**Bộ giao thức IPSec cho mạng đa điểm trên FPGA**

Tác giả :

Mateusz Korona1, Krzysztof Skowron1, Mateusz Trzepiński1, Mariusz Rawski1

1 Instytut Telekomunikacji, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska,

Nowowiejska 15/19, 00-665, Warszawa, Poland

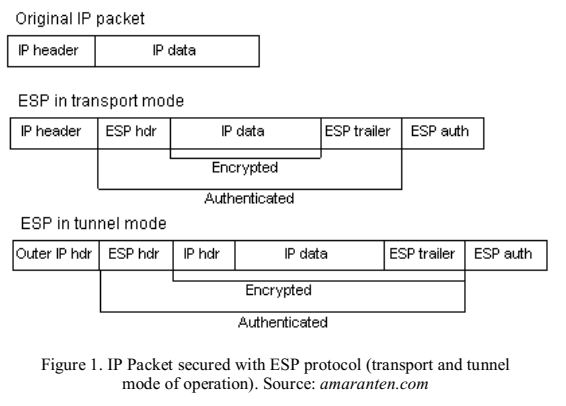
[rawski@tele.pw.edu.pl](mailto:rawski@tele.pw.edu.pl)

* Tóm tắc

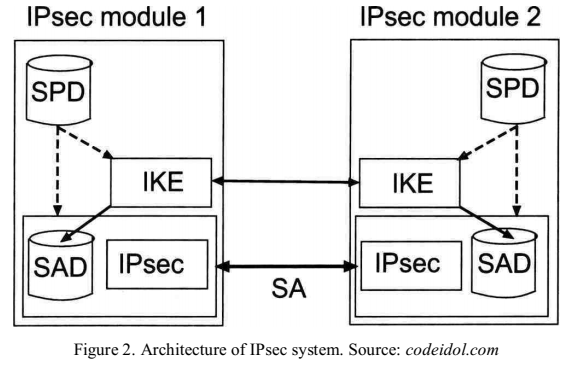
IPSec là một bộ các giao thức bổ sung tính bảo mật thông tin liên lạc ở cấp IP. Tuy nhiên ở mức tính toán lớn thuật toán Ipsec bị giới hạn hiệu năng kết nối mạng. Ở bài báo này sẽ thực hiện phần cứng IPSec gateway trên FPGA. Nó giúp giải quyết vấn đề trên và có thể sử dụng nó trọng mạng ở mức hàng Gbit/s.

* Cấu trúc IPSec

IPsec và đặc biệt là ESP subprotocol của nó (đóng gói An ninh Payload) cung cấp tính bảo mật, tính toàn vẹn và tính xác thực của dữ liệu được truyền đi. Chế độ hoạt động đường hầm cho phép để tạo mạng VPN

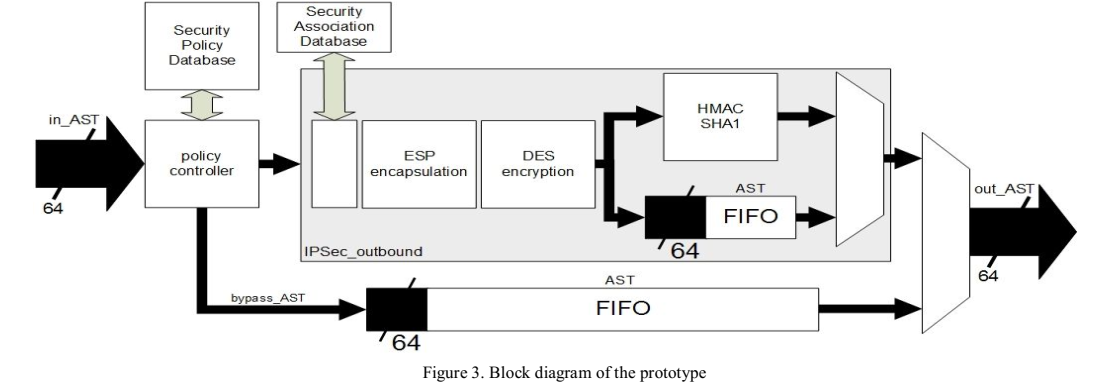


* Kiến trúc của một hệ thốn IPSec



* Thực hiện thử nghiệm mẫu

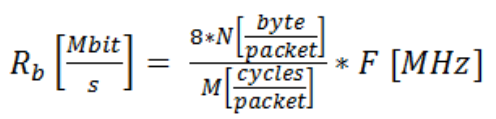
Sau khi tiếp nhận, các gói IP được chuyển sang bảo mật đơn giản bộ điều khiển chính sách. Các bản ghi phù hợp được tìm thấy trong SPD cơ sở dữ liệu, dựa trên hàm băm Pearson được tính từ tiêu đề IP bộ chọn. Mô-đun này xác định liệu dữ liệu có cần được bảo đảm hay không (đường dẫn). Quá trình bảo mật dữ liệu được thực hiện bởi mô-đun IPsec\_outbound. Tiếp theo các bước xử lý là: tra cứu cơ sở dữ liệu SAD, ESP đóng gói và mã hóa DES. Bước cuối cùng là tính toán băm HMAC-SHA1. Gói được lưu trữ trong FIFO, cho đến khi phép tính cuối cùng kết thúc.



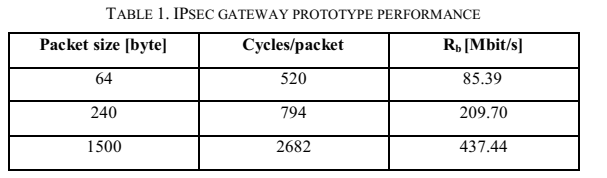
* Phân tích hiệu suất

Thử nghiệm của IPSec gateway được thực hiện trên kit DE 2-70 với Cyclone II FPGA Tần số đồng hồ tối đa của thiết kế là 86,72 MHz với sử dụng logic FPGA 20%

Dựa trên công thức

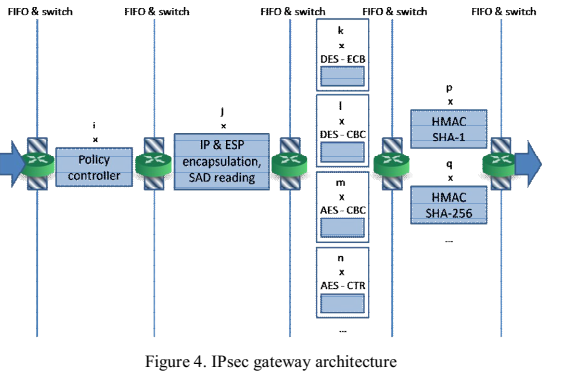


trong đó N - kích thước của gói tin, M - số chu kỳ cần thiết để xử lý gói, tần số xung nhịp tối đa của F thiết kế, thông lượng của cổng IPsec cho một số gói độ dài đã được tính toán .



* IPSEC GATEWAY

Phân tích nguyên mẫu đã trở thành cơ sở cho sự phát triển kiến trúc cổng IPsec phần cứng mới. Nâng cao phương pháp tối ưu hóa phần cứng đã được áp dụng cho thực hiện, dẫn đến tăng tốc độ xử lý và sử dụng logic tốt hơn (Hình 4).

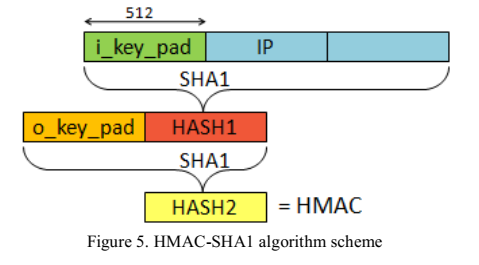


Các chức năng IPsec được chia thành nhiều phần của

thiết kế. Việc tăng số lượng mô-đun tính toán HMAC thời gian nhất dẫn đến tăng thông lượng.

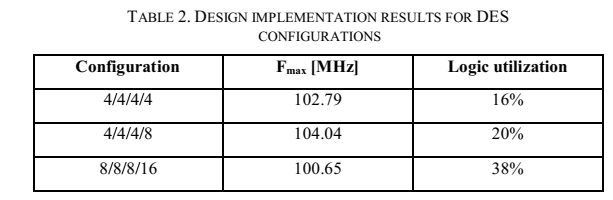
* Tối ưu hóa mô-đun HMAC-SHA1

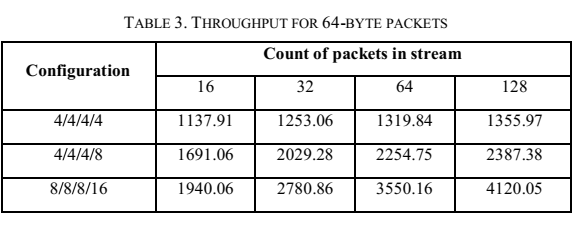
Để cải thiện hiệu suất của cổng IPsec,tối ưu hóa các mô-đun riêng lẻ cũng được thực hiện.Đặc biệt chú ý đến module HMAC-SHA1,vì hiệu quả của nó là tốc độ xử lý quan trọng curtailment trong nguyên mẫu

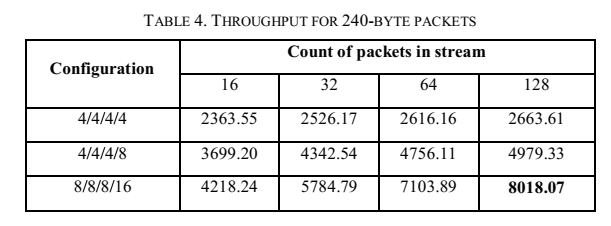


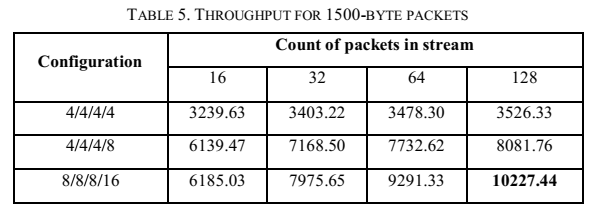
* PHÂN TÍCH HOẠT ĐỘNG

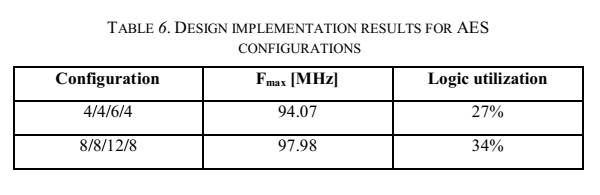
Thiết kế đã được thử nghiệm với Terasic DE5-Net mới được trang bị với Stratter V FPGA của Altera.Tổng hợp cổng IPsec trong các cấu hình khác nhau (với thay đổi số lượng mô-đun cụ thể trong phần cổng) đã được tiến hành. Chuyển hướng. 2 trình bày kết quả tổng hợp cho DES cấu hình. Trong cột Cấu hình, số bộ điều khiển chính sách bảo mật, bộ điều khiển SAD, mã hóa mô-đun và mô-đun HMAC trong mỗi phần được liệt kê tương ứng.

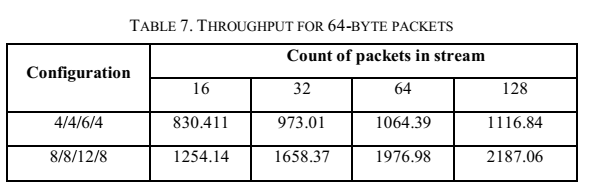


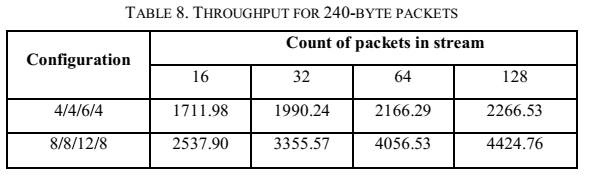


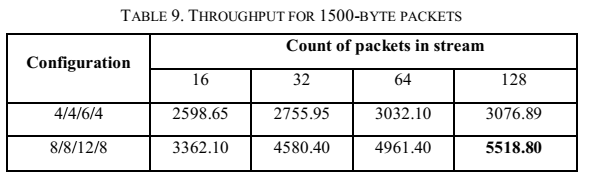












* Kết luận

Bài báo này trình bày việc triển khai phần cứng của Ipsec gateway trong FPGA. Nhờ sử dụng thiết kế tiên tiến phương pháp và tối ưu hóa điển hình cho mạch kỹ thuật số thực hiện, tốc độ xử lý cao đã đạt được. Điều này cho phép áp dụng giải pháp được đề xuất trong các mạng có dữ liệu tỷ lệ của một số Gbit / s. Kết quả trình bày chứng minh rằng đề xuất việc triển khai có thể cạnh tranh với các giải pháp thương mại, đặc biệt là những thực hiện trong FPGA [7]. Nó quan trọng nhấn mạnh, mức sử dụng logic hiện tại của Stratix V FPGA cho phép mở rộng các cấu hình cổng IPsec hiện có và cải thiện thông lượng.

c