như trong các Hình 6 và Hình 7.



Hình 7. Kiến trúc đề xuất cho khối xử lý bản tin PROC_M

3.3 Kiểm thử kiến trúc đề xuất

Dựa trên việc nghiên cứu giải thuật GIFT và mã nguồn thực thi dựa trên ngôn ngữ C++, chúng tôi đề xuất các kiến trúc khả thi để thực thi giải thuật này trên nền tảng FPGA như đã trình bày ở trên. Đồng thời, chúng tôi tiến hành đánh giá. Hình 8 trình bày cụ thể các thành phần cơ bản để triển khai hoạt động kiểm thử bộ mã hóa và giải mã hóa của thuật toán GIFT. Hoạt động kiểm thử này chúng tôi triển khai trên cơ sở giải pháp kiểm thử đa năng – UVM. Toàn bộ nội dung kiểm thử được sử dụng trên nền tảng công cụ trực tuyến **edaplayground**.

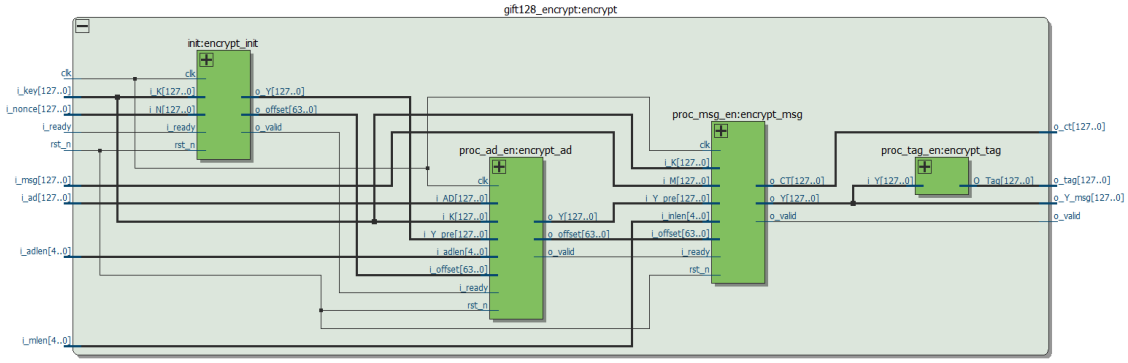


Hình 8. Kiến trúc tổng thể cho hoạt động đánh giá GIFT 128bit

4. MÔ PHỎNG ĐỂ ĐÁNH GIÁ THỬ NGHIỆM

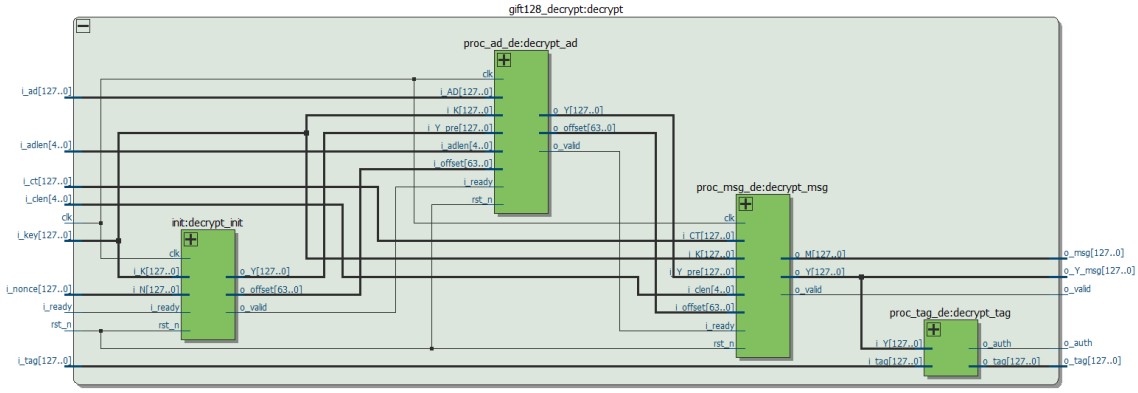
4.1. Tổng hợp thiết kế

Toàn bộ thiết kế của chúng tôi sau đó được triển khai thông qua kỹ thuật mô tả bằng ngôn ngữ mô tả phần cứng Verilog; và sau đó tổng hợp bằng công cụ chuyên môn là Quartus để mô phỏng đánh giá thông qua phần mềm ModelSim. Từ kết quả mô tả chúng tôi đã tiến hành tổng hợp được kiến trúc của bộ mã hóa như trong Hình 9. Kiến trúc này hoàn toàn phù hợp với kiến trúc đề xuất của chúng tôi trong Hình 3. Ở chiều ngược lại, kiến trúc của bộ giải mã cũng được thực hiện theo nguyên tắc phân ba với 4 pha tương ứng lần lượt là khởi tạo (init: decrypt_init); khối xử lý dữ liệu; khối xử lý bản tin và khối tạo bản tin xác thực như trong Hình 10. Đặc điểm riêng có của giải thuật mã hóa GIFT là khóa bảo mật được đưa vào sử dụng để xáo trộn với tất cả các khối thông tin khởi tạo INIT, PROC_AD và PROC_M.



Hình 9. Kiến trúc tổng hợp được của bộ mã hóa GIFT 128bit

Kiến trúc khối giải mã dù vẫn chia 4 pha tương đồng khối mã hóa, tuy nhiên bên trong các khối chức năng bên trong các pha có sự thay đổi nhỏ chi tiết bên trong. Do vậy, các khối chức năng trong các pha giải mã được chúng tôi thiết kế lại để phù hợp với hoạt động giải mã theo đúng thuật toán GIFT đã được công bố.



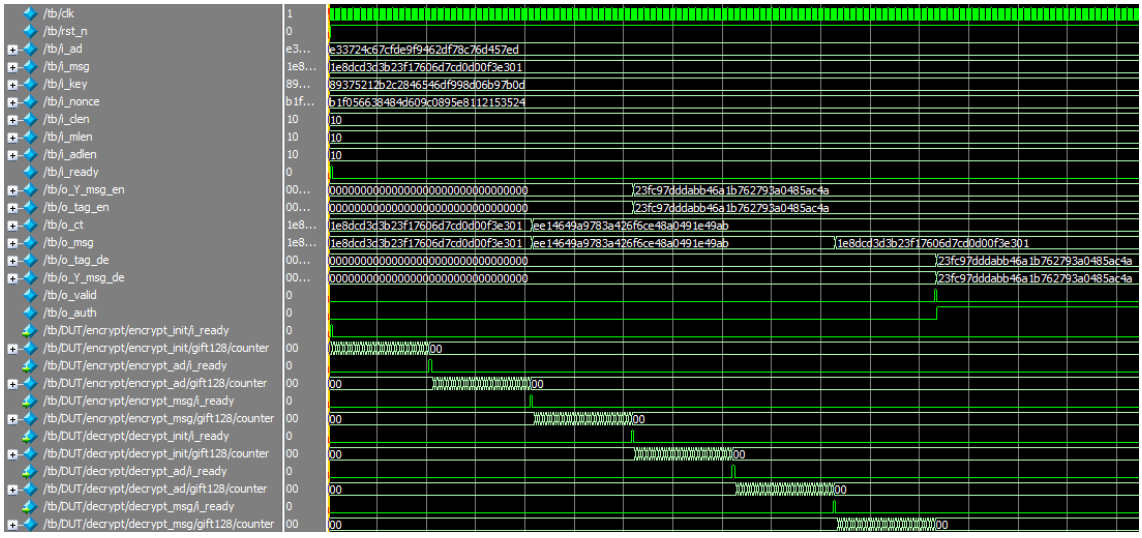
Hình 10. Kiến trúc tổng hợp của khối giải mã GIFT 128bit

Kết quả tổng hợp của toàn bộ thiết kế gồm khối mã hóa (Encoder) và giải mã (Decoder) theo thuật toán mã hóa GIFT-COFB 128bit được tổng hợp với đối chiếu với tài nguyên của KIT FPGA DE115 được liệt kê như trong

Flow Summary	
Flow Status	Flow Failed - Wed Mar 04 14:23:00 2026
Quartus II 64-Bit Version	13.1.0 Build 162 10/23/2013 SJ Web Edition
Revision Name	gift
Top-level Entity Name	gift
Family	Cyclone IV E
Device	EP4CE115F23C7
Timing Models	Final
Total logic elements	282 / 114,480 (< 1 %)
Total combinational functions	282 / 114,480 (< 1 %)
Dedicated logic registers	0 / 114,480 (0 %)
Total registers	0
Total pins	1,302 / 281 (463 %)
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 %)

4.2. Đánh giá hoạt động mã hóa và giải mã

Trong bài báo này chúng tôi sử dụng nguyên lý đánh giá song song khi đồng loạt thực hiện quá trình mã hóa và giải mã trên mã nguồn của NIST cung cấp và kiến trúc được đề xuất trên công cụ Quartus chuyên dụng. Cùng với đó chúng tôi thực hiện quá trình đánh giá dựa trên tập dữ liệu mà NIST cung cấp. Toàn bộ kết quả mô phỏng đánh giá với tập dữ liệu lần 1 (Bảng 1) được thể hiện như trong Hình 11. Các kết quả mô phỏng đánh giá mà chúng tôi nhận được là hoàn toàn tương thích; điều này là minh chứng cho thiết kế của chúng tôi đáp ứng đúng giải thuật mã hóa GIFT đã được NIST công bố.

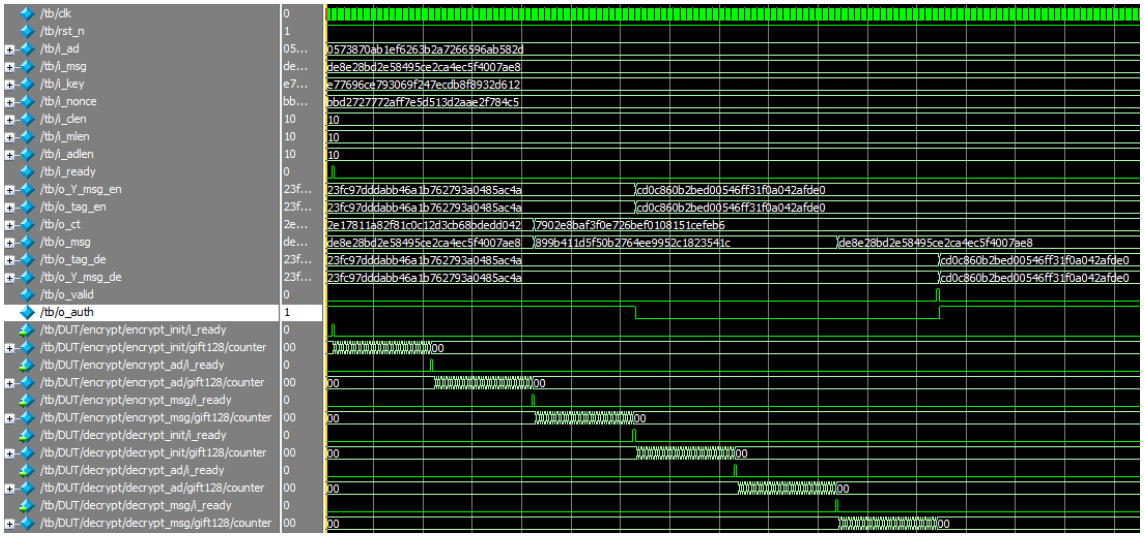


Hình 11. Kết quả mô phỏng đánh giá lần 1

Bảng 1. Bảng dữ liệu trong mô phỏng đánh giá lần 1

PlainText	1E8DCD3C3B23F17606D7CD0D00F3E301
Key	89375212B2C2846546DF998D06B97B0D
AD	E33724C67CFDE9F9462DF78C76D457ED
Nonce	B1F056638484D609C0895E8112153524
CipherText	EE14649A9783A426F6CE48A0491E49AB
Tag	23FC97DDDABB46A1B762793A0485AC4A
PlainText	1E8DCD3C3B23F17606D7CD0D00F3E301

Hoạt động mô phỏng đánh giá thiết kế được chúng tôi đã chứng thực được quy trình mã hóa là hoàn toàn phù hợp với nguyên lý của thuật toán GIFT-COFB đã đề xuất. Với các dữ liệu đầu vào như trong Bảng 1 thì các kết quả thu được cũng trùng khớp với dữ liệu đầu ra khi đối chiếu thông tin mô phỏng ở Hình 11 và giá trị ở Bảng 1.



Hình 12. Kết quả mô phỏng đánh giá lần 2

Kết quả mô phỏng được đánh giá lần hai cũng với bảng thông tin của tài liệu tiêu chuẩn và kết quả thu được cũng hoàn toàn trùng khớp với dữ liệu tiêu chuẩn. Chúng tôi sử dụng tập các khối dữ liệu đầu vào và điều khiển quá trình mã hóa thích hợp thì sau 80 vòng lặp cho mỗi lần mã hóa ở mỗi pha của quá trình mã hóa chúng tôi thu được bản tin mã hóa và TAG tương ứng cho từng khối mã. Sau đó, bản tin mã hóa được đưa vào khối giải mã để khôi phục bản tin gốc và thẻ xác thực TAG để kiểm chứng dữ liệu mã hóa. Tất cả tín hiệu vào/ra và dữ liệu trao đổi bên trong khối mã hóa và giải mã được trình bày trong Hình 12.

Bảng 2. Bảng dữ liệu mô phỏng đánh giá lần 2

PlainText	DE8E28BD2E58495CE2CA4EC5F4007AE8
Key	E77696CE793069F247ECDB8F8932D612
AD	0573870AB1EF6263B2A7266596AB582C
Nonce	BBD2727772AFF7E5D513D2AAE2F784C5
CipherText	7902E8BAF3F0E726BEF0108151CEFEB6
Tag	CD0C860B2BED00546FF31F0A042AFDE0
PlainText	DE8E28BD2E58495CE2CA4EC5F4007AE8

4.3 Kết quả kiểm thử

Nhằm nâng cao độ tin cậy của thiết kế và hướng đến khả năng đánh giá toàn diện thiết kế hướng đến việc triển khai thiết kế trong các hệ thống thực, chúng tôi tiến hành kiểm thử bộ mã hóa và giải mã GIFT bằng phương pháp kiểm thử đa năng – UVM. Trong bài báo này chúng tôi sử dụng công cụ trực tuyến được cung cấp từ trang điện tử [11]; đây là một công cụ trực tuyến chuyên dụng và đáng tin cậy cho các hoạt động mô phỏng và đánh giá các thiết kế vi mạch. Kết quả kiểm thử thiết kế của chúng tôi được trình bày như trong Hình 13. Từ báo cáo này cho thấy rõ kết quả thiết kế của chúng tôi là hoàn toàn phù hợp với các yêu cầu của một thiết kế cho vi mạch chuyên sâu và cũng phù hợp cho cả khả năng triển khai trong môi trường học thuật về thiết kế vi mạch.

```
--- UVM Report Summary ---

** Report counts by severity
UVM_INFO :  123
UVM_WARNING :    0
UVM_ERROR :    0
UVM_FATAL :    0
** Report counts by id
[DRIVER]    56
[MONITOR]    40
[RNTST]     1
[SCOREBOARD]    24
[TEST_DONE]     1
[UVM/RELNOTES]     1

$finish called from file "/apps/vcsmx/vcs/U-2023.03-SP2//etc/uvm-1.2/src/base/uvm_root.svh", line 527.
$finish at simulation time                8065
           V C S   S i m u l a t i o n   R e p o r t
Time: 8065 ns
CPU Time:      0.640 seconds;       Data structure size:   0.4Mb
```

Hình 13. Kết quả kiểm thử được công cụ báo cáo

5. KẾT LUẬN

Giải thuật mã hóa GIFT-COFB thuộc nhóm mã hóa trọng số nhẹ với ưu điểm giảm thiểu các phép tính số phức hợp, tận dụng tối đa các phép tính logic và dịch bit rất phù hợp với khả năng triển khai trên phần cứng. Thiết kế chia 4 pha và kỹ thuật bắt tay bằng tín hiệu xác thực và phản hồi là phù hợp với nguyên lý thực thi phần cứng cho các giải thuật mã hóa trọng số nhẹ. Việc tận dụng các kỹ thuật mô tả bằng thiết kế mạch tổ hợp cho các bước xoắn đã góp phần tiết kiệm chi phí thực thi phần cứng. Các kết quả mô phỏng đánh giá của chúng tôi đã chứng minh được tính đúng đắn của các kiến trúc đề xuất là tương thích với nguyên lý mã hóa GIFT-COFB [10].

Việc vận dụng giải pháp kiểm thử đa năng – UVM trong các thiết kế phần cứng là phù hợp với xu hướng phát triển của lĩnh vực thiết kế vi mạch trong cả hoạt động nghiên cứu cũng như trong công nghiệp. Quá trình vận dụng giải pháp UVM trong qui trình kiểm thử thiết kế bộ mã hóa và giải mã dựa theo thuật toán GIFT-COFB góp phần khẳng định độ tin cậy của thiết kế của chúng tôi.

Trong thời gian sắp tới chúng tôi sẽ tiến hành kiểm thử đa dạng các giải pháp cứng hóa cho các giải thuật mã hóa đã được kiểm chứng qua các vòng đánh giá của NIST [12] [13]. Sau đó sẽ có sự so sánh đánh giá các kết quả thu được một cách toàn diện các chi phí và khả năng triển khai trong các hệ thống IoT thực tiễn.

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] T. M. Phương, "Nghiên cứu ứng dụng công nghệ IoT cho giám sát môi trường," 2016.

[3] R. Boisguene, S.-C. Tseng, C.-W. Huang and P. Lin, "A survey on NB-IoT downlink scheduling: Issues and potential solutions," in *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2017.

[4] 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.

[5] 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.

[6] D. Serpanos and M. Wolf, Internet-of-Things (IoT) Systems Architectures, Algorithms, Methodologies, Atlanta, GA: Springer International, 2018.

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

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

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

[10] S. Banik, A. Chakraborti, A. Inoue, T. Iwata, K. Minematsu, M. Nandi, T. Peyrin, Y. Sasaki, S. M. Sim and Y. Todo, *GIFT-COFB,* 2020.

[11] Doulos, "Edaplayground," [Online]. Available: https://www.edaplayground.com/.

[12] 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.

[13] T. Schweinberger and V. Shoup, "ACE: The Advanced Cryptographic Engine, booktitle=IACR Eprint archive," in *IACR Eprint archive*, 2000.

DESIGN AND VERIFICATION GIFT-COFB 128BIT ENCODER

Le Van Thanh Vu

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

Email: vulvt@hueuni.edu.vn

ABSTRACT

The IoT system is an inevitable development trend for embedded systems, as they continue to expand and diversify in both application domains and technological deployments. The lightweight cryptographic algorithm family is an optimal solution for addressing internal security challenges within IoT systems. In this paper, we focus on presenting the most comprehensive hardware-oriented implementation of the lightweight cryptographic algorithm GIFT-COFB, providing a concrete approach to thoroughly addressing communication security challenges in IoT systems. We propose a detailed design and practical implementation of the 128-bit GIFT encryption algorithm on an FPGA platform, combined with a versatile UVM-based verification solution to enhance the reliability of the proposed design.

Keywords: GIFT-COFB, LWC, encode, UVM.