加密裝置的電磁分析攻擊

陳君朋

摘要

加密裝置的電磁分析攻擊 (Electromagnetic Analysis Attacks) 相較於傳統的功率分析 (Power Analysis Attacks)，可獲得更多裝置運行時洩漏的資訊。在過去的二十年之中，保密設備遇到了許多安全挑戰，銀行，金融業，計算機，甚至物聯網設備，都受到影響。密碼設備的相關研究，大致上可以分為幾種不同分析方法。而在本研究報告中，將討論過去十多年，使用非接觸方式的旁通道和錯誤注入分析。電磁分析適用範圍從整個系統，到部分積體電路，並透過適當的測量設備取得關鍵資訊。由於台灣在全世界的電子與硬體相關產業，扮演極為關鍵且重要的腳色，因此台灣更應在此領域提供積極的研究，未來也可確保輸出產品有更高的安全性。

一、 硬體加密裝置現況

自從 Paul Kocher 在 1996 - 1999 年提出了一系列分析方法[1] - [2]，過去二十年加解密演算法在硬體裝置實現的安全性，已成為全球共同關注的問題。不同於過去針對演算法的弱點分析，Paul Kocher 透過硬體洩漏的物理訊息加以記錄與處理，進而取得關鍵資訊並分析密鑰，此一方式稱之為”旁通道分析” (Side-Channel Analysis)。然而，近年來物聯網（Internet of Thing, IoT）的發展帶來了許多好處，但它同時也帶來了許多安全與隱私等問題。許多攻擊的目的都是獲取密鑰進而取得控制權，因此安全問題對於硬體設備都非常具有挑戰性[3]。在分析方法上，旁通道分析大致可區分為主動和被動 [4]。

- 主動攻擊：透過操縱（篡改）加密設備的運作或其輸入環境，使設備不正常運行獲取密鑰。

- 被動攻擊：在硬體裝置正常執行情況下，透過記錄設備洩露的資訊（如執行時間，功耗和電磁（EM）輻射）來獲取密鑰。

另一種區分是考慮攻擊接觸程度，可分為非侵入式，半侵入式和入侵式攻擊，第一種和第二種區分方式可以在分析時合併使用[5]。

- 非侵入式攻擊：由於攻擊涉及相對便宜的設備，因此這些攻擊方法對加密設備的安全性構成嚴重威脅，大多數旁通道分析是非侵入性的。

- 半侵入式攻擊：加密晶片被開蓋後裸晶曝露於空氣中，但大部分情況下該晶片仍能保持正常運作。搭配雷射、紫外光、電子顯微鏡，可進一步取得重要資訊。若對此晶片執行錯誤注入分析，達成的攻擊效果，也較未開蓋晶片更有效率。

- 侵入式攻擊：攻擊者直接使用探針平台，以量測硬體裝置不同的部分。如果探測平台僅用於量測洩漏訊號，則這部分侵入式攻擊將被定義為被動式攻擊;另一方面，如果裝置的功能發生改變，那麼攻擊將被分類為主動攻擊。為達到此目的，可使用如雷射切割機，探針台，聚焦離子束（FIB）或掃描電子顯微鏡（SEM）的設備。當關注積體電路 (IC) 部分區域，甚至電晶體參數時，侵入式攻擊的效果是非常強大的 [5]。

數位電路中的功耗是一個重要問題。如果能夠輕易地檢測到功耗，那麼加密設備將更容易受到攻擊。如今，數位積體電路的最基本邏輯單元，是由 CMOS（互補金屬氧化物半導體）所組成。當元件正常工作時，元件的總能量功耗等於每個邏輯操作消耗的總和。CMOS 功耗主要可分為靜態型和動態型。靜態類型是指當保持原始邏輯狀態的電路功率損耗，例如 0→0 或 1→1。事實上，主要消耗功率是 0→1 或 1→0 邏輯轉換的動態情況，此時 CMOS 元件具有較大的短路電流 [7]。

在基本分析中，不同的功耗必須映射到不同的值。例如一個位元組 (Byte) 有 8 個位元 (bit)，如果 8 個位元同時改變狀態（即 0→1 或 1→0），該位元組將達到最大功耗；同樣如果位元組沒有任何狀態改變（即 0→0 或 1→1），它將達到最小功耗，因此一個位元組的變化大致可被分成九個不同的數值（即 0→8）。上述的例子通常稱為漢明距離 (Hamming Distance) 模型，可以用來比較同一位元組改變前與後的兩種狀態。漢明距離模型可以用 HD（V_N, V_{N+1}）表示，其中 V_N 是位元的第 N 個狀態，V_{N+1} 是位元的第 N + 1 個狀態。

面對攻擊目標一無所知，或只能取得部分訊息時，漢明權重(Hamming-Weight)模型有利於分析。假定功率消耗程度與處理數據中的位數成正比，並忽略無法獲得位元的狀態差異。舉例而言，如果 $V_N = 0$，則 HD（V_N, V_{N+1}）= HW（$V_N \oplus V_{N+1}$）= HW（V_{N+1}）；如果 $V_N = 1$，則 HD（V_N, V_{N+1}）= HW ($V_N \oplus V_{N+1}$）= N-

HW（V_{N+1}）。如果處理 V_N前後總是儲存相同的值，則 V_N導致的功耗與該位元的值成正比或反比。為了記錄一段時間內的功耗，數位示波器是最合適的儀器之一。

由於數位示波器測量的是電壓訊號，因此如何將功率轉換為等比例的電壓訊號非常重要。一般來說，測量方法有兩種：

1）使用電源和密碼裝置間的功率測量電路。

2）使用近場探棒或天線測量設備收集電磁輻射信號。

有兩種方法可滿足功率測量電路，但原始設備的特性將會稍微改變。直接測量積體電路接腳對地的電壓變化是一種方法；另一方法是在穩壓電路與安全晶片間的電源上串聯小電阻，由於微處理器需要大量電流來改變其工作狀態，因此示波器根據電流變化乘以電阻得到電壓變化。

電子產品的電磁相容性（Electromagnetic Compatibility, EMC）測試，與非接觸式功率分析與有許多共同之處；與 EMC 測試流程一樣，可透過已發布的分析方法進行洩漏資訊檢測。因此，EMC 測量設備可同樣用於非接觸式功率分析。IEC 61967 標準描述透過電磁場的量測設備，取得積體電路的電磁輻射。IEC 61967-3 定義了“表面掃描”測量技術，IEC 61967-6 定義了磁性探針[8]。小型探針頭可分析積體電路輻射的特定區域，許多積體電路的 EMC 檢測，都使用近場掃描儀滿足要求。並且適當地取得 IC 洩漏的電磁場分量，其內容包過振福與相位[9]。非接觸式測量方法使用線圈，近場探頭或天線。基於 H 探針和 E 探針的特性，可以測量設備的電磁場洩漏達成分析目的。除此此外，IEC 62132-3 定義了 RF 錯誤注入系統，並規劃了錯誤注入平台儀器和探針類型[8]。

目前這兩種方法 (功耗測量電路和電磁輻射測量)，都能夠從密碼設備藉由示波器獲取電壓信號。然而，電磁攻擊比功率分析更廣泛使用，從整個密碼設備到積體電路的部分區域，都可利用電磁分析獲得設備的關鍵資訊。因此，密碼設備的分析可分為三個部分：系統、積體電路和積體電路的部分區域。

系統

文獻 [10] - [15] 展示了對電腦、移動設備和 USB 集線器的物理旁通道分析。聲音的旁通道分析具有非常低的頻寬（普通麥克風在 20kHz 以下，超音波麥克風的幾百 kHz 以下）。在文獻[10]描述了一種聲學密碼分析的攻擊方式，該攻擊在一小時內從筆記型電腦取得完整的 4096 位密鑰。此外，透過適當的電磁探測和訊號處理，可在設備或 USB 電纜上測量信號。如在筆記型電腦上實現應用軟體的電磁分析[11]、在[12]中使用非常低的量測頻寬，取得高頻率處理器運行中洩漏的密鑰。除此之外，即使只是在一個房間之外隔了一面牆，來自筆記型電腦的

密鑰仍可在[13]中被提取出來。在文獻[14]，論文演示了 iOS 與 Android 等行動裝置，運行 OpenSSL 與部分軟體如何洩漏密鑰。USB 連接的輸入設備（如鍵盤，讀卡器和指紋讀取器）通常會向電腦發送敏感信息。超過 50 台不同的電腦和外部集線器被測試後，其 90%以上都發現存在串音 (Cross talk) 的洩漏效應 [15]，因此若針對 USB 集線器的串音實施攻擊，同樣可獲得當裝置溝通時洩漏的資訊。

積體電路

對於系統整合晶片（System on a Chip, SoC）這龐大而復雜的電路而言，挑戰在於找到適合的位置與正確的時間，執行旁通道或錯誤注入分析。在文獻[16]評估 SoC 數位訊號的安全性，並且透過其封裝來抵禦電磁攻擊。[17]討論了射頻辨識(Radio Frequency Identification, RFID)裝置的功率消耗和 EM 攻擊的有效性。最顯著的應用是電子護照和非接觸支付系統，它提供了不同測量設置的概述，並展示了兩個 RFID 設備在功率和 EM 攻擊的具體結果。[18]-[20]分析了對稱與非對稱密鑰演算法，在場可程式化邏輯閘陣列(Field Programmable Gate Array, FPGA)的實現。這些論文討論了 FPGA 在加密應用中的優勢，同時也顯示了 FPGA 的潛在安全問題。對於內部時脈運行的設備而言，可以改進旁通道和注入錯誤攻擊[21]的防禦能力，並讓半導體晶片的分析使用更少的資源與時間完成。論文[22]中，將電磁脈衝（Electromagnetic Pulse, EMP）的錯誤注入到嵌入式密碼系統中。加深並理解電磁場與邏輯元件（Application-Specific Integrated Circuit, ASIC）的相互作用。這種分析方式對於可能出現的電路弱點，並驗證 EMP 攻擊最脆弱的區域而言，都非常有用。

積體電路部分區域

論文[23]-[24]從 CMOS 電路的邏輯運算中提出了模型，並描述了設計方法以保護加密演算法，避免遭受邏輯層面的分析。局部積體電路的資訊洩漏雖然量測受到限制，但是[25]-[28]仍然證明了局部旁通道分析的可行性，並驗證了測量局部電磁場的優勢。論文 [25] 配置了一個 FPGA 裝置，並且提供了一個在積體電路上使用磁場探頭的研究。[26]允許區分電路中暫存器的活動，而在[27]中使用多通道高分辨率的 EM 測量，來提取相關資訊。此外利用電路佈局的特性 [28]，同樣可進一步展現分析和實現的成果。使用增強型探頭執行 EM 錯誤注入攻擊[29]，其方法不僅產生定時錯誤，還可使部分密碼電路產生設置和重設錯誤。在論文 [30]中深入地研究了電磁干擾故障注入，對微控制器的影響，並建立了相關的暫存器傳輸故障模型。

演算法

硬體系統安全使用加密演算法來提供資訊的保密性、完整性和真實性。這些演算法通常需要兩個輸入參數的數學函數：明文和密鑰，將這些參數映射到輸出

稱之為密文。加密演算法的所有細節都為公眾所悉知，只有加密密鑰是保密的，這類演算法包括對稱和非對稱式。加密和解密共享相同的一把密鑰，稱為對稱式加密演算法，如高級加密標準 (Advanced Encryption Standard, AES）[3l]，三重資料加密標準 TDES（Triple Data Encryption Standard, TDES）[32]、Serpent [33]。然而，在非對稱密碼學中，密鑰對由公鑰和私鑰組成。目前有許多非對稱密碼算法，如 RSA（Rivest-Shamir-Adleman）[34]和橢圓曲線密碼學(Elliptic Curves in Cryptography, ECC) [35]。在[1]，[2]和[36] - [39]中，這些文章首先提及針對這些演算法的旁通道分析。

隨著物聯網議題被關注，具有收集資訊能力的智慧裝置可以相互通信，如射頻辨識和無線感測網路 (Wireless Sensor Network, WSN) 等相關研究；這些相關裝置被廣泛使用於物流業、供應鏈管理、家庭自動化、交通控制、醫療監控系統等。由於這些模組的安全需求，激發了許多演算法的相關研究[40]。因此在過去的 10 年中，輕量級密碼學（LightWeight Cryptography, LWC）一直是一個活躍的研究領域，許多創新的演算法被提出增進各種性能標準，並成為重要的主題 [3]。例如，PRIDE [41]，PRESENT [42]，CLEFIA [43]，PRINCE [44]，KLEIN [45]，SIMON[46]或 SPECK [46]等對稱式加密演算法。這些演算法在安全需求，占用晶片面積、硬體實作性能等中取得平衡。同樣的，製造這些對稱式演算法在 IoT 的電子產品，仍需要考慮相關電子檢測，這些測試與電磁旁通道分析方法類似，因此在理想的規劃上，對電子產品做檢測的同時，也對它們的安全防護能力做分析。

二、 旁通道分析方式

如第一部分所述，加密設備由印刷電路板（Printed Circuit Board, PCB）和 IC 所組成。除了功率分析外，雷射 [47]，X 光 [48]和聲音 [10]，這些物理量也都是取得密鑰的方法。然而無論是密碼系統還是安全晶片，使用最廣泛的仍是電磁分析。由於馬克士威方程組 (Maxwell's equations) 所描述，載有金屬線的電流會產生磁場，隨時間變化的磁場產生電場，反之亦然[49]。密碼設備執行加密和解密運算時，通過電路的電流產生磁場，因此使用中的電子設備總是會輻射電磁波。

電磁分析使用線圈、近場探棒，微探針或天線來捕獲電磁輻射能量。由於密碼設備的運行頻率為 MHz 至 GHz，因此最好以適合的取樣頻率獲得關鍵訊號。再使用示波器或類比數位轉換器（ADC），針對固定工作時脈對電磁波進行採樣，並將輻射的類比訊號轉換為數位信號，接著使用電腦或伺服器進一步處理。除此之外，在電磁錯誤注入攻擊中，探針與設備提供了一種快速且可預測的脈衝，可以滿足國際測試的要求[50]，因此在晶片上執行區域化錯誤注入，是一種相對簡單而有效的方法。

天線與近場探棒

攻擊者可以用線圈或電磁探棒，來接收設備洩漏的訊號。由於該訊號基於電場和磁場之間的相互作用引起電磁感應，因此如果隨時間變化的磁場通過一個閉合的探棒（例如線圈，Qi 接收器模塊[51]或磁場探頭[52]），那麼在該探棒將產生一個隨時間變化的感應電流。磁通量的強度發生變化，探針中的電流相對於磁通量的變化會增加或減少；如果磁通量的極性改變，則電流的方向也被切換。一般而言，天線被設計用於接收 100 MHz 以上的頻率，其位置和方向會嚴重影響測量結果。儘管筆記型電腦被標準牆面（15 厘米厚，用金屬螺栓加固）隔開，但帶有放大器的實驗設備，仍然可以透過天線從筆記形電腦獲取信號[13]。測量的方法在[10] - [15]，[17]有關鍵的描述。

近場微探針

微探針設備用於量測積體電路的部分區域，測量時最適當的距離約 1 毫米，而探針尺寸通常小於 1 毫米。電場、磁場微探針以極高的分辨率和靈敏度，測量積體電路部分區域洩漏的電磁場。然而磁場微探針有兩種類型：測量線圈在待測電路上方水平或垂直排列[53]。這些精確的測量方式，可以使探針區分不同電路上細微的儲存活動[26]。因此，局部電磁分析通常使用微探針，取得部分積體電路存取的位置與相關洩漏訊息。適當的測量方法與位置，可取得最高的訊雜比。在[25] - [28]這些論文討論中，當微處理器正在處理加解密訊息時，使用這種設備與分析方式，能夠提供更好的量測結果。

電磁故障注入

安全設備的錯誤注入（Fault- Injection）分析，是一種安全性的主動分析方式。通常透過設備的正常運行和注入錯誤的比較結果，來獲取關鍵信息。電磁輻射的錯誤注入有兩種方式，第一種稱為瞬態脈衝電磁故障注入（EM-FI），基於通過線圈的瞬間電壓變化，感應電流產生磁場，然後在目標區域產生瞬態脈衝 [54]。根據瞬間變化電壓的極性和類型，電流可能因此改變目標區域的電晶體狀態。第二種脈衝電磁錯誤注入稱為諧波分析。使用電磁場在晶片中感應諧波電流。通過調整感應訊號的頻率，可以修改晶片電路的操作。諧波 EM-FI 的典型設置見[55] [56]。這種 EM-FI 設置的探針，與用於瞬態脈衝 EM-FI 的探針不同。該探針主要在尖端釋放高電場，因此可與晶片內部的金屬走線耦合。電磁錯誤注入方式在[16]、[22]、[30]和[54] - [56]有較詳細的描述。

分析方式

簡單功耗分析（Simple Power Analysis, SPA）是一種分析技術，它直接解譯密碼操作期間收集的功耗測量結果[2]。如果給定一組輸入，只有一條或很少條的

功率消耗記錄可用，就可使用此方式實現分析成果。SPA 有不同類型的攻擊方式，如電源痕跡的視覺檢查方式、基於建立模板的簡單功率分析等[57]。在密碼設備上運行的每個算法都是按順序執行的，並由微處理器翻譯成指令。微處理器具有算術指令（諸如加法），邏輯指令（諸如互斥或），數據傳送指令（諸如移動）和分支指令（諸如跳轉）組成的指令集。微處理器的指令涉及不同的組件，並且工作在多個位元組上（例如暫存器，運算邏輯單元或某些外圍設備）。然而指令具有功耗，因此不同指令很容易造成不同的功率消耗軌跡[4]。如果指令序列與密鑰有關，則這些指令造成的波型變化被分析後，將可能導致密鑰洩漏的安全問題。例如，如果一個位元是 1 或 0，則運算出不同形式的電源軌跡，對於公鑰密碼系統的實現，這將會成為嚴重的安全問題。

與 SPA 相比，差分功率分析（Differential Power Analysis, DPA）需要大量的電壓變化紀錄，此種分析方法是對稱密碼演算法最流行的一種攻擊類型。DPA 不需要了解太多關於待分析設備的詳細知識，即使記錄的軌跡包含雜訊，該方法也可以揭示設備的密鑰。該分析策略由五個步驟組成[4] [58]：

步驟 1：選擇演算法執行的中間值。

DPA 的第一步，是獲取設備執行加密演算法的中間值。這個中間值必須是一些已知數據和一小部分密鑰的函數。通常分析人員知道明文，密文或甚至兩者，這取決於加密演算法的結構。如果分析人員能夠選擇明文或密文，則可以定位更多中間值或獲得更多資訊。

第 2 步：衡量訊息。

DPA 的第二步，是測量加密設備在執行運算時的訊息洩漏。如果知道傳輸的明文，示波器或 ADC 的觸發位置，將設置觸發在電腦傳送給密碼設備的明文位置上；如果知道傳輸的是密文，示波器或 ADC 的觸發位置，將觸發設置在密碼設備回傳給電腦的密文位置上。因此，步驟 1 和步驟 2 中的觸發位置彼此相互依賴。

第 3 步：計算假設的中間值。

對於密鑰和所有明文（或密文），DPA 的第三步是計算假設的中間值。由於對稱密碼演算法的設計方法，分析人員只需猜測一小部分密鑰即可計算相對應的中間值。

第 4 步：將中間值映射到訊息值。

第四步，需要選擇適當的模型映射，例如漢明權重模型、漢明距離模型等，目的將中間值映射到假設的訊息值。如果分析師不確定哪種模型是合適的，則應嘗試

所有可能的模型。功率模型與量測設備的特性有關，如果量測模型是確定的，則可進一步進行基於模板的 DPA 攻擊[59]。

步驟 5：比較假設訊息值與測量痕跡。

將關鍵假設的訊息值與位置記錄的軌跡進行比較，並且藉由統計測試完成結果，例如使用相關係數分析找出最接近密鑰的數值。

結論

與功耗分析相比，電磁分析滿足了密碼硬體不同的量測需求。台灣的硬體研究環境很好，晶圓代工、積體電路設計和電子產品檢測的發展，也有利於製造安全的電子產品或物聯網設備。不幸的是，在過去的 20 年裡，這個領域的人才並沒有得到高度重視，優秀的安全產品也沒有出現。去年（2017 年），首次在台灣舉辦的硬體與嵌入式系統安全研討會，內容包含旁通道分析，錯誤注入和安全晶片分析等相關議題。實際上，台灣很多學生願意參與資訊安全相關研究，因此現在正是時候，擴大這領域的研究實力以及產業合作與應用。

參考資料

[1] P. Kocher, “Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other System.” in *Proc. Advances in Cryptology-(CRYPTO)*, 1996, pp.104-113.

[2] P. Kocher, J. Jaffe, and B. Jun, “Differential Power Analysis,” in *Proc. Advances in Cryptology-(CRYPTO)*, 1999, pp.388-397.

[3] A. Adomnicai, B. Lac, A. Canteaut, J. J. A. Fournier, L. Masson, R. Sirdey, and A. Tria, “On the importance of considering physical attacks when implementing lightweight cryptography,” in *Int. Workshop on NIST Lightweight Cryptography*, 2016.

[4] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks - Revealing the Secrets of Smart Cards*, New York, NY: Springer, 2007, Ch. 1 – 6.

[5] S. P. Skorobogatov, “*Semi-invasive Attacks- A new approach to hardware security analysis*,” Tech. Rep., Comput. Lab., Comput. Sci. and Tech. Dept., Cambridge Univ., Cambridge, U.K., 2005, (UCAM-CL-TR-630).

[6] A. Dehbaoui, J.-M. Dutertre, B. Robisson, and A. Tria, "Electromagnetic Transient Faults Injection on a hardware and a software implementations of AES," in *Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC)*, 2012, pp.7-15.

[7] A. S. Sedra, and K. C. Smith, *Microelectronic Circuits*, 5ed, New York, NY, USA: Oxford Univ. Press 2004, pp. 998-1001.

[8] Ross M. Carlton, “An Overview of Emerging International Measurement Standards in Electromagnetic Compatibility for Integrated Circuits,” in *Proc. IEEE EMC-S int. Symp.*, Boston, MA, USA, 2003, pp. 108-113.

[9] S. B. Dhia, M. Ramdani, and E. Sicard, *Electromagnetic Compatibility of Integrated Circuits*, New York, NY, USA: Springer 2006, ch. 4.

[10] D. Genkin, A. Shamir, and E. Tromer, “RSA key extraction via low-bandwidth acoustic cryptanalysis,” in *Proc. Advances in Cryptology-(CRYPTO)*, 2014, pp. 444–461.

[11] D. Genkin, I. Pipman, and E. Tromer, “Get your hands off my laptop: Physical side-channel key-extraction attacks on PCs,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2014, pp. 242–260.

[12] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2015, pp. 207–228.

[13] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer, “ECDH Key-Extraction via Low-Bandwidth Electromagnetic Attacks on PCs,” in *Proc. CT-RSA*, 2016, pp. 219-235.

[14] D. Genkin, L. Pachmanov, I. Pipman, E. Tromer, and Y. Yarom, “ECDSA Key Extraction from Mobile Devices via Nonintrusive Physical Side Channels,” in *Proc. ACM Comput. and Commun. Security (CCS)*, 2016, pp.1626–1638.

[15] Y. Su, D. Genkin, D. Ranasinghe, and Y. Yarom, “USB Snooping Made Easy Crosstalk Leakage Attacks on USB Hubs,” in *Proc. USENIX Security Symp.*, 2017, pp. 1145-1161.

[16] F. Majéric, E. Bourbao, L. Bossuet, “Electromagnetic security tests for SoC,” in *Proc. IEEE Electronics, Circuits and Syst. (ICECS)*, 2016, pp.265-268

[17] M. Hutter, S. Mangard, and M. Feldhofer, “Power and EM Attacks on Passive 13.56 MHz RFID Devices,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2007, pp. 320–333.

[18] T. Wollinger, J. Guajardo, and C. Paar, “Security on FPGAs: State-ofthe-art implementations and attacks,” *ACM Trans. Embedded Comput. Syst.*, vol. 3, no. 3, pp. 534–574, 2004.

[19] S. B. Örs, E. Oswald, and B. Preneel, “Power-Analysis Attacks on an FPGA – First Experimental Results,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2003, pp. 35-50.

[20] F.-X. Standaert, S. B. Örs, and B. Preneel, “Power Analysis of an FPGA,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2004, pp. 30-44.

[21] S. P. Skorobogatov, “Synchronization method for SCA and fault attacks,” *Cryptographic Engineering*, vol. 1, no. 1, pp. 71–77, April 2011.

[22] D. Alberto, P. Maistri, R. Leveugle, “Investigation of Electromagnetic Fault Injection Effects on Embedded Cryptosystems,” in *TRUDEVICE*, 2013.

[23] D. Suzuki, M. Saeki, and T. Ichikawa, “DPA Leakage Models for CMOS Logic Circuits,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2005, pp. 366-382.

[24] K. Tiri and I. Verbauwhede, “Securing Encryption Algorithms against DPA at the Logic Level：Next Generation Smart Card Technology,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2005, pp. 125-136.

[25] J. Heyszl, D. Merli, B. Heinz, F. D. Santis, and G. Sigl “Strengths and Limitations of High-Resolution Electromagnetic Field Measurements for Side-Channel Analysis,” in *Proc. Smart Card Res. and Advanced Appl. Conf. (CARDIS)*, 2012, pp. 248–262.

[26] J. Heyszl, S. Mangard, B. Heinz, F. Stumpf, and G. Sigl, “Localized Electromagnetic Analysis of Cryptographic Implementations,” in *Proc. CT-RSA*, 2012, pp. 231–244.

[27] R. Specht, J. Heyszl, M. Kleinsteuber, and G. Sigl, “Improving Non-profiled Attacks on Exponentiations Based on Clustering and Extracting Leakage from Multi-channel High-Resolution EM Measurements,” in *Proc. Constructive Side-Channel Analysis and Secure Design (COSADE) Int. Workshop*, 2015, pp. 3-19.

[28] V. Immler, R. Specht, and F. Unterstein, “Your Rails Cannot Hide from Localized EM：How Dual-Rail Logic Fails on FPGAs,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2017, pp. 403-424.

[29] S. Ordas, L. Guillaume-Sage, K. Tobich, J.-M.Dutertre, P. Maurine, “Evidence of a larger EM-induced fault model,” in *Proc. Smart Card Res. and Advanced Appl. Conf. (CARDIS)*, 2014, pp. 245–259.

[30] N. Moro, A. Dehbaouiy, K. Heydemannz, B. Robisson, and E. Encrenaz, “Electromagnetic fault injection towards a fault model on a 32-bit microcontroller,” in *Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC) Int. Workshop*, 2013, pp. 77-88.

[31] FIPS-197: Advanced Encryption Standard, National Institute of Standards and Technology (NIST), 2001. Available: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf

[32] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, National Institute of Standards and Technology

(NIST), 2017. Available: https://csrc.nist.gov/csrc/media/publications/sp/800-67/rev-2/draft/documents/sp800-67r2-draft.pdf

[33] R. Anderson, E. Biham, and L. Knudsen, "SERPENT: A Candidate Block Cipher for the Advanced Encryption Standard," Available: http://www.cl.cam.ac.uk/~rja14/serpent.html

[34] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *ACM Commun. Mag.*, vol. 21, no. 2, pp. 120-126, Feb. 1978.

[35] V. Miller, "Uses of elliptic curves in cryptography," in *Proc. Advances in Cryptology-(CRYPTO)*, 1986, pp. 417-426.

[36] E. N. Supérieure, G. C. International, "Resistance against differential power analysis attacks for elliptic curve cryptosystems," in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 1999, pp. 292-302.

[37] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "A Cautionary Note Regarding Evaluation of AES Candidates on Smart-Cards," in *Second Advanced Encryption Standard (AES) Candidate Conf.*, Rome, Italy, 1999.

[38] N. A. Howgrave-Graham and N. P. Smart, "Lattice Attacks on Digital Signature Schemes," Int. J. Designs, Codes and Cryptography, vol. 57, pp. 283-290, 2001.

[39] T. Römer and J.-P. Seifert, "Information Leakage Attacks against Smart Card Implementations of the Elliptic Curve Digital Signature Algorithm," in *Proc. Research in Smart Cards: Smart Card Programming and Security (E-SMART)*, E-Smart 2001, pp. 211–219.

[40] A. Heuser, S. Picek, S. Guilley, N. Mentens, "Side-channel Analysis of Lightweight Ciphers: Current Status and Future Directions," in *Int. Workshop on NIST Lightweight Cryptography*, 2016.

[41] M. R. Albrecht, B. Driessen, E. B. Kavun, G. Leander, C. Paar, and T. Yalçin, "Block Ciphers - Focus on the Linear Layer (feat. PRIDE)," in *Proc. Advances in Cryptology-(CRYPTO)*, 2014, pp. 57–76.

[42] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, and C. Vikkelsoe, "PRESENT: An ultra-lightweight block cipher," in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2007, pp. 450-466.

[43] T. Shirai, K. Shibutani, T. Akishita, S. Moriai, and T. Iwata, "The 128-Bit Blockcipher CLEFIA (Extended Abstract)," in *Proc. Fast Software Encryption (FSE)*, 2007, pp. 181–195.

[44] J. Borghoff, A. Canteaut, T. Güneysu, E. B. Kavun, M. Knežević, L. R. Knudsen, G. Leander, V. Nikov, C. Paar, C. Rechberger, P. Rombouts, S. S. Thomsen, and

T. Yalçin, “PRINCE - A low-latency block cipher for pervasive computing applications - extended abstract,” in *Proc. Advances in Cryptology – (AsiaCrypt)*, 2012, pp. 208-225.

[45] Z. Gong, S. Nikova, and Y. W. Law, “KLEIN: A New Family of Lightweight Block Ciphers,” in *Int. Workshop of RFID Security and Privacy (RFID Sec.)*, 2011, pp. 1–18.

[46] R, Beaulieu, D. Shors, J. Smith, S. Treatman-Clark, B. Weeks, and L. Wingers, “SIMON and SPECK: Block Ciphers for the Internet of Things,” in *Proc. ACM/EDAC/IEEE Design Automation Conf. (DAC)*, 2015.

[47] S. P. Skorobogatov and R. J. Anderson, “Optical Fault Induction Attacks,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2002, pp. 2–12.

[48] S. Anceau, P. Bleuet, J. Clédière, L. Maingault, J.-L. Rainard, and Rémi Tucoulou, “Nanofocused X-Ray Beam to Reprogram Secure Circuits,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2017, pp. 175-188.

[49] John David Jackson, *Classical Electrodynamics*, 3ed. Hoboken, NJ, USA: Wiley, 1999, pp. 237-239

[50] R. Vlelgalati, R. V. Spyk, and J. V. Woudenberg, “Electromagnetic Fault Injection in Practice,” in *Int. Cryptographic Module Conf. (ICMC)*, 2013.

[51] Qi-Wireless, Available: http://www.qiwireless.com/

[52] Near-Field Probes, Available: https://www.langer-emv.de/en/category/near-field-probes/19

[53] Near-Field Microprobes H- and E-Field, Available: https://www.langer-emv.com/en/category/near-field-microprobes-h-and-e-field/69

[54] Maurice Aarts, “Electromagnetic Fault Injection using Transient Pulse Injections,” MA thesis, Math. and Comput. Sci. Dept., Eindhoven Univ. of Tech., Eindhoven, Nederland, 2013, pp. 17-22.

[55] P. Bayon, L. Bossuet, A. Aubert, V. Fischer, F. Poucheret, B. Robisson, and P. Maurine, “Contactless electromagnetic active attack on ring oscillator based true random number generator,” in *Proc. Constructive Side-Channel Analysis and Secure Design (COSADE) Int. Workshop*, 2012, pp. 151-166.

[56] F. Poucheret, K. Tobich, M. Lisarty, L. Chusseau, B. Robisson, and P. Maurine, “Local and Direct EM Injection of Power into CMOS Integrated Circuits,” in *Proc. Fault Diagnosis and Tolerance in Cryptography (FDTC) Int. Workshop*, 2011, pp. 100-104.

[57] S. Chari, J. R. Rao, and P. Rohatgi, “Template Attacks,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2002, pp. 13-28.

[58] E. Brier, C. Clavier, and F. Olivier, “Correlation Power Analysis with a Leakage Model,” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2004, pp. 16-29.

[59] D. Agrawal, B. Archambeault, J. R. Rao, and P. Rohatgi, “The EM Side-channel(s),” in *Proc. Cryptographic Hardware Embedded Syst. (CHES)*, 2002, pp. 13-15.