CYBERSEC 2022 臺灣資安大會

CHANGE NOW

數位轉型　資安升級

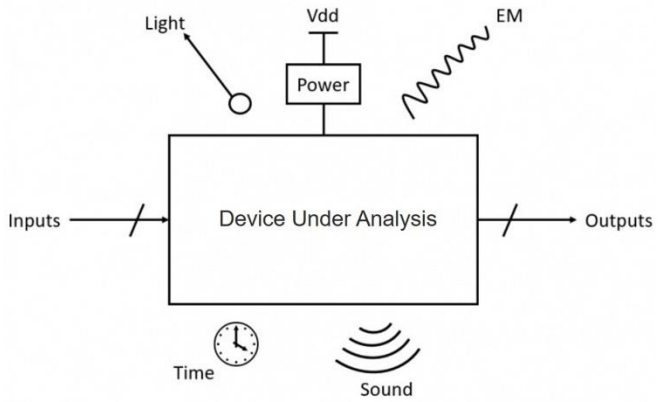
SEP. 20-22 臺北南港展覽二館

隔空抓鑰！旁通道攻擊安全探討

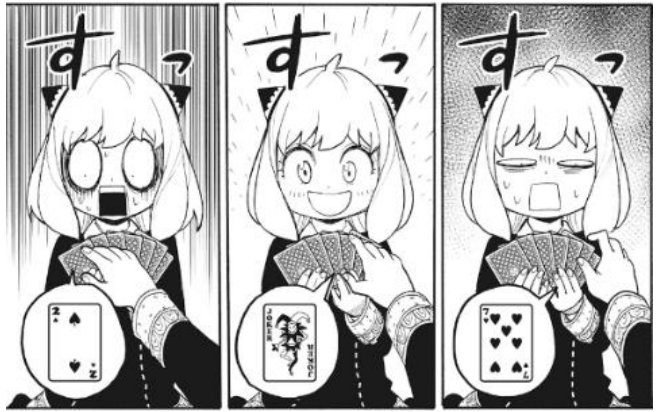
陳智偉
資策會資安所
2022.09.22

旁通道攻擊概念

In computer security, a side-channel attack is any attack based on **extra information** that can be gathered because of the **fundamental way a computer protocol or algorithm is implemented**, rather than flaws in the design of the protocol or algorithm itself. (From Wikipedia)



M. Tehranipoor and C. Wang (eds.), Introduction to Hardware Security and Trust, DOI 10.1007/978-1-4419-8080-9 8, © Springer Science+Business Media, LLC 2012



抽鬼牌: 透過對象流露出的表情變化，進行解讀與猜測

影響範圍

電話按鍵音

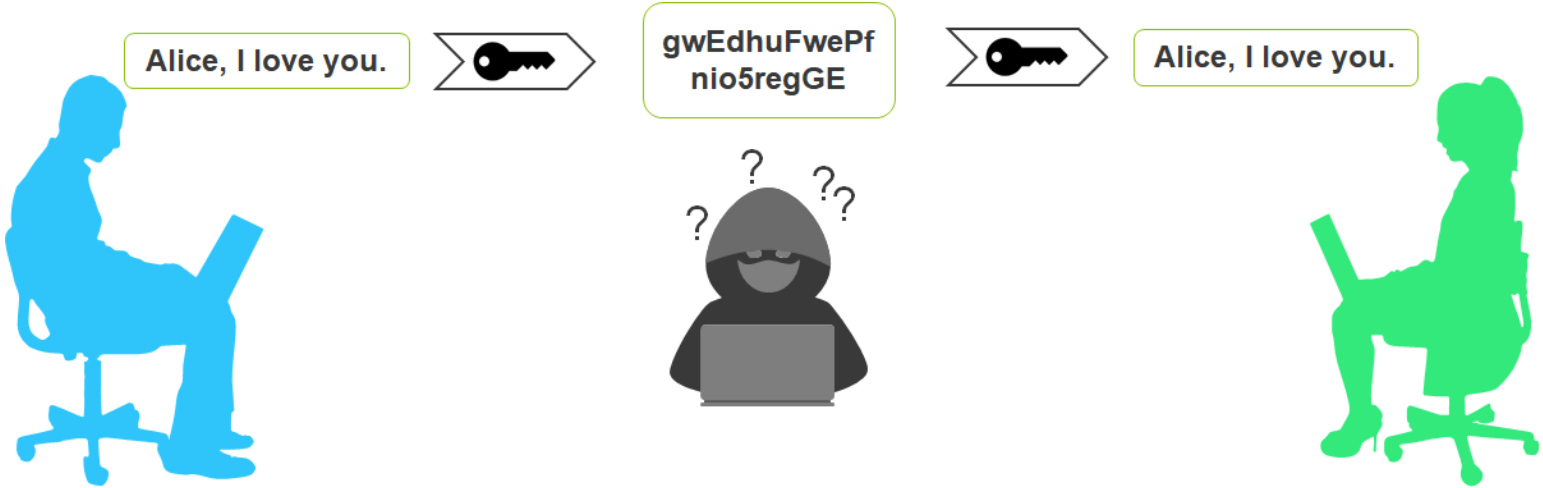
保險箱轉盤鎖

聲波造成光波的影響

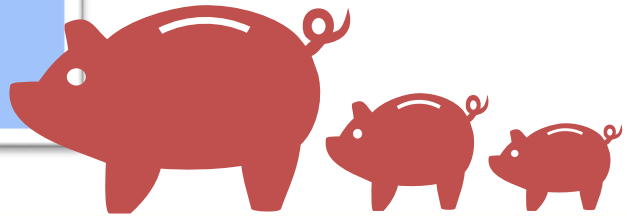
電子元件(晶片)運作

加密防護

- 為避免資料傳輸時受到有心人士竊聽(中間人攻擊)，通常採用對**資料進行加密的方式**來防護
  - Advanced Encryption Standard (AES) 進階加密標準
  - Data Encryption Standard (DES) 資料加密標準

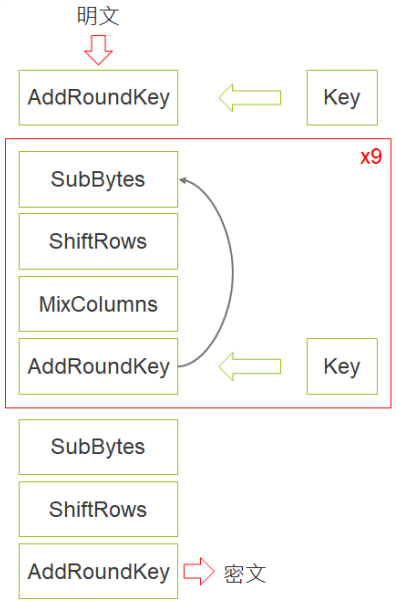


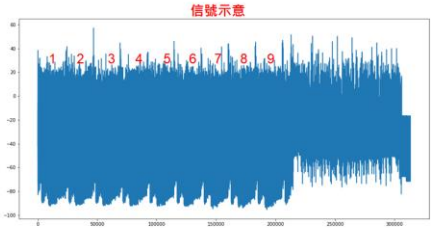
Q1：應該把陷阱放在哪裡



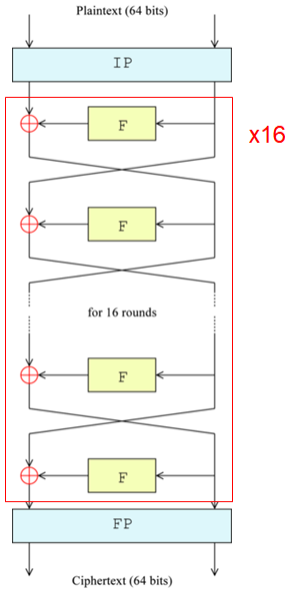
加密過程風險

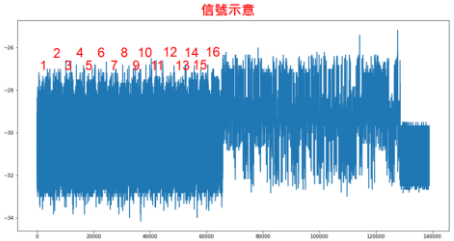
AES





DES

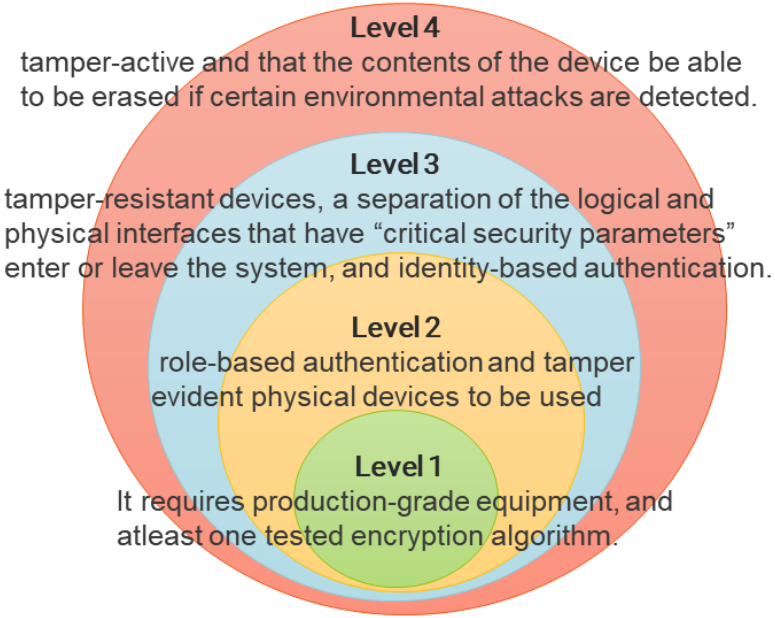




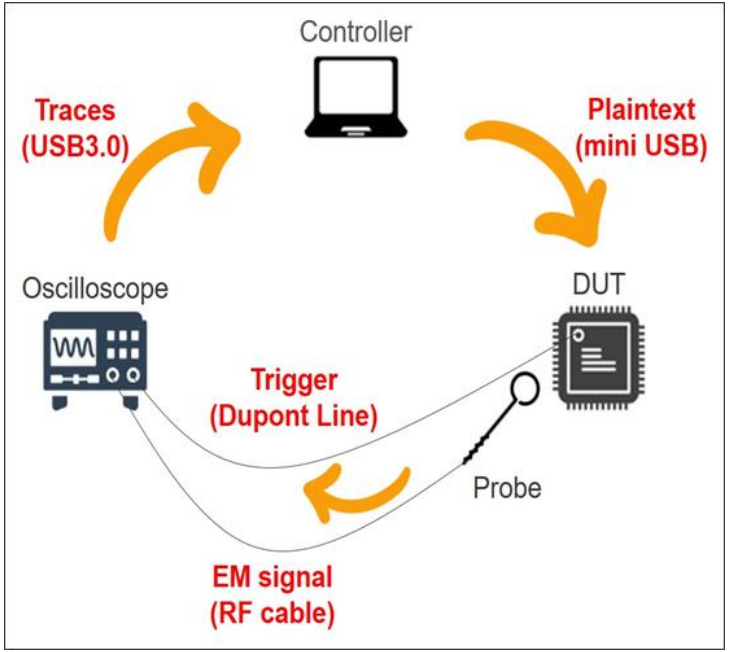
FIPS 140

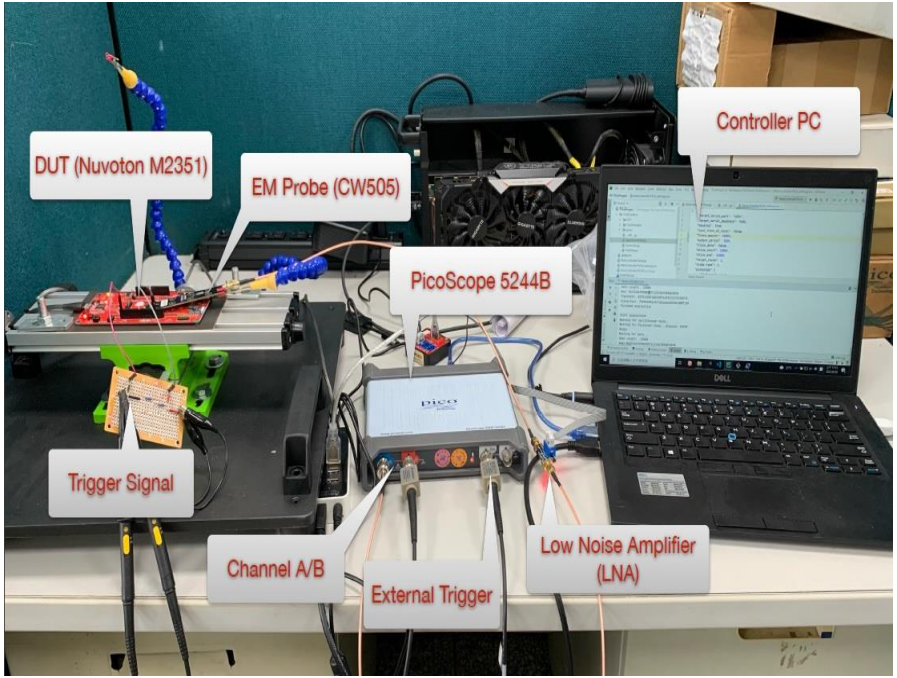
#	Security policy	說明
1	General	產品Security Level以下列最低之Level為產品的security level
2	Cryptographic Module Specification	密碼模組規格
3	Cryptographic Module Interfaces	密碼模組介面
4	Roles, Services, and Authentication	權限角色、服務、身分驗證
5	Software/Firmware Security	軟體/韌體安全
6	Operational Environment	操作環境安全
7	Physical Security	實體安全
8	Non-invasive Security	非侵入式安全
9	Sensitive Security Parameter Management	敏感參數管理
10	Self-Tests	自我測試
11	Life-cycle Assurance	生命週期保證
12	Mitigation of Other Attacks	抵擋其他攻擊方法

Security Level



檢測環境


Controller
Traces
(USB3.0)
Plaintext
(mini USB)
Oscilloscope
DUT
Trigger
(Dupont Line)
Probe
EM signal
(RF cable)


DUT (Nuvoton M2351)
EM Probe (CW505)
Controller PC
PicoScope 5244B
Trigger Signal
Channel A/B
External Trigger
Low Noise Amplifier
(LNA)

旁通道攻擊檢測流程

量測 —功率跡線集→ 信號分析 —加密區段→ 破解/評估

Measurement
- XYZ
- Scope

→ **Data selection**
- Trim samples
- Mix traces
- Transpose
- Split

→ **Data processing**
- Resample
- Pattern resample
- Windowed resample
- Compress
- Moving average
- Abs
- Low pass
- Binary
- Chain
- Filter

→ **Alignment**
- Static alignment
- Dynamic alignment
- Round alignment
- Elastic Average

→ **Statistics & Analysis**
- Average
- Standard deviation
- Statistics
- Correlation
- Cross correlation
- Analysis

→ **Crypto**
- TVLA
- NICV
- SNR
- 洩漏指標
- First order analysis
- AES chosen input FOA
- DES partly constant
- RSA high order
- ECC byte-multiply
- 破密

→ **Report**

信號分析

- **理解信號參數**

  信號頻率 vs 取樣率

  Downsampling、Resampling vs Raw trace of samples

- **濾波器應用**

  選用適當之濾波器以過濾雜訊

- **感興趣區域**

  利用經驗與分析方法找尋可能的加密區段

- **對齊(Alignment)**

  根據框選範圍，統一整理要破解的區段

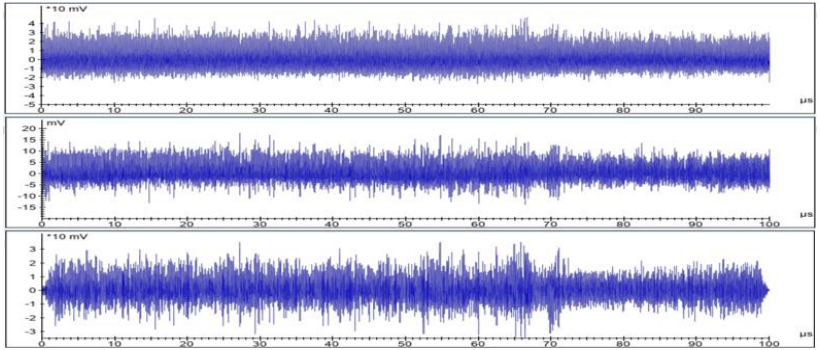
- **加密演算法**

  加密運作過程的特徵(AES:9個Round Des:16個Round)

raw trace

resample

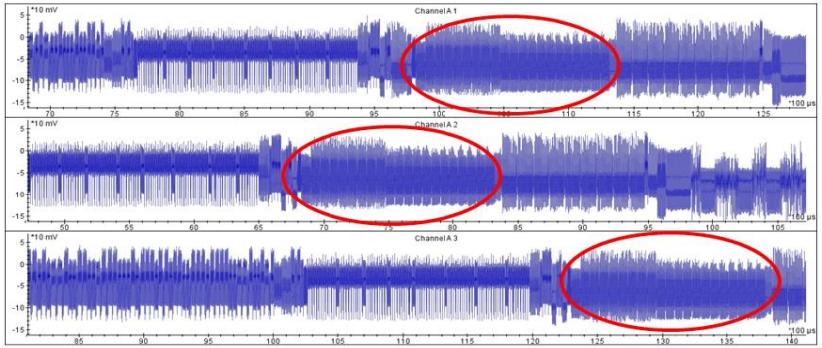
filter



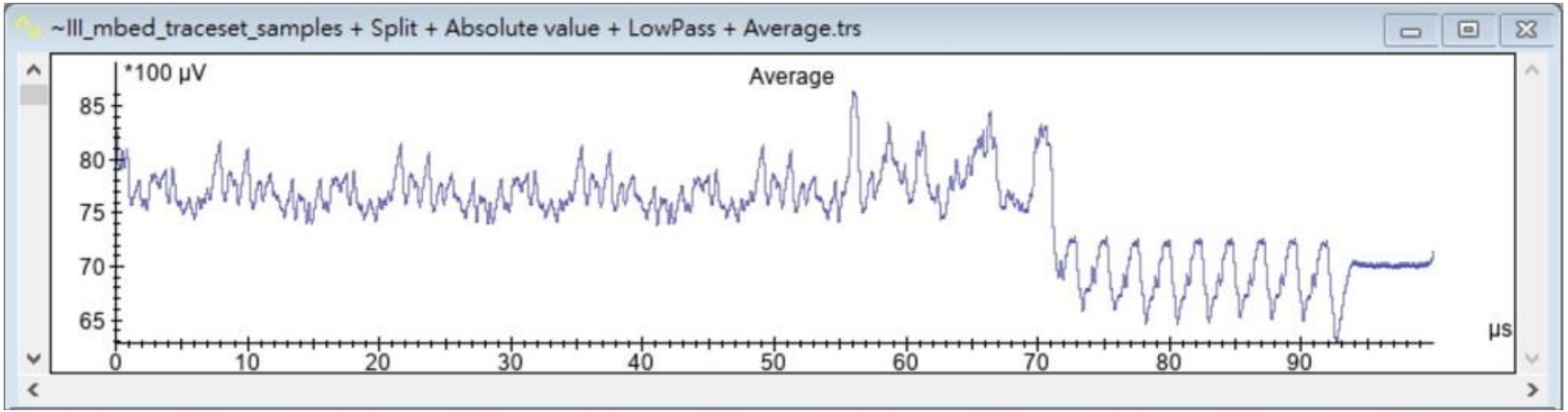
Trace # 0

Trace # 1 (Ref.)

Trace # 2



Q2：猜猜哪裡有九個ROUND



檢測分析所需時間

	Activity	Indicative time: easy – high end
1	Talk to the chip	
2	Mount your probe, trigger, oscilloscope	
3	Find the crypto signal	4 hrs - 5 days
4	Create the most efficient measurement setup	
5	Perform measurements (e.g. 1k – 20m)	
6	Post processing, e.g. alignment	1 day – 15 days
7	Differential analysis of crypto (DPA)	
8	Key leakage interpretation & reporting	

ParaLink Paralink Networks, Inc.

riscure

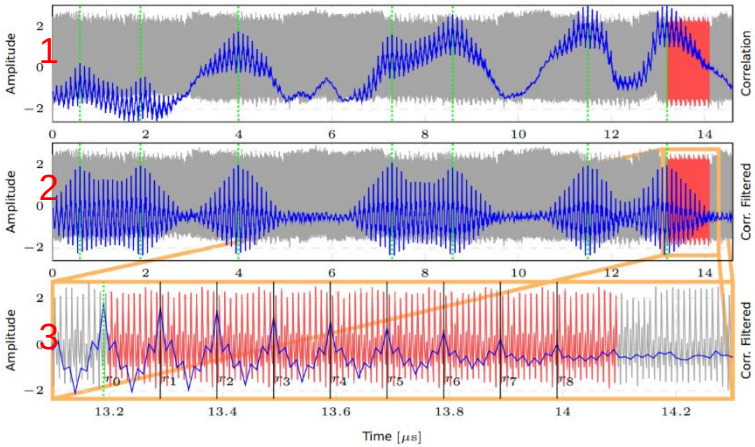
資料來源
https://www.paralink.com.tw/
https://www.riscure.com/

加密區段智慧定位

- 自動化旁通道資訊分析流程，減少分析所需背景知識，降低硬體檢測技術跨入門檻

學界技術Survey

- 此技術透過硬體資訊推估一次之加密時間後，以AES有重複九回之特性建立九個相連固定長之模板，計算九個模板間之相似分數，以此得知加密起點。
- 此技術可適用於不同平台，如果能正確推估加密時間，就能抓取加密區段之起點。



1. 固定模板寬度(紅色)取EM軌跡(灰色)和模板之間的疊加相關性(藍色)
2. 將算好之疊加相關性曲線透過移動平均過濾
3. 最後即可取出相關性分數較高的點為加密起點

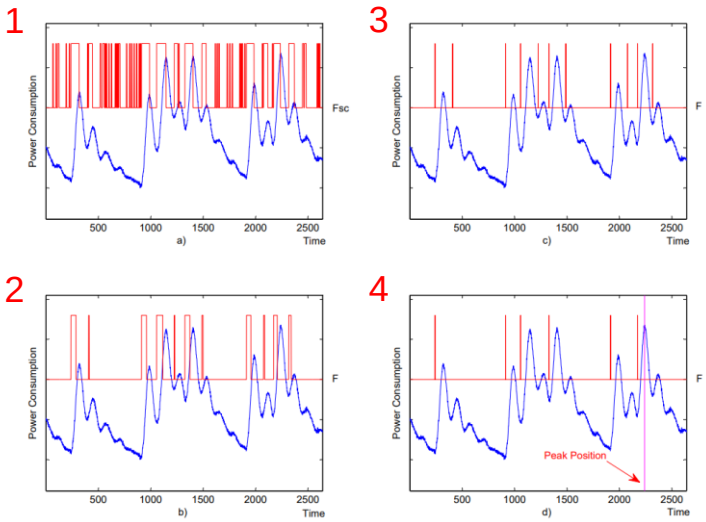
ref: Semi-Automatic Locating of Cryptographic Operations in Side-Channel Traces

學界技術Survey2

- 此技術透過計算訊號中點與點之間的差值(即斜率)，推估訊號中之波峰分佈，再藉由比對各個大小波峰得知可能之加密起點。
- 此技術藉由訊號趨勢之方式，可克服示波器錄製時所造成功耗雜訊振幅過大之問題。

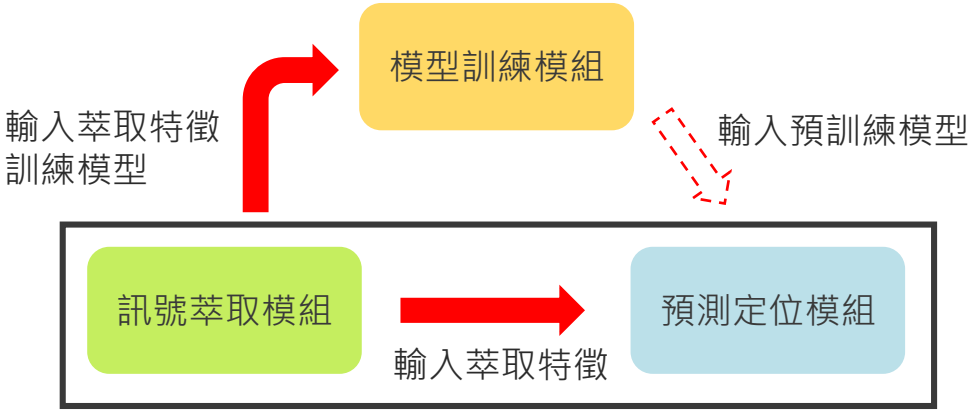
1. 計算訊號點與點之間的斜率，並標記正斜率
2. 將標記點連接，取一閥值將過短區域刪除
3. 取出剩餘區域的起始點，即為各個主(子)峰之起點
4. 比對子峰之間的值取出主峰，即為加密起點

ref: A General Approach to Power Trace Alignment for the Assessment of Side-Channel Resistance of Hardened Cryptosystems



加密區段技術架構

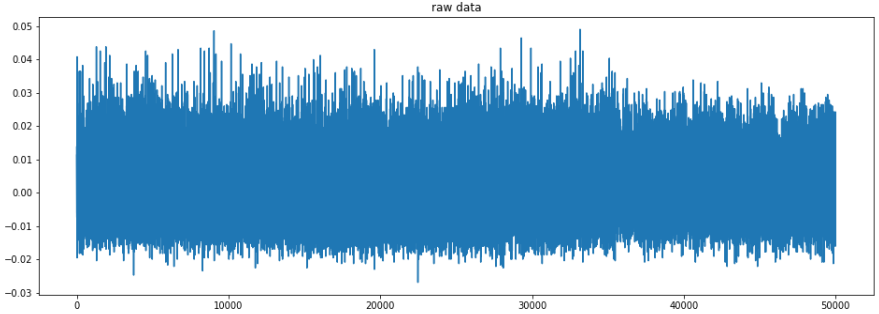
- 本技術整體架構主要分為三部分：
  - 訊號萃取模組
  - 模型訓練模組
  - 預測定位模組



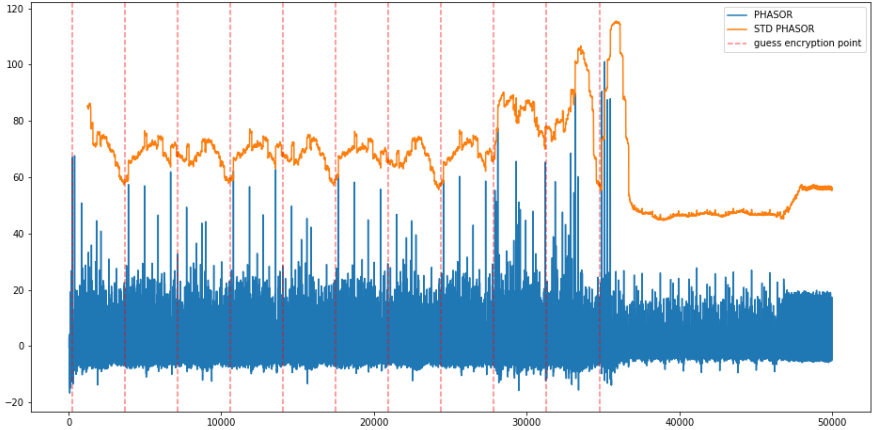
訊號萃取模組

- 利用Hilbert Transform，結合滑動窗口計算標準差，以此做為輸入機器學習模型之資料。

原始訊號



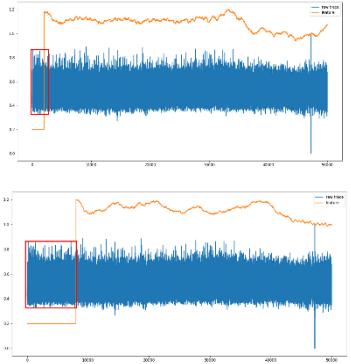
處理後訊號

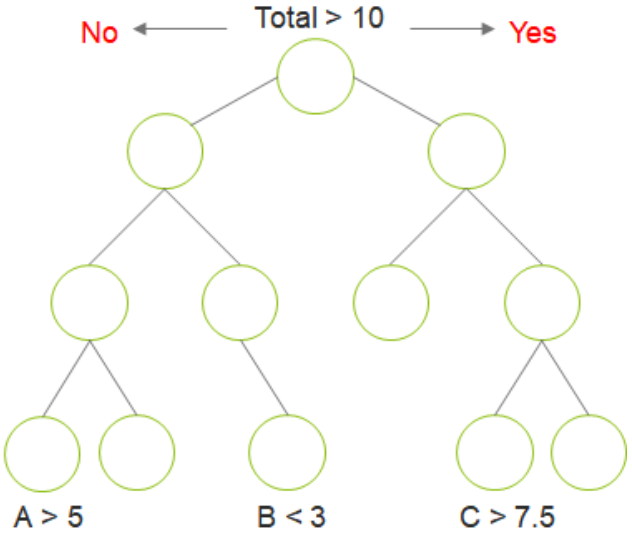


模型訓練模組

- 本技術選用隨機森林(Random Forest)為機器學習模型，透過萃取訊號之特徵後，學習Trace Sample點與點之間特徵的差異將其分類，以此來對點進行分類。

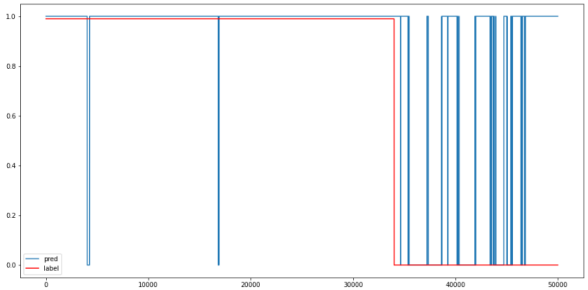
- 隨機森林是一種決策樹，藉由學習評估每個點上不同之決策，最後得出一個加權總分來分類最後結果。



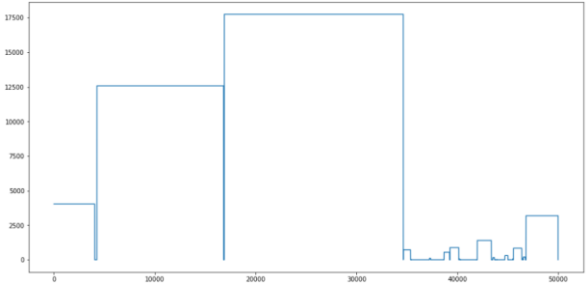


預測定位模組

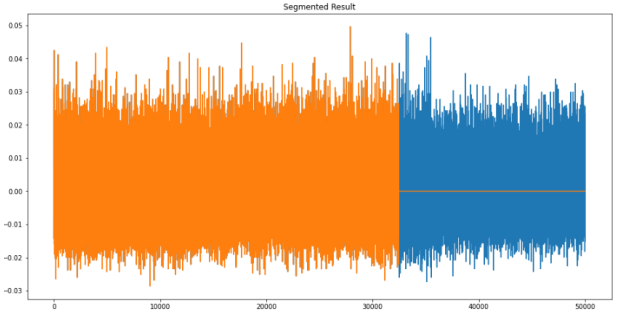
- 透過訓練機器學習模型，學習輸入之訊號特徵，以此分類加密點及非加密點，再**計算預測加密點之連通長度**，取出高於閥值之區域來過濾預測時的雜訊。如右下圖，後半段之雜訊就會被過濾掉，保留前半段的加密區段



模型預測輸出



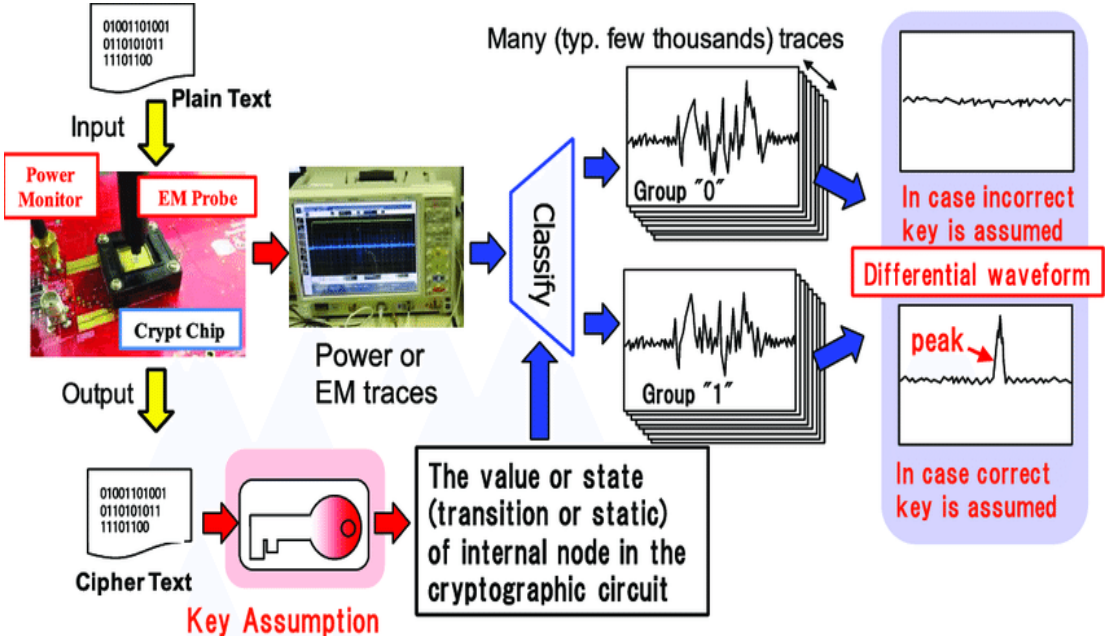
計算各個區域連通長度



閥值篩選區域，過濾預測雜訊

金鑰破解

- 猜 ↔ 大數據統計(Differential Power Analysis)



Ref:Tamper-resistant cryptographic hardware - Scientific Figure on ResearchGate. Available from: https://www.researchgate.net/figure/DPA-Differential-power-analysis-attack-exploiting-a-lot-of-power-traces-on-the_fig3_312873398 [accessed 10 Aug, 2022]

晶片安全聯合檢測實驗室

透過產學研結盟，於9/15揭牌成立我國首座晶片安全聯合檢測實驗室，累積台灣晶片安全檢測實戰經驗

➔ 結合產學研專家，建立晶片安全可遵循指標，打造聯合檢測實驗室

1. **與電電公會合作，制定符合我國產業需求且 接軌國際的晶片安全標準及測試規範**
   - <資通訊產品供應鏈資安標準暨測試規範 >
     - 第一部 晶片安全
     - 第二部 系統軟體
2. **完成10份晶片安全指引，並公開業界使用**
   - 晶片安全設計指引
   - 晶片安全設計最佳範例...
3. **聯合國內外晶片專業領域專家，構築我國晶片安全聯合檢測實驗室**
   - 荷蘭著名資安檢測實驗室SGS Brightsight
   - 國立中興大學
   - 國立成功大學

開源

01

資通訊產品供應鏈資安標準暨測試規範

https://www.teema.org.tw/industry-information-detail.aspx?infoid=38541

02

Chip Security Lab 官網可免費索取晶片安全指引

https://csl.iii.org.tw/

Chip Security Lab

03

電磁旁通道訊號資料庫

https://github.com/jianwei76/SCA_TRACESET

未來發展趨勢

- 後量子加密演算破解

riscure

Issue 55 | September 7, 2022

Security Highlight: Post Quantum Crypto - are we done yet?

The US standards institute recently completed the third round of the Post Quantum Crypto (PQC) standardization process. This milestone was long-awaited, and even though we are one step closer to a PQC standard, the race is not over yet.

PQC is a new generation of cryptographic algorithms that can withstand brute-forcing attacks executed with future quantum computers. While these machines do not yet exist, it is very relevant to prepare for their advent. Many experts expect quantum computing to be practical before the current decade is out. Some cryptographic applications do require a long time of secrecy, and therefore it is not a luxury to be preparedio

But, there is another reason to be working on PQC standardization. Read about the other reasons to consider PQC in the full Security Highlight.

Contributed by Marc Witteman, Riscure CEO. If you have any questions, contact us at inforequest@riscure.com.

Read the full Security highlight now

- AI演算權重破解

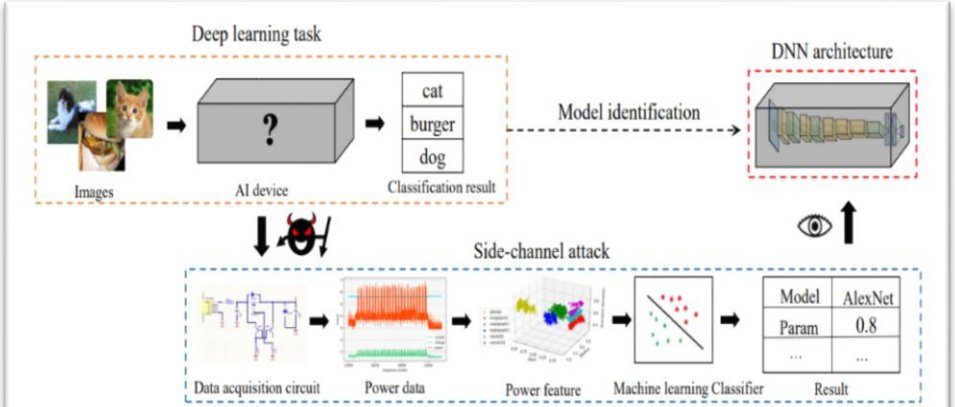
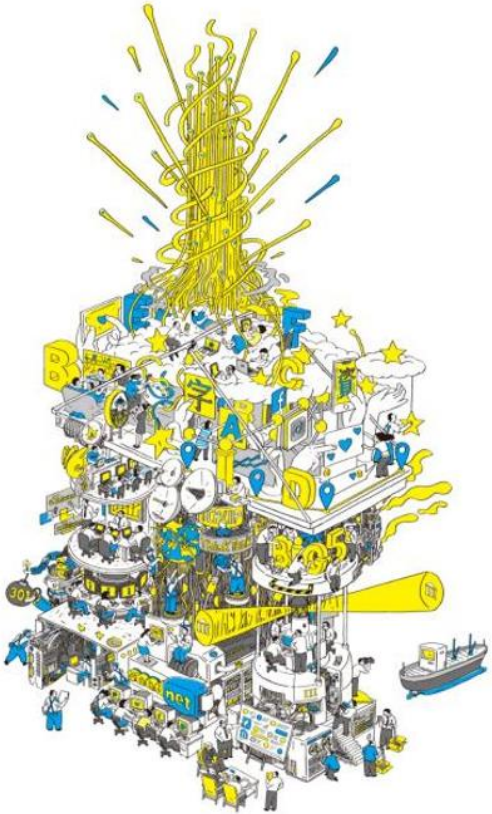


Fig. 3. The framework of our SCA on DNN models. We collect voltage and current data while the AI device is running a model, get the power features, and then establish the classifier to identify the DNN structure and sparsity, so as to realize the attack.

Ref: Xiang, Yun, et al. "Open dnn box by power side-channel attack." *IEEE Transactions on Circuits and Systems II: Express Briefs* 67.11 (2020): 2717-2721.



1擘劃我國資訊工業發展藍圖 2開啟電腦中文化時代 3打造台灣資訊品牌 4培養台灣資訊人才
5開創產業顧問服務 6提升網路基礎建設 7E化政府系統 8普及網路應用人口
9建構資訊法案制度 10縮減城鄉數位落差 11推動數位內容 12推動數位科技外交
13策進 e-Taiwan / m-Taiwan 14精進5G智慧科技創新應用 15支援文創與設計產業奠基
16培育創新創業新動能 17擔任數位國家智庫 18活化原鄉無線寬頻環境
19協助產業拓展商機並強化資安防護 20數位轉型化育者

THANK YOU