Mẫu 1
11/2014/TT-BKHCN

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Hà Nội, ngày 16 tháng 8 năm 2021

BÁO CÁO KẾT QUẢ TỰ ĐÁNH GIÁ NHIỆM VỤ KHOA HỌC VÀ CÔNG NGHỆ CẤP QUỐC GIA

I. Thông tin chung về nhiệm vụ:

1. Tên nhiệm vụ, mã số: Nghiên cứu, thiết kế và chế tạo vi mạch bảo mật dữ liệu ứng dụng trong IoT và phát triển thiết bị ứng dụng. Mã số: KC.01.21/16-20

Thuộc:

- Chương trình: "Nghiên cứu công nghệ và phát triển sản phẩm công nghệ thông tin phục vụ Chính phủ điện tử"; mã số KC.01/16-20.

- Khác *(ghi cụ thể)*:

2. Mục tiêu nhiệm vụ:

- Làm chủ công nghệ thiết kế, chế tạo vi mạch bảo mật dữ liệu ứng dụng trong hệ thống IoT.
- Chế tạo, triển khai thử nghiệm thiết bị bảo mật dữ liệu dùng trong thiết bị thu, phát và lưu trữ dữ liệu IoT trên có sử dụng vi mạch chế tạo được.

3. Chủ nhiệm nhiệm vụ: Trần Xuân Tú

4. Tổ chức chủ trì nhiệm vụ: Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội

5. Tổng kinh phí thực hiện: 6.930 triệu đồng.

Trong đó, kinh phí từ ngân sách SNKH: 6.930 triệu đồng.

Kinh phí từ nguồn khác: triệu đồng.

6. Thời gian thực hiện theo Hợp đồng:

Bắt đầu: 1/7/2019

Kết thúc: 31/12/2020

Thời gian thực hiện theo văn bản điều chỉnh của cơ quan có thẩm quyền: 30/8/2021

7. Danh sách thành viên chính thực hiện nhiệm vụ nêu trên gồm:

Số TT	Họ và tên	Chức danh khoa học, học vị	Cơ quan công tác
1	Trần Xuân Tú	PGS.TS.	Viện Công nghệ Thông tin, Đại học Quốc gia Hà Nội
2	Bùi Duy Hiếu	TS.	Viện Công nghệ Thông tin, Đại học Quốc gia Hà Nội
3	Đặng Nam Khánh	TS.	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
4	Mai Đức Thọ	ThS.NCS	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
5	Đinh Văn Nam	ThS.NCS	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
6	Nguyễn Duy Anh	ThS.NCS	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
7	Trần Huy Toàn	ThS.NCS	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
8	Đồng Phạm Khôi	ThS.NCS	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
9	Trần Đình Lâm	TS.	Viện Khoa học và Công nghệ Quân sự
10	Nguyễn Khâm Hồng Quang	ThS.	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
11	Trần Đức Mạnh	KS.	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
12	Phan Hải Phong	TS.	Trường Đại học Khoa học Huế
13	Lê Văn Thanh Vũ	TS.	Trường Đại học Khoa học Huế
14	Nguyễn Ngô Doanh	KS.	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội
15	Đặng Hải Ninh	KS.	Trường Đại học Công nghệ, Đại học Quốc gia Hà Nội

II. Nội dung tự đánh giá về kết quả thực hiện nhiệm vụ:

1. Về sản phẩm khoa học:

1.1. Danh mục sản phẩm đã hoàn thành:

Số TT	Tên sản phẩm	Số lượng			Khối lượng			Chất lượng		
		Xuất sắc	Đạt	Không đạt	Xuất sắc	Đạt	Không đạt	Xuất sắc	Đạt	Không đạt
I	**Sản phẩm Dạng I**									
1	Vi mạch bảo mật dữ liệu ứng dụng trong IoT có các tính năng, thông số kỹ thuật chính sau: - Đáp ứng các yêu cầu bảo mật cơ bản của chuẩn AES; - Dữ liệu vào, ra: 128 bits/khối dữ liệu (luồng dữ liệu 32 bits); - Chiều dài khóa (key size): 128, 192, và 256 bits; - Thông lượng mã hóa tối thiểu: 10Mbps (ở tần số 10MHz); ***thực tế: 20Mps @10MHz*** - Năng lượng tiêu thụ: tối đa khoảng 10pJ/bit/encryption (ở tần số 10MHz); ***thực tế: 6,17 ÷ 8,33pJ/bit/encryption*** - Hỗ trợ các chế độ hoạt động: AES-CCM, AES-GCM, AES-OFB. AES-CBC. - Sinh khóa ngẫu nhiêu tuân theo tiêu chuẩn FIPS. - Giao diện cấu hình SPI; - Bộ nhớ lưu trữ: SRAM, ROM;		**X** *25 mẫu*			**X**			**X**	

	- Công nghệ: CMOS 65nm hoặc mới hơn; ***thực tế: công nghệ CMOS 65nm của TSMC.*** - Điện áp nguồn: nhỏ hơn 1,2 vôn; ***thực tế: 0,7 ÷ 1,2 vôn***									
2	Thiết bị bảo mật dữ liệu IoT công suất thấp có các tính năng, thông số kỹ thuật chính như sau: - Đáp ứng các yêu cầu cơ bản của chuẩn AES; - Chiều dài khóa có thể cấu hình: 128, 192, 256 bits; - Thông lượng truyền thông tối thiểu: 10 Mbps; ***thực tế: 20Mps @ 10MHz*** - Các chuẩn giao tiếp hỗ trợ: USB 2.0, SPI, GPIO, UART, SD Card; - Điện áp nguồn nuôi: 1,2 ÷ 5 Vôn; ***thực tế: 3,3 ÷ 5 vôn***	**X** *04 thiết bị (vượt 1 thiết bị)*				**X**			**X**	
II	**Sản phẩm Dạng II**									
1	Lõi mã hóa dữ liệu AES dưới dạng IP. - Đáp ứng các yêu cầu bảo mật cơ bản của chuẩn AES; - Dữ liệu vào, ra: 128 bits/khối dữ liệu (luồng dữ liệu 32 bits); - Chiều dài khóa (key size): 128, 192, và 256 bits; - Thông lượng mã hóa tối thiểu: 10Mbps (ở tần số 10MHz); ***thực tế: 20Mps @10MHz*** - Năng lượng tiêu thụ: tối đa khoảng 10pJ/bit/encryption (ở tần số 10MHz); ***thực tế: 6,17 ÷ 8,33pJ/bit/encryption***		**X**			**X**			**X**	

	- Độc lập về mặt công nghệ; ***thực tế: thử nghiệm thành công trên cả FPGA và CMOS 65nm của TSMC*** - Mô hình hóa ở mức RTL; - Cung cấp kèm kịch bản kiểm chứng.									
2	Lõi thực hiện các chế độ hoạt động của vi mạch bảo mật dữ liệu AES dưới dạng IP. - Hỗ trợ các chế độ hoạt động: AES-CCM, AES-GCM, AES-OFB. - Sinh khóa ngẫu nhiêu tuân theo tiêu chuẩn FIPS-140-2 được miêu tả chi tiết trong tài liệu NIST SP-800-90A, mục 10.2 bộ tạo số ngẫu nhiên dùng mã khối AES. - Giao diện cấu hình SPI; - Bộ nhớ lưu trữ: SRAM, ROM; - Điện áp nguồn: nhỏ hơn 1,2 vôn; ***thực tế: 0,7 ÷ 1,2 vôn*** - Dữ liệu vào, ra: 32 bits.		**X**			**X**			**X**	
3	Bộ tài liệu kỹ thuật bao gồm: - Tài liệu thiết kế, quy trình công nghệ chế tạo vi mạch và thiết bị bảo mật dữ liệu IoT; - Tài liệu hướng dẫn sử dụng thiết bị bảo mật dữ liệu IoT; - Báo cáo triển khai thử nghiệm hệ thống trong việc giám sát môi trường (nước thải, không khí) tại Khu Công nghệ cao Hòa Lạc.		**X**			**X**			**X**	

III	**Sản phẩm Dạng III**									
1	01 bài báo khoa học đăng tạp chí		**X**			**X**			**X**	
2	01 bài báo đăng kỷ yếu hội nghị khoa học quốc tế; ***thực tế: 3 bài báo đăng kỷ yếu hội nghị khoa học quốc tế)***	**X**				**X**			**X**	
3	Sở hữu trí tuệ: 01 đơn chấp nhận hợp lệ; ***thực tế: 01 đơn chấp nhận hợp lệ (đăng ký sáng chế)***		**X**			**X**			**X**	
IV	**Sản phẩm đào tạo**									
1	01 thạc sỹ (đăng ký 02 thạc sỹ)			**X**		**X**			**X**	
2	01 nghiên cứu sinh; ***thực tế: tham gia đào tạo 03 nghiên cứu sinh***	**X**				**X**			**X**	

1.2. Danh mục sản phẩm khoa học dự kiến ứng dụng, chuyển giao (nếu có):

Số TT	Tên sản phẩm	Thời gian dự kiến ứng dụng	Cơ quan dự kiến ứng dụng	Ghi chú
1	Thiết bị bảo mật dữ liệu IoT công suất thấp	2022	Sunshine Technology; VNPT Technology	*Đang xúc tiến*

1.3.Danh mục sản phẩm khoa học đã được ứng dụng *(nếu có)*:

Số TT	Tên sản phẩm	Thời gian ứng dụng	Tên cơ quan ứng dụng	Ghi chú
1				

2. Về những đóng góp mới của nhiệm vụ:

So với các sản phẩm của nước ngoài, sản phẩm của đề tài này có tính năng và công dụng tương đương bao gồm:

- Chiều dài khóa: 128 bit (hỗ trợ đến chiều dài khóa 256 bit)
- Hỗ trợ các chế độ hoạt động: AES-CCM và AES-CBC
- Hỗ trợ sinh khóa ngẫu nhiên theo chuẩn FIPS-140-2 phụ lục C (được miêu tả chi tiết ở tài liệu NIST SP-800-90A cho các bộ tạo số ngẫu nhiên dùng mã khối AES)
- Có các bộ nhớ SRAM, ROM
- Hỗ trợ chuẩn giao tiếp SPI.

Điểm khác biệt của sản phẩm đề tài này với các sản phẩm của nước ngoài:

- Hỗ trợ chiều dài khóa từ 128 bit đến 256 bit cấu hình có thể thay đổi được.
- Kiến trúc 32-bit datapath, phù hợp với hầu hết các hệ vi xử lý nhúng.
- Hỗ trợ thêm các chế độ hoạt động như: AES-GCM, AES-OFB
- Công suất tiêu thụ thấp.

Ngoài ra, nhóm nghiên cứu đã đề xuất phương pháp mới "Phương pháp mã hóa và giải mã nhờ xử lý đồng thời phần cứng và phần mềm sử dụng thuật toán xác thực và định danh AES-CCM", được đăng ký bằng sáng chế. Hồ sơ đăng ký đã được chấp nhận hợp lệ theo Quyết định số 4149w/QĐ-SHTT.

3. Về hiệu quả của nhiệm vụ:

3.1. Hiệu quả kinh tế

Các kỹ thuật bảo mật là một phần không thể thiếu cho các hệ thống thông tin, truyền thông và thu thập dữ liệu, đặc biệt trong bối cảnh ứng dụng các thiết bị IoT đang trở nên ngày càng phổ biến như hiện nay. Thiết bị này có thể được sử dụng để làm tăng mức độ an toàn thông tin của hệ thống. Đặc biệt là các hệ thống liên quan đến an ninh và quốc phòng của quốc gia. Việc làm chủ công nghệ cho phép chúng ta không chỉ giảm chi phí mua sắm trang thiết bị trong thời gian tới mà còn giúp chúng ta tránh được các rủi ro trong bảo mật thông tin.

Thiết bị bảo mật dữ liệu có thể được sử dụng như một mô-đun cộng thêm vào các ứng dụng IoT đã triển khai để tăng tính bảo mật của hệ thống. Mô-đun bảo mật dữ liệu theo chuẩn AES có thể được sử dụng cho các dự án sản xuất vi mạch khác.

3.2. Hiệu quả xã hội

Việc làm chủ công nghệ bảo mật từ thiết kế phần cứng đến ứng dụng là hết sức quan trọng để làm chủ xu thế IoT và cách mạng công nghiệp 4.0. Đề tài nghiên cứu sẽ đưa ra thiết kế bảo mật công suất thấp, phù hợp cho các ứng dụng IoT, tạo nên sự tin tưởng đối với người sử dụng, từ đó thúc đẩy sự phát triển của các ứng dụng IoT trong nước. Việc làm chủ công nghệ cũng có vai trò quan trọng đối với nền KHCN Việt Nam.

Với tổ chức chủ trì, việc thực hiện đề tài từ nghiên cứu công nghệ lõi đến triển khai ứng dụng sẽ tăng cường năng lực nghiên cứu và triển khai của đơn vị, gia tăng kinh nghiệm của các thành viên tham gia đề tài và khẳng định vị thế của đơn vị trong giới khoa học và công nghệ.

Với đơn vị ứng dụng kết quả nghiên cứu: đảm bảo tính bảo mật cao nhất và có thể làm chủ hoàn toàn công nghệ (thông qua chuyển giao). Đây cũng là chìa khoá quyết định sự thành công và tính bền vững trong sản xuất và kinh doanh các thiết bị công nghệ cao. Ngoài ra, về lâu dài thì với việc làm chủ công nghệ sẽ cho phép doanh nghiệp giảm chi phí sản xuất để gia tăng lợi nhuận.

Việc thực hiện đề tài sẽ hỗ trợ đào tạo đội ngũ, từng bước khẳng định khả năng tiếp cận và làm chủ công nghệ thiết kế vi mạch – là một công nghệ cao đòi hỏi sự kết hợp kiến thức liên ngành. Điều này sẽ có tác động to lớn đến việc thu hút các nguồn đầu tư nước ngoài vào Việt Nam trong các lĩnh vực công nghệ cao và từng bước phát triển ngành công nghiệp điện tử của Việt Nam cũng như các ngành công nghiệp liên quan (công nghiệp ô tô, CNTT…). Thực tiễn cho thấy, với gần 3000 kỹ sư tham gia thiết kế vi mạch đã thu hút nhiều đầu tư của các tập đoàn công nghệ lớn trên thế giới như Renesas (khu Chế xuất Tân Thuận), AMCC (Tp. HCM), Toshiba (Hà Nội), e-Silicon, Active Semi, Dolphin-IC Vietnam… gần đây xuất hiện các doanh nghiệp công nghệ thuần Việt như Trung tâm Thiết kế vi mạch của Tập đoàn Viễn thông Quân đội Viettel (VIC).

III. Tự đánh giá, xếp loại kết quả thực hiện nhiệm vụ

1. Về tiến độ thực hiện: *(đánh dấu √ vào ô tương ứng)*:

- *Nộp hồ sơ đúng hạn* ☒
- *Nộp chậm từ trên 30 ngày đến 06 tháng* ☐
- *Nộp hồ sơ chậm trên 06 tháng* ☐

2. Về kết quả thực hiện nhiệm vụ:

- *Xuất sắc* ☐
- *Đạt* ☒
- *Không đạt* ☐

Giải thích lý do: hoàn thành tất cả các nội dung nghiên cứu, sản phẩm đăng ký, đáp ứng các yêu cầu về chủng loại, số lượng và chất lượng đăng ký trong thuyết minh; một số nội dung có số lượng và chất lượng vượt yêu cầu.

Cam đoan nội dung của Báo cáo là trung thực; Chủ nhiệm và các thành viên tham gia thực hiện nhiệm vụ không sử dụng kết quả nghiên cứu của người khác trái với quy định của pháp luật.

CHỦ NHIỆM NHIỆM VỤ	**THỦ TRƯỞNG**
(Học hàm, học vị, Họ, tên và chữ ký)	**TỔ CHỨC CHỦ TRÌ NHIỆM VỤ**
	(Họ, tên, chữ ký và đóng dấu)
	KT. HIỆU TRƯỞNG
	PHÓ HIỆU TRƯỞNG
Trần Xuân Tú	Chử Đức Trình