Regular Paper

Communications of the CCISA
Vol. 29 No. 4 Nov. 2023

基於自動編碼器消除雜訊對旁通道攻擊的干擾實作與分析

郭崇韋[1*]、蔡國裕[2]、翁偉銘[3]、林駿璋[4]、洪宇義[5]、汪冠伶[6]
[1,2,3,4,5]逢甲大學資訊工程學系、[6]逢甲大學經濟學系
[1]cwkuo@mail.fcu.edu.tw、[2]nicklas@seed.net.tw、[3]willy890913@gmail.com、
[4]M1205003@o365.fcu.edu.tw、[5]M1221097@o365.fcu.edu.tw、[6]my890823@gmail.com

摘要

旁通道攻擊(Side Channel Attack, SCA)屬於硬體攻擊的方式，透過裝置的運算晶片在執行加密演算法的過程中，竊取敏感資訊的攻擊方式。當晶片運作時，內部電路的動作，將產生功率消耗以及電磁輻射，攻擊者可利用有線或無線的感應探棒，擷取晶片的電源接腳或外洩的輻射，在蒐集大量的訊號後進行特徵分析，將加密演算法的金鑰資訊透過統計或是機器學習的方法推測，如此造成電子裝置極大的威脅。在預防 SCA 上，可採用在輸出的訊號上添加雜訊，降低攻擊的成功率，常用作法是在控制晶片的電源接腳添加雜訊，以干擾原始的特徵，防禦攻擊。本論文採用自動編碼器(Auto Encoder, AE)，實作於 ChipWhisperer 硬體電路中，將摻入雜訊的訊號跡線進行預處理，消除雜訊干擾，提高了攻擊成功率，此外，也將加密演算法實作於 Arduino Uno 實驗板，並提出運用濾波電容抑制電源的輸出特徵訊號，有效的防禦相關性消耗功率分析(Correlation Power Analysis, CPA)攻擊的成功率。

關鍵詞：旁通道攻擊、功率消耗、電磁輻射、機器學習、雜訊、自動編碼器

* 通訊作者 (Corresponding author.)

Regular Paper

Communications of the CCISA
Vol. 29 No. 4 Nov. 2023

Implementation and Analysis of Side-Channel Attack Mitigation Based on Autoencoder

Chung-Wei Kuo[1*], Kuo-Yu Tsai[2] , Wei-Ming Weng[3], Chun-Chang Lin[4], Yu-Yi Hong[5], Guan-Lin Wang[6]
[1,2,3,4,5]Department of Information Engineering and Computer Science, Feng Chia University
[6]Department of Economics, Feng Chia University
[1]cwkuo@mail.fcu.edu.tw, [2]nicklas@seed.net.tw, [3]willy890913@gmail.com,
[4]M1205003@o365.fcu.edu.tw, [5]M1221097@o365.fcu.edu.tw, [6]my890823@gmail.com

Abstract

A side-channel attack is a method of stealing confidential data from a computer chip's encryption process. This kind of attack specifically targets a computing device's hardware by exploiting its power consumption and electromagnetic radiation discharge while operational. Attackers may use wired or wireless probes to try and access the chip's power pins or intercept the leaked radiation. After collecting a lot of signals, they analyze the features using statistics and machine learning to figure out the key information of the encryption algorithm. This is a big danger to the device's security. To prevent SCA, they can add noise to the output signal. This makes the attack less effective. Injecting noise is an often used method. Introducing noise into the power pins of a chip can disrupt its original features and use the noise waveform as a defense against attacks. Our research presents a novel approach to improve the efficacy of side-channel attacks. We employ an autoencoder (AE) to preprocess noised signal traces, which is seamlessly integrated into the ChipWhisperer hardware. The AE excels at significantly reducing interference caused by noise, which ultimately enhances the effectiveness of the side-channel attacks. We tested the encryption algorithm on the Arduino Uno board and introduced a strategy to reduce distinctive signals produced by the power supply through a filter capacitor. This approach is a highly effective defense against correlation power analysis (CPA) attacks.

Keywords: Side-Channel Attack, Power Consumption, Electromagnetic Radiation, **Machine Learning**, **Noise**, **Autoencoder**

壹、前言

隨著物聯網(IoT, Internet of Thing)應用領域的快速發展，許多應用透過 IoT 感測元件實現智慧化，例如將感測元件與車聯網系統結合[1]，實現車輛間的交通資訊共享，使車輛能夠自動規劃行程和避開交通擁擠的道路。然而，這些應用也面臨著嚴重的安全威脅。攻擊者可以利用 IoT 裝置在執行計算時產生的功率消耗或外洩的電磁輻射，進行 SCA 以竊取敏感資訊，例如個人隱私和加密的金鑰。

SCA 是一種利用加密系統物理實現中的特性，而不是攻擊加密演算法本身。在執行加密演算法期間，硬體裝置會產生各種物理訊號，例如電磁輻射[2]、功率消耗[3]、執行時間等。這些訊號會受到金鑰資訊的影響，形成相關性，攻擊者可以通過分析這些訊號中的相關性，來獲取訊號的重要特徵。根據攻擊方法的不同，SCA 可以分為兩大類：直接攻擊和分析攻擊。其中，直接攻擊是針對攔截到的訊號進行分析，例如簡單功率分析(Single Power Analysis, SPA)和差分功率分析(Differential Power Analysis, DPA)等。而分析攻擊則是使用已知的數據集訓練攻擊模型，然後對實際測量到的訊號進行分析，這包括模板攻擊(Template Attack, TA)[4]和基於機器學習的攻擊方法[5][6][7][8]。為了防禦晶片受到 SCA，常用的對策為掩蔽和隱藏。掩蔽對策是將敏感資訊分割成不同的部分，以減少對金鑰的依賴性[9][10]。例如，利用分組加密技術將金鑰分割成不同的區塊，並在每個區塊上進行加密。另一個隱藏對策，是在輸出訊號添加雜訊，以使攻擊者無法提取有效的特徵，達到保護訊號安全傳送。例如，直接向訊號中添加雜訊[11]或使用雙軌邏輯設計[12]。因此，使用 SCA 雖然能取出特徵，但會造成這些特徵的相關性下降，攻擊就會變得不再有效。為了解決這個問題，常用的方法包括低通濾波器[13]、執行軌跡對齊[14]以及各種特徵工程[15][16]方法來消除保護對策的干擾。然而，近年來，研究學者開始探索使用深度學習技術來進行有效特徵提取[17]，通過學習訊號跡線中的相關性，還原未加雜訊的訊號。

在參考文獻[18][19]提出以 AE 的機制來消除雜訊的干擾，文中提到 ASCAD 資料集，雖然加入了保護的雜訊，仍可去除雜訊，使得擷取到的訊號跡線可容易被提取金鑰。有鑑於該研究的成果，本研究提出運用此機制來進行實體電路真實訊號跡線的攻擊，驗證是否能有一致性的效果，此外，針對 SCA 對於電子裝置硬體攻擊的威脅，我們引入了濾波電路的設計，成功的抑制電源接腳輸出的波形特徵，經過 2,000 條訊號跡線的攻擊，仍然無法成功的破解，具有良好防禦效果。

貳、文獻探討

本研究所運用的相關成果，如實作進階加密標準(Advanced Encryption Standard, AES)、相關功率分析(Correlation Power Analysis, CPA)、消除雜訊的 AE 機制以及濾波電

路，將於本節介紹。

2.1 進階加密標準(Advanced Encryption Standard, AES)

AES 屬於對稱式加密機制，傳送端及接收端共用一把金鑰，如此可在較高的效率下，於 IoT 的裝置控制晶片中實現。為了提高傳送資料的加密安全性，有些傳輸的系統會採用非對稱式的金鑰，系統需管理公鑰與私鑰，雖可以提高安全性，但在一般 IoT 的環境之中，多數為輕量級的微控制器，若要在其中實現非對稱式加密機制，會有執行效率的問題產生，也有部份因記憶體容量有限而無法採用。

此加密源自於 Rijndael[20][21][22]加密標準，屬於區塊加密，金鑰長度分為 128、192 以及 256 位元三類，而文本採用的是 AES-128，總長度為 16 位元組。實作 AES 演算法有 3 項重要的參數，包含加解密區塊數目、金鑰區塊數目以及運算回合次數如表一所示。

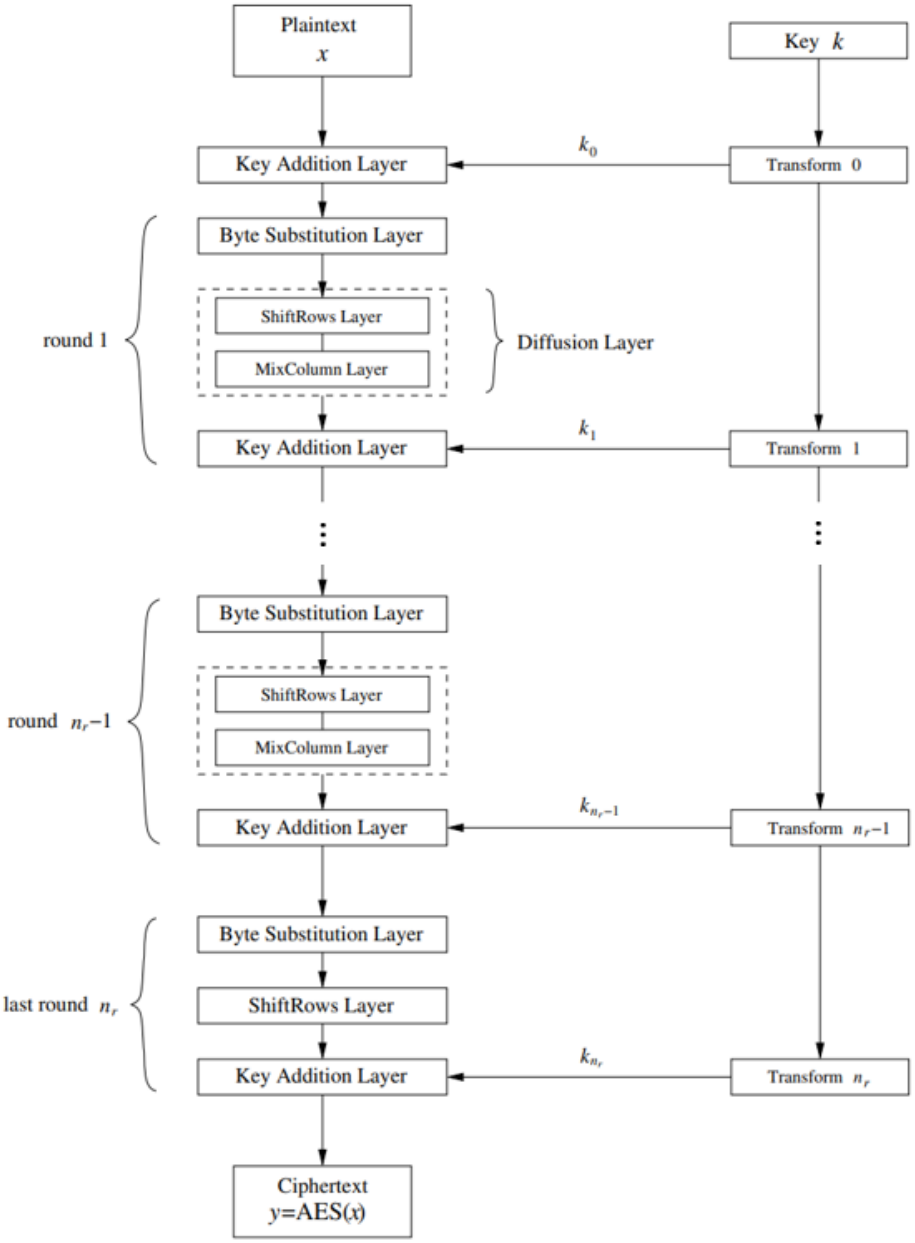
表一：三種 AES 加密演算法之運算回合數

	金鑰區塊數目	加解密區塊數目	運算回合次數
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

在各回合運算中，還包含以下 4 個步驟[23]：

1. SubBytes：將明文各個位元組替換成 S-Box 中對應的位元組，如圖一中的 Byte Substitution Layer。
2. ShiftRows：將矩陣中的每個橫列，依照列別進行不同位數之循環式移位。
3. MixColumns：使用線性轉換來混合每行內的四個位元組，另外在最後一個加密回合中省略 MixColumns 步驟。
4. AddRoundKey：矩陣中的每一個位元組都與對應之回合金鑰(Round Key)位元組做 XOR 運算。

本研究採用的攻擊目標為演算法中第一回合的金鑰與明文區塊進行 XOR 運算，觀測每次運算的功率消耗跡線，分析出每一把子金鑰(Sub-Key)的相關係數，並依分析後相關性最高的 16 位元組合併，如此將可獲取 AES-128 的主金鑰(Master Key)。



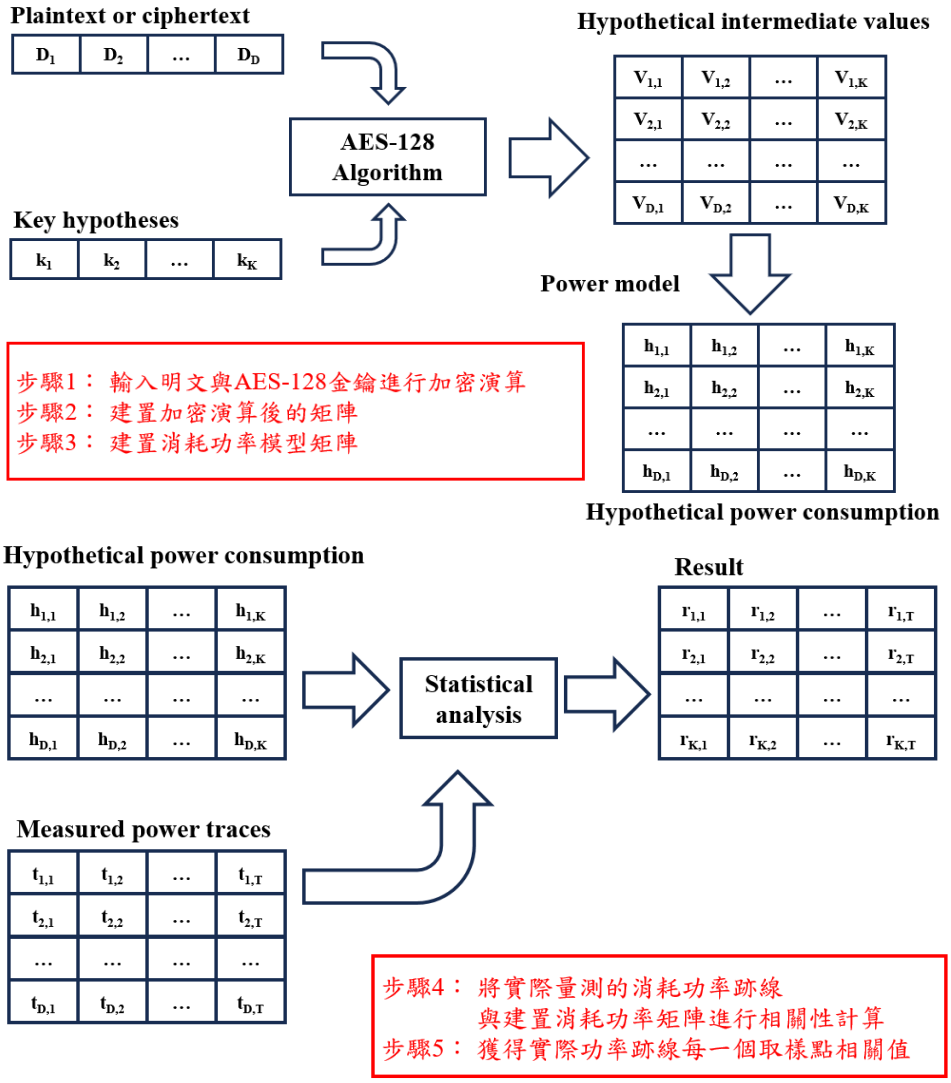
圖一：AES 加密流程圖[23]

2.2 相關功率分析(Correlation Power Analysis, CPA)

CPA 為旁通道攻擊的密鑰分析手法，由 Brier 等人在 2004 年提出[24]。CPA 為選擇明文攻擊，攻擊的目的是擷取加密系統內的安全訊息，基於被攻擊的設備在運行中的功率消耗模型進行相關係數分析，對於 AES 進行演算的第一個過程 S-Box 進行分析，此階段為明文跟金鑰間之具有線性關係的地方，也就是 16 位元組的金鑰尚未被混合的地方，因此，對這個演算的過程進行猜測。在本研究採用的方法，是透過漢明權重(Hamming Weight)建置出功率消耗模型，計算方式為利用 16 位元組的明文以及 16 位元組的金鑰進

行 XOR 運算，例如：對 2 組二進制的訊號一個一個位元計算，S1=0011 0000；S2=0010 0011，經過 S-Box 和 Hamming Weight 轉換後，求得 Hamming Weight(SBox(0001 0011))=6，攻擊步驟的每個流程如圖二所示，完成預估的模型建置，接著透過公式(1)的x, y雙變量相關係數公式求每一個取樣點的相關係數。

$$r = \frac{\sum_{i=1}^{n}(x_i - \bar{x})\,(y_i - \bar{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \bar{x})^2 \sum_{i=1}^{n}(y_i - \bar{y})^2}} \tag{1}$$



圖二：CPA 攻擊流程

2.3 去雜訊自動編碼器(Denoising Autoencoder, DAE)機制

DAE 一開始被應用在圖像上，後來也被用於進行雜訊的去除工作[19]。Wu 等人[18]使用卷積自動編碼器(Convolutional Autoencoder, CAE)實作出 DAE 並應用在功率消耗的

雜訊去除工作。表二提供 Wu 對於 CAE 選擇的參數，CAE 屬於一種 AE，與一般 AE 不同的是以 Convolutional layer 替代原本的 Hidden layer，目的在於更好的還原訊號在時間鏈的相關性。

表二：自動編碼器超參數設定表

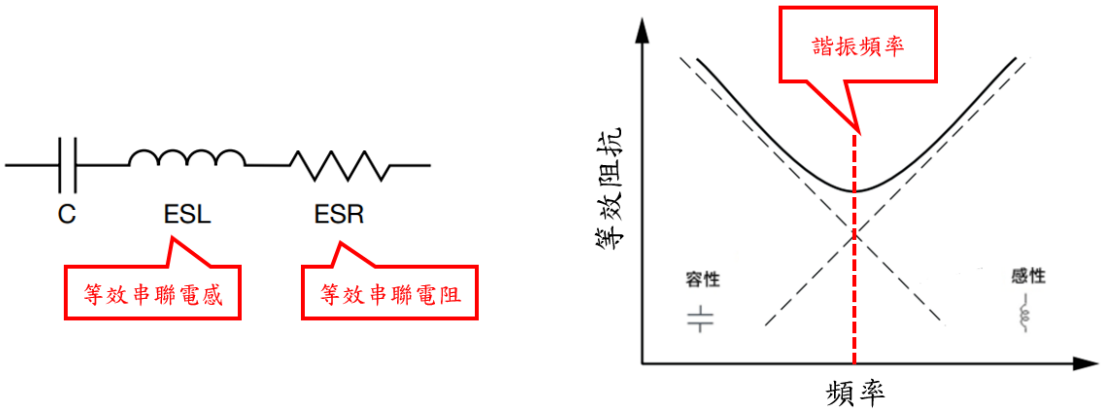
Hyperparameter	**Selected**
Optimizer	Adam
Activation function	SeLU
Batch size	128
Epochs	100
Training sets	10,000
Validation sets	5,000

Wu[18]等人使用 10,000 筆資料集進行 DAE 的訓練，每筆資料中包含一條原始之訊號與添加雜訊後的訊號，DAE 之學習目標是最小化兩者間的差異，藉由學習降低含有雜訊與未含雜訊的訊號的差異，進而讓 DAE 更好的訓練如何還原訊號。並在 5,000 筆含有雜訊的資料測試集中，運用訓練完成的 DAE 可取得相對應的 5,000 筆完成去雜訊的功率消耗訊號。

2.4 濾波電路

本研究另一個主要目的為實作加密演算的微控制器硬體電路，硬體裝置在運作過程，因操作動作的不同，將產生不同程度的雜訊，如電源、傳輸線干擾、耦合以及電磁干擾雜訊等，SCA 就是利用裝置操作時，不同動作產生的雜訊特徵，反推可能的操作行為或傳輸的資料內容。因應硬體裝置的雜訊，可採取濾波電容來過濾訊號輸出時的雜訊位準，如此可避免雜訊對於裝置操作的影響。濾波電路可由電容、電感以及電阻等元件組合而成，透過阻抗匹配的方式，將雜訊干擾抑制住，在數位電路的設計中，防止電源輸出時的雜訊干擾，最常使用電容濾波。但因硬體裝置的操作頻率範圍差異，電容濾波僅能適用於某頻段才具有抑制雜訊的效果，造成的原因為電容本身的元件特性，依文獻[25]所述，電容等效元件含有串聯等效電阻(Equivalent Series Resistance, ESR)、串聯等效電感(Equivalent Series Inductance, ESL)以及本身的電容值如圖三，其中各元件的大小視製程以及材料而定，此外，電容及電感會因頻率的不同，而產生不同的阻抗，可由公式(2)推算，當 C 和 ESL 形成串聯諧振電路，可由圖三觀察，電容的等效阻抗在諧振頻率的位置，開始反轉特性，由電容性轉換為電感性[26]，其中諧振頻率可通過公式(3)推算。為能將微控制器的輸出訊號雜訊有效抑制，需要搭配不同電容值的濾波器，數位電路設計常用的抑制雜訊的電容值如表三所示，由於電路中存在多個雜訊來源，本研究將於實

驗過程搭配能有效抑制 AES-128 加密操作時所產生雜訊特徵的電容濾波之組合，以防止旁通導攻擊破解金鑰。



(a) 電容器等效元件　　(b) 電容器寄生元件效應

圖三：電容之等效電路以及諧振頻率

$$X_C = \frac{1}{2\pi fC};\ X_L = 2\pi fL \tag{2}$$

$$f_{諧振頻率} = \frac{1}{2\pi\sqrt{C \times ESL}} \tag{3}$$

表三: 雙排直插封裝(Dual In-line Package, DIP)IC 之濾波電容建議值

電容值	有效操作頻段
10.uF	2.5 MHz
0.1uF	8 MHz
0.01uF	25 MHz

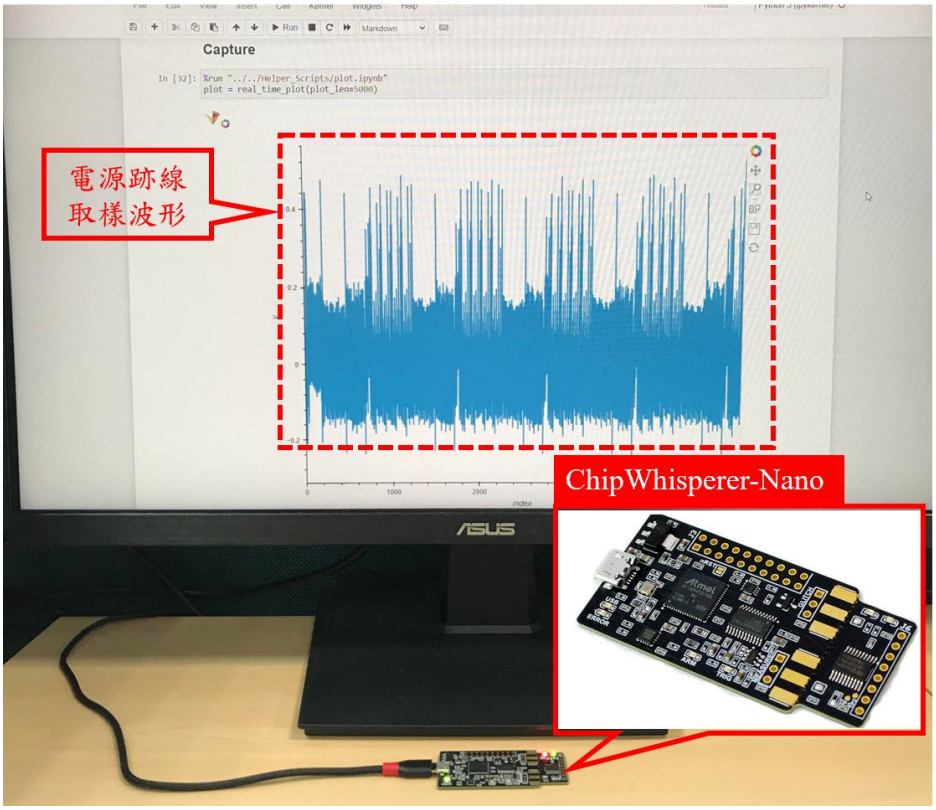
參、實驗結果

本章節將介紹 SCA 實驗的配置、訊號跡線的模擬、加入雜訊後攻擊的成果以及利用濾波電路抑制特徵訊號防禦的效益。

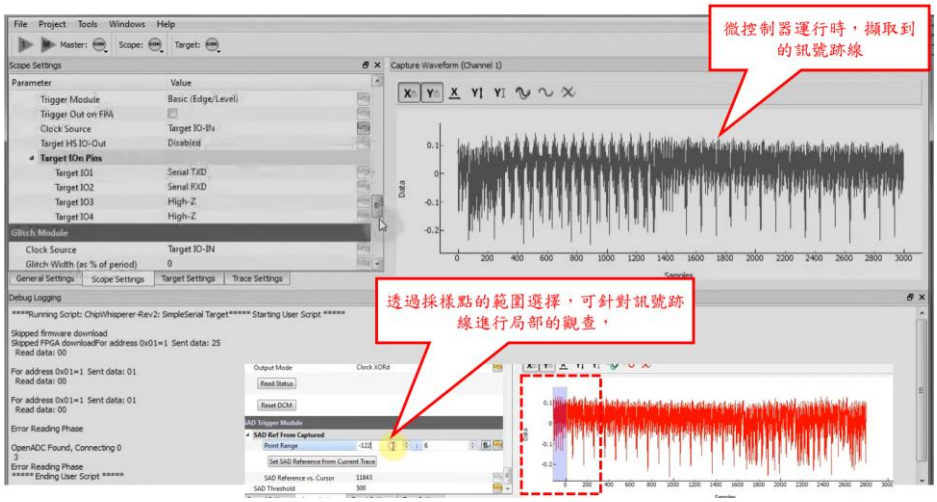
3.1 實驗的配置

本研究的實驗採用 NewAE Technology Inc.所製作的 ChipWhisperer-Nano 實驗板(如圖四，訊號的採樣率為 20MS/s，採樣的緩衝區大小為 50,000 點，實驗環境建置於 Jupyter

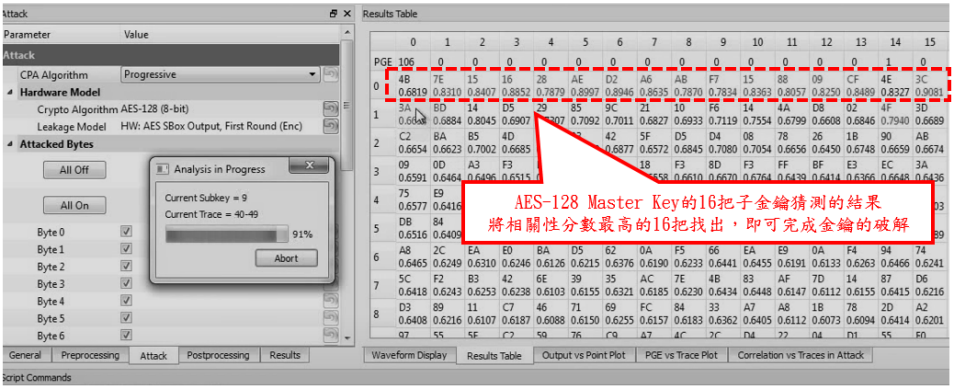
notebook，圖五為實驗板中的 8 位元類比/數位轉換器擷取硬體所產生的訊號跡線，其中可設定要觀察的訊號區段進行特徵分析，而圖六為我們實驗執行 AES-128 加密演算過程中進行攻擊的效果，0~15 代表 16 把子金鑰，金鑰猜測熵值(Private Key Guessing Entropy, PGE)的統計結果，將每一把子金鑰求出的最大值全部找出，即可達成破解的目的。



圖四：ChipWhisperer-Nano 實驗板&Jupyter Notebook 攻擊環境



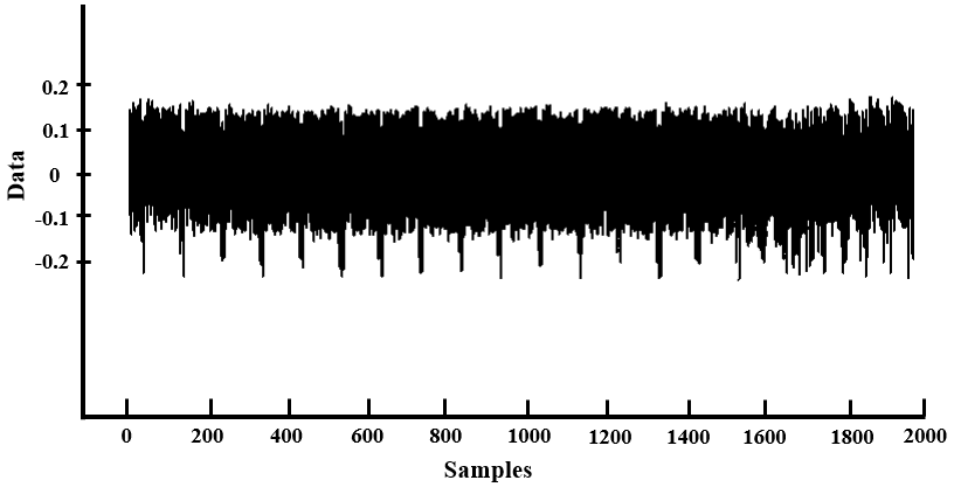
圖五：分析訊號跡線特徵的視窗畫面



圖六：AES-128 子金鑰相關性統計結果

3.2 原始訊號跡線分析

圖七為 ChipWhisperer Nano 實驗板執行 AES-128 加密運算一次的訊號跡線，透過實驗板內建 ADC 擷取硬體實際波形，我們依據這個作法，開始給予不同的明文資料，重覆執行 AES-128 演算過程，如此可以產生出不同的特徵訊號，建立攻擊訊號的模型。



圖七：原始功率訊號跡線

當攻擊模型建置完成後，接著利用 CPA 對硬體裝置實際量測到的每條訊號跡線攻擊分析，圖八左側編號代表子金鑰猜測的相關係數高低排名，共有 00~FF(256 種)的排名，接近 0 代表相關係越高，在沒有任何防禦機制的情況下，該攻擊只需 50 條以內的訊號跡線，即可將 Master Key 的 16 把子金鑰全數破解。

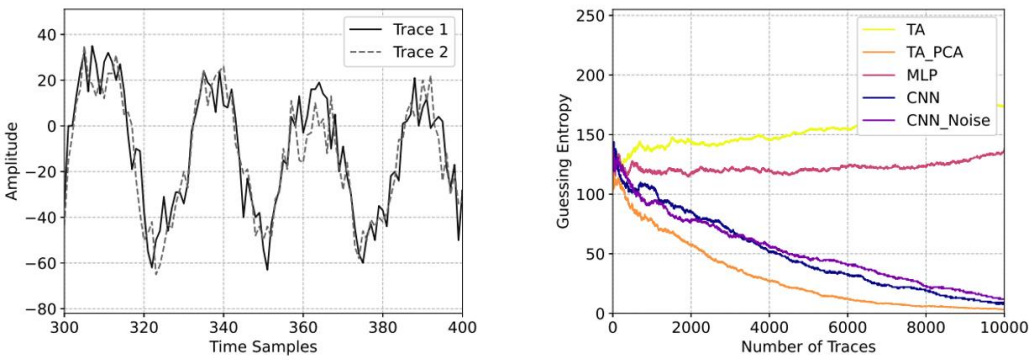
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
PGE=	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
0	C9 0.902	72 0.932	9E 0.915	BC 0.918	ED 0.900	5E 0.920	91 0.918	8D 0.940	CC 0.907	68 0.927	9C 0.906	CE 0.915	E5 0.898	1C 0.908	AD 0.907	93 0.922
1	CA 0.325	66 0.317	A2 0.319	75 0.320	F0 0.321	AB 0.327	07 0.313	EF 0.354	50 0.318	F4 0.320	1C 0.333	C0 0.299	66 0.316	F6 0.341	AE 0.371	4C 0.349
2	C4 0.313	9D 0.311	68 0.314	49 0.311	59 0.311	A3 0.314	3A 0.312	B3 0.329	FD 0.312	6B 0.307	1F 0.317	70 0.294	02 0.306	5F 0.314	33 0.311	92 0.298
3	2F 0.306	4E 0.304	81 0.299	10 0.311	CE 0.311	F6 0.294	65 0.303	F9 0.307	A3 0.305	86 0.305	15 0.308	C6 0.292	10 0.300	5D 0.312	59 0.296	67 0.293
4	F0 0.299	E3 0.299	D1 0.290	1A 0.310	5B 0.304	9B 0.294	74 0.299	A4 0.302	8D 0.289	F1 0.302	65 0.308	90 0.292	34 0.289	29 0.311	DE 0.293	3D 0.289

圖八：原始訊號之相關係數分析結果

接著採用 AE 對訊號跡線預處理，再重新攻擊，如文獻[18]成果，原始跡線使用 CNN 的攻擊方式，需經過 831 條訊號跡線才能破解，而透過 AE 的方法重建跡線後，則可以下降到 751 條，但相對於 CPA 的攻擊，這兩種方法並無獲得最佳的效果。

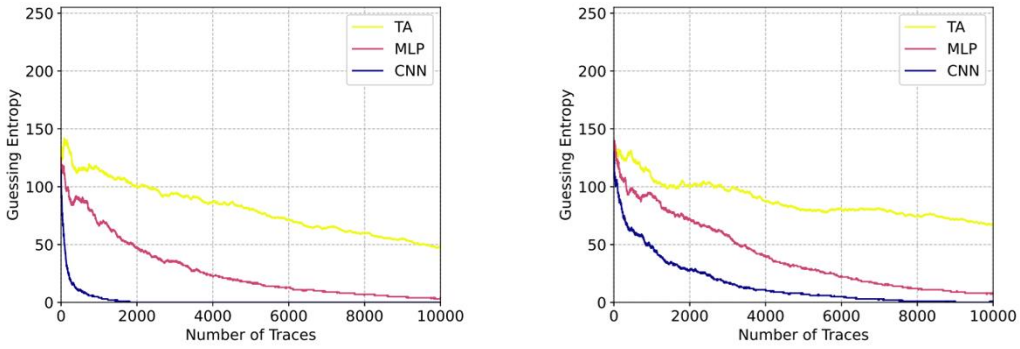
3.3 添加雜訊的訊號跡線分析

當原始訊號跡線摻入高斯雜訊後，對於不同攻擊方法的影響分析，圖九(a)為加入高斯雜訊的波形，(b)為不同攻擊方法的熵值猜測，首先是基於主要成份分析(Principal Component Analysis, PCA)的 TA 攻擊，在執行了 10,000 的跡線分析，熵值為 3 接近 0，可成功分析 AES 加密演算法之金鑰，而一般的 TA 以及多層感知器(Multilayer Perceptron, MLP)攻擊，則無法降低熵值。接著對於摻入雜訊的訊號跡線，採用 AE 預處理，也同時將訊號跡線取 10 條的平均值，在處理後的攻擊結果如圖十所示，兩個方法都能有效的將熵值收斂至 0，可成功破解 AES 加密金鑰，其中 CNN 在平均跡線的方法之下，只需要 1,754 條即可破解，該方法證明了 AE 消除高斯雜訊後，能有效提高攻擊效率。



(a) 摻入高斯雜訊的波形　　(b) 不同攻擊方法猜測的熵值比較

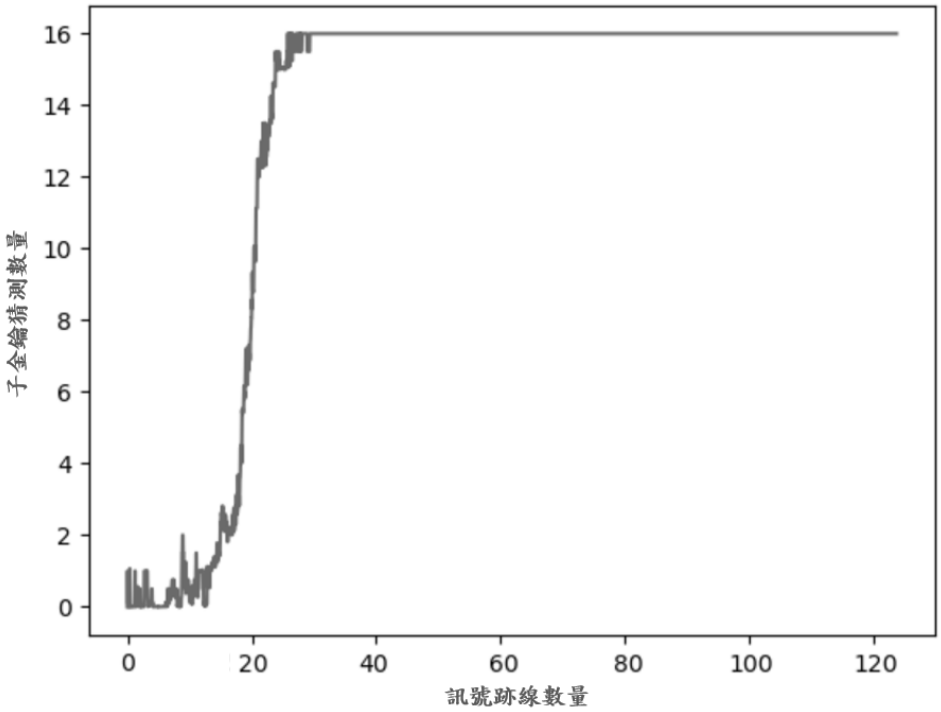
圖九：摻入高斯雜訊對於不同攻擊方法的影響[19]



(a) 取10條訊號跡線之平均值　　(b) 採用AE預處理之訊號跡線

圖十：不同攻擊方法對熵值的猜測比較[19]

圖十一為消除雜訊後硬體實驗板攻擊成果，橫軸為攻擊訊號跡線的數量，縱軸為 0~16 把子金鑰破解的數量，經 AE 的訊雜抑制，最後在 40 條以內的訊號軌跡即達成破解。



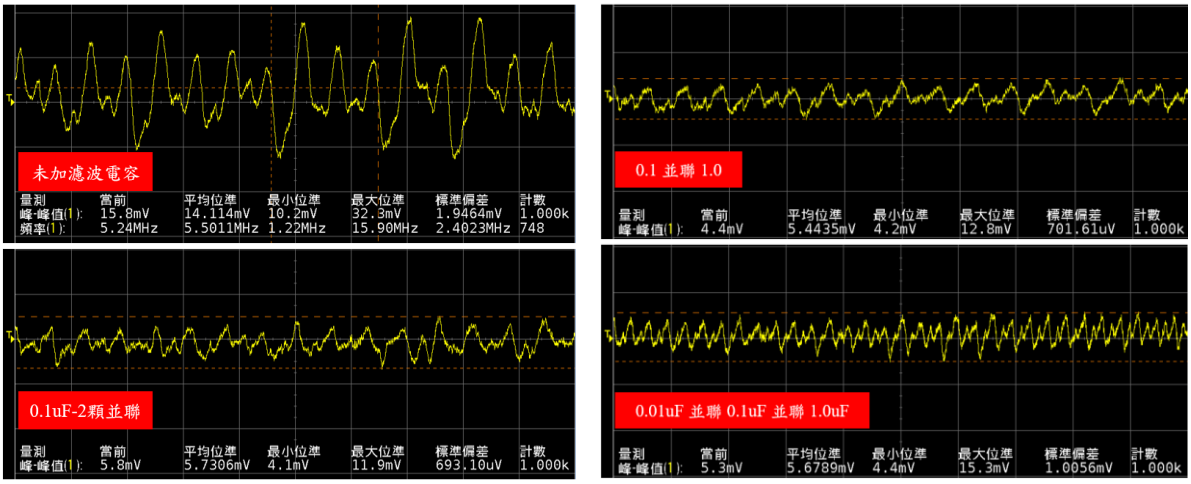
圖十一：經 AE 預處理之攻擊成果

3.4 濾波電路抑制雜訊位準之分析

根據上述模擬訊號跡線攻擊的實驗成果，本研究將 AES-128 實作於 Arduino Uno 實驗板，作者 Peng 以及 Xin[27]提出了以濾波器的方式來整合自動編碼器，使得訓練資料在重新分類後，可以得到更準確及穩定的攻擊成效，我們參考濾除雜訊的作法，引用到

硬體電路，測試能否去除電源輸出的特徵，防禦 SCA 對訊號跡線特徵分析，解析出金鑰。在印刷電路設計的技術上，若要抑制元件輸出訊號位準，可應用濾波電路調整輸出訊號的干擾，在實際的硬體電路上進行 SCA 分析，是透過有線或無線的接收探棒，擷取輸出電壓訊號跡線特徵，透過特徵的分析，使得加密金鑰的資料，逐一的比對分析，完成金鑰的破解。

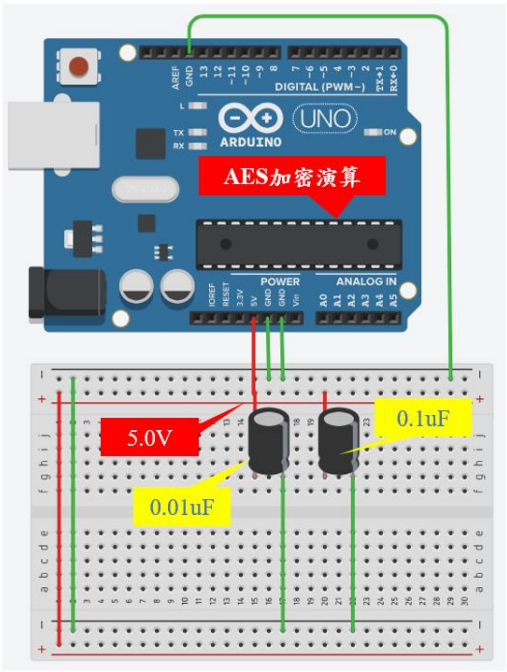
依 2.4 節的說明，本節分析不同濾波電容對於輸出雜訊值的影響，並找出最有效抑制訊號特徵的組合，由圖十二觀察可知，在進行 AES 加密演算的過程，Arduino Uno 電源輸出接腳的波形，很明顯的上下浮動，其中雜訊振幅的峰對峰值 15.8mv(本研究實驗量測數據採用 Agilent DSO6032A 示波器，對訊號取樣 1,000 次取平均值)，電路運行過程中，造成電源輸出波形雜訊的主要原因包含電路的熱雜訊、電路運作的切換雜訊以及電路資料搬移產生的雜訊。表四為一系列濾波電容對於雜訊位準抑制效果的比較，首先，利用單一電容值之電容器，依不同顆電容器並聯，可將雜訊位準的峰對峰值降至 5.73mv~6.62mv，然而，由 0.1uF 以及 1.0uF 兩顆電容器並聯的抑制效果，雜訊位準降至 5.44mv，而三顆電容並聯的最佳效果電容值分別為 0.01、0.1 及 1.0，可達到 5.68mv，濾波電容並接方式如圖十三。電容器等效電路由圖三可知，隨著操作的頻率變化，引發串聯電阻及電感效應，因此，濾波電容採用串接，會造成更嚴重的串聯元件效應。最後，選用三種並聯組合的最佳抑制效果，再次進行 SCA 分析，未加濾波電容的狀況之下，實體電路攻擊約 80 條可以破解成功，而在 0.1uF 以及 1.0uF 兩顆電容濾波電路之下，經過 2,000 條訊號跡線(如圖十三)，子金鑰被破解數在 3 以下，其餘的濾波電路組合約在 4~5 之間，驗證了採用濾波電容無法有效破解金鑰，成功防禦 SCA。



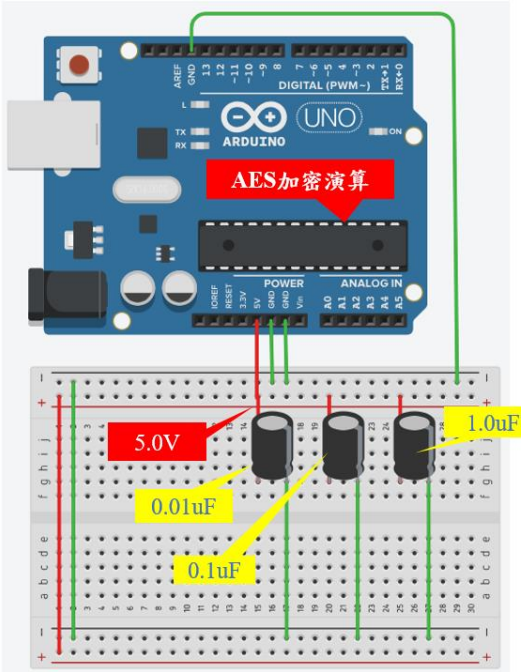
圖十二：未加濾波電容與使用濾波電容電源雜訊位準

表四：濾波電容抑制電源雜訊位準比較表

濾波電容(uF)	電源雜訊位準-峰對峰值(mV)		
	1 顆	2 顆並聯	3 顆並聯
0.01	6.62	6.44	6.40
0.1	6.60	**5.73**	6.16
1.0	6.38	6.34	6.28
10	6.14	5.65	5.94
2 顆並聯	電源雜訊位準-峰對峰值(mV)		
0.01 並聯 0.1	5.56		
0.01 並聯 1.0	5.54		
0.01 並聯 10	5.59		
0.1 並聯 1.0	**5.44**		
0.1 並聯 10	5.49		
1.0 並聯 10	5.60		
3 顆並聯	電源雜訊位準-峰對峰值(mV)		
0.01 並聯 0.1 並聯 1.0	**5.68**		
0.01 並聯 0.1 並聯 10	5.84		
0.01 並聯 1.0 並聯 10	5.99		
0.1 並聯 1.0 並聯 10	6.07		

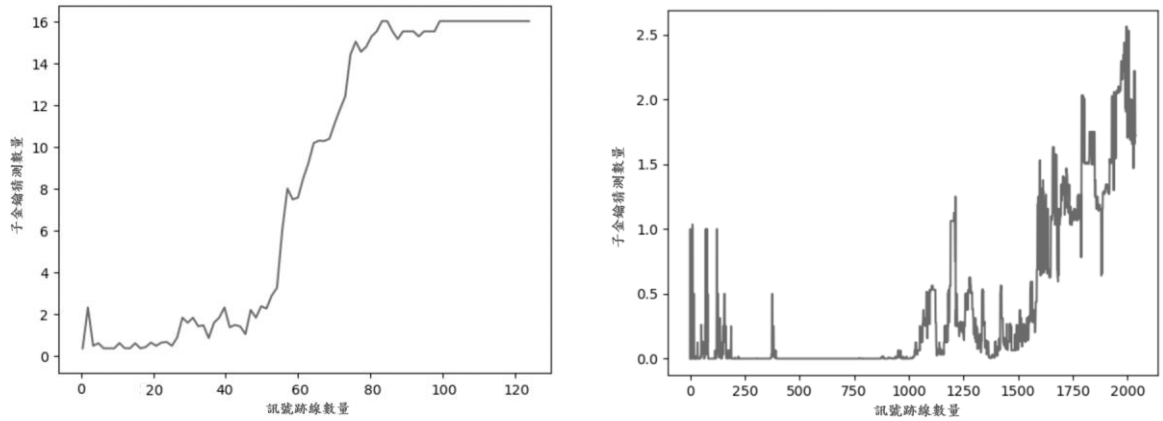


(a)使用 2 顆濾波電容示意圖



(b)使用 3 顆濾波電容示意圖

圖十三：Arduino 微控制器濾波電路示意圖



(a)未加濾波電容之攻擊效果 (b)加入 2 顆濾波電容之攻擊效果

圖十四：未加濾波電容與並聯 2 顆濾波電容之攻擊成果

肆、結論

本研究完成了在 ChipWhisperer-Nano 電路板上實作出 AE 去除雜訊的機制，並成功的提高了攻擊的成功率，一般加密裝置為防止旁通道攻擊，會透過隨機或是人為製造的方式添加雜訊於電源端，防止訊號特徵提取，而本研究採用的 AE 成功過濾加入的雜訊，獲得一個乾淨的訊號源，接著，以 CPA 的攻擊手法，進行明文與金鑰之間的漢明權重統計，透過 CPA 取得每一條訊號跡線的相關係數，在大量輸入明文的條件下，逐一的計算金鑰的相關係數，經由每個子金鑰提出的係數大小，排出最有可能的組合，最後完成 16 把子金鑰推測，達成破解的目標。在完成攻擊的目的後，我們掌握到硬體電路在遭遇旁通道攻擊的弱點，於 Arduino Uno 實驗板實作 AES-128 加密演算法，針對控制晶片電源輸出的雜訊位準進行濾波的處理，透過不同頻段作用的濾波電容，設計電容並聯電路，將晶片內部電路運作過程中，造成的電源特徵抑制，使得特徵無法被有效的提取，最後，在進行 CPA 的攻擊過程，晶片所洩露出來的訊號跡線特徵已被濾除，即使加長攻擊的時程，仍無法成功破解金鑰，證明了此方法對於 SCA 防禦的成效。

[致謝]
本研究感謝國家科學及技術委員會計畫(NSTC 112-2222-E-035-002- and NSTC 112-2221-E-035-049-)經費補助，謹此致謝。

參考文獻

[1] R. Chougule and K. Suganthi, "IoT Based Smart Car Monitoring System," *2018 Tenth*

International Conference on Advanced Computing (ICoAC), Chennai, India, 2018, pp. 281-285.

[2] K. Gandolfi, C. Mourtel, and F. Olivier, "Electromagnetic analysis: Concrete results," *In Cryptographic Hardware and Embedded Systems—CHES 2001: Third International Workshop,* Paris, France, May 14–16, 2001 Proceedings 3 (pp. 251-261).

[3] P. Kocher, J. Jaffe, B. Jun, and P. Rohatgi, "Introduction to differential power analysis," *Journal of Cryptographic Engineering*, 2011, 1, 5-27.

[4] N. Hanley, M. Tunstall, and W. P. Marnane, "Unknown plaintext template attacks. In Information Security Applications," *10th International Workshop*, WISA 2009, Busan, Korea, August 25-27, 2009, Revised Selected Papers 10 (pp. 148-162).

[5] E. Cagli, C. Dumas, and E. Prouff, "Convolutional neural networks with data augmentation against jitter-based countermeasures: Profiling attacks without pre-processing," *In Cryptographic Hardware and Embedded Systems–CHES 2017: 19th International Conference*, Taipei, Taiwan, September 25-28, 2017, Proceedings (pp. 45-68).

[6] S. Hou, Y. Zhou, and H. Liu, "Convolutional neural networks for profiled side-channel analysis," *Radioengineering*, 2019, 28(3), 651-658.

[7] H. Maghrebi, T. Portigliatti, and E. Prouff, "Breaking cryptographic implementations using deep learning techniques," *In Security, Privacy, and Applied Cryptography Engineering: 6th International Conference,* SPACE 2016, Hyderabad, India, December 14-18, 2016, Proceedings 6 (pp. 3-26).

[8] S. Picek, I. P. Samiotis, K. Kim, A. Heuser, S. Bhasin, and A. Legay, "On the performance of convolutional neural networks for side-channel analysis," *In Security, Privacy, and Applied Cryptography Engineering: 8th International Conference*, SPACE 2018, Kanpur, India, December 15-19, 2018, Proceedings 8 (pp. 157-176).

[9] G. Barthe, F. Dupressoir, S. Faust, B. Grégoire, F. X. Standaert, and P. Y. Strub, "Parallel implementations of masking schemes and the bounded moment leakage model," *In Advances in Cryptology–EUROCRYPT 2017: 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Paris, France, April 30–May 4, 2017, Proceedings, Part I 36 (pp. 535-566).

[10] S. Chari, C. S. Jutla, J. R. Rao, and P. Rohatgi, "Towards sound approaches to counteract power-analysis attacks," *In Advances in Cryptology—CRYPTO'99: 19th Annual International Cryptology Conference Santa Barbara*, California, USA, August 15–19, 1999 Proceedings 19 (pp. 398-412).

[11] C. Clavier, J. S. Coron, and N. Dabbous, "Differential power analysis in the presence of hardware countermeasures," *In Cryptographic Hardware and Embedded Systems—CHES*

2000: Second International Workshop Worcester, MA, USA, August 17–18, 2000 Proceedings 2 (pp. 252-263).

[12] K. Tiri, and I. Verbauwhede, "Securing encryption algorithms against DPA at the logic level: Next generation smart card technology," *In Cryptographic Hardware and Embedded Systems-CHES 2003: 5th International Workshop*, Cologne, Germany, September 8–10, 2003. Proceedings 5 (pp. 125-136).

[13] L. Wei, B. Luo, Y. Li, and Q. Xu, "I know what you see: Power side-channel attack on convolutional neural network accelerators," *In Proceedings of the 34th Annual Computer Security Applications Conference* (pp. 393-406), 2018.

[14] H. Thiebeauld, G. Gannerot, A. Wurcher, and C. Clavier, "Scatter: A new dimension in side-channel," *In International Workshop on Constructive Side-Channel Analysis and Secure Design* (pp. 135-152), 2018.

[15] S. Picek, A. Heuser, A. Jovic and L. Batina, "A systematic evaluation of profiling through focused feature selection," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, 27(12), 2802-2815, 2019.

[16] Y. Zheng, Y. Zhou, Z. Yu, C. Hu, and H. Zhang, "How to compare selections of points of interest for side-channel distinguishers in practice?," *In Information and Communications Security: 16th International Conference, ICICS 2014*, Hong Kong, China, December 16-17, 2014, Revised Selected Papers 16 (pp. 200-214).

[17] G. Zaid, L. Bossuet, A. Habrard, and A. Venelli, "Methodology for efficient CNN architectures in profiling attacks," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 1-36, 2020.

[18] Wu, and S. Picek, "Remove some noise: On pre-processing of side-channel measurements with autoencoders," *IACR Transactions on Cryptographic Hardware and Embedded Systems*, 389-415, 2020.

[19] L. Gondara, "Medical image denoising using convolutional denoising autoencoders," *In 2016 IEEE 16th international conference on data mining workshops (ICDMW)* (pp. 241-246). IEEE.

[20] O. Lo, W. J. Buchanan, and D. Carson, "Power analysis attacks on the AES-128 S-box using differential power analysis (DPA) and correlation power analysis (CPA)," *Journal of Cyber Security Technology*, 1(2), 88-107.

[21] A. A. Pammu, K. S. Chong, W. G. Ho, and B. H. Gwee, "Interceptive side channel attack on AES-128 wireless communications for IoT applications," *In 2016 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)* (pp. 650-653).

[22] F. E. Potestad-Ordóñez, E. Tena-Sánchez, A. J. Acosta-Jiménez, C. J. Jiménez-Fernández and R. Chaves, "Design and Evaluation of Countermeasures Against Fault Injection

Attacks and Power Side-Channel Leakage Exploration for AES Block Cipher," *in IEEE Access*, vol. 10, pp. 65548-65561, 2022.

[23] C. Paar, and J. Pelzl, *Understanding cryptography: a textbook for students and practitioners*, Springer Science & Business Media, 2009.

[24] E. Brier, C. Clavier, and Olivier, "Correlation power analysis with a leakage model," *In Cryptographic Hardware and Embedded Systems-CHES 2004: 6th International Workshop Cambridge*, MA, USA, August 11-13, 2004. Proceedings 6 (pp. 16-29).

[25] J. Cain, "The effects of ESR and ESL in digital decoupling applications," *In CARTS-CONFERENCE-* (pp. 190-194). COMPONENTS TECHNOLOGY INSTITUTE INC.

[26] XLINX, Zynq-7000 SoC PCB Design Guide, https://docs.xilinx.com/v/u/en-US/ug933-Zynq-7000-PCB (2019/3/14)

[27] W. Peng, and B. Xin, "An integrated autoencoder-based filter for sparse big data," *Journal of Control and Decision*, 2021, 8(3), 260-268.