為什麼硬體信任根需要抗攻擊設計

淺談如何強化硬體信任根中的抗攻擊設計來抵禦攻擊

PUFsecurity

Whitepaper

Mar. 2022

Dr. Meng-Yi Wu
吳孟益博士

前言

隨著智慧聯網應用(AIoT) 的發展日趨多元，舉凡人工智慧、影像辨識、智能感測或智慧醫療等，在技術蓬勃發展的同時，也帶出更多安全性的需求--因為每一個 AIoT 終端裝置都暴露在資安風險之中。如何確保裝置是安全且可信的變成極為關鍵。在晶片安全中，從應用層、操作系統層、韌體層、至硬體層皆須有對應設計，缺一不可。而整體安全防護網中最重要的設計，便是硬體層中作為整個晶片信任基礎的硬體信任根(root of trust)。

硬體信任根提供整個晶片安全運作需要的信任基礎(根密鑰)、硬體識別碼 (UID)、硬體獨特鑰匙(HUK)、與隨機數 (entropy)，因此經常成為駭客攻擊的焦點。如果缺乏可以有效抵擋攻擊的設計，整個晶片安全運作的機密就很容易被攻擊者取得，用來破解身分認證、資料加密、竊取產品設計 know-how 等，造成各種應用安全問題。

駭客常用的晶片攻擊的方法

目前晶片攻擊方法主要可以分成三種：侵入式攻擊、半侵入式攻擊以及非侵入式攻擊。侵入式與半侵入式攻擊利用物理方法將晶片一層層地剝開，再利用 TEM、SEM 或者是奈米探針(nano probe) 的方式直接取得、解析實體電路層的設計與運作資訊，來了解晶片安全設計運作流程、獲得安全運作時的晶片機密。非侵入式攻擊通常是指軟韌體攻擊，利用軟、韌體程式設計或運作的漏洞(bug)來了解或取得安全運作的秘密。例如故障注入(fault injection) 即是利用不合規的指令輸入(illegal command) 或數位邏輯控制 (fatal logic control) 引發晶片運作資源不足造成系統當機重置，因而造成晶片安全運作空窗期與漏洞；或是以電壓突波攻擊 (power attack)等方式造成晶片工作不穩定而洩漏系統機密或避開必要的安全檢查。了解進一步晶片攻擊手法，請參閱 Tamper Resistance。

如何強化硬體信任根的保護設計來抵擋駭客攻擊

硬體信任根是用來保護晶片最重要的安全資訊，例如硬體識別碼 (UID)、硬體獨特金鑰(HUK)、對外溝通的共享金鑰或者是相關安全服務憑證的公鑰等等。然而，單純地利用非揮發性記憶體(Non-volatile Memory; NVM)，例如 eFuse, OTP 以及 Flash Memory 來儲存機密資料仍不夠安全。想完整地提升晶片中硬體安全信任根的防禦力，可從以下三個面向加強防護設計：

- **確保資料安全儲存 (Secure Storage):** 用以存放晶片中重要安全資訊的儲存單元須包含 1.取用控制與管理權限、2.對資料讀取與儲存進行混淆與加密，避免上電及斷電時被電性或物理逆向工程讀出儲存的資訊。

- **可信任的安全環境 (Secure Environment):** 晶片設計須包含安全運作專屬的邏輯電路設計與專用的暫存器等等，並且需要設計其他輔助電路來偵測整個區塊的異常行為。這是為了避免電路設計上有任何漏洞，讓駭客可以通過讀取時的能量分析來竊取機密資料。
- **具偵測與權限管控的安全運作 (Secure Operation):** 整體設計須有運作權限控制，監測機密資訊的讀取是否合法，避免駭客藉由故障注入(fault injection)製造晶片邏輯功能運作的錯誤來掌控或取得運作時的重要資訊。

所以一個合格的硬體信任根需要完整的抗攻擊設計 (anti-tampering) 以及完整的安全策略 (secure policy) 來保護整個系統，進一步了解 anti-tampering 設計可以參閱 tamper-proofing。要評斷晶片保護設計的有效性，必須參考相關的設計準則與認證標準，且需要通過具公信力的第三方安全認證實驗室的認證，確認抗攻擊設計能有效降低攻擊風險、提升晶片運作安全。這類的審核通常會是以白盒 (white-box) 設計以及實體晶片破解，從元件、電路以及功能設計等面向來評估整體設計與機密資料保護上的風險。通過安全風險評估後，則取得安全認證實驗室核發安全報告或證書。進一步瞭解第三方認證實驗室，請參閱 PSA。

PUFrt 結合晶片指紋來強化硬體信任根保護設計

PUFrt 是 PUFsecurity 新推出的硬體信任根 IP，整合了原生晶片指紋以及真隨機數產生器與安全存儲 OTP，並結合來自晶片指紋 PUF 的靜態隨機數與 TRNG 的動態隨機數來保護整個設計。PUFrt 的抗攻擊安全設計架構如圖一所示，以軟核(soft macro)的數位電路功能搭配硬核(hard macro)的類比電路設計來實現防止侵入式、非侵入式、半侵入式攻擊手法的抗攻擊設計，目前 PUFrt 安全防護與抗攻擊設計已經通過 Riscure 第三方實驗室的白盒分析，並且已經被 FPGA、AIOT、Vertical 以及 Military 相關應用客戶所採用。相關的抗攻擊技術特徵，根據前文所提三個防護面向分類如下：

對資料安全儲存的保護設計: 安全儲存需要同時考慮數位設計以及類比儲存區塊的抗攻擊強度。除了 NVM 元件本身安全之外，需要具備加密混淆功能的電路設計與抗逆向工程的電路布局。

1 安全儲存元件與布局：反熔絲 Anti-Fuse OTP 元件天生可以抵抗 SEM 以及 TEM 探測。

2 實時資料加密以及混淆：利用每個晶片內建指紋的唯一靜態隨機數來對 OTP 儲存單元進行實時加密

3 安全布局與金屬遮罩保護(top metal shielding)：多層次的安全部署以及上層金屬保護，可以有效防止任何侵入性與非侵入性探測的可能性。

提供可信任的的安全運作環境: 硬體信任根的設計除了需要獨立的安全電路設計之外，需要其他的設計來構建完整的安全環境。PUFrt 的功能，即包含以下：

4 後遮罩設計(post masking)：可以限定硬體讀取動作的次數，避免重放攻擊(replay attack)。

5 安全權限管理(access privilege management)：利用安全 OTP 實現的字元鎖定(word lock) 、不可讀取 (NA) 或是歸零 (zeroization)，再結合 APB 中的安全領域設定 (secure/non-secure) 可以實現完整的權限設定。

6 健康度檢查 (health check)：整個操作環境、舉凡電路是否異常、靜態或動態隨機數的產生電路或輸出品質是否正常，都可以利用自我檢查電路與演算法做進一步的確認。

提供攻擊偵測與權限管控的安全操作: 額外的輔助偵測電路可以來監測並保護整個區塊的正常操作。

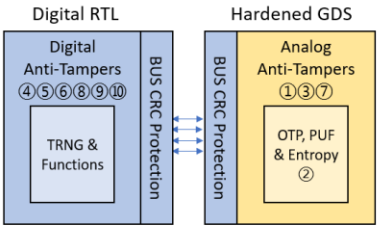
7 抗電壓、抗功耗分析攻擊 (resistance to power analysis)：利用類比穩壓電路及比較器，可以偵測異常電壓行為、增加功率分析的難度。

8 動態隨機讀取(random dummy read)：利用自帶的動態隨機數來隨機化操作，可以避免定址攻擊及故障注入攻擊。

9 傳輸匯流排保護 (BUS protection)：硬體信任根的操作模式與定址，都可以利用 CRC(Cyclic Redundancy Check) 做保護，避免駭客任意變動輸入值。

10 抗故障輸入攻擊 (resistance to fault injection)：類比讀取路徑與暫存器(register)都有可能受到惡意攻擊，輸入不正確的值輸出，此時也可以利用 CRC 來作保護。

圖 1 是 PUFrt 的抗攻擊安全設計架構，包含數位(digital) 抗攻擊設計 (藍色區塊) 與類比(analog) 抗攻擊設計 (黃色區塊) ，右表並將各項抗攻擊設計對應不同攻擊形式(侵入式、半侵入式以及非侵入式)列出供參考。



Types	PUFrt Security Design Features	
Invasive	Analog	Intrinsically Physical Security ①
	Digital	Real time encryption using PUF ②
Semi-invasive	Analog	Secure-oriented Layout ③
	Digital	Output Data Fault Detection ⑧⑨⑩
Non-invasive	Analog	Power Detection, Unified Read/Write Power ⑦
	Digital	Access Privilege, Post-masking, Zeroization, BUS protection, Register protection ④⑤⑥⑨⑩

圖 1. PUFrt 設計架構以及對應各種不同攻擊型態的抗攻擊設計

結論

硬體信任根是整個晶片安全運作的基石。除了提供安全運作所需的身分、密鑰、熵源外，也要具備抵抗各種入侵攻擊的保護設計，保護晶片的信任基礎不被盜取、確保晶片運作的安全。PUFrt 以自帶晶片指紋為基礎結合儲存單元與真隨機亂數產生器，搭配各項數位、類比抗攻擊設計來防止駭客入侵攻擊、避免晶片安全資訊外洩或遭竄改，有效滿足硬體安全信任根對安全儲存、安全環境、安全操作的保護要求，進而確保晶片運作安全與系統應用服務的安全。

PUFsecurity

8F, No. 5, Tai-Yuan 1st St.,
Jhubei City, Hsinchu County,
302082, Taiwan

Tel: +886-3-560-1010
www.pufsecurity.com