彥陽科技 推出取代滾碼式遙控器方案

By 市場開發部

PROMASTER TECH LTD.

2018 年 4 月 2 日

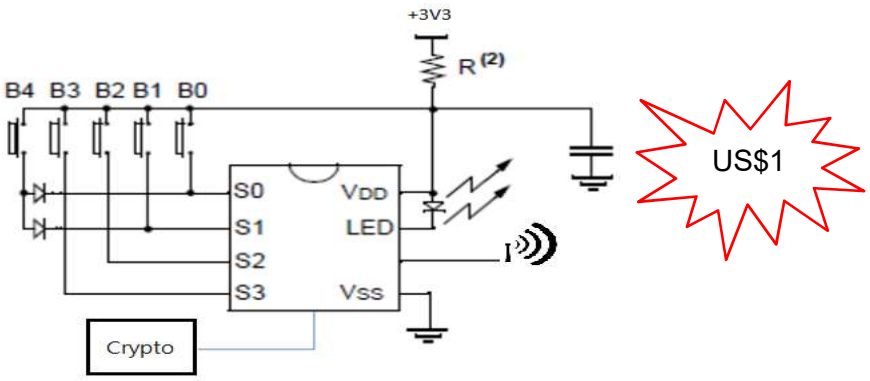
撰寫人: Marten Huang

彥陽科技 推出取代滾碼式遙控器方案

By 市場開發部

滾碼技術，主要透過一份共同的密碼簿和一個同步計數器的設計，通訊兩方必須先約定好相同計數器的數值，利用這數值查詢密碼本，得出相對應的秘密金鑰，因為數值和密碼簿相同，所以能取得相同的密鑰。該密鑰即可應用在發送及接收時的數據加、解密；當數據發送後，雙方同步計數器會同時增加，也同步改變使用的密鑰，也因此每次使用的密鑰都不相同。不過藏於 IC 當中的密碼簿和金鑰長度是決定滾碼技術強度的主要依據。

彥陽科技 代理及推廣 Microchip 滾碼技術為基礎的 KEELOQ 系列晶片多年。建議目前滾碼技術的使用者，評估使用 Microchip 新式 Crypto IC，讓加解密的金鑰位元數提昇至２５６位元，以提高破解的難度。滾碼技術在市場應用十分普遍，早期運用在車門的遙控以及目前大部份車庫門、倉庫門的產品中，而遙控器的拷貝、被開鎖的案例，也是層出不窮。



因此 彥陽科技 推出了一個密碼強度為 256 位元的遙控器參考設計方案，使用標準密碼學 SHA-256 運算，再以 256 位元動態隨機碼的問與答方式來取代密碼本的設計，有效提

高密碼強度。方案中搭配一家位於新竹科學園區內，耕耘無線通訊十年以上的晶片設計廠商，選用最新低耗電設計之 RF MCU，並支持 315~915MHz 頻段，一般睡眠可達 4uA，最低耗電至 1.6uA。

本方案特色：

- 國際晶片大廠 Microchip (ATMEL) 的品質技術保證
- 使用完全隨機動態碼加上 SHA-256 演算法，取代滾碼技術
- 系統安全等級及金鑰密碼長度均為 256 bits，遠高滾碼長度 (66bits)
- 裝置間雙向身份認證技術 (Authentication)
- 遙控器在坊間無法被複製，唯有遙控器廠商能再生產製造
- 沒有掉碼、需要重新配對的問題
- 完整的設計參考方案
- 提昇產品安全性、產品競爭力，創造利潤空間

~ 歡迎詢問及了解 ~