

**VIETNAM GOVERNMENT INFORMATION SECURITY COMMISSION
ACADEMY OF CRYPTOGRAPHY TECHNIQUES**

TRAN SY NAM

**PERFORMANCE ENHANCEMENT SOLUTIONS FOR
SELECTED CRYPTOGRAPHIC ALGORITHMS IN IP
NETWORK SECURITY**

Major: Cryptography Techniques

Code: 9520209

**SUMMARY OF THE PHD DISSERTATION
OF CRYPTOGRAPHY TECHNIQUES**

HA NOI – 2026

The dissertation was completed at:
Academy of Cryptography Techniques.

Supervisor:

1. Associate Professor, Dr. Luong The Dung
2. Dr. Hoang Van Thuc

Reviewer 1: Assoc. Dr. Trinh Quang Kien

Reviewer 2: Dr. Dao Ba Anh

Reviewer 3: Assoc. Dr. Nguyen Duc Minh

The dissertation was defended before the Doctoral Dissertation
Evaluation Council at the Academy of Cryptography Techniques.

At 1:30 PM, on June 11, 2026

The dissertation can be found at the following libraries:

1. Academy of Cryptography Techniques Library
2. National Library of Vietnam

INTRODUCTION

The explosion of the digital era is shaping an increasingly complex communication network, in which data is generated, transmitted, and processed in real time on an unprecedented scale. From large-scale data centers and edge artificial intelligence to 5G/6G networks and the Internet of Things (IoT), network security infrastructure must satisfy not only security requirements but also security delivered with maximum performance: high throughput, low latency, and flexible scalability. This challenge exposes the limitations of traditional CPU-based processing as data volumes continue to grow, while cryptographic primitives (encryption, authentication, integrity) that act directly on real-time data flows can no longer meet these requirements. This has driven a shift toward dedicated hardware solutions such as FPGA and ASIC to increase speed and reduce latency while still guaranteeing security — properties that are difficult to achieve with software alone.

There are currently many algorithms that provide different cryptographic services, but not all of them are suitable for efficient implementation on hardware platforms. For example, DES and 3DES no longer guarantee adequate security and are unsuitable for high-performance applications. In contrast, AES (Advanced Encryption Standard) continues to be widely applied both in practice and in academic research thanks to its advantages in security and its suitability for hardware implementation, especially in the AES-GCM

mode. This mode belongs to the AEAD (Authenticated Encryption with Associated Data) family, which simultaneously provides confidentiality, authentication, and integrity within a unified scheme, with a clear security model and reduced risk of configuration errors. Notably, AES-GCM also shows outstanding hardware performance thanks to the high parallelizability of both the encryption process and the Galois multiplication function (GHASH). For this reason, improving the hardware performance of AES/AES-GCM remains a topic of strong interest within the international research community.

In addition, AEAD has become a mandatory requirement in the design of lightweight cryptographic algorithms for IoT networks, since AES was not truly designed for this purpose. In August 2025, NIST standardized Ascon as the lightweight authenticated encryption standard. In the context of IoT networks, where optimization for resource-constrained devices is a key factor, some use cases prioritize high performance and low latency to satisfy security requirements in real-time communication environments, such as central security servers, edge servers, and IoT gateway devices. Consequently, improving the hardware performance of Ascon has also become an important and increasingly researched trend in recent years.

The performance of encryption algorithms can be improved in two ways: (i) optimizing the internal components of the algorithm, or (ii) optimizing the architecture used for hardware implementation. However, optimizing the internal components of an encryption algorithm, such as the S-box and the MDS (Maximum Distance

Separable) matrix, is genuinely suitable and yields much clearer benefits for AES than for Ascon, owing to differences in structure and computation:

- AES (an SPN block cipher): Performance is strongly governed by the S-box (SubBytes) and the MDS matrix (MixColumns). Selecting and redesigning these components in a hardware-friendly direction can significantly improve throughput and latency.

- Ascon (a lightweight AEAD scheme based on the sponge/permutation construction): It is designed to be minimal for resource-constrained devices, and each round is implemented in a simple manner, so there is little room left for improvement by modifying internal components. Performance gains here come mainly from architectural changes such as loop unrolling, iterative execution, and state/bus organization.

Based on the analyses above, in order to enhance the performance of the AES and Ascon encryption algorithms in IP traffic security, this dissertation targets three specific goals: increasing data-processing throughput, reducing latency, and reducing the hardware resources used during implementation. To achieve these goals, the dissertation focuses on three main research directions:

First, the dissertation studies, selects, and designs new cryptographic components for AES; specifically, it proposes an S-box and an MDS matrix with hardware-friendly structures to improve throughput and latency while still guaranteeing the required level of security.

Second, the dissertation studies the construction of high-speed hardware architectures for AES and Ascon, proposing new architectures that use parallelization techniques, pipelining, loop unrolling, and optimized register organization, in order to find architectures suitable for high-performance security systems.

Third, the dissertation focuses on proposing a new hardware architecture for the IPSec protocol, since when considering the overall problem, improving individual cryptographic components alone is not enough to meet the requirements of high-speed systems. The new architecture is designed to directly leverage the results of the two research directions above, using the improved AES and Ascon algorithms, while also proposing efficient packet-processing and data-flow algorithms to increase throughput and reduce latency.

CHAPTER 1

BACKGROUND AND LITERATURE REVIEW

1.1. The AES Encryption Algorithm

The Advanced Encryption Standard (AES) is an iterated block cipher with a 128-bit block size, supporting key sizes of 128, 192, and 256 bits, corresponding to 10, 12, and 14 rounds respectively. Each AES round consists of four basic steps: AddRoundKey, SubBytes, ShiftRows, and MixColumns.

1.2. The Ascon Encryption Algorithm

Ascon is a family of algorithms that provides Authenticated Encryption with Associated Data (AEAD) services. Ascon's authenticated encryption/decryption process consists of four phases: Initialization, Associated Data (AD) processing, Plaintext/Ciphertext processing, and Finalization.

1.3. The IPSec Security Protocol

The current version of IPSec and ESP is version 3, defined in RFC 4301 and RFC 4303. ESP supports two modes: transport and tunnel. In tunnel mode, a new IP packet is created from the original IP packet through the following steps: 1) inserting the ESP header and trailer into the original IP packet; 2) encrypting the original IP packet and the ESP trailer; 3) computing the Integrity Check Value (ICV) over the ESP header and the encrypted data; 4) appending the ICV to the end of the packet; 5) adding a new IP header to the packet.

1.4. Analysis of Recently Published Research and the Research Direction of the Dissertation

1.4.1. Analysis of research on cryptographic components

The dissertation proposes a method for generating S-boxes from smaller components, and proposes a cyclic-shift-based MDS matrix aimed at balancing security and hardware implementability..

1.4.2. Analysis of research on high-speed hardware architectures for encryption algorithms

Although many pipelined AES architectures have achieved very high processing speeds, most of them still suffer from limitations such as high hardware resource consumption or high latency. At present, there is still no design method that effectively balances all three factors simultaneously: processing speed, latency, and resource cost. Therefore, this dissertation proposes a design method for an AES architecture aimed at high performance, low latency, and reasonable resource cost. In addition, the dissertation also proposes a high-speed Ascon hardware architecture capable of performing authenticated encryption within a single clock cycle, together with an efficient interface for the AEAD algorithm, aiming toward practical deployment in security protocols, including IPSec.

1.4.3. Analysis of research on high-speed architectures for the IPSec protocol

The dissertation proposes a new hardware architecture called **HMS-IPSec** (High-speed Multi-Cryptographic Secure IPSec architecture), which effectively combines the dissertation's above

research results on cryptographic components and high-speed hardware architectures for AES and Ascon, in order to enhance the operational performance of IPSec while overcoming the limitations of existing solutions.

1.5. Conclusion of Chapter 1

Chapter 1 provides a comprehensive overview of the research issues related to the AES encryption algorithm, the Ascon authenticated encryption algorithm, and the IPSec security protocol. By analyzing core cryptographic components such as the S-box and the MDS matrix, the chapter clarifies the role of these cryptographic quantities in ensuring security as well as efficient hardware implementation. The chapter also reviews recent research on S-box design, the linear layer, and the development of high-speed hardware architectures for AES, Ascon, and IPSec.

CHAPTER 2

RESEARCH ON SELECTING SECURE AND EFFICIENT CRYPTOGRAPHIC COMPONENTS FOR AES HARDWARE IMPLEMENTATION

2.1. Research on selecting a secure and efficient 8-bit S-box

Chapter 2 constructs Algorithm 2.1, which searches for n bit S-boxes based on the Butterfly structure, in which the component permutations are generated from power functions over the finite field $\mathbb{F}_{2^m}$.

Algorithm 0.1. Algorithm for generating an n -bit S-box S_p based on the Butterfly structure

Input: n, m với $n = 2m$

Output: n -bit S-box 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 $best_S$

The proposed algorithm significantly reduces the search space compared with an exhaustive search over all m . Specifically, for the case $m = 4$, the algorithm's complexity is $O(64)$, compared with $O(16!)^2 \approx O(4.37 \times 10^{26})$ for an exhaustive search over all permutations. From this algorithm, the 8-bit S-box S_p is proposed as follows:

```

 $S_p[256] = \{$ 
    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
 $\};$ 

```

Table 2.1. Comparison of the cryptographic properties of S-box S_p with other S-boxes

Property	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

The S-box S_p is optimized for more efficient hardware implementation, particularly in applications that require high speed and low latency. The optimized logic representation of S-box S_p has a complexity of 191 basic logic operations.

Table 2.6. Comparison of LUT count for S-box S_p on 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. Research on selecting a secure and efficient MDS matrix

The matrix $M_p = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 2 & 3 \\ 1 & 3 & 1 & 2 \\ 1 & 2 & 140 & 1 \end{pmatrix}$ is proposed to guarantee

the following security and efficiency criteria: 1) it is an MDS matrix with maximal branch number; 2) it has a single fixed point; 3) it has 9 coefficients equal to 1, with the remaining coefficients chosen so that they can be implemented efficiently in hardware.

2.3. Security evaluation of the AES block cipher with the new cryptographic components

The security of the AES block cipher with the new cryptographic components (referred to as AES-P) is evaluated through three main groups of criteria: 1) diffusion criteria; 2) statistical randomness testing; and 3) computational complexity. The security evaluations

show that AES-P has strong diffusion properties and remains secure against differential and linear cryptanalysis. Notably, AES-P is resistant to algebraic cryptanalysis attacks that could be executed on a quantum computer..

2.4. Performance evaluation of the AES block cipher with the new cryptographic components

The performance of the AES block cipher with the new cryptographic components is unchanged when implemented in the OpenSSL library. Regarding hardware performance, Chapter 3 presents the proposed high-speed AES architecture and provides a detailed performance evaluation when implemented on an FPGA platform.

2.5. Conclusion of Chapter 2

Chapter 2 has comprehensively presented the research and proposal of safe and efficient cryptographic components for the AES algorithm, including the 8-bit S-box S_p and the MDS matrix M_p . Security evaluations through the Avalanche Criterion (AC) and Strict Avalanche Criterion (SAC) effects show that AES with the new components has strong diffusion capability and remains secure against differential and linear cryptanalysis. Notably, the proposed AES is resistant to algebraic cryptanalysis attacks on a quantum computer. The software performance of AES with the new components remains stable in the OpenSSL library, while the hardware implementation is analyzed in detail in the next chapter.

CHAPTER 3

RESEARCH ON BUILDING HIGH-SPEED HARDWARE ARCHITECTURES FOR THE AES AND ASCON ENCRYPTION ALGORITHMS

3.1. Research on building a high-speed hardware architecture for AES

To develop an efficient pipelined AES architecture, the research approach here includes: 1) improving the components that most strongly affect latency, such as SubBytes, MixColumns, and the key schedule; 2) determining the position and number of pipeline registers appropriately in order to balance three factors: speed, latency, and resources. To address this problem, a general efficiency metric is needed - one that applies to any pipelineable block cipher on hardware and ensures a balanced trade-off among speed, resources, and latency. The following proposition is therefore introduced as the basis for the pipeline-architecture search..

Proposition 3.1. Let $H = \frac{T}{A \times L}$ be the parameter used to evaluate the efficiency of a pipeline architecture for any block cipher, where T is the speed, A is the resource usage, L is the latency. Let k be the number of registers that can be added to the pipeline architecture. Then there exists a value k^* at which H is maximized, and at this point the pipeline architecture achieves the optimal trade-off among speed, resources, and latency.

Based on Proposition 3.1, an algorithm is constructed to find the optimal number of registers. The proposed architecture is compared with other works:

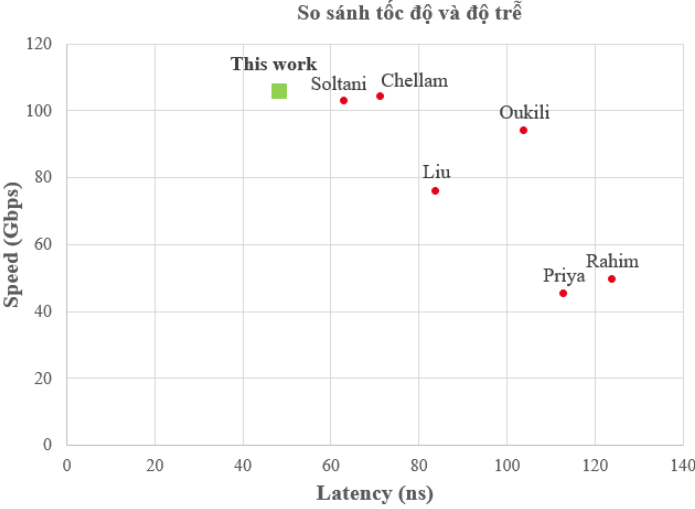


Figure 3.8. Speed and latency comparison with other high-speed AES designs

3.2. Research on building a high-speed hardware architecture for Ascon

The Ascon architecture proposed in this section aims to overcome the limitations identified earlier. The architecture is designed with a clear separation between the processing stages of the Ascon-128a algorithm, combining an iterative loop with $\times 8$ unrolling, which allows the architecture to process an entire 128-bit data block within a single clock cycle. Compared with the work of Khan [50], although the maximum throughput of the proposed architecture is about 8%

lower (13.3 Gbps versus 14.5 Gbps), its practical system-level efficiency is superior thanks to two factors:

1. Elimination of protocol bottlenecks: The proposed architecture completely removes the control headers of the LWC API, allowing the actual throughput to approach the theoretical throughput.

2. Improved system-integration efficiency: With its one-cycle-per-block processing characteristic, the architecture requires no input/output buffer memory, which reduces overall system latency and simplifies integration into complex data-processing pipelines such as IPSec or IoT gateways.

3.3. Security Evaluation

The security of the AES and Ascon architectures is evaluated from two aspects: algorithmic security and implementation security. The security of the AES algorithm was analyzed in Section 2.3, while Ascon was proposed to increase performance without affecting security. Regarding implementation, the evaluation focuses on resistance to side-channel attacks such as DPA, CPA, EMA, and timing attacks. Both architectures are secure against timing attacks because they use no conditional branches and process every plaintext in a fixed number of cycles. Techniques such as pipelining and unrolling also help increase resistance to DPA. However, there is not yet a dedicated protection mechanism against more advanced attacks such as CPA or EMA, and this remains a direction for future research.

3.4. Conclusion of Chapter 3

Chapter 3 has built optimized hardware architectures for the AES and Ascon encryption algorithms, addressing the requirements for high speed, low latency, and resource efficiency in modern systems. The results show that the proposed AES architecture achieves a throughput of 105.7 Gbps, with an efficiency of 31.48 Mbps/Slice on Virtex-7. The design's latency is reduced by 32% compared with [38], 53% compared with [37], and 42% compared with [35]. The Ascon architecture achieves a maximum speed of 13,312 Mbps, eliminating the need for large buffer memory and reducing complexity compared with the LWC API. These results are not only of theoretical value but also open up practical application potential in high-performance encryption systems. The next chapter presents the application of these architectures to the IPSec protocol, an important protocol for ensuring information security on IP networks.

CHAPTER 4

RESEARCH PROPOSING A HARDWARE ARCHITECTURE TO ENHANCE THE OPERATIONAL PERFORMANCE OF IPSEC

4.1. Research proposing an overall hardware architecture

Based on the analysis of the limitations of existing FPGA-based IPSec architectures presented in Section 1.4.3, including:

- no clear separation between the data plane and the control plane,
- high resource consumption when using multiple encryption cores,
- lack of support for practical deployment features such as NAT traversal and ESN,
- the efficiency of lightweight encryption algorithms has not yet been evaluated.

The dissertation proposes the HMS-IPSec architecture. This architecture is designed to optimize throughput, reduce latency, and ensure resource efficiency on FPGA, while meeting the strict security requirements of real-time applications.

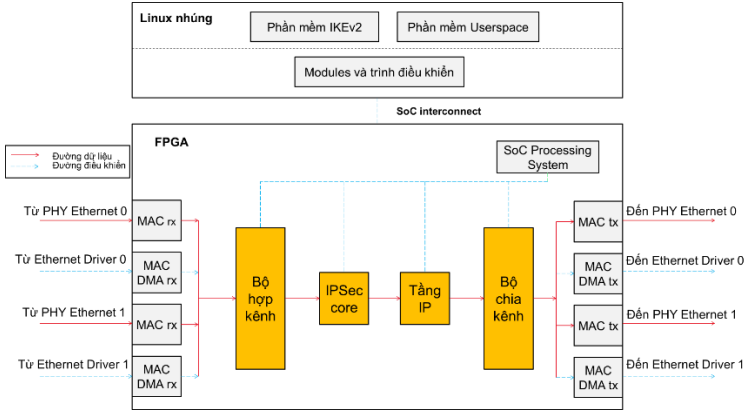


Figure 0.1. The HMS-IPSec architecture

The dissertation proposes Algorithms 4.1 through 4.4 for the components of the HMS-IPSec architecture, comprising: the multiplexer, the IPSec layer, the IP layer, and the demultiplexer.

4.2. Research proposing a high-speed IPSec architecture

The architecture performs packet-based processing divided into two stages: Pre-ESP and ESP processing. The Pre-ESP stage includes three components: the Header parser, the Policy controller, and the SA controller. The ESP-processing stage includes the following components: ESP encapsulation, IPSec crypto, and IPSec NAT, as follows::

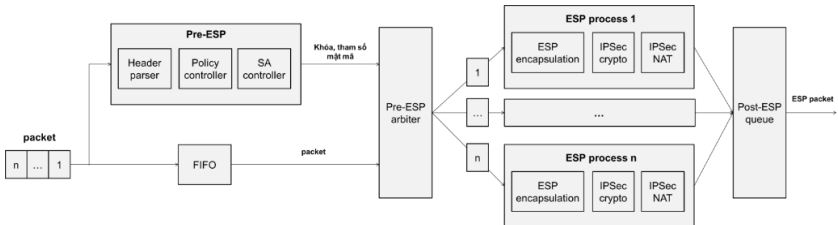


Figure 4.6. The proposed high-speed IPSec architecture

Algorithm 4.4. The IPSec processing algorithm

SPD output: policy table for outbound packets

SPD input: policy table for inbound packets

SPD secure: policy table for secured packets

SAD output: key/parameter table for outbound packets

SAD input: key/parameter table for inbound packets

Input: IP packet

Output: IPSec-processed packet

1. *Header parser* determines the packet type: from LAN/WAN or from the device itself.
2. *Policy controller* builds a tuple consisting of source IP address, destination IP address, source port, destination port, and protocol of the packet.
3. Look up the tuple against the *SPD output*, *SPD input*, *SPD secure* tables using TCAM.
4. Store the results of steps 1 and 3.
5. Read the results of step 4.
6. **if** ((packet is ARP) || (packet is from the device) || (packet is to the device)) **then**
7. Forward the packet without any further processing.
8. Go to step 1.
9. **else if** (packet is from LAN) **then**
10. **if** (match *SPD output*) **then**
11. Forward the packet without any further processing.
12. Go to step 1.
13. **else if** (match *SPD secure*) **then**
14. *SA controller* looks up the *SAD output* table using *sa_id* from *SPD secure* to obtain the key and cryptographic parameters.
15. *ESP encapsulation* creates a new IP header and inserts it into the packet.
16. *ESP encapsulation* creates the ESP header and ESP trailer and inserts them into the packet.
17. *IPSec crypto* encrypts the packet.
18. *IPSec crypto* computes the Integrity Check Value (ICV) of the packet and inserts it into the packet.
19. *IPSec NAT* checks whether the device is behind a NAT.
20. **if** (NAT) **then**
21. Update the new IP header for the UDP-ESP packet.
- Create and insert the UDP header.

```

22. |         |         | Forward the UDP-ESP packet.
23. |         |         | Go to step 1.
24. |         | else
25. |         |         | Forward the ESP packet.
26. |         |         | Go to step 1.
27. |         | end if
28. | else
29. |         | Drop the packet.
30. |         | Go to step 1.
31. | end if
32. else if (packet is from WAN) then
33. | if (match SPD input) then
34. | | if (packet is ESP) then
35. | |         | Extract the spi, esn, icv values from the packet.
36. | |         | SA controller looks up the SAD input tables using
37. | |         | spi to obtain the key and cryptographic parameters.
38. | |         | if (match spi) then
39. | |         | | SA controller check esn against the sliding
40. | |         | | window and bitmap in SAD input SAD input.
41. | |         | | if (packet is a replay) then
42. | |         | |         | Drop the packet.
43. | |         | |         | Go to step 1.
44. | |         | | else
45. | |         | |         | IPSec crypto decrypts the packet.
46. | |         | |         | IPSec crypto computes the integrity value
47. | |         | |         | icv_c of the packet.
48. | |         | |         | if (icv_c == icv) then
49. | |         | |         | | SA controller cập updates the sliding
50. | |         | |         | | window and bitmap in SAD input.
51. | |         | |         | | Forward the ESP packet.
52. | |         | |         | | Go to step 1.
53. | |         | |         | else
54. | |         | |         | | Drop the packet.
55. | |         | |         | | Go to step 1.
56. | |         | |         | end if
57. | |         | | end if
58. | |         | end if

```

```

59.      |      |      | Remove the UDP header.
60.      |      |      | Go to step 35.
61.      |      | else
62.      |      |      | Forward the packet without any further processing.
63.      |      |      | Go to step 1.
64.      |      | end if
65.      | else
66.      |      | Drop the packet.
67.      |      | Go to step 1.
68.      | end if
69. else
70.      | Drop the packet.
71.      | Go to step 1.
72. end if

```

The proposed architecture is compared with other works:

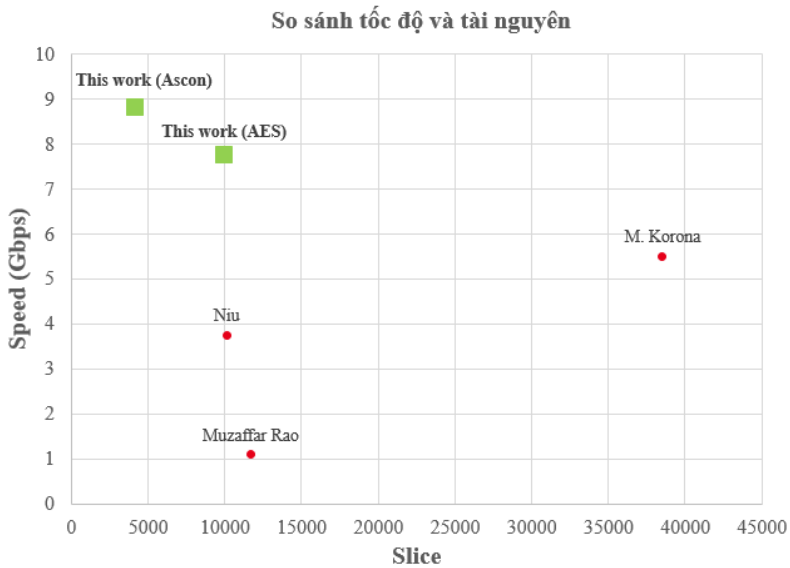


Figure 4.9. Speed and resource comparison of the IPsec architecture with other high-speed IPsec design

The architecture's latency is compared with other works:

Table 4.7. Latency comparison across works

Work	Latency
This dissertation (Ascon)	1,313 μs
This dissertation (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

HMS-IPSec architecture is implemented using the following components:

Table 4.9. IP cores used in the design

STT	Component	IPCore	Source
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	Author-designed
4	IPSec	ipsec_0	Author-designed
5	Tầng IP	IP_port_lookup_0	Author-designed
6	Bộ chia kênh	port_demux_0	Author-designed

The HMS-IPSec design was successfully synthesized and implemented as a bitstream, which was then loaded onto a ZC706 development kit.

4.3. Conclusion of Chapter 4

Chapter 4 has presented the proposed research and implementation of the HMS-IPSec hardware architecture, achieving a maximum throughput of up to 23.26 Gbps and a latency of 1471 ns for AES-GCM. The Ascon-128a algorithm achieves a low latency of 1313 ns and a very high implementation efficiency (2.08 Mbps/Slice), up to 2.1 times higher than other studies.

CONCLUSION

This dissertation focuses on researching solutions to enhance the performance of several encryption algorithms in IP network security, meeting the security needs of modern network systems.

I. Contribution Highlights

1) Enhancing the performance of the AES-P and ASCON encryption algorithms: A 4-stage pipelined AES-P architecture is proposed, incorporating new cryptographic components, namely S-box S_p and MDS matrix M_p , designed with hardware-friendly structures. The proposed AES-P architecture achieves a throughput of 105.7 Gbps with a latency of 48.4 ns, reducing latency by up to 53% compared to related works on the same Virtex-7 FPGA platform. The security of AES-P is preserved against differential and linear cryptanalysis, while enhancing resistance to algebraic attacks, with consideration toward potential quantum computing threats. In addition, a novel architecture for Ascon is proposed, comprising both the cryptographic core and interface modules, achieving a throughput of 13.312 Gbps per cycle, eliminating memory dependency, and making it well-suited for real-time IoT systems. These results have been published in works [J1], [J2], [C1], [C2].

2) Proposing the HMS-IPSec system architecture on an SoC device: The HMS-IPSec hardware architecture is designed and implemented, integrating AES-P-GCM, AES-P-CTR-HMAC-SHA256, and Ascon-AEAD128. The architecture features a strict

separation between the data plane and the control plane, combined with full support for essential features such as NAT traversal and 64-bit Extended Sequence Numbers (ESN), thereby addressing practical deployment limitations of prior works. It enables flexible switching between AES-P and Ascon without modifying the packet processing structure, ensuring both high throughput and low latency for real-time applications. This is the first work to systematically evaluate the feasibility and effectiveness of integrating the lightweight cipher Ascon-AEAD128 into the IPsec protocol on a hardware SoC platform. These research results have been published in work [J2].

II. Future Research Directions

- Researching and integrating side-channel attack countermeasures.
- Extending support for post-quantum cryptographic algorithms.
- Researching the development of architectures on ASIC hardware platforms and new technologies.

LIST OF PUBLICATIONS

I. Publications Related to the Dissertation

- [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. Other Publications Produced During the Course of the Dissertation

- [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)