ĐỀ XUẤT KIẾN TRÚC VÀ ĐÁNH GIÁ THỬ NGHIỆM KHỐI MÃ HÓA KHÔNG DÙNG SBOX CHO HOẠT ĐỘNG TRUYỀN THÔNG CỦA CÁC HỆ THỐNG IOT

Lê Văn Thanh Vũ[1*], Trần Hữu Tuấn[2]

[1] Khoa Điện-Điện tử & CNVL, Trường Đại học Khoa học, Đại học Huế

[2] Khoa Điện – Điện tử, Trường CĐ Công nghiệp Huế

*Email: vulvt@hueuni.edu.vn

Ngày nhận bài: 02/7/2021; ngày hoàn thành phản biện: 5/7/2021; ngày duyệt đăng: 4/4/2022

TÓM TẮT

Hoạt động truyền thông luôn là thách thức chính của các thiết kế IoT hiện đại, giải quyết bài toán truyền thông hiệu quả cân bằng giữa chi phí (năng lượng, năng lực xử lý) và hiệu quả góp phần chính vào thành công chung. Vấn đề bảo mật IoT tuy không mới nhưng vẫn luôn là một thách thức lớn, nhất là với các hệ thống IoT trong không gian rộng khả năng bao quát của người dùng hạn chế. Bài báo này được phát triển theo xu thế tích hợp chức năng bảo mật vào bên trong các hệ thống IoT với ưu điểm tiêu thụ năng lượng thấp, không yêu cầu năng lực xử lý và hiệu quả truyền thông cao. Thuật toán bảo mật không sử dụng sbox cho phép người thiết kế tối ưu chi phí thiết kế thực thi để từ đó tối đa hóa hiệu quả chung của toàn hệ thống IoT.

Từ khóa: Bảo mật, truyền thông IoT, COMET, blockcipher.

PROPOSE ARCHITECTURE AND TESTBENCH A BLOCKCIPHER WITHOUT SBOX USING FOR COMMUNICATION IN IOT SYSTEMS

Le Van Thanh Vu[1*], Tran Huu Tuan[2]

[1]Faculty of Electrics, Electronics Engineering and Material Technology, University of Sciences, Hue University

Facultty of Eclectricity, Hue Industial College

*Email: vulvt@hueuni.edu.vn

ABSTRACT

Communication activities are the main issue when designing advantage IoT systems; solving the communication effective with trade-off design costs (energy, processing cost) with performance is always a key issue. Although IoT cryptography is not new, but it is always a big challenge; especially for IoT systems used in large space with limited user coverage. The article is developed according to the trend of integrated cryptography function into IoT systems with the advantage of low power consumption, without processing capacity and high communication efficiency. The cryptography algorithm without-sbox allows designers to optimize implementing cost to maximize the efficiency of IoT systems.

Keywords: COMET, cryptography, blockcipher, IoT

Lê Văn Thanh Vũ sinh ngày 20/05/1977 tại TP Huế. Ông nhận bằng cử nhân đại học ngành Vật lý tại Trường Đại học Khoa học, Đại học Huế. Năm 2004, ông nhận bằng thạc sỹ ngành Điện tử - Viễn thông tại Khoa Công nghệ thuộc Đại học Quốc gia Hà Nội. Năm 2017, ông nhận bằng tiến sĩ tại Trường ĐH Công nghệ - ĐHQG Hà Nội. Hiện đang là giảng viên tại Khoa Điện tử - Viễn thông, Trường Đại học Khoa học – Đại học Huế và tham gia nghiên cứu tại Phòng thí nghiệm trọng điểm Hệ thống tích hợp thông minh (SISLAB) tại Trường Đại học Công nghệ - Đại học Quốc gia Hà Nội từ năm 2010.

Lĩnh vực nghiên cứu: Thiết kế vi mạch, hệ thống nhúng – IoT.

Trần Hữu Tuấn sinh ngày 10/11/1976 tại TT. Huế. Ông nhận bằng kỹ sư đại học ngành Kỹ Thuật Điện tại trường Đại học Bách Khoa, Đại học Đà nẵng. Năm 2009, ông nhận bằng thạc sỹ ngành Mạng và Hệ thống điện tại trường Đại học Bách Khoa, Đại học Đà nẵng. Hiện ông đang là giảng viên tại Khoa Điện, Điện tử trường Cao đẳng Công nghiệp Huế.

Lĩnh vực nghiên cứu: Tiết kiệm năng lượng và lưới điện thông minh trên các nền tảng số.