A22-204

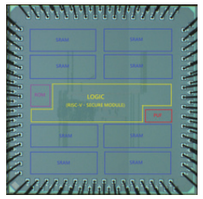
具低功耗機制及多層式硬體安全性之物聯網微處理器系統

An Integrated IoT Microprocessor System with Ultra Low Power Wake-Up Mechanism and Multi-Layer Hardware Security

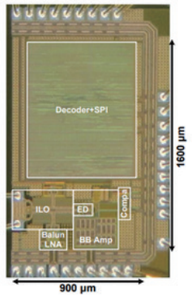
隊伍名稱　具低功耗及多層式硬體安全性之物聯網微處理器系統
An Integrated IoT Microprocessor System with Hardware-Secure and Ultra Low Power Wake-up Receiver
隊　　長　鄧士瑩 / 成功大學電機工程研究所
隊　　員　林晨哲 / 成功大學電機工程研究所
林宜駿 / 成功大學電腦與通信工程研究所
葉品蓁 / 成功大學電腦與通信工程研究所

作品摘要

隨著物聯網中智慧醫療時代滲透於人們的生活，醫療裝置的安全性是軟硬體及系統設計者需要面對的挑戰。若裝置所儲存之病人資訊或是病狀特徵遭受有心人士惡意竊取，甚至裝置設計被惡意竄改造成偵測裝置停擺，都會造成名譽、金錢甚至人命之損失。另一方面，智慧居家照護監測系統需要長期保持開機狀態，若是為可攜式或穿戴型醫療裝置，將傾向於小型化及低功耗喚醒機制著重設計。因此本團隊所研發出的硬體安全處理器晶片配合低功耗喚醒接收機可以同時滿足醫療穿戴裝置安全性與低功耗之需求。本團隊設計一具硬體安全性的多層式保護微處理器，平台中有兩顆32位元RISC-V IMC作為核心，ISA中使用壓縮（C）指令集可明顯的降低功耗。而兩顆RISC-V核心分別執行一般權限（user mode）和特殊權限（privileged mode）的程式，達到有效區分安全與不安全的世界。利用物理不可複製函數（PUF）作為信任根，將其響應作為金鑰來驗證與保護系統，並搭配進階加密標準-伽羅瓦/計數器模式（AES-GCM）加解密硬體，驗證程式的完整性（integrity），並達到安全開機，進而保護及認證韌體。將PUF、ECC和AES-GCM等安全性相關的硬體模組整合成一個安全模組（Secure Module），確保機密訊息只保留在此模組內，不會透過匯流排傳遞，降低機密訊息被竊聽或竄改的風險。此外本團隊針對功耗旁路攻擊（power side-channel attack），設計將金鑰暫存器的功耗在晶片金鑰產生的過程中保持相同的增加頻率，並且讓響應對產生過程像是每次皆產生1，攻擊者就無法由此推測真正的響應值。由於安全性微處理器位於裝置或體內，不易更換電池且電量有限，因此本團隊結合前端低功耗喚醒接收機（low power wake-up receiver），只有在受到使用者端傳送需求時，才會喚醒後段的安全性微處理器將資料進行加密，進而減少微處理器長時間開啟的功率消耗。當收到喚醒碼(wake-up pattern) 的時候，喚醒接收機會判斷該碼是否正確，若正確才會送出喚醒訊號，額外提供一層安全性防護。



圖一 具高安全性處理器晶片下線圖



圖二 RX 晶片下線圖

指導教授

邱瀝毅　成功大學電機工程學系

成功大學電機工程學士、美國路易斯安那大學計算機工程碩士、美國普渡大學電機與計算機工程博士，現為成功大學電機工程學系教授、敏求智慧運算學院未來運算研究中心主任，及成功大學智慧半導體及永續製造學院晶片設計學位學程主任。

研究領域

低功率超大型積體電路設計、可重新規劃電路系統、超大型積體電路電腦輔助設計

鄭光偉　成功大學電機工程學系

臺灣大學電機工程學士、碩士，美國華盛頓大學電機與工程博士，現為成功大學電機工程學系副教授。曾任聯發科資深 IC 設計工程師、美國國家半導體電路設計工程師、新加坡科技研發局微電子研究院生醫晶片組之計畫主持人。

研究領域

超低功耗射頻、類比積體電路設計、低功耗無線收發機、低功耗類比數位轉換器和鎖相迴路設計

Abstract

As the IoT demands of smart healthcare have increased dramatically in recent years, the security issue of medical devices has become critical for hardware systems or firmware designers. Once the patient’s private information or physiological data is stolen, or the device is being tampered with maliciously to the extent that the health monitor is shut down, pecuniary damages will occur and human lives may even be lost. On the other side, the smart healthcare detection system must be kept running. Portable or wearable devices tend to be smaller and require less power to wake up; therefore, we have designed a hardware secure processor chip that can simultaneously satisfy the demand for security and low power consumption. Our team has designed a multi-layered protection microprocessor for hardware security. The platform uses two 32-bit RISC-V IMC as the core, and uses a compressed (C) instruction set extension that shows evident power reduction. The two RISC-V cores can run in user mode and privileged mode, achieving an effective division of safe and unsafe spaces. We use Physically Unclonable Function (PUF) as Root of Trust, and use its responses as the key to authenticate and protect the system. Also, we encrypt/ decrypt data by designing the Advanced Encryption Standard Galois/Counter Mode (AES-GCM), which authenticates the integrity of the program and achieves secure booting to protect and authenticate firmware. We integrate PUF, ECC, and AES-GCM into a hardware security module, which ensures confidential data will only be retained in this module and will not be transmitted by bus; the risk of confidential data being tapped or tampered will be reduced. Moreover, in dealing with power side-channel attacks, we created a mechanism that maintains the power consumption of the key register at the same increasing frequency during the generation of the key, and produces the CRP difficult to be identified by the attackers. Since the security microprocessor is located in the device or in the body, the battery cannot be easily replaced and the energy is limited. Therefore, our team integrate the low power wake-up receiver to detect if there is a transmission request from the user, thereby reducing power consumption when the microprocessor is turned off for long periods of time. When the wake-up pattern is received, the wake-up receiver will determine whether the code is correct or not; if it is valid, the wake-up signal will be sent, providing an additional layer of security protection for the IoT edge devices.

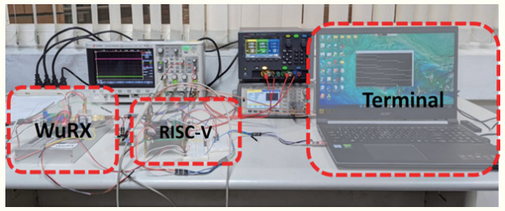


Fig. 3 Integration of system