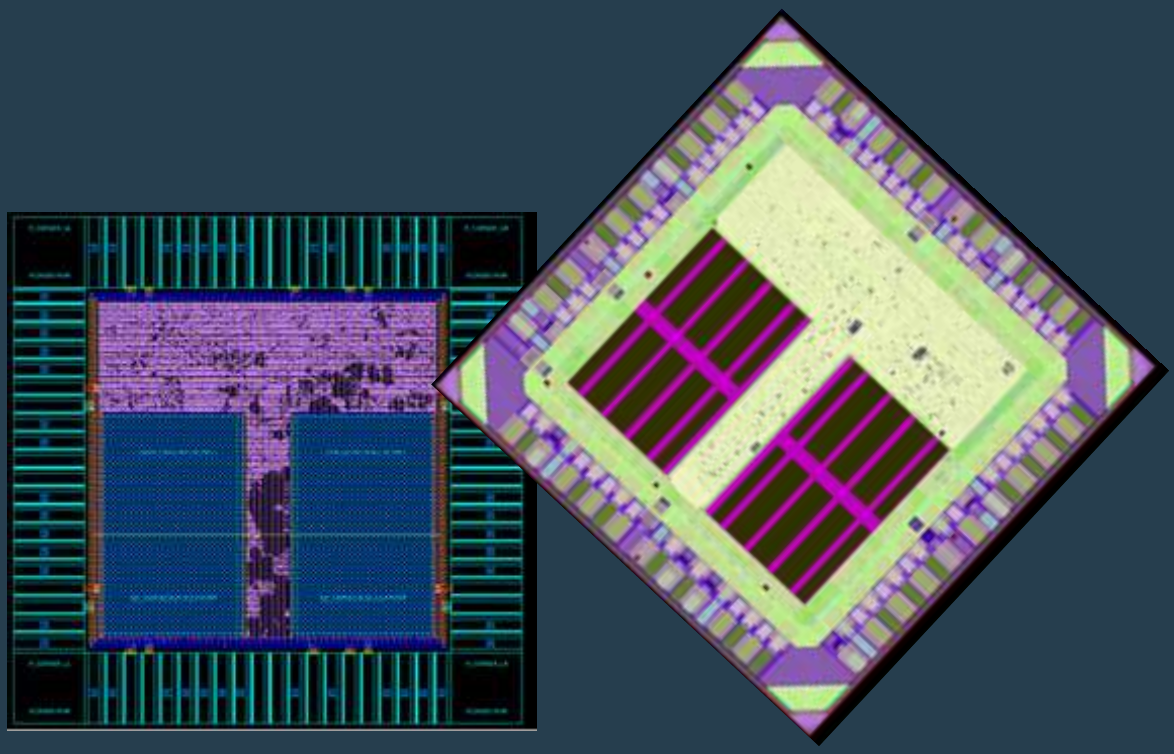
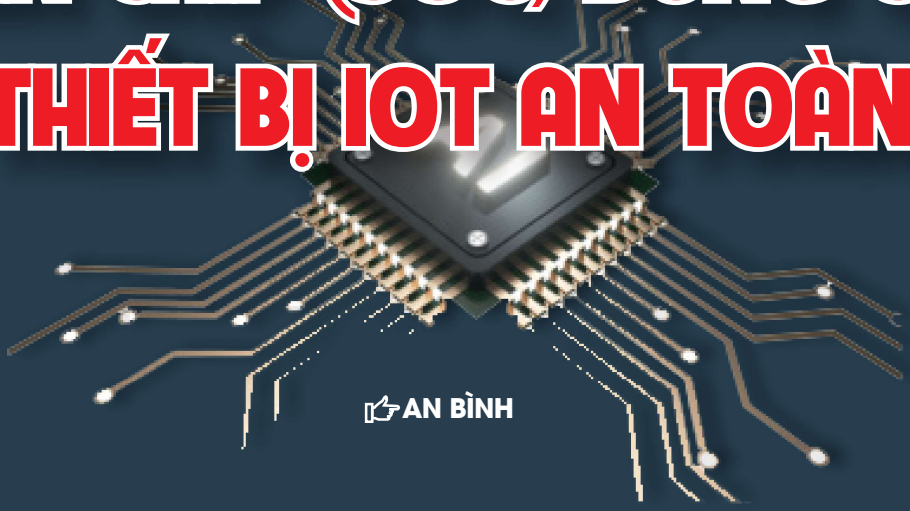


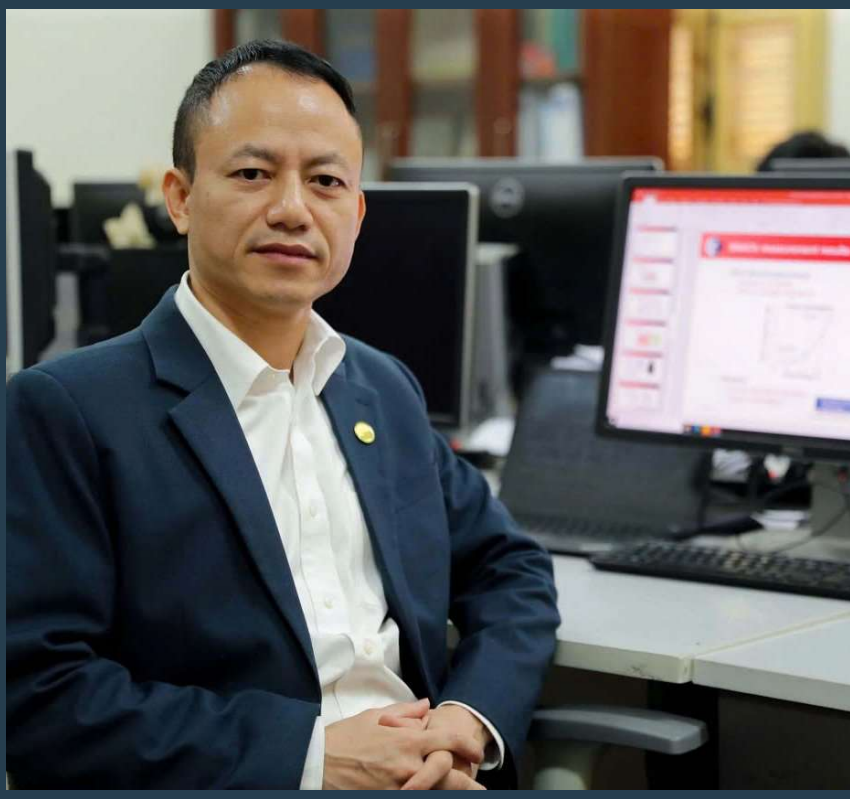
# VI MẠCH BÁN DẪN HỆ THỐNG TRÊN CHIP (SOC) DÙNG CHO THIẾT BỊ IOT AN TOÀN



AN BÌNH

MẠNG LƯỚI VẠN VẬT KẾT NỐI INTERNET (IOT) LÀ MỘT HƯỚNG NGHIÊN CỨU VÀ PHÁT TRIỂN ỨNG DỤNG TIỀM NĂNG, HỨA HẸN ĐEM LẠI HIỆU QUẢ CAO CHO NỀN KINH TẾ TRI THỨC TRONG TƯƠNG LAI GẦN. NẮM ĐƯỢC CÁC XU HƯỚNG NÀY, NHÓM NGHIÊN CỨU HỆ THỐNG TÍCH HỢP THÔNG MINH TẠI VIỆN CÔNG NGHỆ THÔNG TIN, ĐHQGHN ĐÃ ĐỀ XUẤT BỐN ĐỊNH HƯỚNG ĐỂ PHÁT TRIỂN CÁC HỆ THỐNG IOT TRONG TƯƠNG LAI, GIÚP TẠO THÀNH MỘT HỆ SINH THÁI HOÀN CHỈNH ĐỂ XÂY DỰNG CÁC THIẾT BỊ IOT ĐẢM BẢO BẢO MẬT, AN TOÀN THÔNG TIN, SỰ THÔNG MINH VÀ KHẢ NĂNG ĐÁP ỨNG CÁC TÁC VỤ PHỨC TẠP KHÁC NHAU VỚI CÔNG SUẤT VÀ NĂNG LƯỢNG TIÊU THỤ THẤP, CÓ THỂ SỬ DỤNG NGUỒN PIN HOẶC TỰ THU THẬP NĂNG LƯỢNG.

ĐỂ HIỂU RÕ HƠN VỀ NHỮNG TÍNH NĂNG ƯU VIỆT CŨNG NHƯ GIÁ TRỊ THỰC TIỄN VÀ KHẢ NĂNG THƯƠNG MẠI HÓA CỦA SẢN PHẨM, BẢN TIN ĐHQGHN ĐÃ CÓ CUỘC TRAO ĐỔI VỚI GS.TS TRẦN XUÂN TÚ - TRƯỞNG NHÓM NGHIÊN CỨU MẠNH HỆ THỐNG TÍCH HỢP THÔNG MINH (SISLAB), VIỆN TRƯỞNG VIỆN CÔNG NGHỆ THÔNG TIN, ĐHQGHN.



**Xin GS cho biết xuất phát từ đâu mà nhóm nghiên cứu lựa chọn xây dựng sản phẩm vi mạch bán dẫn hệ thống trên chip (SoC) dùng cho thiết bị IoT an toàn?**

IoT là kết quả của sự phát triển của nhiều công nghệ bao gồm công nghệ về cảm biến, công nghệ thông tin và truyền thông, công nghệ điện toán đám mây, công nghệ thiết kế vi mạch bán dẫn và nhiều công nghệ khác. IoT với khả năng thu thập, xử lý dữ liệu tại nguồn, truyền thông không dây, tương tác với các dịch vụ điện toán đám mây và phản ứng lại các thay đổi của môi trường sẽ giải quyết được nhiều vấn đề nhức nhối hiện nay. IoT có thể được áp dụng để quản lý năng lượng, theo dõi thiên tai và dịch bệnh, làm nông nghiệp thông minh, ứng dụng để xây dựng mô hình thành phố thông minh, chính phủ điện tử và thúc đẩy chuyển đổi số. Theo dự báo của McKinsey, đến năm 2030, mạng lưới vạn vật kết nối Internet sẽ đóng góp vào nền kinh tế thế giới từ 5,5 nghìn tỉ đô đến 12,6 nghìn tỉ đô. Theo dự báo của IDC, kinh phí chi tiêu cho lĩnh vực IoT tại khu vực châu Á - Thái Bình Dương là 277,5 tỉ đô năm 2023 và sẽ đạt 435 tỷ đô vào năm 2027. Đây là một hướng nghiên cứu và phát triển ứng dụng tiềm năng, có yếu tố liên ngành và hứa hẹn đem lại hiệu quả cao cho nền kinh tế tri thức trong tương lai gần.

Nắm được các xu hướng này, Nhóm nghiên cứu Hệ thống tích hợp thông minh đã đề xuất bốn định hướng để phát triển các hệ thống IoT trong tương lai bao gồm: (1) định hướng thiết kế các bộ vi xử lý, các lõi IP phần cứng giúp xử lý dữ liệu hiệu quả trong IoT; (2) hướng thiết kế tối ưu công suất và năng lượng tiêu thụ của vi mạch; (3) hướng nghiên cứu tối ưu hóa các ứng dụng AI để chạy trên các thiết bị IoT, giúp cho thiết bị IoT trở nên thông minh hơn; và (4) hướng nghiên cứu thiết kế các khối phần cứng cho bảo mật và an toàn thông tin. Bốn định hướng nghiên cứu này giúp tạo thành một hệ sinh thái hoàn chỉnh để xây dựng các thiết bị IoT đảm bảo bảo mật, an toàn thông tin, sự thông minh và khả năng đáp ứng các tác vụ phức tạp khác nhau với công suất và năng lượng tiêu thụ thấp, có thể sử dụng nguồn pin hoặc tự thu thập năng lượng.

Sự phát triển nhanh chóng của các ứng dụng chính phủ điện tử trên nền công nghệ IoT và Cách mạng Công nghiệp lần thứ tư mở ra nhiều cơ hội nhưng cũng đặt ra thách thức về bảo mật và an toàn thông tin. Các ứng dụng chính phủ điện tử có thể thu thập, truyền nhận và lưu trữ các dữ liệu bí mật của cá nhân, tổ chức và của chính phủ. Dữ liệu của cá nhân hay tổ chức đang là mục tiêu tấn công của các hacker trên thế giới và được rao bán với giá trị cao. Do vậy, đảm bảo bảo mật và an toàn thông tin là một yêu cầu bắt buộc trong các hệ thống IoT hiện nay. Đối với

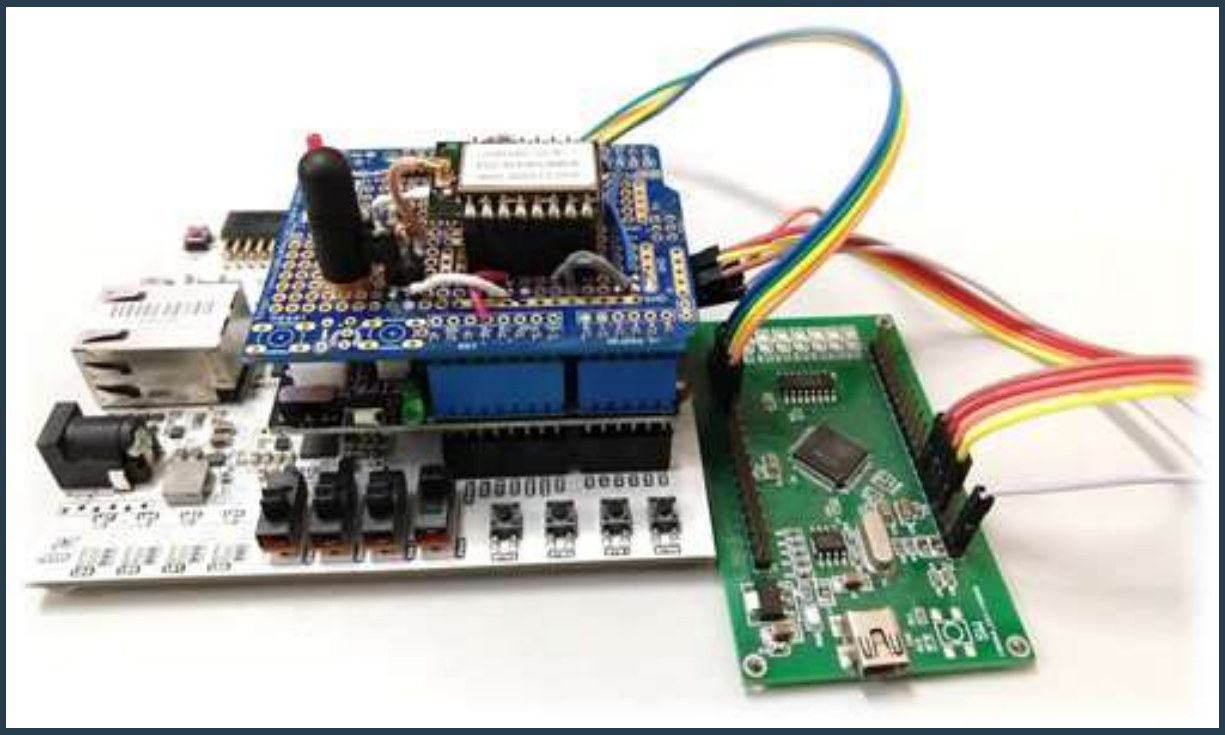
các hệ thống IoT sử dụng nguồn pin hoặc tự thu thập năng lượng, việc tích hợp các chức năng bảo mật như mã hóa dữ liệu và các giao thức bảo mật khác gây tiêu tốn điện năng và công suất tiêu thụ do các thuật toán mật mã thường là các thuật toán có độ phức tạp cao, tốn nhiều tài nguyên tính toán đặc biệt khi được thực hiện bằng phần mềm chạy trên CPU do phần mềm thực hiện các lệnh một cách tuần tự. Do vậy, nhóm nghiên cứu đã thực hiện việc tối ưu công suất tiêu thụ và thông lượng tính toán bằng cách thiết kế khối bảo mật dữ liệu bằng phần cứng và tích hợp vào một hệ thống trên chip sử dụng vi xử lý tập lệnh mở RISC-V cho các ứng dụng IoT.

**Theo GS, đâu là nền tảng công nghệ ưu việt mà nhóm nghiên cứu đã lựa chọn nhằm tăng hiệu quả của hệ thống IoT cũng như giảm thiểu công suất tiêu thụ?**

Từ các ý tưởng về hệ thống IoT với tính năng bảo mật và an toàn thông tin, nhóm nghiên cứu tìm hiểu các công trình có liên quan đến bảo mật và an toàn thông tin cho hệ thống IoT, thiết kế các mô-đun phần cứng tăng tốc mã hóa dữ liệu công suất thấp và các kỹ thuật tối ưu hóa công suất tiêu thụ. Từ các công trình đó, nhóm nghiên cứu đã rút ra các bài học kinh nghiệm và đề xuất kiến trúc của bộ tăng tốc mã hóa dữ liệu sử dụng chuẩn AES - chuẩn mã hóa dữ liệu nâng cao được đề xuất bởi Viện Khoa học và Công nghệ Hoa Kỳ (NIST) đang được sử dụng phổ biến trên mạng Internet và trên thiết bị IoT. Bên cạnh đó, nhóm nghiên cứu cũng thực hiện các nghiên cứu về các nền tảng hệ thống trên chip có thể tái sử dụng cho dự án. Nhóm đã quyết định lựa chọn nền tảng PULP và tích hợp kiến trúc của khối tăng tốc mã hóa dữ liệu do nhóm đề xuất vào nền tảng này. Việc thiết kế hệ thống dựa trên các kiến thức về kiến trúc máy tính nâng cao, các kỹ thuật truy cập bộ nhớ trực tiếp và điều khiển để tăng hiệu quả của cả hệ thống và giảm thiểu công suất tiêu thụ.

Việc kiểm tra và kiểm chứng được thực hiện trên từng mô-đun và trên cả hệ thống. Mô-đun bảo mật theo chuẩn mã hóa dữ liệu theo chuẩn AES được kiểm chứng sử dụng kịch bản kiểm tra dùng ngôn ngữ SystemVerilog; trong đó, chức năng của khối phần cứng mã hóa dữ liệu theo chuẩn AES được đảm bảo tương đồng với chức năng của mã nguồn phần mềm tham chiếu bằng cách so sánh kết quả ở lối ra của bộ mã hóa với kết quả nhận được từ phần mềm. Sau đó, các mô-đun giao tiếp thông qua bus AXI4 và truy cập bộ nhớ trực tiếp được thiết kế và kiểm tra để đảm bảo hoạt động đúng như đặc tả. Cuối cùng, mô-đun bảo mật dữ liệu theo chuẩn AES cùng các khối liên quan được tích hợp vào hệ thống và được kiểm tra để đảm bảo tương thích thông qua việc mô phỏng các hệ thống trên chip dùng các ngôn ngữ miêu tả phần cứng và lập trình phần mềm bằng công cụ mô phỏng ngôn ngữ hỗn hợp.

Để có thể thúc đẩy tốc độ triển khai dự án, hệ thống được đề xuất sau khi được mô phỏng và kiểm chứng đã được triển khai thử nghiệm trên công nghệ FPGA với bo mạch phát triển Arty A7 100T với các chức năng quan trọng nhất như mã hóa dữ liệu theo chuẩn AES, kết nối đến các bộ truyền nhận dữ liệu theo chuẩn LoRa.



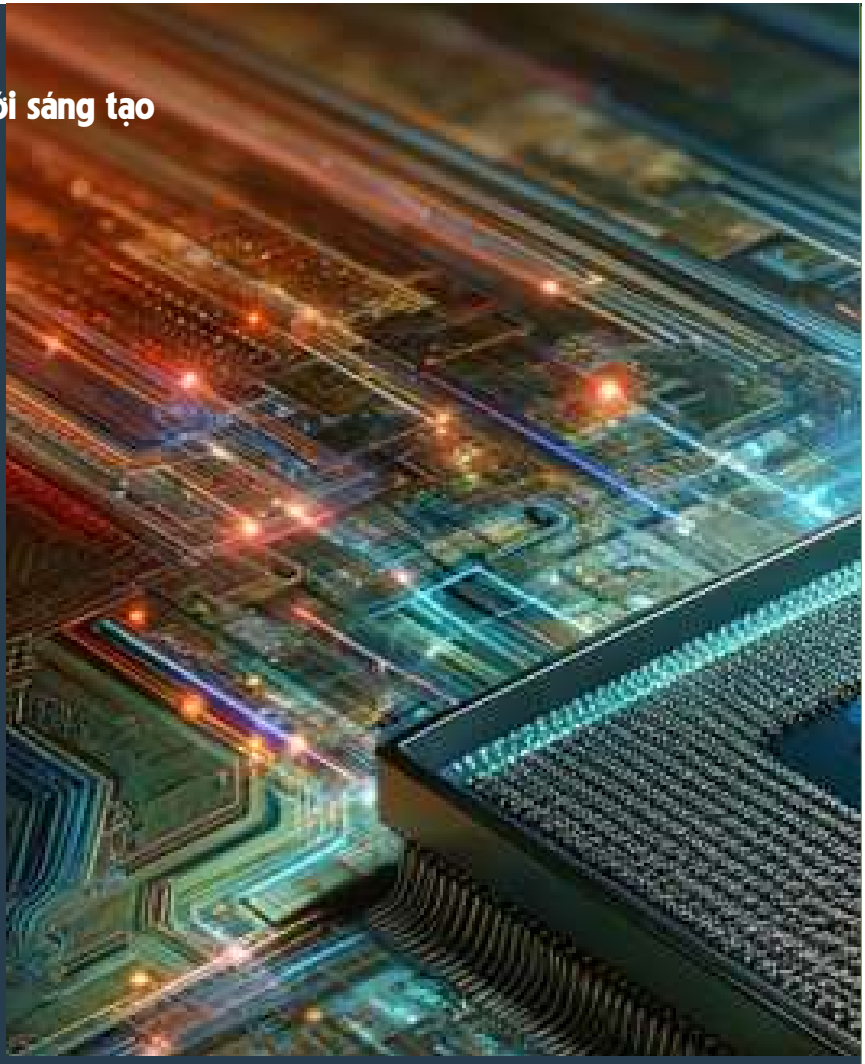
Việc này giúp đẩy nhanh tốc độ phát triển phần mềm nhúng để chạy trên vi mạch sau khi sản xuất.

Mã nguồn của hệ thống sau khi được kiểm chứng về mặt chức năng được chuyển sang công đoạn tổng hợp phần cứng và thực thi trên công nghệ CMOS 65nm của hãng TSMC. Công nghệ TSMC 65nm được lựa chọn vì đây là công nghệ tiên tiến và giá thành phải chăng. Công nghệ này có thể được dùng cho nhiều loại ứng dụng từ hiệu năng cao đến các ứng dụng công suất thấp. Sử dụng công nghệ TSMC 65nm, nhóm có thể làm quen và thực hiện các dự án phức tạp hơn trong tương lai. Để có được quyền sử dụng công nghệ CMOS 65nm của hãng TSMC, nhóm nghiên cứu đã phải liên hệ và ký hợp đồng cam kết đảm bảo bí mật công nghệ với hãng thông qua sự giới thiệu của các đối tác quốc tế.

Sau khi hệ thống được tổng hợp và thực thi phần cứng trên công nghệ CMOS 65nm, nhóm nghiên cứu đã thực hiện các bước kiểm tra cuối cùng để gửi đi sản xuất. Vi mạch đã được sản xuất tại nhà máy của hãng TSMC tại Đài Loan (Trung Quốc) trong 2,5 tháng và được gửi về Hoa Kỳ để thực hiện đóng vỏ để sẵn sàng cho việc đo kiểm và kiểm chứng mặt chức năng. Để tiến hành đo kiểm vi mạch và xây dựng ứng dụng thử nghiệm, nhóm nghiên cứu đã tự xây dựng một bo mạch kiểm tra với các thành phần giúp lập trình vi mạch sau khi chế tạo và chạy các bài kiểm tra và đo đạc thông số. Bo mạch thử nghiệm được thiết kế layout và sản xuất tại nhà máy Fab-9 tại thành phố Hồ Chí Minh. Sau đó, nhóm nghiên cứu thực hiện việc gắn các linh kiện và vi mạch lên bo mạch. Kết quả cho thấy vi mạch đã hoạt động như mong đợi và nhóm có thể tiến hành triển khai các ứng dụng thử nghiệm. Có thể nói, để ra một sản phẩm công nghệ hoàn chỉnh, nhóm nghiên cứu phải tự trang bị cho mình nhiều năng lực nghiên cứu phát triển khác nhau, không chỉ mỗi khâu thiết kế chip mà còn phải biết thiết kế bo mạch, hệ thống ứng dụng và phát triển phần mềm điều khiển.

**Trong quá trình phát triển sản phẩm, nhóm nghiên cứu gặp phải thách thức gì, thưa GS?**

Việc thiết kế vi mạch từ thiết kế, mô phỏng, kiểm chứng, thực thi và gửi đi chế tạo là một quá trình phức tạp với rất nhiều thách thức. Thách thức đầu tiên là việc tiếp cận các công nghệ chế tạo. Trước đây, Việt Nam thuộc danh sách các nước bị Mỹ cấm vận về các công nghệ lưỡng dụng (công nghệ có thể dùng cho mục đích quân sự). Do vậy, Việt Nam không thể truy cập vào các thư viện công nghệ CMOS nhỏ hơn 130nm. Tuy nhiên, nhờ có sự nỗ lực của Chính phủ cùng với mạng lưới hợp tác quốc tế, lệnh cấm vận đã được dỡ bỏ. Nhóm nghiên cứu may mắn đã ký được thỏa thuận hợp tác hỗ trợ các trường đại học với hãng TSMC thông qua một đối tác hợp tác quốc tế của nhóm. Thông qua thỏa thuận này, nhóm nghiên cứu đã có quyền truy cập vào thư viện công nghệ CMOS 65nm của hãng TSMC và bộ biên dịch bộ nhớ SRAM của ARM cho công nghệ này để sử dụng trong đề tài.



"Môi trường nghiên cứu đặc biệt quan trọng đối với nhà khoa học trong hành trình sáng tạo và truyền thụ tri thức. Người làm khoa học phải thấy thoải mái, tự do trong tranh luận và thực hành khoa học cũng như được đồng nghiệp, các nhà lãnh đạo ghi nhận những nỗ lực của họ. ĐHQGHN với bề dày truyền thống của mình đã tạo dựng được một môi trường như vậy trong vô vàn khó khăn chung của đất nước. Cơ sở vật chất, trang thiết bị nghiên cứu mặc dù chưa thực sự được đầu tư một cách đồng bộ, đủ tốt cho các hoạt động nghiên cứu đỉnh cao tuy nhiên về cơ bản cũng tốt hơn nhiều so với các đơn vị khác. Và quan trọng hơn cả, tinh thần nghiên cứu khoa học, đổi mới sáng tạo của tập thể thầy và trò luôn là nguồn cảm hứng hứa hẹn tạo nên những kỳ tích mới"

*GS.TS TRẦN XUÂN TÚ*

Việc truy cập thư viện công nghệ đã giúp nhóm nghiên cứu có thể sử dụng các công cụ thiết kế vi mạch của Synopsys như Design Compiler, IC Compiler, StarRC, Primetime, IC Validator v.v... để chuyển từ mã nguồn RTL sang danh sách cổng logic và layout, vượt qua các bài kiểm tra khắt khe của luật thiết kế để sẵn sàng gửi đi sản xuất.

Việc gửi vi mạch đi chế tạo cũng là một thách thức với các nhóm nghiên cứu trong các trường đại học. Các trường đại học khi được cấp kinh phí cũng khó có thể thực hiện việc gửi đi chế tạo trực tiếp mà phải hình thành thủ tục đấu thầu, thuê dịch vụ sản xuất và đóng gói qua một bên thứ ba. Các thủ tục này tiêu tốn nhiều thời gian và cần hiểu về Luật Đấu thầu cũng như các quy định chặt chẽ về mặt tài chính, cần sự vào cuộc của đơn vị chủ trì.

Khi vi mạch đã được chế tạo đóng vỏ, việc nhận vi mạch về Việt Nam để tiến hành kiểm tra, đo đạc và phát triển ứng dụng cũng gặp khó khăn do yêu cầu khắt khe của Tổng cục Hải quan. Đây là sản phẩm mẫu, chưa có trên thị trường; do vậy, không có căn cứ trên mạng để khai báo các tính năng của sản phẩm theo yêu cầu của Hải quan cũng như xác định giá thành sản phẩm, dẫn đến thời gian thông quan bị kéo dài, gián đoạn hoạt động nghiên cứu phát triển (phải chờ nhận được vi mạch để bắt đầu đo đạc và tiến hành thử nghiệm).

Ngoài các khó khăn trên, việc đo kiểm vi mạch bảo mật dữ liệu cũng cần có các thiết bị chuyên dụng như máy phát nguồn với độ phân giải cao, các máy đo nguồn điện, dòng điện và máy phát sóng với độ chính xác cao. Một số bài kiểm tra cần có các máy giao động ký với bộ nhớ lớn và băng thông cao. Nhóm nghiên cứu đã tận dụng và mượn các thiết bị sẵn có tại ĐHQGHN để thực hiện việc đo kiểm các thông số này của mạch.

Nhóm nghiên cứu đã phải tìm các giải pháp để vượt qua tất cả các khó khăn trên. Các thành viên trong nhóm nghiên cứu đã rất háo hức và vui mừng khi vi mạch được thông quan và lắp vào bo mạch thử nghiệm. Tuy nhiên, nhóm nghiên cứu lại gặp phải những vấn đề mới trong quá trình kiểm thử vi mạch. Một số chức năng cơ bản của vi mạch bắt đầu hoạt động, nhưng một số chức năng không hoạt động như mong muốn. Nhóm đã phải chỉnh sửa lại thiết kế của bo mạch in (PCB) dùng để đo kiểm vi mạch. Sau các nỗ lực không ngừng nghỉ của nhóm nghiên cứu, các chức năng của bo mạch kiểm thử đã được sửa lỗi và hoàn thiện để

có thể triển khai các ứng dụng thử nghiệm.

Thử nghiệm cũng là một câu chuyện khó khăn khác. Vi mạch sau khi được chế tạo được triển khai thử nghiệm tại Hòa Lạc vào mùa hè năm 2021, khi nhiệt độ ngoài trời lên đến trên 45$^{0}$C. Thiết bị hoạt động ổn định nhưng cục pin Li-ion đã bị phồng và bị hỏng. Nhóm nghiên cứu đã phải thay thế bằng cục pin chất lượng cao hơn và thực hiện chống nóng cho thiết bị. Thực hiện các dự án với triển khai thực nghiệm tại hiện trường chưa bao giờ là dễ dàng đối với bất kỳ nghiên cứu nào. Việc triển khai thử nghiệm vi mạch ADEN4IoT đã đem lại cho nhóm nghiên cứu nhiều kinh nghiệm và bài học quý giá.

**Những điểm vượt trội của sản phẩm vi mạch bán dẫn hệ thống trên chip (SoC) dùng cho thiết bị IoT an toàn và nền tảng IoT an toàn trên công nghệ FPGA/ASIC là gì, thưa GS?**

Với đề tài ADEN4IoT, chúng tôi đã nghiên cứu, thiết kế và chế tạo thử nghiệm vi mạch bảo mật dữ liệu theo chuẩn mã hóa tiên tiến AES cho các ứng dụng chính phủ điện tử dựa trên hệ thống IoT nhỏ gọn, có công suất tiêu thụ thấp trên nền tảng công nghệ CMOS 65nm của hãng TSMC, Đài Loan (Trung Quốc). Vi mạch đã được ứng dụng thử nghiệm trên các nút mạng IoT với giao thức thu phát LoRa/BLE và được thử nghiệm thành công tại Khu Công nghệ cao Hòa Lạc. Điểm nhấn đáng chú ý là kiến trúc mô-đun bảo mật dữ liệu theo chuẩn AES đề xuất ở đề tài này có đường dữ liệu 32-bit, được tối ưu về chi phí phần cứng và công suất tiêu thụ, phù hợp với các nút mạng IoT nhỏ gọn. Theo đó, lõi bảo mật dữ liệu theo chuẩn AES có diện tích phần cứng khoảng 23 kGEs, có thông lượng đạt 20 Mbps@10MHz và công suất tiêu thụ 182 uW (năng lượng tiêu thụ 8 pJ/bit), đáp ứng lưu lượng truyền thông cao như truyền hình ảnh hay video. Đề tài này cũng đề xuất một phương pháp mã hóa và giải mã nhờ xử lý đồng thời phần cứng và phần mềm cho mã hóa, giải mã hóa sử dụng thuật toán bảo mật xác thực và định danh AES-CCM nhằm giúp tối ưu hiệu năng tiêu thụ và cải thiện hiệu suất mã hóa và giải mã dữ liệu. Các đóng góp mới về mặt khoa học của đề tài được đăng tải trên ba bài báo hội nghị khoa học quốc tế thuộc hệ thống Scopus, một bài báo tạp chí quốc tế thuộc danh mục WoS và hai bằng độc quyền sáng chế đã được chấp nhận đơn hợp lệ.

**GS có thể cho biết sản phẩm có những khả năng ứng dụng thực tiễn như thế nào?**

Sản phẩm vi mạch ADEN4IoT có thể được sử dụng để bảo mật dữ liệu trong các thiết bị IoT yêu cầu công suất thấp; sử dụng trong các ứng dụng chính phủ điện tử với tính năng an toàn cao, trong lĩnh vực xe ô tô điện, trong nhà máy hay thậm chí các ứng dụng giám

sát trong thành phố thông minh. Đây cũng là một nền tảng hệ thống trên chip có thể được tùy chỉnh để thực hiện nhiều ứng dụng khác nhau ví dụ như tăng tốc tính toán AI với dữ liệu được bảo mật khi truyền qua mạng. Bên cạnh đó, vi mạch có thể được sử dụng để bảo mật các ứng dụng cần truyền thông tốc độ cao như mã hóa dữ liệu âm thanh và hình ảnh; mã hóa dữ liệu đầu cuối. Hệ thống hỗ trợ các hệ thống truyền thông tốc độ thấp và trung bình.

**Vậy đâu là điểm hạn chế ở sản phẩm mà nhóm nghiên cứu mong muốn cải thiện trong thời gian tới?**

Mặc dù được thiết kế và phát triển thành hệ thống trên chip, sản phẩm hiện tại vẫn chưa trở một hệ thống thương mại đầy đủ, các tính năng phụ trợ còn hạn chế. Trong thời gian tới, nhóm nghiên cứu sẽ phát triển thêm một số tính năng phụ trợ như phát triển thêm các mô-đun giao tiếp vào/ra tiên tiến, tích hợp bộ biến đổi tương tự - số và số - tương tự... để hình thành một hệ thống hoàn thiện hơn. Từ đó, chúng tôi có thể thực thi sản xuất các hệ thống trên chip an toàn này với tập các tính năng theo yêu cầu của ứng dụng.

**GS đánh giá như thế nào về tiềm năng phát triển của hướng nghiên cứu về vi mạch bán dẫn hệ thống trên chip (SoC) dùng cho thiết bị IoT an toàn và nền tảng IoT an toàn trên công nghệ FPGA/ASIC?**

Hiện nay, vấn đề bảo mật và an toàn thông tin ngày càng được quan tâm không chỉ đối với các cơ quan chính phủ mà cả với các ứng dụng dân dụng. Các thuật toán mật mã truyền thống tập trung vào việc bảo vệ dữ liệu với mức độ bảo mật cao. Tuy nhiên, các thuật toán này lại ít quan tâm đến các yếu tố khác như thông lượng mã hóa, công suất tiêu thụ, độ trễ mã hóa v.v... Đối với ứng dụng IoT, công suất tiêu thụ là vấn đề rất quan trọng. Nhiều nhà nghiên cứu đang thực hiện các nghiên cứu về mật mã hạng nhẹ (lightweight cryptography) để có thể thực thi các thuật toán mật mã trên phần cứng và phần mềm một cách hiệu quả. Bên cạnh đó, theo dự đoán của các nhà nghiên cứu, máy tính lượng tử với kích thước 2000 QuBit có thể được xây dựng trong 30 năm tới. Do vậy, các loại mật mã khóa công khai đang được sử dụng rộng rãi như ECC, RSA sẽ bị tấn công một cách dễ dàng nhờ sử dụng thuật toán Shor trên các máy tính lượng tử này. Do vậy, trong tương lai gần, nghiên cứu các thuật toán và cơ chế để chống lại các tấn công vào các thuật toán mật mã trong thời kỳ hậu lượng tử đang là vấn đề nhức nhối, được nhiều nhà khoa học nghiên cứu.

Các tiến bộ mới về các bộ sinh số ngẫu nhiên thực, các hàm vật lý không thể sao chép, sự tin tưởng trong phần cứng (hardware root of trust) cũng đang được các nhóm nghiên cứu lớn trên thế giới triển khai phát triển. Nhóm nghiên cứu cũng đã thực hiện một số đề tài để tích hợp các hàm vật lý không thể sao chép, xây dựng sự tin tưởng dựa trên phần cứng vào hệ thống ADEN4IoT để có thể ứng dụng bảo mật các hệ thống tự thu thập năng lượng (energy harvesting).

**Xin GS cho biết lộ trình mà nhóm nghiên cứu sẽ tiến hành trong thời gian tới để thương mại hoá sản phẩm?**

Thương mại hóa sản phẩm và tiếp cận thị trường luôn là một thách thức đối với các nhà nghiên cứu. Các nhà nghiên cứu tập trung vào việc giải quyết các bài toán nghiên cứu trong khi đó việc thương mại hóa sản phẩm và tiếp cận thị trường lại liên quan đến việc kinh doanh và bán hàng. Sự đối lập này là một thách thức và rào cản để đưa sản phẩm ra thị trường.

Nhóm nghiên cứu tiếp tục thực hiện các ứng dụng, các hệ thống thử nghiệm để giới thiệu giải pháp và tiếp cận thị trường là các công ty công nghệ muốn đưa các tính năng này vào sản phẩm của họ. Các công nghệ và kiến thức đã được áp dụng trong sản phẩm có thể được chuyển giao cho các doanh nghiệp quan tâm thông qua các sản phẩm trí tuệ như tư vấn thiết kế, chuyển giao toàn bộ hệ thống để doanh nghiệp tiếp tục phát triển.

Bên cạnh đó, nhóm nghiên cứu cũng hướng đến xây dựng một hệ sinh thái IoT với bốn định hướng đã nêu ở trên. Hệ sinh thái này cho phép cung cấp các giải pháp toàn diện từ tối ưu tính toán, bảo mật và an toàn thông tin, tính thông minh và sử dụng công nghệ thu thập năng lượng để giảm chi phí bảo trì và thay pin.

**Xin cảm ơn GS!**