能量洩露刻畫方法與區分器構造技術研究現狀

張海龍[1,2]，周永彬[1]
[1] 中國科學院信息工程研究所 信息安全國家重點實驗室
[2] 中國科學院大學
{zhanghailong, zhouyongbin}@iie.ac.cn

摘要

實際應用中，密碼演算法通常以軟體或硬體邏輯的形式存在於密碼設備中。密碼設備在執行過程中會產生不同形式關於敏感中間值的洩露資訊（例如，能量洩露資訊、電磁洩露資訊等），這些洩露資訊統稱為側資訊。利用側資訊恢復密碼設備所使用金鑰的攻擊被稱作側通道攻擊。實踐表明，側通道攻擊對密碼設備的物理安全性造成了巨大的現實威脅。作為一種典型的側通道攻擊，由於具有實施簡單、代價低廉等突出特點，能量分析攻擊對密碼設備帶來的物理安全威脅尤為突出。

鑒於能量分析攻擊對密碼設備物理安全性帶來的巨大威脅，一種重要的評估密碼設備物理安全性的手段是對其實施能量分析攻擊，並且以攻擊效果作為衡量其物理安全性的指標。為了更清晰、更準確地審視與分析密碼設備物理安全性，發展高效、新穎的能量分析攻擊方法是一種最直接的重要技術途徑。為此，針對能量分析攻擊的研究得到了學術界與產業界人員的持續關注，該領域的研究成果也大量湧現。本文圍繞能量洩露刻畫方法、範本攻擊技術、通用側通道區分器構造方法、針對遮罩類密碼實現的能量分析攻擊等研究現狀展開論述，旨在較準確反映當前能量分析攻擊領域最新研究進展。

關鍵詞：側通道密碼分析，能量分析攻擊，能量洩露刻畫，範本攻擊，側通道區分器，遮罩類密碼實現

壹、前言

傳統密碼分析中，通常將密碼演算法看作一個黑盒子。分析人員僅利用密碼演算法的輸入、輸出資訊恢復密碼演算法所使用金鑰。恢復金鑰的過程中分析人員通常借助密碼演算法的數學性質。然而，隨著電子技術、半導體技術的迅猛發展，密碼演算法在實際應用中往往以硬體邏輯或者軟體程式的形式存在於密碼設備中。典型的密碼設備包括微控制器、智慧卡、FPGA、ASIC等。

因此，密碼設備物理安全性成為保障各行各業資訊安全的重要問題。我們指出，密碼設備在運行過程中存在不同形式關於敏感中間值的洩露資訊（例如，能量洩露資訊、電磁洩露資訊等），我們將這些洩露資訊統稱為側資訊。我們可以利用側資訊恢復密碼設備所使用金鑰，此類攻擊被稱為側通道攻擊。1996年，Kocher在美國密碼學年會上首次提出了計時攻擊的概念，並對無保護RSA演算法實現成功實施了計時攻擊。自此，針對側通道攻擊的研究得到了國際密碼學界的廣泛關注。經過十餘年的發展，多種形式側通

道攻擊被先後提出。典型的側通道攻擊包括：計時攻擊、故障攻擊、能量分析攻擊、電磁輻射攻擊、多通道攻擊、代數側通道攻擊以及側通道碰撞攻擊等。

實踐表明，不同形式的側通道攻擊對密碼設備的物理安全性帶來了巨大威脅。典型側通道攻擊中，能量分析攻擊對密碼設備帶來的物理安全威脅尤為突出。原因在於，能量分析攻擊在實際應用中易於實施，並且實施能量分析攻擊所需的代價較低。事實上，在側通道攻擊領域的研究中，針對能量分析攻擊的研究最多，研究成果也最豐富。

能量分析攻擊的基本原理是利用密碼設備執行過程中的能量洩露資訊與其所處理中間值的統計依賴性恢復出密碼設備所使用金鑰。能量分析攻擊由Kocher於1999年首次提出。經過十餘年的發展，多種形式能量分析攻擊被先後提出。典型的能量分析攻擊包括簡單能量分析(Simple Power Analysis, SPA)、差分能量分析(Differential Power Analysis, DPA)、高階差分能量分析(Higher Order Differential Power Analysis, HODPA)、範本攻擊(Template Attack, TA)、相關係數能量分析(Correlation Power Analysis, CPA)、隨機模型分析(Stochastic Model based Power Analysis, SMPA)、基於劃分的能量分析(Partitioning Power Analysis, PPA)、互資訊分析(Mutual Information Analysis, MIA)、差分簇分析(Differential Cluster Analysis, DCA)、基於KS檢測的能量分析(KS Test based Power Analysis, 包括KSA與PKS)、以及碰撞-相關係數能量分析(Collision-Correlation Power Analysis, CCPA)等。

能量分析攻擊的實施過程分為兩個階段，即洩露採集階段與金鑰恢復階段。在洩露採集階段，分析人員使用測量配置採集得到密碼設備執行過程中的能量洩露資訊；在金鑰恢復階段，分析人員借助某種統計工具（亦稱為區分器）分析採集到的能量洩露資訊與被攻擊中間值之間的統計依賴性，從而恢復出密碼設備所使用金鑰。不同能量分析攻擊在洩露採集階段沒有區別，主要差異在於金鑰恢復階段恢復密碼設備所使用金鑰方式不同。首先，不同能量分析攻擊借助不同的能量洩露刻畫方法刻畫得到被攻擊中間值所對應假設能量洩露資訊；其次，不同能量分析攻擊借助不同的區分器分析假設能量洩露資訊與真實能量洩露資訊之間的相關性。

鑒於能量分析攻擊對密碼設備物理安全性帶來的巨大威脅，實際上可以借助能量分析攻擊評估密碼設備的物理安全性。為了準確評估密碼設備物理安全性，需要不斷優化能量分析攻擊能力。因此，如何從不同角度提升能量分析攻擊能力對於準確評估密碼設備的物理安全性具有重要意義。

本文分別從能量分析攻擊領域四個研究方向（包括能量洩露刻畫方法、範本攻擊技術、差分能量分析攻擊方法、以及針對遮罩類密碼實現的能量分析攻擊）的研究現狀進行論述，旨在較準確反映出能量分析攻擊領域最新研究進展。

本文其餘部分組織結構如下：第二節介紹能量洩露刻畫領域的研究現狀。第三節介紹範本攻擊領域的研究現狀。第四節介紹差分能量分析攻擊領域的研究現狀。第五節介紹針對遮罩類密碼實現的能量分析攻擊領域的研究現狀。最後，在第六章展望了能量分析攻擊領域需要進一步研究的問題。

貳、能量洩露刻畫方法

能量分析攻擊中，分析人員利用密碼設備執行過程中能量洩露資訊與被攻擊中間值之間統計依賴性恢復密碼設備所使用金鑰。分析人員採集得到的能量跡通常包括兩個分量，即，信號分量與雜訊分量。其中，信號分量依賴於被攻擊中間值，而雜訊分量由能量跡採集過程中的測量誤差造成。我們指出，分析人員採集得到能量跡中雜訊分量會影響到能量分析攻擊金鑰恢復效率。為了保證能量分析攻擊金鑰恢復效率，分析人員通常需要對採集得到能量跡中信號分量進行準確刻畫。

事實上，Coron在[13]中已揭示出能量分析攻擊與能量洩露資訊之間的關係。在1999年Kocher等人首次提出差分能量分析攻擊時，他們採用單比特洩露刻畫方法刻畫得到密碼設備執行過程中暫態能量洩露資訊。然而，單比特洩露刻畫方法僅能夠刻畫被攻擊中間值單個比特的能量洩露資訊，攻擊者對密碼設備執行過程中的暫態能量洩露資訊刻畫不充分。在Multi-bit DPA中，Messergers等人採用多比特洩露刻畫方法刻畫得到密碼設備執行過程中暫態能量洩露資訊。隨後，Brier等人在CPA中採用漢明重量與漢明距離洩露刻畫方法刻畫得到密碼設備執行過程中暫態能量洩露資訊[4]。漢明重量與漢明距離洩露刻畫方法能夠利用中間值所有比特能量洩露資訊。但是，兩種刻畫方法假設中間值不同比特的洩露量相同；同時，這兩種刻畫方法無法刻畫中間值相鄰比特間相互作用。事實上，Bevan等人在2003年指出，中間值不同比特洩露量並不同。同時，Akkar等人在[1]中研究了相鄰比特相互作用對能量洩露資訊的影響，但是Akkar等人並沒有深入研究該問題。基於此，Doget等人在[17]提出了一般性能量洩露資訊信號刻畫方法。Doget等人採用高階模型刻畫出了中間值與密碼設備暫態能量洩露資訊之間統計關係。2012年Heuser等人基於Doget所提出高階模型對DPA Contest v2階段所公佈密碼實現進行了刻畫與分析。同時，Lemke-Rust 等人在[30]中針對遮罩設備能量洩露特徵提出了一種二階隨機模型洩露刻畫方法。Martinzsek等人在[35]中提出使用神經網路方法盡可能充分刻畫密碼設備暫態能量洩露資訊，從而最優化能量分析攻擊。從硬體電路角度講，Liu等人在[34]中提出了一種針對switch glitch的能量洩露刻畫方法。Suzuki等人在[49]中提出了一種針對CMOS電路的DPA洩露模型。

綜上所述，目前學術界對密碼設備能量洩露資訊刻畫方法研究相對較充分。當然，能量洩露刻畫領域尚存在一些問題，主要難點在於對高階洩露資訊的刻畫方法、針對多點能量洩露資訊的刻畫方法、以及針對特定密碼設備能量洩露資訊刻畫方法的研究。

參、範本攻擊技術

範本攻擊由於其強大的金鑰恢復效率被廣泛用於評估密碼設備物理安全性。然而，針對範本攻擊優化技術的研究始終沒有停止。事實上，為了盡可能準確認識密碼設備物理安全性，就需要不斷優化範本攻擊金鑰恢復效率。

首先，從預處理角度講，Rechberger等人在[43]中分析了範本攻擊在實際應用中特徵點選取問題；隨後Archambeau等人提出基於PCA的範本攻擊以避免範本攻擊中在實際應用中特徵點選取困難的問題；Elaabid等人分析了PCA中主成分數量對範本攻擊金鑰恢復效率帶來的影響；近幾年，Standaert等人在2008年提出了基於FLDA的範本攻擊以進一步優化範本攻擊金鑰恢復效率；Reparaz等人在2012年提出了基於MIA的特徵點選取技術有效提取特徵點。從計算角度講，Lemke-Rust等人在2007年提出了一種高斯混合模型以更精確刻畫密碼設備執行過程中的能量洩露特徵。近年來，Lommé等人在[32]中針對範本攻擊計算方式進行優化改進，提升範本攻擊實現效率；Choudary等人在[12]中分析了影響範本攻擊的一些計算問題；從攻擊策略角度講，Hanley等人在2009年提出未知明文範本攻擊以擴大範本攻擊適用場景；隨後Veyrat-Charvillon等人提出一種適應性選擇明文範本攻擊有效恢復密碼設備所使用金鑰；Lerman等人在[29]中提出了半監督式範本攻擊有效降低範本攻擊實施條件。從評估角度講，Standaert等人[46]在模擬場景與實際場景中對範本攻擊與基於隨機模型的能量分析金鑰恢復效率進行了對比；2014年Choudary等人分析了刻畫設備與被攻擊密碼設備不同時範本攻擊金鑰恢復效率表現；同年，Oren等人提出了一種針對範本攻擊的新型框架。從應用角度講，Ye等人在[55]中使用範本攻擊找到wide collisions。另一方面，研究人員將一些新穎模式識別、時間序列方法應用在範本攻擊中並且取得不錯的效果。例如，Bartkewitz等人在[6]中提出了基於支持向量機的TA。Heuser等人在[26]中使用支援向量機的範本攻擊。Lerman等人在[28]中提出基於時間序列的範本攻擊有效恢復正確金鑰。

綜上所述，針對範本攻擊的研究始終是個熱點問題，主要原因在於範本攻擊能夠勇於準確評估密碼設備無力安全性。研究人員從不同角度對範本攻擊進行了研究與改進以提升範本攻擊金鑰恢復效率。我們指出，改進後的範本攻擊金鑰恢復效率更高，從而會指導密碼設備評估人員更準確認識密碼設備物理安全性。

肆、差分能量分析攻擊

自從Kocher於1999年首次提出差分能量分析攻擊以來，針對差分能量分析攻擊的研究始終是能量分析攻擊領域的研究重點，包括能量跡預處理技術、區分器改進技術、區分器效率評估技術、新型區分器的研究等。

從攻擊效率的改進角度講，Batina等人在[5]中提出RCPA進一步提升CPA金鑰恢復效率；隨後Souissi等人分析了CPA的最優化問題；Standaert等人分析了二階DPA的最優化預處理技術。從預處理角度講，Batina等人在2012年利用PCA提升能量分析攻擊效率；Muijrers等人與Woudenberg等人分別在[37][54]中提出能量跡對齊技術；Oswald等人在[38]中提出基於最優線性變換的能量跡預處理技術。從區分器金鑰恢復效率評估角度講；2012年Fei等人量化分析各種因素與DPA金鑰恢復效率的關係；Guilley等人與Prouff分別在[20][39]中形式化分析DPA金鑰恢復效率與S盒之間的關係；Lomné等人在[33]中量化評估

影響高階能量分析攻擊成功率的因素；Heuser等人在[24]中理論研究基於KS檢測通用區分器與傳統密碼分析技術間的聯繫；同時，研究人員在[42]中對通用區分器在實際應用中的優點與不足進行分析與評估；Standaert等人與Whitnall等人分別在[47][53]中提出評估框架有效評估能量分析攻擊金鑰恢復效率；Thillard等人在[51]中從confidence角度出發分析能量分析攻擊成功率；Reparaz等人在[41]中對成功率與相對區分度兩類度量指標進行分析對比；Standaert等人在[48]中分析了密碼設備針對DPA攻擊安全上限；Lu等人在[31]中分析了基於AES密碼實現抵抗一階、二階能量分析攻擊的原理；研究人員在[45]中比較評估了不同區分器在實際應用中的金鑰恢復效率；最後，Veyrat-Charvillon等人在[52]中提出一種超越計算能力的安全評估技術用於有效評估能量分析攻擊金鑰恢復效率。從新型區分器研究角度講，Elaabid等人與Souissi等人分別在[19][44]中提出組合側通道攻擊，將區分器組合後提升差分能量分析攻擊金鑰恢復效率；Heuser等人在[25]中分析提出一種最優側通道區分器； Menicocci等人[36]提出一種實際的二階DPA用於評估特定遮罩方案；但早在2004年Waddle等人提出一種利用密碼設備並行處理洩露特徵的二階DPA攻擊；2005年Peeters等人給出了一種改進版高階DPA；在2011年Pan等人利用DPA尖峰所提供信息進一步優化DPA金鑰恢復效率；同年，Sahara等人提出PKDPA進一步提升DPA金鑰恢復效率；Souissi等人提出基於PCA的差分能量分析有效恢復密碼設備所使用金鑰。

綜上所述，針對能量分析攻擊的研究成果非常豐富、涉及範圍也比較廣泛。原因在於差分能量分析攻擊對敵手攻擊能力要求較低，在實際場景中更易於實施。

伍、針對遮罩類密碼實現的能量分析攻擊

鑒於能量分析攻擊對密碼設備帶來的物理安全威脅，研究人員提出使用防禦對策保護密碼設備物理安全性。在各種軟、硬體防禦對策中，關於遮罩防禦對策的研究最深入、研究成果也最多。原因在於遮罩可以在軟體演算法層面實現，實現代價較低。

遮罩對策首先由Goubin等人與Itoh等人分別于1999年和2002年提出。自此，多種形式的遮罩方案被相繼提出。其中，研究人员如Coron[8]等分別提出基於查閱資料表的遮罩防禦對策抵抗能量分析攻擊的能力； Genelle[21]等人提出使用乘法遮罩保護密碼設備物理安全性；Herbst等人在[23]中研究了基於AES加密演算法的遮罩方案。但是，一階遮罩無法有效保護密碼設備物理安全性。為此，研究人員一方面提出使用高階遮罩與可證明安全遮罩有效保護密碼設備物理安全性；另一方面提出一些基於特定工具（例如，多項式、傅里葉變換等）的新型遮罩方案[15]。同時，Coron等人與Genelle等人分別在[9][22]中提出不同類型遮罩組合使用以有效抵抗能量分析攻擊，而Schaumont等人在[50]中研究將遮罩與硬體防禦對策組合使用以有效抵抗能量分析攻擊。需要說明的是，不同類型遮罩組合使用時可以使用[11]中所提出演算法有效轉換不同類型的遮罩。然而，遮罩方案通常會增加密碼設備實現代價。為了降低遮罩方案實現代價，研究人員研究出了低熵遮罩方案，並且評估低熵遮罩方案的安全性[7]。最後，研究人員如Coron[10]等分別從理論

與實際方面分析、評估已有遮罩防禦對策的安全性與應用前景。在針對遮罩方案的能量分析攻擊研究方面，研究人員研究受低熵遮罩RSM保護AES軟體實現在實際應用中抵抗能量分析攻擊的能力，提出了針對低熵遮罩方案RSM的能量分析攻擊（包括一階、二階能量分析攻擊以及範本攻擊等）[3]；Prouff等人在[40]中給出針對查閱資料表防禦對策的一階能量分析攻擊；在2002年Akkar等人提出了兩種針對one-mask的攻擊；Coron等人[10]在2008年對基於傅里葉變換的遮罩方案進行了分析改進；同時，Coron等人在[14]中分析了高階遮罩方案；Fumaroli等人在2007年給出了針對duplication的一階攻擊；最後，來自不同研究機構的研究人員對不同遮罩方案進行了實際安全性分析。在攻擊技術的改進方面，Dabosville等人在[16]中提出基於線性回歸的二階能量分析攻擊；Ding等人在[18]中量化分析不同因素對高階DPA攻擊成功率的影響； Joye等人在[27]中分析二階差分能量分析攻擊的實際效率。

綜上所述，針對遮罩方案（包括針對遮罩方案的能量分析攻擊）研究更像是一種矛與盾的較量。一種遮罩方案提出時，研究人員自然會分析該遮罩方案在實際應用中抵抗能量分析攻擊的能力。

陸、能量分析攻擊領域研究展望

通過對能量分析攻擊不同研究方向研究進展進行論述，我們可以看到能量分析攻擊領域中不同方向的研究依然存在一些問題需要進一步去探討解決，在此我們將其中一些值得研究的問題進行描述：

- 多點能量洩露刻畫方法研究

目前的能量洩露刻畫方法僅能夠對密碼設備執行過程中單個時刻能量洩露資訊中信號分量進行刻畫。鑒於分析人員可以利用多個時刻能量洩露資訊中信號分量進行準確刻畫，一個很自然的問題是能否提出能夠同時刻畫密碼設備執行過程中多個時刻能量洩露資訊的洩露刻畫方法？

- 基於機器學習的範本攻擊技術研究

本文中，我們介紹了目前針對傳統範本攻擊的一些改進方案。事實上，我們可以將機器學習領域一些新型技術應用在範本攻擊技術中。我們可以研究新型技術在範本攻擊中的金鑰恢復效率表現。

- 最優通用側通道區分器研究

隨著密碼設備生產工藝的提升，密碼設備能量洩露資訊與被攻擊中間值越來越多呈現出一種非線性關係。如何充分利用密碼設備能量洩露資訊與被攻擊中間值之間各種依賴關係成為一個需要研究的重要問題。

- 高階能量分析攻擊研究

儘管遮罩方案能夠抵抗傳統能量分析攻擊，但是遮罩方案依然無法抵抗高階能量分析攻擊，僅僅是加大了攻擊成功的代價。為此，我們一個自然的問題是是否能夠提出高

效的高階能量分析攻擊？從而有效降低分析人員實施攻擊所需要的代價。我們指出，高階能量分析攻擊將會指導密碼設備評估人員準確認識密碼設備物理安全性。

參考文獻

[1] M.L. Akkar, R. Bevan, P. Dischamp, and D. Moyart, "Power Analysis,What Is Now Possible," ASIACRYPT 2000, LNCS 1976, pp. 489-502, 2000.

[2] M.L. Akkar, R. Bévan, and L. Goubin., "Two Power Analysis Attacks against One-Mask Methods," FSE 2004, LNCS 3017, pp. 332–347, 2004.

[3] P. Belgarric, S. Bhasin, N. Bruneau, J.L. Danger, N. Debande, S. Guilley, A. Heuser, Z. Najm and O. Rioul, "Time-Frequency Analysis for Second-Order Attacks," CARDIS 2013, LNCS 8419, pp. 108–122, 2014.

[4] E. Brier, C. Clavier and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, LNCS 3156, pp. 16–29, 2004.

[5] L. Batina, B. Gierlichs and K. Lemke-Rust, "Comparative Evaluation of Rank Correlation Based DPA on an AES Prototype Chip," ISC 2008, LNCS 5222, pp. 341-354, 2008.

[6] T Bartkewitz and K. Lemke-Rust, "Efficient Template Attacks Based on Probabilistic Multi-class Support Vector Machines," CARDIS 2012, LNCS 7771, pp. 263–276, 2013.

[7] C. Carlet, "Correlation-Immune Boolean Functions for Leakage Squeezing and Rotating S-Box Masking against Side Channel Attacks," SPACE 2013, LNCS 8204, pp. 70–74, 2013.

[8] J.S. Coron, "A New DPA Countermeasure Based on Permutation Tables," SCN 2008, LNCS 5229, pp. 278–292, 2008.

[9] J.S. Coron and L. Goubin, "On Boolean and Arithmetic Masking against Differential Power Analysis," CHES 2000, LNCS 1965, pp. 231-237, 2000.

[10] J.S. Coron, C. Giraud, E. Prouff and M. Rivain, "Attack and Improvement of a Secure S-Box Calculation Based on the Fourier Transform," CHES 2008, LNCS 5154, pp. 1–14, 2008.

[11] J.S. Coron, J. Großschädl and P.K. Vadnala, "Secure Conversion between Boolean and Arithmetic Masking of Any Order," CHES 2014, LNCS 8731, pp. 188–205, 2014.

[12] O. Choudary and M.G. Kuhn, "Efficient Template Attacks," CARDIS 2013, LNCS 8419, pp. 253–270, 2014.

[13] J.S. Coron, P.Kocher and D. Naccache, "Statistics and Secret Leakage," FC 2001, LNCS 1962, pp. 157-173, 2001.

[14] J.S. Coron, E. Prouff and M. Rivain, "Side Channel Cryptanalysis of a Higher Order Masking Scheme," CHES 2007, LNCS 4727, pp. 28–44, 2007.
[15] J.S. Coron, E. Prouff and T. Roche, "On the Use of Shamir's Secret Sharing against Side-Channel Analysis," CARDIS 2012, LNCS 7771, pp. 77–90, 2013.
[16] G. Dabosville, J. Doget and E. Prouff, "A New Second-Order Side Channel Attack Based on Linear Regression," IEEE Trans. on Computers, vol. 62, No.8, pp. 1629-1640, 2013.
[17] J. Doget, E. Prouff, M. Rivain and F.X. Standaert, "Univariate side channel attacks and leakage modeling," Journal of Cryptographic Engineering, Vol.1, No.2, pp.123-144, 2011.
[18] A.A. Ding, L.W. Zhang, Y.S. Fei and P.Luo, "A Statistical Model for Higher Order DPA on Masked Devices," CHES 2014, LNCS 8731, pp. 147–169, 2014.
[19] M.A. Elaabid, O. Meynard, S. Guilley and J.L. Danger, "Combined Side-Channel Attacks," WISA 2010, LNCS 6513, pp. 175–190, 2011.
[20] S. Guilley, P. Hoogvorst and R. Pacalet, "Differential Power Analysis Model and Some Results," CARDIS 2004, KAP 153, pp. 127-142, 2004.
[21] L.Genelle, E. Prouff and M. Quisquater, "Secure Multiplicative Masking of Power Functions," ACNS 2010, LNCS 2010, pp. 200-217, 2010.
[22] L. Genelle, E. Prouff and M. Quisquater, "Thwarting Higher-Order Side Channel Analysis with Additive and Multiplicative Maskings," CHES 2011, LNCS 6917, pp. 240–255, 2011.
[23] C. Herbst, E. Oswald and S. Mangard, "An AES Smart Card Implementation Resistant to Power Analysis Attacks," ACNS 2006, LNCS 3989, pp. 239–252, 2006.
[24] A. Heuser, O. Rioul and S. Guilley, "A Theoretical Study of Kolmogorov-Smirnov Distinguishers," COSADE 2014, LNCS 8622, pp. 9–28, 2014.
[25] A. Heuser, O. Rioul and S. Guilley, "Good Is Not Good Enough: Deriving Optimal Distinguishers from Communication Theory," CHES 2014, LNCS 8731, pp. 55–74, 2014.
[26] A. Heuser and M. Zohner, "Intelligent Machine Homicide - Breaking Cryptographic Devices Using Support Vector Machines," COSADE 2012, LNCS 7275, pp. 249–264, 2012.
[27] M. Joye, P. Paillier and B. Schoenmakers, "On Second-Order Differential Power Analysis," CHES 2005, LNCS 3659, pp. 293–308, 2005.
[28] L. Lerman, G. Bontempi, S.B. Taieb and O. Markowitch, "A Time Series Approach for Profiling Attack," SPACE 2013, LNCS 8204, pp. 75–94, 2013.
[29] L. Lerman, S.F. Medeiros, N. Veshchikov, C. Meuter, G. Bontempi and O. Markowitch, "Semi-Supervised Template Attack," COSADE 2013, LNCS 7864, pp. 184–199, 2013.

[30] K. Lemke-Rust and C. Paar, "Analyzing Side Channel Leakage of Masked Implementations with Stochastic Methods," ESORICS 2007, LNCS 4734, pp. 454-468, 2007.

[31] J.Q. Lu, J. Pan and J.D. Hartog, "Principles on the Security of AES against First and Second-Order Differential Power Analysis," ACNS 2010, LNCS 6123, pp. 168-185, 2010.

[32] V. Lomné, E. Prouff and T. Roche, "Behind the Scene of Side Channel Attacks," ASIACRYPT 2013, LNCS 8269, pp. 506–525, 2013.

[33] V. Lomné, E. Prouff, M. Rivain, T. Roche and A. Thillard, "How to Estimate the Success Rate of Higher-Order Side-Channel Attacks?" CHES 2014, LNCS 8731, pp. 35–54, 2014.

[34] H.Y. Liu, G.Y. Qian, S. Goto and Y. Tsunoo, "Correlation Power Analysis Based on Switching Glitch Model," WISA 2010, LNCS 6513, pp. 191–205, 2011.

[35] Z. Martinasek, J. Hajny and L. Malina, "Optimization of Power Analysis Using Neural Network," CARDIS 2013, LNCS 8419, pp. 94–107, 2014.

[36] R. Menicocci, A. Simonetti, G. Scotti and A. Trifiletti, "On Practical Second-Order Power Analysis Attacks for Block Ciphers," ICICS 2009, LNCS 6476, pp. 155-170, 2009.

[37] R. A. Muijrers, J.G.J. van Woudenberg and L. Batina, "RAM: Rapid Alignment Method," CARDIS 2011, LNCS 7079, pp. 266–282, 2011.

[38] D. Oswald and C. Paar, "Improving Side-Channel Analysis with Optimal Linear Transforms," CARDIS 2012, LNCS 7771, pp. 219–233, 2013.

[39] E. Prouff, "DPA Attacks and S-Boxes," FSE 2005, LNCS 3557, pp. 424-441, 2005.

[40] E. Prouff and T. Roche, "Attack on a Higher-Order Masking of the AES Based on Homographic Functions," INDOCRYPT 2010, LNCS 6498, pp. 262–281, 2010.

[41] O. Reparaz, B. Gierlichs and I. Verbauwhede, "A note on the use of margins to compare distinguishers," COSADE 2014, LNCS 8622, pp. 1–8, 2014.

[42] O. Reparaz, B. Gierlichs and I. Verbauwhede, "Generic DPA attacks: curse or blessing?" COSADE 2014, LNCS 8622, pp. 98–111, 2014.

[43] C. Rechberger and E. Oswald, "Practical Template Attacks," WISA 2004, LNCS 3325, pp. 440–456, 2004.

[44] Y. Souissi, S. Bhasin, S. Guilley, M. Nassar and J.L. Danger, "Towards Different Flavors of Combined Side Channel Attacks," CT-RSA 2012, LNCS 7178, pp. 245-259, 2012.

[45] F.X. Standaert, B. Gierlichs and I. Verbauwhede, "Partition vs. Comparison Side-Channel Distinguishers: An Empirical Evaluation of Statistical Tests for Univariate Side-Channel Attacks against Two Unprotected CMOS Devices," ICISC 2008, LNCS 5461, pp.

253-267, 2009.

[46] F.X. Standaert, F. Koeune and W. Schindler, "How to Compare Profiled Side-Channel Attacks?" ACNS 2009, LNCS 5536, pp. 485-498, 2009.

[47] F.X. Standaert, T.G. Malkin and M. Yung, "A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks," EUROCRYPT 2009, LNCS 5479, pp. 443-461, 2009.

[48] F.X. Standaert, E. Peeters, C. Archambeau and J.J. Quisquater, "Towards Security Limits in Side-Channel Attacks," CHES 2006, LNCS 4249, pp. 30–45, 2006.

[49] D. Suzuki, M. Saeki and T. Ichikawa, "DPA Leakage Models for CMOS Logic Circuits," CHES 2005, LNCS 3659, pp. 366–382, 2005.

[50] P. Schaumont and K. Tiri, "Masking and Dual-Rail Logic Don't Add Up," CHES 2007, LNCS 4727, pp. 95–106, 2007.

[51] A. Thillard, E. Prouff and T. Roche, "Success through Confidence: Evaluating the Effectiveness of a Side-Channel Attack," CHES 2013, LNCS 8086, pp. 21–36, 2013.

[52] N. Veyrat-Charvillon, B. Gérard and F.X. Standaert, "Security Evaluations beyond Computing Power," EUROCRYPT 2013, LNCS 7881, pp. 126-141, 2013.

[53] C. Whitnall and E. Oswald, "A Fair Evaluation Framework for Comparing Side-Channel Distinguishers," Journal of Cryptographic Engineering. Vol.1, No.2, pp.145-160, 2011.

[54] J.G. J. van Woudenberg, M.F. Witteman and B. Bakker, "Improving Differential Power Analysis by Elastic Alignment," CT-RSA 2011, LNCS 6558, pp. 104-119, 2011.

[55] X. Ye and T. Eisenbarth, "Wide Collisions in Practice," ACNS 2012, LNCS 7341, pp. 329-343, 2012.