新時代的資料加解密需求

■ 作者：顏睿余

隨著最近提款機被駭客入侵的事件已經不只是電影情節，社群軟體、通訊軟體帳號被盜用的新聞不絕於耳，駭客手法不斷精進，社會大眾也都開始注意到了這個一直存在的安全議題。其實不單純是在個人的帳號密碼保密上需要被注意，對於產品在生產線上與線上軟體更新時的安全問題，更是所有產品開發商所密切關注的。

針對資安問題，其實學術論文與相關的演算法很多。其中主要可分成三個面向討論之，那就是資訊隱蔽 (Privacy)、資料完整性 (Integrity) 和身分認證 (Authenticity)。

在資料完整性 (Integrity) 的面向上，一般我們都利用雜湊函數 (Hash Function) 搭配金鑰 (Key) 將欲保護的資料進行單向計算獲得一個雜湊認證碼 (MAC - Message Authentication Code)，該資料經過傳輸或複製或存放一段時間之後，若透過同樣的雜湊函數運算後的認證碼不變則可代表該資料的完整性，過程中資料內容沒有變動。著名的雜湊函數為 SHA、MD5 與 CRC 等等。

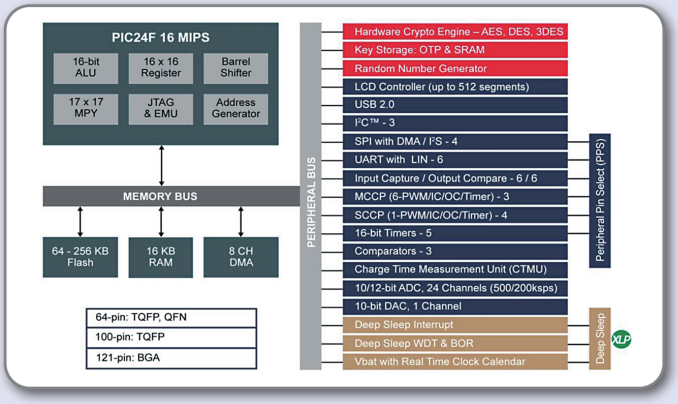
在資訊隱蔽 (Privacy) 的面向上，一般我們將資訊加解密的方式分為對稱式 (Symmetric) 和非對稱式 (Asymmetric) 兩大類，其主要差異是在對於資料加密與解密時使用相同或是不同的密碼 (Key)。對於採用相同密碼進行加解密的演算法 (Symmetric Cipher) 來說，其概念上較為單純，計算較快，著名演算法 (Cipher) 有 DES、3DES、AES... 等等。而非對稱式加解密 (Asymmetric Cipher) 的著名演算法如 RSA、ECC... 等，其在使用上較為安全，但計算上就相對複雜。

不管是對稱式或非對稱式的加解密機制，密碼的保護是最重要的一件事情，對稱式加解密演算法 (Symmetric Cipher) 主要的缺點就是容易在發派密碼 (Key) 到加密端時被盜取，或者因防範措施需加倍嚴謹而造成密碼庫相當龐大。舉例說明某老師請其該班 100 名學生們繳交期末作業時採用某密碼加密，若大家共用同一組密碼，則該密碼被其他人發現的機會大增，且學生們都能互相破解他人的作業，為此該老師只好發放 100 組不同的密碼給每位同學，如此一來儲存與管理密碼的困難增加了很多。該狀況若老師採用非對稱加解密方式 (Asymmetric Cipher) 進行，因為加解密採用不同的密碼 (Public/Private Key)，他只需要發放同一組開放的加密密碼 (Public Key) 給每位同學，就算有其他人盜取該密碼也無法解開加密過後的檔案，同學間也無法破解他人的檔案，而唯一可以解密的密碼 (Private Key) 是在老師手上，因為不需對外派送，所以安全性增加許多。

Microchip 在 16 位元，32 位元 MCU 與 MPU 上皆提供硬體加速引擎供程式設計師處理資料加解密與資料認證工程：

■ PIC24GB2 和 PIC24GB4 系列產品

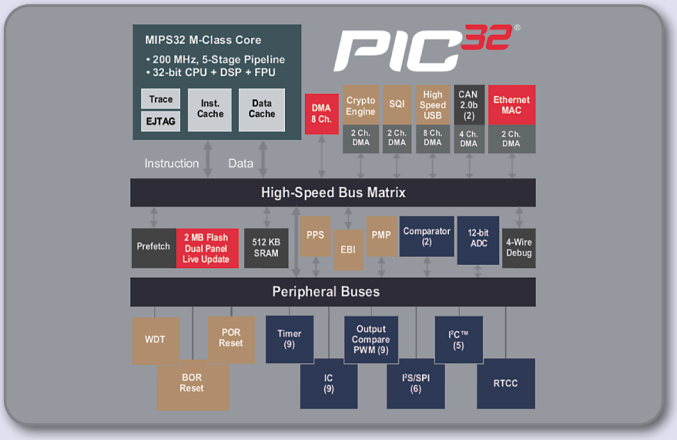
- 提供硬體 Symmetric Cipher AES、DES 和 3DES。



- 另外在密碼 (Key) 的存放上也加入了一次性燒錄密碼 (OTP Key) 和能動態產生的軟體密碼 (SRAM Key)，因為在加解密時是硬體模組在運作，所以在程式中與通訊中並無法得知該密碼，擁有高等級的安全性。
- 內建的硬體亂數產生器 (Random Number Generator) 亦可以應用在各式加解密演算法當中。

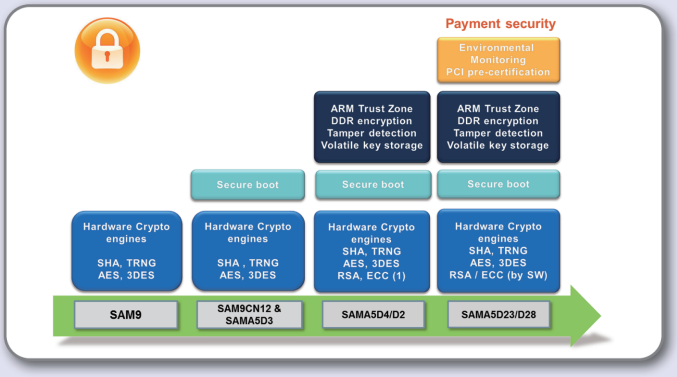
■ PIC32MZ 系列產品

- 同樣包含了硬體 Symmetric Cipher AES、DES 和 3DES。
- 另外還有硬體模組可計算 MD5、SHA1、SHA-256、AES-GCM 和 HMAC 等雜湊函數 (Hash Function)。



■ MPU32 系列產品

- 提供硬體 Symmetric Cipher AES 和 3DES
- 支援軟體 Asymmetric Cipher RSA 和 ECC
- 硬體亂數產生器 (Random Number Generator)
- 硬體雜湊引擎 SHA
- DDR Encryption
- Tamper Detection
- Volatile Key Storage
- PCI Pre-certification



面對現今產品的資安需求，MCU 能夠內建硬體加解密運算引擎是很重要的功能，主要提供快速的運算與硬體層面的密碼保護，如此一來，產品開發商才能方便地讓其產品在通訊、在線升級、配件認證 (如印表機如何認證原廠墨水夾)、甚至是工廠生產上能跟得上這個社會的腳步，擁有新時代的資安等級。

microchip DIRECT
www.microchipdirect.com

MICROCHIP

聯繫信息
Microchip 台灣分公司
電郵：rtc.taipei@microchip.com
技術支援專線：0800-717-718

聯絡電話：
- 新竹 (03) 577-8366
- 高雄 (07) 213-7830
- 台北 (02) 2508-8600

歡迎參加第五屆
台灣技術精英年會2016
Inspire. Inform. Innovate
台北 11月17-18日 • 高雄 11月30日-12月1日
嵌入式控制工程師的盛會 www.microchip.com/tm

Microchip 的名稱和徽標組合及 Microchip 徽標均為 Microchip Technology Incorporated 在美國和/或其他國家或地區的註冊商標。
在此提及的所有其他商標均為各持有公司所有。© 2016 Microchip Technology Inc. 版權所有。