THỰC HIỆN VÀ ĐÁNH GIÁ THUẬT TOÁN HÀM BĂM SHA-3 TRÊN CÁC NỀN TẢNG VI XỬ LÝ

Hứa Nguyên Khang, Thái Hồng Hải, Mã Khải Minh, Lê Thành Nghị, Nguyễn Thanh Lộc, Lê Đức Hùng
Khoa Điện tử - Viễn thông,
Trường Đại học Khoa học Tự Nhiên, ĐHQG-HCM
ldhung@hcmus.edu.vn

Tóm tắt

Trong nghiên cứu này, nhóm tác giả trình bày kết quả tìm hiểu và thực hiện thuật toán hàm băm SHA-3. Thuật toán SHA-3 được ứng dụng trong mật mã hóa dữ liệu. Thuật toán SHA-3 được viết bằng ngôn ngữ lập trình C và được thực hiện trên bo mạch vi điều khiển STM32F103, bo mạch Raspberry Pi 3, và CPU Core i5-2450M để đánh giá thời gian xử lý của hệ thống ứng với các thông tin có độ dài ký tự khác nhau. Các mã hash đã được kiểm tra đúng tính chất của hàm băm, độ dài mã hash đều là 128 ký tự mỗi mã. Nội dung mỗi mã hash sau khi thực hiện là khác nhau, sự chuyển đổi đều thỏa mãn tính một chiều. Kết quả này quan trọng để đánh giá việc triển khai hệ thống trên nền tảng phần cứng có giá thành phù hợp, kiến trúc hợp lý trong các ứng dụng Internet of Things để đảm bảo hệ thống bảo mật đạt hiệu năng và chi phí tốt nhất.

Từ khóa: SHA-3, Internet of Things, mật mã hóa.

IMPLEMENTATION AND EVALUATION OF SHA-3 ALGORITHM ON MICROPROCESSOR PLATFORMS

Hua Nguyen Khang, Thai Hong Hai, Ma Khai Minh, Le Thanh Nghi, Nguyen Thanh Loc, Le Duc Hung
Faculty of Electronics and Telecommunications,
University of Science, VNU-HCM
ldhung@hcmus.edu.vn

Abstract

In this research, the authors present the SHA-3 hash algorithm. The SHA-3 algorithm is applied in data cryptography. This algorithm is written in C programming language and then is implemented on the STM32F103 microcontroller board, Raspberry Pi 3 board, and Core i5-2450M CPU to evaluate its processing time corresponding to the information messages which have different character lengths. The hash codes have been properly checked for hash functions, the length of the hash code is 128 characters per on. The content of each hash code is different, the conversion is one-dimensional. This result is important to

evaluate the cost-effective, affordable hardware-based architecture of a security system in Internet of Things applications.

Keyword: SHA-3, Internet of Things, cryptography.