TĂNG CƯỜNG TÍNH BẢO MẬT TRONG HỆ THỐNG IoT TRÊN NỀN TẢNG SoC FPGA

Trần Tuấn Kiệt, Đặng Tấn Phát, Cao Trần Bảo Thương,

Bùi Trọng Tú và Huỳnh Hữu Thuận

Khoa Điện tử - Viễn Thông
Trường Đại học Khoa học tự nhiên, ĐHQG-HCM

ttkiet@fetel.hcmus.edu.vn, dtphat@fetel.hcmus.edu.vn, ctbthuong@fetel.hcmus.edu.vn,

bttu@fetel.hcmus.edu.vn, hhthuan@hcmus.edu.vn

Tóm tắt

Ngày nay, IoT đang là một trong những lĩnh vực phát triển mạnh mẽ của cuộc cách mạng công nghiệp 4.0, do đó nó dẫn đến việc sinh ra một số lượng các thiết bị kết nối với nhau. Vì vậy, bảo mật là vấn đề quan trong trong việc phát triển các thiết IoT. Trong bài báo này, chúng tôi đề xuất một thiết kế để tăng cường tính bảo mật của các thiết bị IoT và các kết nối của nó trên nền tảng SoC FPGA. Trong đó, chúng tôi kết hợp bộ xử lý mạnh mẽ ARM cùng với các IP core có khả năng tùy biến linh hoạt và tốc độ xử lý mạnh mẽ trên FPGA. Cụ thể, chúng tôi đã phát triển Hệ thống chữ ký kỹ thuật số trên bo mạch SoC FPGA DE10-Nano sử dụng lõi bộ xử lý ARM tích hợp và hai lõi IP tự phát triển hoạt động như bộ đồng xử lý 1024 bit RSA và 256 bit SHA. Về kết quả đạt được, hệ thống mật mã được đề xuất nhỏ gọn nhưng đạt được hiệu suất cao ngay cả với tần số thấp. Cụ thể, các Core có DMA hoạt động ở tần số 150 MHz có thể đạt tốc độ 1200 Mbps. Ngoài ra, lõi RSA 1024-bit và SHA 256-bit hoạt động ở tần số 50 MHz và 100 MHz có thông lượng tương ứng là 25 Kbps và trên 700 Mbps.

ENHANCING SECURITY IN IoT SYSTEMS BASED ON SoC FPGA PLATFORMS

Tuan-Kiet Tran, Tan-Phat Dang, Bao-Thuong Cao Tran,

Trong-Tu Bui and Huu-Thuan Huynh

Faculty of Electronics and Telecommunications
University of Science, VNU-HCM

ttkiet@fetel.hcmus.edu.vn, dtphat@fetel.hcmus.edu.vn, ctbthuong@fetel.hcmus.edu.vn,

bttu@fetel.hcmus.edu.vn, hhthuan@hcmus.edu.vn

Abstract

Today, the IoT is one of the strongly growing fields of Industrial Revolution 4.0, thus leading to the birth of a number of interconnected devices. Therefore, security is of utmost importance in the development of IoT devices. In this article, we propose a design to enhance the security of IoT devices and their connections on the SoC FPGA platforms. In it, we combine powerful ARM processors with IP cores with flexible customization and powerful processing speed on FPGAs. Specifically, we developed the FPGA DE10-Nano SoC Onboard Digital Signature System that uses integrated ARM processor cores and two self-developed IP cores that act as co-processors are 1024 bit RSA and 256-bit SHA. As for the results, the proposed cryptosystem is compact but achieves high performance even at low frequencies. Specifically, Core with DMA operating at 150 MHz can reach speeds of 1200 Mbps. In addition, the 1024-bit RSA and 256-bit SHA cores operate at the frequencies of 50 MHz and 100 MHz with throughputs of 25 Kbps and above 700 Mbps, respectively.