

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ

TRẦN SỸ NAM

NGHIÊN CỨU GIẢI PHÁP NÂNG CAO HIỆU NĂNG CỦA
MỘT SỐ THUẬT TOÁN MÃ HÓA TRONG BẢO MẬT
LUỒNG IP

NGÀNH: KỸ THUẬT MẬT MÃ

MÃ SỐ: 9520209

TÓM TẮT LUẬN ÁN TIẾN SĨ KỸ THUẬT

HÀ NỘI – 2026

Công trình được hoàn thành tại:

Học viện kỹ thuật mật mã

Người hướng dẫn khoa học:

1. PGS.TS. Lương Thế Dũng

2. TS. Hoàng Văn Thức

Phản biện 1:

Phản biện 2:

Phản biện 3:

Luận án được bảo vệ trước Hội đồng đánh giá luận án tiến sĩ cấp
Học viện họp tại Học viện kỹ thuật mật mã

Vào hồi giờ, ngày tháng năm

Có thể tìm hiểu luận án tại thư viện:

1. Thư viện Học viện kỹ thuật mật mã

2. Thư viện Quốc gia Việt Nam

MỞ ĐẦU

Sự bùng nổ của kỷ nguyên số đang định hình một mạng lưới truyền thông ngày càng phức tạp, nơi dữ liệu được tạo ra, truyền tải và xử lý theo thời gian thực trên quy mô chưa từng có. Từ các trung tâm dữ liệu quy mô lớn, trí tuệ nhân tạo tại biên, đến mạng 5G/6G và Internet vạn vật (IoT), hạ tầng an ninh mạng phải đáp ứng không chỉ yêu cầu an toàn mà còn an toàn với hiệu suất tối đa: thông lượng cao, độ trễ thấp, khả năng mở rộng linh hoạt. Thách thức này bộc lộ hạn chế của xử lý dựa trên CPU truyền thống khi khối lượng dữ liệu ngày càng tăng, trong khi các nguyên thủy mật mã (mã hóa, xác thực, toàn vẹn) tác động trực tiếp lên luồng dữ liệu thời gian thực không còn đáp ứng được yêu cầu này. Điều này dẫn đến sự chuyển hướng sang các giải pháp phần cứng chuyên dụng như FPGA, ASIC nhằm nâng cao tốc độ, giảm độ trễ mà vẫn đảm bảo độ an toàn - những đặc tính khó đạt được nếu chỉ dựa vào phần mềm.

Hiện nay có nhiều thuật toán cung cấp dịch vụ mật mã khác nhau, song không phải tất cả đều phù hợp để triển khai hiệu quả trên nền tảng phần cứng. Ví dụ, DES và 3DES không còn đảm bảo an toàn và không thích hợp với bài toán hiệu năng cao. Ngược lại, AES (Advanced Encryption Standard) tiếp tục được ứng dụng rộng rãi cả trong thực tiễn và nghiên cứu học thuật nhờ những ưu điểm về độ an toàn và tính tối ưu khi triển khai trên phần cứng, đặc biệt là chế độ AES-GCM. Chế độ này thuộc nhóm AEAD (Authenticated Encryption with Associated Data), cho phép cung cấp đồng thời các

thuộc tính bí mật, xác thực và toàn vẹn trong một lược đồ thống nhất, với mô hình an toàn rõ ràng và hạn chế sai sót cấu hình. Đáng chú ý, AES-GCM còn tỏ ra vượt trội về hiệu năng khi hiện thực trên phần cứng nhờ khả năng song song hóa cao của cả quá trình mã hóa và hàm nhân Galois (GHASH). Chính vì vậy, việc nâng cao hiệu năng của AES/AES-GCM trên phần cứng vẫn là chủ đề được quan tâm mạnh mẽ trong cộng đồng nghiên cứu quốc tế.

Bên cạnh đó, AEAD đã trở thành yêu cầu bắt buộc trong thiết kế thuật toán mã hóa hạng nhẹ (Lightweight Cryptography) cho các mạng IoT, do AES không thực sự được thiết kế cho bài toán này. Tháng 8 năm 2025, NIST đã chuẩn hoá Ascon là tiêu chuẩn thuật toán mã hoá xác thực hạng nhẹ.. Trong bối cảnh mạng IoT, nơi việc tối ưu hóa cho các thiết bị tài nguyên hạn chế là yếu tố then chốt, một số trường hợp ưu tiên hiệu năng cao và độ trễ thấp để đáp ứng các tiêu chí bảo mật trong môi trường truyền thông thời gian thực, chẳng hạn như máy chủ bảo mật trung tâm, máy chủ biên, thiết bị IoT Gateway. Bởi vậy, vấn đề nghiên cứu cải thiện hiệu năng của Ascon trên nền tảng phần cứng cũng trở thành một xu hướng quan trọng và được quan tâm đáng kể trong những năm gần đây.

Các thuật toán mã hóa có thể được cải thiện hiệu suất theo hai cách: (i) tối ưu các thành phần bên trong thuật toán hoặc (ii) tối ưu kiến trúc khi triển khai trên phần cứng. Tuy nhiên, việc tối ưu các thành phần bên trong của thuật toán mã hoá như S-box, ma trận MDS (Maximum Distance Separable) sẽ thực sự phù hợp và mang lại hiệu

quả rõ rệt hơn cho AES so với Ascon, bởi sự khác biệt về cấu trúc và tính toán:

- AES (mã khối SPN): Hiệu năng bị chi phối mạnh bởi S-box (SubBytes) và ma trận MDS (MixColumns). Việc lựa chọn, thiết kế lại các thành phần này theo hướng phù hợp phần cứng sẽ giúp cải thiện đáng kể thông lượng và độ trễ.

- Ascon (AEAD hạng nhẹ dựa trên sponge/hoán vị): Được thiết kế tối giản cho các thiết bị có tài nguyên hạn chế, mỗi vòng được thực hiện đơn giản nên không gian cải tiến không còn nhiều khi chỉnh sửa các thành phần bên trong. Cải thiện hiệu năng chủ yếu đến từ các thay đổi kiến trúc như mở vòng lặp (unroll), lặp lại (iterative), tổ chức trạng thái/bus.

Trên cơ sở các phân tích và đánh giá nêu trên, để nâng cao hiệu năng của các thuật toán mã hóa AES và Ascon trong bảo mật luồng IP, luận án hướng đến ba mục tiêu cụ thể: tăng thông lượng xử lý dữ liệu, giảm độ trễ, giảm tài nguyên phần cứng sử dụng trong quá trình triển khai. Để đạt được các mục tiêu đó, luận án tập trung vào ba hướng nghiên cứu chính sau:

Thứ nhất, luận án nghiên cứu, lựa chọn và thiết kế các thành phần mật mã mới dành cho AES; cụ thể, đề xuất S-hộp và ma trận MDS có cấu trúc thân thiện với phần cứng để cải thiện thông lượng và độ trễ, đồng thời vẫn bảo đảm yêu cầu an toàn.

Thứ hai, luận án nghiên cứu xây dựng các kiến trúc phần cứng tốc độ cao cho AES và Ascon. Trong đó đề xuất các kiến trúc mới sử dụng các kỹ thuật song song hóa, kỹ thuật đường ống (pipeline), mở vòng

lập, tối ưu tổ chức thanh ghi, từ đó tìm ra kiến trúc phù hợp cho các hệ thống bảo mật hiệu năng cao.

Thứ ba, luận án tập trung vào việc đề xuất một kiến trúc phân cứng mới cho giao thức IPSec bởi khi xét đến bài toán tổng thể, việc cải thiện các thành phần mật mã riêng lẻ là chưa đủ để đáp ứng yêu cầu của các hệ thống tốc độ cao. Kiến trúc mới được thiết kế để tận dụng trực tiếp các kết quả ở hai hướng nghiên cứu trên, trong đó sử dụng thuật toán mã hoá AES và Ascon đã cải tiến, đồng thời đề xuất các thuật toán xử lý gói tin và phân luồng dữ liệu hiệu quả để nâng cao thông lượng và giảm độ trễ.

CHƯƠNG 1

TỔNG QUAN CÁC VẤN ĐỀ NGHIÊN CỨU

1.1. Thuật toán mã hóa AES

Advanced Encryption Standard (AES) là mã khối cấu trúc lặp với kích thước khối 128 bit, hỗ trợ các kích thước khóa 128 bits, 192 bits, và 256 bits tương ứng với 10, 12 và 14 vòng. Có bốn bước cơ bản trong một vòng mã của AES là: AddRoundKey, SubBytes, ShiftRows, và MixColumns.

1.2. Thuật toán mã hóa Ascon

Ascon là bộ thuật toán cung cấp các dịch vụ mã hóa xác thực với dữ liệu liên quan (AEAD). Quá trình mã hóa hoặc giải mã có xác thực của Ascon bao gồm bốn giai đoạn: Khởi tạo, Dữ liệu liên kết (AD), Xử lý bản rõ/bản mã và Kết thúc.

1.3. Giao thức bảo mật IPSec

Phiên bản hiện tại của IPSec và ESP là phiên bản 3 đã được ban hành trong RFC 4301 và 4303. ESP hỗ trợ hai chế độ: transport và tunnel. Trong chế độ tunnel, một gói IP mới được tạo ra từ gói tin IP nguyên gốc bằng cách: 1) chèn ESP header và trailer vào gói tin IP ban đầu; 2) mã hóa gói IP ban đầu và ESP trailer; 3) tính giá trị kiểm tra toàn vẹn ICV cho ESP header và các dữ liệu mã hóa; 4) chèn ICV vào cuối của gói tin; 5) thêm IP header mới cho gói tin.

1.4. Phân tích các công trình nghiên cứu công bố gần đây và định hướng nghiên cứu của đề tài luận án

1.4.1. Phân tích các công trình về thành phần mật mã

Luận án đề xuất một phương pháp sinh S-box từ các thành phần nhỏ hơn, và đề xuất ma trận MDS dạng dịch vòng nhằm cân bằng giữa độ an toàn và khả năng hiện thực trên phần cứng.

1.4.2. Phân tích các công trình về kiến trúc phần cứng tốc độ cao cho thuật toán mã hóa

Mặc dù nhiều kiến trúc AES pipeline đã đạt được tốc độ xử lý rất cao, nhưng phần lớn vẫn tồn tại những hạn chế như tiêu tốn nhiều tài nguyên phần cứng hoặc có độ trễ lớn. Hiện nay, vẫn chưa có một phương pháp thiết kế nào thực sự hiệu quả trong việc cân bằng đồng thời ba yếu tố: tốc độ xử lý, độ trễ, và chi phí tài nguyên. Vì vậy, trong luận án này, đề xuất một phương pháp thiết kế kiến trúc AES hướng tới hiệu suất cao, độ trễ thấp, và chi phí tài nguyên hợp lý. Ngoài ra, luận án cũng đề xuất một kiến trúc phần cứng Ascon tốc độ cao với khả năng xử lý mã hóa xác thực trong một chu kỳ clock, đồng thời đề xuất giao tiếp hiệu quả cho thuật toán AEAD, hướng đến khả năng triển khai thực tế lên các giao thức bảo mật, trong đó có IPSec.

1.4.3. Phân tích các công trình về kiến trúc tốc độ cao cho giao thức IPSec

Luận án đề xuất một kiến trúc phần cứng mới có tên là **HMS-IPSec (High-speed Multi-Cryptographic Secure IPSec architecture)**, trong đó kết hợp hiệu quả các kết quả nghiên cứu ở trên của luận án về các thành phần mật mã, kiến trúc phần cứng tốc độ cao

cho AES, Ascon, để nâng cao hiệu năng hoạt động của IPSec, đồng thời khắc phục các hạn chế của các giải pháp đã có.

1.5. Kết luận chương 1

Chương 1 cung cấp một tổng quan toàn diện về các vấn đề nghiên cứu liên quan đến thuật toán mã hóa AES, thuật toán mã hóa xác thực Ascon, và giao thức bảo mật IPSec. Qua việc phân tích các thành phần mật mã cốt lõi như S-box và ma trận MDS, chương đã làm rõ vai trò của các đại lượng mật mã trong việc đảm bảo độ an toàn cũng như hiệu quả triển khai trên phần cứng. Đồng thời, chương đã đánh giá các công trình nghiên cứu gần đây về thiết kế S-box, tăng tuyến tính, và phát triển các kiến trúc phần cứng tốc độ cao cho AES, Ascon, và IPSec.

CHƯƠNG 2

NGHIÊN CỨU LỰA CHỌN CÁC THÀNH PHẦN MẬT MÃ AN TOÀN HIỆU QUẢ CHO CÀI ĐẶT TỐI ƯU AES

2.1. Nghiên cứu lựa chọn S-box 8-bit an toàn hiệu quả

Chương 2 xây dựng Thuật toán 2.1. Thuật toán thực hiện việc tìm kiếm các S-box n bit dựa trên cấu trúc Butterfly, trong đó các hoán vị thành phần được sinh từ các hàm lũy thừa trên trường hữu hạn $\mathbb{F}_{2^m}$.

Thuật toán 2.1. Thuật toán sinh S-box n -bit S_p dựa trên cấu trúc Butterfly

Đầu vào: n, m với $n = 2m$

Đầu ra: S-box n -bit S_p

$best_score = 0$

$best_S = none$

For $i \leftarrow 0$ **to** $2^m - 1$:

For $j \leftarrow 0$ **to** $2^m - 1$:

if $(gcd(i, 2^m - 1) = 1 \ \&\& \ gcd(j, 2^m - 1) = 1)$

$S = GenSbox(\pi[i], \pi[j], \hat{\pi})$

$(NL, MDP, MLP, AD, degIO, FP) \leftarrow$

$SboxProperties(S)$

$score \leftarrow$

$weighted_eval(NL, MDP, MLP, AD, degIO, FP)$

if $score > best_score$

$best_score \leftarrow score$

$best_S \leftarrow S$

else continue

Return $best_S$

Thuật toán đề xuất giúp giảm đáng kể không gian tìm kiếm so với phương pháp duyệt toàn bộ các hoán vị m bit. Cụ thể với trường hợp

$m = 4$ độ phức tạp thuật toán là $O(64)$ so với $O(16!)^2 \approx O(4.37 \times 10^{26})$ nếu duyệt toàn bộ các hoán vị. Từ thuật toán, S-box 8-bit S_p được đề xuất:

```

 $S_p[256] = \{$ 
    01, 11, 91, E1, D1, B1, 71, 61, F1, 21, C1, 51, A1, 41, 31, 81,
    00, 10, E3, 92, B5, D4, 77, 66, 89, 38, AB, 4A, CD, 5C, 2F, FE,
    08, 5F, 3E, B0, 1C, C2, 83, DD, E8, F6, 47, 79, 95, 2B, AA, 64,
    0F, 48, D0, 29, A3, 1A, F2, BB, 65, CC, E4, 3D, 57, 7E, 86, 9F,
    0C, 2A, F4, 1F, 5B, 90, EE, C5, 36, 6D, 73, 88, BC, A7, 49, D2,
    0A, 3C, 18, 85, E0, 4D, 99, A4, B3, 5E, DA, C7, 72, FF, 6B, 26,
    06, 76, CF, A8, 4E, 59, 60, 17, DC, 9B, 32, F5, 23, 84, ED, BA,
    07, 67, 2D, 3B, FA, 8C, 16, 70, 54, A2, 98, BE, EF, D9, C3, 45,
    0E, A9, 62, 5A, 27, BF, 34, 9C, FD, D5, 8E, E6, 1B, 43, 78, C0,
    03, B2, 87, C4, 9D, 6E, 4B, F8, 7A, E9, 2C, AF, D6, 15, 50, 33,
    0D, FB, 56, EC, 3F, 75, B8, 42, 1E, 24, C9, 93, 80, 6A, D7, AD,
    04, E5, B9, 7D, 82, A6, CA, 2E, 97, 13, 6F, DB, 44, 30, FC, 58,
    0B, 8D, 9A, 46, 74, 28, DF, 53, CB, B7, F0, 6C, AE, E2, 35, 19,
    05, 94, 7B, DE, C6, F3, AC, 39, 4F, 8A, 55, 20, 68, BD, 12, E7,
    02, D3, A5, F7, 69, EB, 5D, 8F, 22, 40, B6, 14, 3A, C8, 9E, 7C,
    09, CE, 4C, 63, D8, 37, 25, EA, A0, 7F, 1D, 52, F9, 96, B4, 8B
 $\};$ 

```

Bảng 2.1. So sánh tính chất mật mã của S-box

S_p với các S-box khác

Tính chất	S_p	AES	Kuznyechik	Camellia	SEED_S0	Kalyna_Pi0
NL	108	112	100	112	112	104
MDP	0.0234	0.0156	0.0312	0.0156	0.0156	0.0312
MLP	0.0244	0.0156	0.0478	0.0156	0.0156	0.0351
AD	7	7	7	7	7	7
degIO	3	2	3	2	2	3
FP	0	0	0	0	2	0
CLR	False	True	False	True	True	False
SAC	0.5166	0.5049	0.5125	0.4983	0.5042	0.5039
BIC-SAC	0.4907	0.4954	0.5059	0.4967	0.4983	0.4985
BIC-NL	111.57	112	106.79	112	112	106.64

S-box S_p được tối ưu nhằm hướng đến việc triển khai hiệu quả hơn trên phần cứng, đặc biệt là trong các ứng dụng yêu cầu tốc độ cao và độ trễ thấp. Biểu diễn logic tối ưu của S-box S_p có độ phức tạp 191 phép toán logic cơ bản.

Bảng 2.6. So sánh số lượng LUT của S-box S_p trên FPGA

Work	Device	LUT	Max Freq (Mhz)	Throughput (Gbps)	Mbps/LUT
This work	Virtex-6	35	800	6.4	183
[30]	Virtex-6	31	724.638	5.79	187
[43]	Virtex-6	32	696.37	5.57	170
[37]	Virtex-6	40	732.279	5.86	146
This work	Virtex-7	32	826	6.60	206
[38]	Virtex-7	32	813	6.5	203
[35]	Virtex-7	40	593	4.74	118

2.2. Nghiên cứu lựa chọn ma trận MDS an toàn hiệu quả

Ma trận $M_p = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 \\ 1 & 3 & 1 & 2 \\ 1 & 2 & 140 & 1 \end{pmatrix}$ được đề xuất nhằm đảm bảo

tiêu chí an toàn và hiệu quả như sau: 1) là ma trận MDS với số nhánh cực đại; 2) có một điểm bất động; 3) có 9 hệ số 1 nhất và các hệ số còn lại cài đặt được hiệu quả trên phần cứng.

2.3. Đánh giá độ an toàn của mã khối AES với các thành phần mật mã mới

Độ an toàn của mã khối AES với các thành phần mật mã mới (gọi là AES-P) được đánh giá thông qua ba nhóm tiêu chí chính: 1) Tiêu chí khuếch tán; 2) Kiểm thử thống kê ngẫu nhiên; và 3) Độ phức tạp tính toán. Các đánh giá an toàn cho thấy AES-P có khả năng khuếch tán mạnh, vẫn đảm bảo an toàn trước thám mã vi sai và tuyến tính.

Đặc biệt AES-P có khả năng chống lại tấn công thám mã đại số trên máy tính lượng tử.

2.4. Đánh giá hiệu năng của mã khối AES với các thành phần mật mã mới

Hiệu năng của mã khối AES với các thành phần mật mã mới không thay đổi trong thư viện OpenSSL. Đối với hiệu năng phần cứng, chương 3 sẽ trình bày kiến trúc AES tốc độ cao được đề xuất và đánh giá chi tiết hiệu năng khi triển khai trên nền tảng FPGA.

2.5. Kết luận chương 2

Chương 2 đã trình bày một cách toàn diện quá trình nghiên cứu và đề xuất các thành phần mật mã an toàn, hiệu quả cho thuật toán AES, bao gồm S-box 8-bit S_p và ma trận MDS M_p . Các đánh giá an toàn thông qua hiệu ứng AC, SAC cho thấy AES với các thành phần mới có khả năng khuếch tán mạnh, vẫn đảm bảo an toàn trước thám mã vi sai và tuyến tính. Đặc biệt AES đề xuất có khả năng chống lại tấn công thám mã đại số trên máy tính lượng tử. Hiệu năng phần mềm của AES với các thành phần mới được duy trì ổn định trong thư viện OpenSSL, trong khi triển khai phần cứng sẽ được phân tích chi tiết ở chương tiếp theo.

CHƯƠNG 3

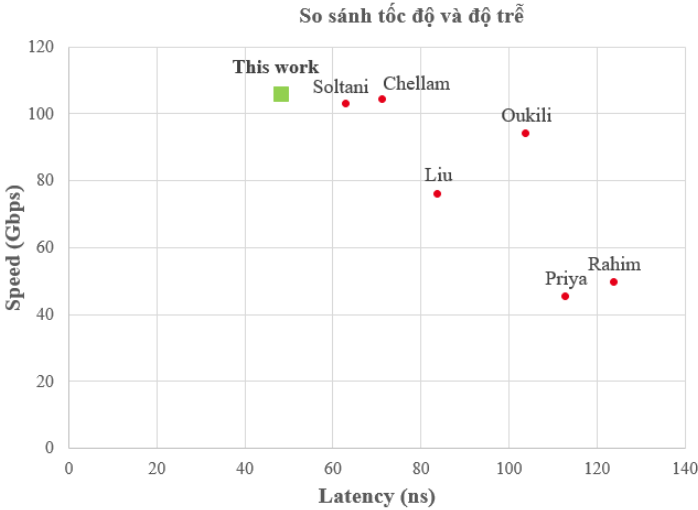
NGHIÊN CỨU XÂY DỰNG CÁC KIẾN TRÚC PHẦN CỨNG TỐC ĐỘ CAO CHO THUẬT TOÁN MÃ HÓA AES VÀ ASCON

3.1. Nghiên cứu xây dựng kiến trúc phần cứng tốc độ cao cho AES

Để phát triển một kiến trúc AES pipeline hiệu quả, phương pháp nghiên cứu ở đây bao gồm: 1) cải tiến các thành phần ảnh hưởng lớn nhất đến độ trễ như SubBytes, MixColumns và lược đồ khóa; 2) xác định vị trí và số lượng thanh ghi (registers) cho các tầng pipeline một cách hợp lý nhằm cân bằng giữa ba yếu tố: tốc độ, độ trễ, và tài nguyên. Nhằm giải quyết bài toán này, cần một thước đo hiệu quả tổng quát, áp dụng cho các mã khối có thể pipeline được trên phần cứng, nhằm đảm bảo sự đánh đổi (tradeoff) cân bằng giữa tốc độ, tài nguyên và độ trễ. Do vậy mệnh đề dưới đây được đưa ra để làm cơ sở tìm kiếm kiến trúc pipeline.

Mệnh đề 3.1. Gọi $H = \frac{T}{A \times L}$ là tham số đánh giá hiệu quả của kiến trúc pipeline cho một mã khối bất kỳ, trong đó T là tốc độ, A là tài nguyên, L là độ trễ. Gọi k là số thanh ghi có thể thêm được vào kiến trúc pipeline, khi đó tồn tại giá trị k^* sao cho H là cực đại, tại đó kiến trúc pipeline đạt sự đánh đổi tối ưu giữa tốc độ, tài nguyên và độ trễ.

Dựa trên Mệnh đề 3.1, NCS xây dựng thuật toán 3.1 để tìm số thanh ghi tối ưu. Kiến trúc đề xuất được so sánh với các công trình khác:



Hình 3.8. So sánh tốc độ và độ trễ với các thiết kế AES tốc độ cao khác

3.2. Nghiên cứu xây dựng kiến trúc phần cứng tốc độ cao cho Ascon

Kiến trúc Ascon được đề xuất trong phần này nhằm khắc phục được các hạn chế đã chỉ ra. Kiến trúc được thiết kế với sự phân chia rõ ràng giữa các giai đoạn xử lý của thuật toán Ascon-128a, kết hợp giữa iterative loop và unrolling $\times 8$ cho phép kiến trúc xử lý toàn bộ một khối dữ liệu 128 bit chỉ trong một chu kỳ xung nhịp. So sánh với công trình của Khan [50], mặc dù thông lượng tối đa của kiến trúc đề xuất thấp hơn khoảng 8% (13,3 Gbps so với 14,5 Gbps), nhưng hiệu quả thực tế trong hệ thống lại vượt trội hơn nhờ hai yếu tố:

1. Loại bỏ gánh nặng cho giao thức: Kiến trúc đề xuất loại bỏ hoàn toàn các header điều khiển của LWC API, giúp thông lượng thực tế tiệm cận với thông lượng lý thuyết.

2. Nâng cao hiệu quả tích hợp hệ thống: Với đặc tính xử lý 1 chu kỳ/khối, kiến trúc không yêu cầu bộ nhớ đệm đầu vào/đầu ra, giúp giảm thiểu độ trễ hệ thống và đơn giản hóa việc tích hợp vào các đường ống xử lý dữ liệu phức tạp như IPSec hay IoT Gateway.

3.3. Đánh giá độ an toàn

Độ an toàn của kiến trúc AES và Ascon được đánh giá trên hai khía cạnh: độ an toàn của thuật toán và độ an toàn của cài đặt. Thuật toán AES đã được phân tích tại Mục 2.3, còn Ascon được đề xuất nhằm tăng hiệu suất mà không ảnh hưởng đến độ an toàn. Về cài đặt, tiêu chí tập trung vào khả năng kháng các tấn công kênh kề như DPA, CPA, EMA và timing. Cả hai kiến trúc đều an toàn trước tấn công timing nhờ không sử dụng nhánh điều kiện và xử lý mỗi bản rõ trong số chu kỳ cố định. Các kỹ thuật như pipeline, unrolling cũng giúp tăng khả năng kháng DPA. Tuy nhiên, chưa có cơ chế bảo vệ đặc thù cho các tấn công nâng cao như CPA hay EMA, và đây sẽ là hướng nghiên cứu trong tương lai.

3.4. Kết luận chương 3

Chương 3 đã xây dựng các kiến trúc phần cứng tối ưu cho thuật toán mã hóa AES và Ascon, nhằm giải quyết những yêu cầu về tốc độ cao, độ trễ thấp và hiệu quả tài nguyên trong các hệ thống hiện đại. Kết quả cho thấy kiến trúc AES đề xuất đạt được thông lượng 105,7 Gbps, với độ hiệu quả là 31,48 Mbps/Slice trên Virtex-7. Độ trễ của

thiết kế giảm 32% so với [38], 53% so với [37], 42% so với [35]. Kiến trúc Ascon đạt tốc độ tối đa 13312 Mbps, loại bỏ nhu cầu bộ nhớ đệm lớn và giảm độ phức tạp so với LWC API. Những kết quả này không chỉ có giá trị về mặt lý thuyết mà còn mở ra tiềm năng ứng dụng thực tiễn trong các hệ thống mã hóa hiệu năng cao. Chương tiếp theo sẽ trình bày việc áp dụng các kiến trúc này vào giao thức IPSec, một giao thức quan trọng trong việc đảm bảo an toàn thông tin trên các mạng IP.

CHƯƠNG 4

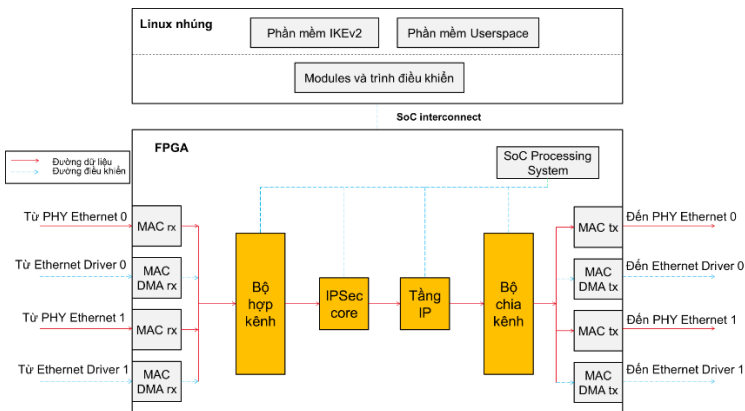
NGHIÊN CỨU ĐỀ XUẤT KIẾN TRÚC PHẦN CỨNG ĐỂ NÂNG CAO HIỆU NĂNG HOẠT ĐỘNG CỦA IPSEC

4.1. Nghiên cứu đề xuất kiến trúc phần cứng tổng thể

Dựa trên các phân tích về hạn chế của các kiến trúc IPsec trên FPGA trong phần 1.4.3, bao gồm:

- không phân tách rõ ràng giữa đường dữ liệu và đường điều khiển,
- tiêu thụ tài nguyên lớn khi sử dụng nhiều lõi mã hóa,
- thiếu hỗ trợ các tính năng triển khai thực tế như vượt NAT và ESN,
- chưa đánh giá hiệu quả của thuật toán mã hoá hạng nhẹ.

Luận án đề xuất kiến trúc HMS-IPsec. Kiến trúc này được thiết kế để tối ưu hóa thông lượng, giảm độ trễ, và đảm bảo hiệu quả tài nguyên trên FPGA, đồng thời đáp ứng các yêu cầu bảo mật khắt khe của các ứng dụng thời gian thực.

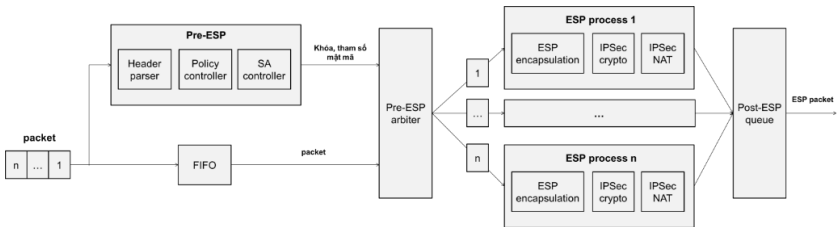


Hình 4.1. Kiến trúc HMS-IPsec

L luận án đề xuất các thuật toán từ 4.1 đến 4.4 cho các thành phần của kiến trúc HMS-IPSec bao gồm: bộ hợp kênh, tầng IPSec, tầng IP, và bộ chia kênh.

4.2. Nghiên cứu đề xuất kiến trúc IPSec tốc độ cao

Kiến trúc thực hiện xử lý theo gói tin được chia làm hai giai đoạn *Pre-ESP* và *ESP process*. Giai đoạn *Pre-ESP* bao gồm ba thành phần: Header parser, Policy controller và SA controller. Giai đoạn *ESP process* gồm các thành phần: ESP encapsulation, IPSec crypto và IPSec NAT như sau:



Hình 4.6. Kiến trúc IPSec tốc độ cao đề xuất

Thuật toán 4.4. Thuật toán xử lý IPSec

SPD output: Bảng chính sách cho gói tin đi ra

SPD input: Bảng chính sách cho gói tin đến

SPD secure: Bảng chính sách cho gói tin bảo mật

SAD output: Bảng khóa, tham số mật mã cho gói tin đi ra

SAD input: Bảng khóa, tham số mật mã cho gói tin đến

Đầu vào: Gói tin IP

Đầu ra: Gói tin được xử lý IPSec

1. Header parser xác định loại gói tin, từ LAN/WAN hay từ thiết bị.
2. Policy controller tạo tuple gồm địa chỉ IP nguồn, IP đích, port nguồn, port đích, protocol của gói tin.
3. Tra tuple với bảng *SPD output*, *SPD input*, *SPD secure* sử dụng TCAM.
4. Lưu các kết quả của bước 1 và bước 3.
5. Đọc kết quả bước 4.
6. **if** ((gói tin là ARP) || (gói tin từ thiết bị) || (gói tin đến thiết bị)) **then**

```

7. | | Chuyển gói tin đi không cần xử lý gì thêm.
8. | | Nhảy đến bước 1.
9. | else if (gói tin từ LAN) then
10. |   if (match SPD output) then
11. |     | Chuyển gói tin đi không cần xử lý gì thêm.
12. |     | Nhảy đến bước 1.
13. |   else if (match SPD secure) then
14. |     | SA controller thực hiện tra bảng SAD output sử dụng
15. |     | sa_id từ SPD secure để lấy khóa, tham số mật mã.
16. |     | ESP encapsulation tạo IP header mới và chèn vào gói tin.
17. |     | ESP encapsulation tạo ESP header và ESP trailer và chèn
18. |     | vào gói tin.
19. |     | IPSec crypto thực hiện mã hóa gói tin.
20. |     | IPSec crypto thực hiện tính giá trị toàn vẹn ICV của gói
21. |     | tin và chèn vào gói tin.
22. |     | IPSec NAT kiểm tra thiết bị có nằm sau NAT.
23. |     | if (NAT) then
24. |       | Cập nhập IP header mới cho gói tin UDP ESP.
25. |       | Tạo và chèn UDP header.
26. |       | Chuyển gói tin UDP ESP đi.
27. |       | Nhảy đến bước 1.
28. |     | else
29. |       | Chuyển gói tin ESP đi.
30. |       | Nhảy đến bước 1.
31. |     | end if
32. |   else
33. |     | else if (gói tin từ WAN) then
34. |       | if (match SPD input) then
35. |         | if (gói tin là ESP) then
36. |           | Lấy các giá trị spi, esn, icv từ gói tin.
37. |           | SA controller thực hiện tra bảng SAD input sử dụng
38. |           | spi để lấy khóa, tham số mật mã.
39. |           | if (match spi) then
40. |             | SA controller thực hiện kiểm tra esn với cửa sổ
41. |             | trượt và bitmap trong SAD input.
42. |             | if (gói tin phát lại) then
43. |               | Loại bỏ gói tin.

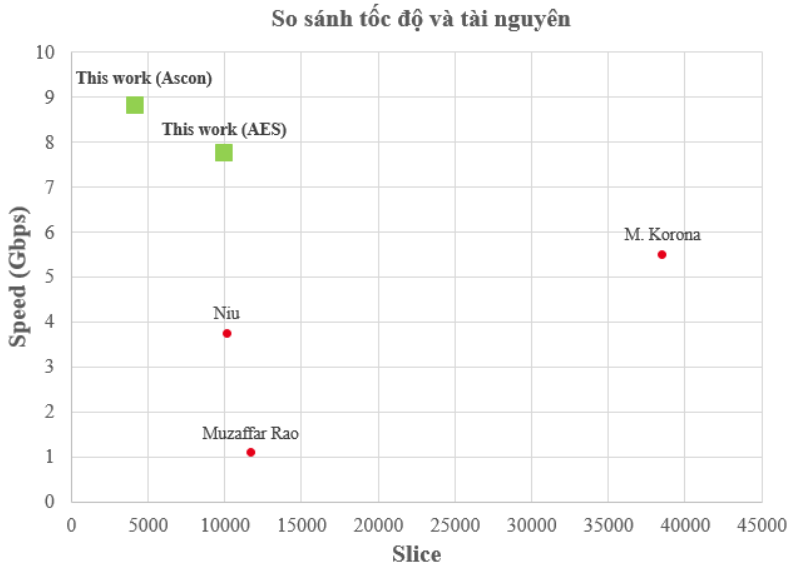
```

```

41. | | | | Nhảy đến bước 1.
42. | | | else
43. | | |   IPSec crypto thực hiện giải mã gói tin.
44. | | |   IPSec crypto thực hiện tính giá trị toàn vẹn
45. | | |   icv_c của gói tin.
46. | | |   if (icv_c == icv) then
47. | | |     SA controller cập nhập cửa sổ trượt và
48. | | |     bitmap trong SAD input.
49. | | |     Chuyển gói tin ESP đi.
50. | | |     Nhảy đến bước 1.
51. | | |   end if
52. | | | end if
53. | | end if
54. | | else
55. | |   Loại bỏ gói tin.
56. | |   Nhảy đến bước 1.
57. | | end if
58. | else if (gói tin là ESP_UDP) then
59. |   Gỡ bỏ UDP header.
60. |   Nhảy đến bước 35.
61. | else
62. |   Chuyển gói tin đi không cần xử lý gì thêm.
63. |   Nhảy đến bước 1.
64. | end if
65. | else
66. |   Loại bỏ gói tin.
67. |   Nhảy đến bước 1.
68. | end if
69. | else
70. |   Loại bỏ gói tin.
71. |   Nhảy đến bước 1.
72. | end if

```

Kiến trúc đề xuất được so sánh với các công trình khác:



Hình 4.9. So sánh tốc độ và tài nguyên của kiến trúc IPsec với các các thiết kế IPsec tốc độ cao khác

Độ trễ của kiến trúc được so sánh với các công trình khác:

Bảng 4.7. So sánh độ trễ của các công trình

Công trình	Độ trễ
Luận án (Ascon)	1,313 μs
Luận án (AES-GCM)	1,471 μs
Muzaffar Rao [64]	4,166 μs
Lastinec [66]	1,5 ms
Wang [67]	250,63 μs
Liu [69]	15 ms

NCS thực hiện cài đặt HMS-IPsec với các thành phần như sau:

Bảng 4.9. Các IPCore sử dụng trong thiết kế

STT	Thành phần	IPCore	Nguồn gốc
0	SoC Processing System	ZYNQ7 Processing System	Xilinx
1	MAC rx và MAC tx	AXI 1G/2.5G Ethernet Subsystem	Xilinx
2	MAC DMA rx và MAC DMA tx	AXI Direct Memory Access	Xilinx
3	Bộ hợp kênh	port_mux_0	NCS cài đặt
4	IPSec	ipsec_0	NCS cài đặt
5	Tầng IP	IP_port_lookup_0	NCS cài đặt
6	Bộ chia kênh	port_demux_0	NCS cài đặt

Thiết kế HMS-IPSec được tổng hợp và triển khai thành công dưới dạng bitstream, sau đó được nạp vào Kit phát triển ZC706.

4.3. Kết luận chương 4

Chương 4 đã trình bày nghiên cứu đề xuất và triển khai kiến trúc phần cứng HMS-IPSec, trong đó thông lượng tối đa lên đến 23,26 Gbps, độ trễ 1471 ns cho AES-GCM. Thuật toán Ascon-128a có độ trễ thấp 1313 ns và hiệu quả cài đặt rất cao (2,08 Mbps/Slice), gấp đến 2,1 lần so với các nghiên cứu khác.

KẾT LUẬN

Luận án này tập trung nghiên cứu các giải pháp nâng cao hiệu năng của một số thuật toán mã hoá trong bảo mật luồng IP, đáp ứng nhu cầu bảo mật cho các hệ thống mạng hiện đại.

I. Đóng góp mới của luận án

1) Nâng cao hiệu năng của thuật toán mã hoá AES-P và ASCON: Luận án đề xuất một kiến trúc AES-P đường ống 4 tầng, trong đó sử dụng các thành phần mật mã mới, bao gồm S-box S_p và ma trận MDS M_p , được thiết kế theo hướng thân thiện với phần cứng. Kiến trúc AES-P đạt thông lượng 105,7 Gbps với độ trễ là 48,4 ns, cải thiện đến 53% về độ trễ so với các công trình liên quan trên cùng nền tảng FPGA Virtex-7. Độ an toàn của AES-P vẫn được bảo toàn đối với các tấn công vi sai và tuyến tính, đồng thời nâng cao khả năng kháng tấn công đại số, hướng tới chống lại các tấn công đại số có thể thực thi trên máy tính lượng tử. Bên cạnh đó, luận án đề xuất một kiến trúc mới cho Ascon, bao gồm lõi thuật toán và khối giao tiếp, giúp đạt thông lượng 13,312 Gbps trong 1 chu kỳ, loại bỏ sự phụ thuộc vào bộ nhớ và phù hợp cho các hệ thống IoT thời gian thực. Các kết quả này được công bố trong các công trình [J1], [J2], [C1], [C2].

2) Đề xuất kiến trúc hệ thống HMS-IPSec trên thiết bị SoC: Luận án thiết kế và xây dựng kiến trúc phần cứng HMS-IPSec tích hợp thống nhất các bộ thuật toán AES-P-GCM, AES-P-CTR-HMAC-SHA256 và Ascon-AEAD128. Điểm nổi bật của kiến trúc là sự phân tách triệt để giữa đường dữ liệu và đường điều khiển,

kết hợp với việc hỗ trợ đầy đủ các tính năng quan trọng như cơ chế vượt NAT, ESN 64-bit, giúp khắc phục các hạn chế về khả năng triển khai thực tế trong các công trình trước đây. Kiến trúc cho phép chuyển đổi linh hoạt giữa AES-P và Ascon mà không làm thay đổi cấu trúc xử lý gói tin, qua đó đảm bảo đồng thời yêu cầu về thông lượng lớn, độ trễ thấp cho các ứng dụng thời gian thực. Đây là nghiên cứu đầu tiên đánh giá một cách hệ thống tính khả thi và hiệu quả của việc tích hợp thuật toán mã hoá hạng nhẹ Ascon-AEAD128 vào giao thức IPSec trên nền tảng phần cứng SoC. Các kết quả nghiên cứu này đã được công bố trong công trình [J2].

II. Hướng nghiên cứu tiếp theo

- Nghiên cứu và tích hợp các kỹ thuật chống tấn công kênh kề.
- Mở rộng hỗ trợ các thuật toán mật mã hậu lượng tử.
- Nghiên cứu phát triển các kiến trúc trên các nền tảng phần cứng ASIC và công nghệ mới.

DANH MỤC CÁC CÔNG TRÌNH KHOA HỌC ĐÃ CÔNG BỐ

I. CÔNG TRÌNH CÔNG BỐ LIÊN QUAN ĐẾN LUẬN ÁN

- [J1] Nam, T. S., Dung, L. T., & Long, N. V. (2024). *A High Throughput, Low Latency 105 Gbps Four-Pipeline Stage AES*. Journal of Science and Technology on Information Security, 1(21), 58-66. (HĐGSNN, 0.75)
- [J2] Nam, Tran Sy, Hoang Van Thuc, and Bui Duy Hieu. "A Hardware Architecture of NIST Lightweight Cryptography applied in IPSec to Secure High-throughput Low-latency IoT Networks." IEEE Access (2023). (Q1, IF = 3.4).
- [J3] Nam, T. S., Long, N. V., & Cuong, N. B. (2023). *An efficient and secure linear diffusion layer for 256-bit block cipher based on FLC structure*. Journal of Science and Technology on Information Security, 2(16), 31-38. (HĐGSNN, 0.75)
- [C1] Nam, Tran Sy, Le Quoc Dat, Nguyen Van Long, and Nguyen Bui Cuong. "An Optimized Bit-Slice Implementation of Secure 8-Bit Sbox Based on Butterfly Structure." 2023 15th International Conference on Knowledge and Systems Engineering (KSE). IEEE, 2023. (ISBN 979-8-3503-2974-2)
- [C2] Nguyen, Cuong, Nam Tran, and Long Nguyen. "FLC: A New Secure and Efficient SPN-Based Scheme for Block Ciphers." 2022 9th NAFOSTED Conference on Information and Computer Science (NICS). IEEE, 2022. (ISBN 978-1-6654-5422-3)

II. CÔNG TRÌNH CÔNG BỐ KHÁC TRONG QUÁ TRÌNH THỰC HIỆN LUẬN ÁN

- [C3] Van Nghi, Nguyen, Tran Sy Nam, Tran Thi Hanh, and Hoang Van Thuc. "A Flexible and Balanced Hardware Architecture of RSA Modulo Exponentiation on FPGA." In The International Conference on Intelligent Systems & Networks, pp. 416-422. Singapore: Springer Nature Singapore, 2024. (ISBN 978-981-97-5504-2)