Information-technology
Promotion
Agency, Japan

ハードウェア脆弱性評価の最新技術動向に関するセミナー

― COSADE2014参加報告 ―

2014年7月15日

独立行政法人　情報処理推進機構
技術本部 セキュリティセンター

目次

- サイドチャネル攻撃・故障利用攻撃の紹介
- COSADE2014の発表の概要
- IPAの取り組み

サイドチャネル攻撃・故障利用攻撃の紹介

サイドチャネル攻撃 (Side Channel Analysis)

- 暗号機能を実装したハードウェア(スマートカード等)の動作中に、そのハードウェアの状態を観測することで得られる情報を利用して、暗号鍵といった秘密情報の復元を試みる
  - 電力解析(Power Analysis)
    - ハードウェアの消費電力を測定し、その情報から解析する。
      - SPA (Simple Power Analysis): 1つの電力波形を直接調べる。IC内の処理のパターンを見る
      - DPA (Differential Power Analysis): 多数の電力波形を統計処理して解析する。消費電力のデータ依存部分を抽出することができ、また、ノイズを軽減することができる。
    - CMOS半導体の特性上、トランジスタのスイッチング(0→1, 1→0)が起こる時に消費電力が大きくなることを利用。
  - 電磁波解析(Electromagnetic Analysis)
    - 動作中のハードウェアのからの漏洩電磁波から解析する。電力解析同様、1つの波形から解析するSEMA、多数の波形から解析するDEMAがある。

AESアルゴリズム

IPA

- 暗号化処理の流れ

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin   平文              暗号文              拡大鍵
     byte state[4,Nb]                  //内部変数(4行, Nb列の行列)

     state = in

     AddRoundKey(state, w[0, Nb-1]) //

     for round = 1 step 1 to Nr-1
          SubBytes(state) //
          ShiftRows(state) //
          MixColumns(state) //
          AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
     end for

     SubBytes(state)
     ShiftRows(state)
     AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])

     out = state
end
```

Nb:4,
Nr:10,12,14
　for 128, 192, 256-bit key,
w:拡大鍵, 要素数Nb *(Nr+1)

SubBytes:行列要素の置換

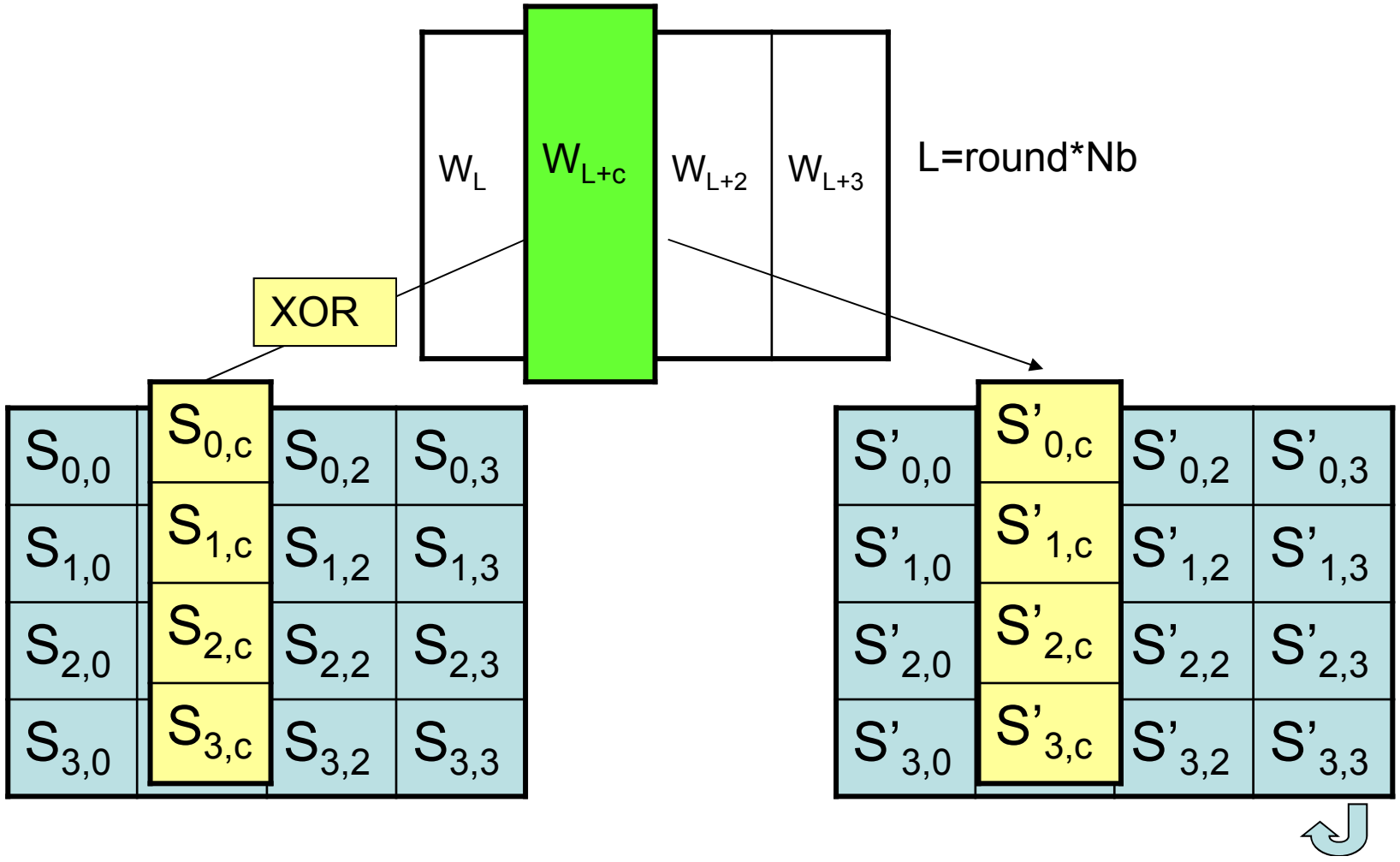
ShiftRows:
行単位の左シフト処理

MixColumns:
列ベクトル単位のデータの変換

AddRoundKey:
列ベクトルと拡大鍵wとのXOR演算

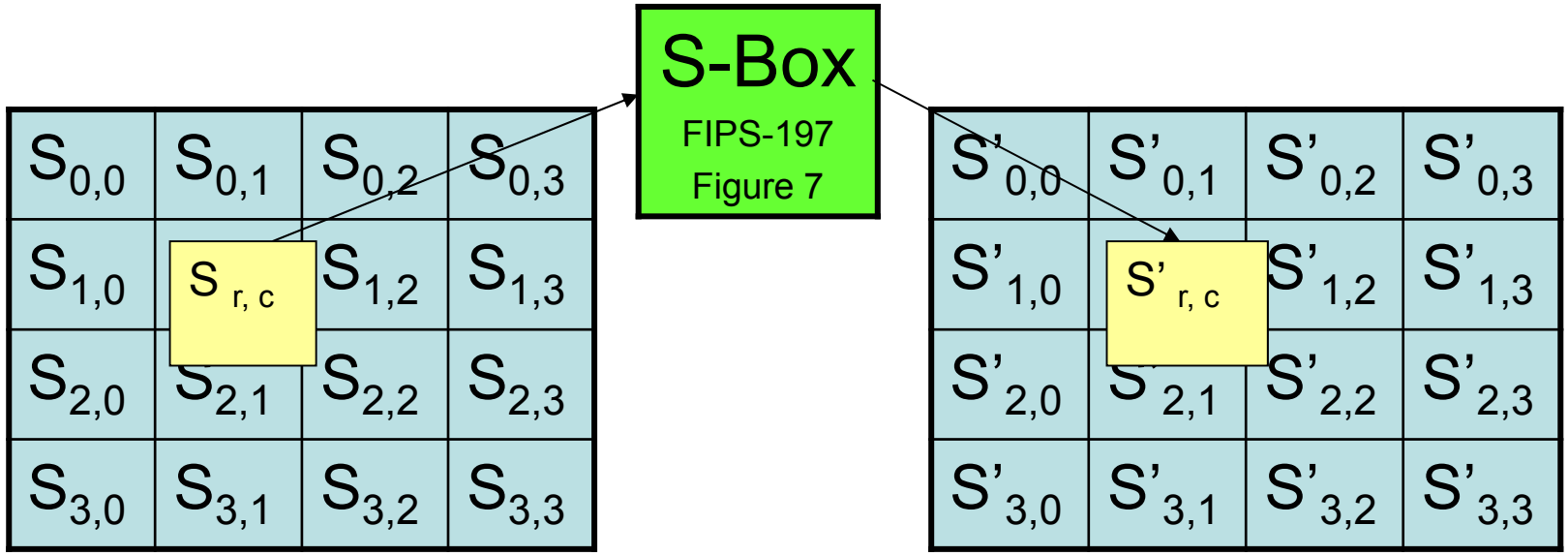
AES：AddRoundKeyの処理

- 4ブロックを1列として，列ごとに拡大鍵とXOR処理。



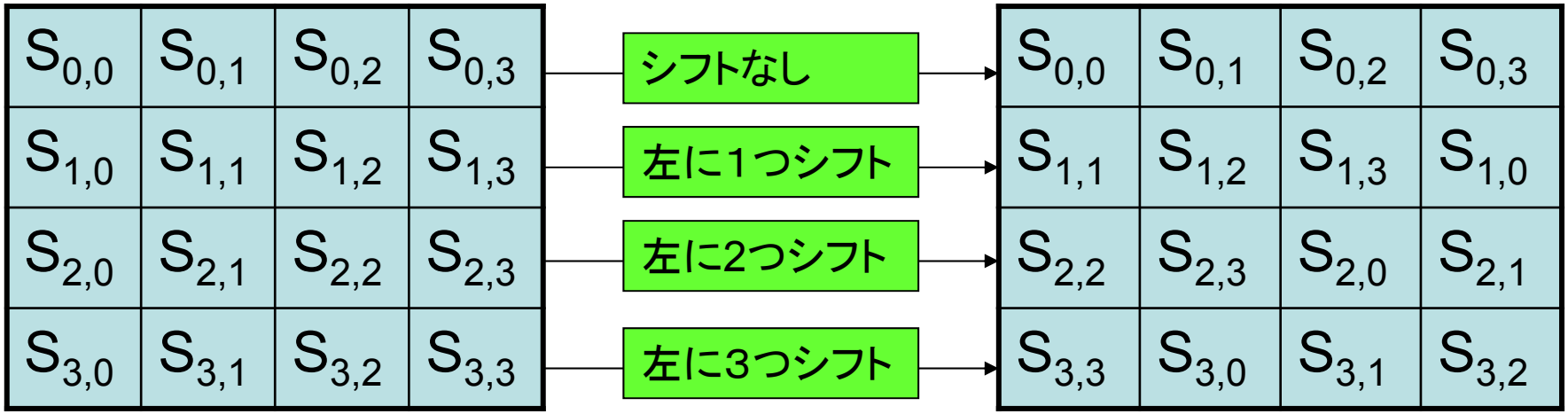
AES：SubBytesの処理

- 128ビットのデータを1バイト（8ビット）ごとに16のサブブロックに分割。
- 各ブロックでは1バイトの入力データを1バイトの出力データへ置換。



AES：ShiftRowsの処理

- 4ブロックを1行として，行ごとに左シフト処理。

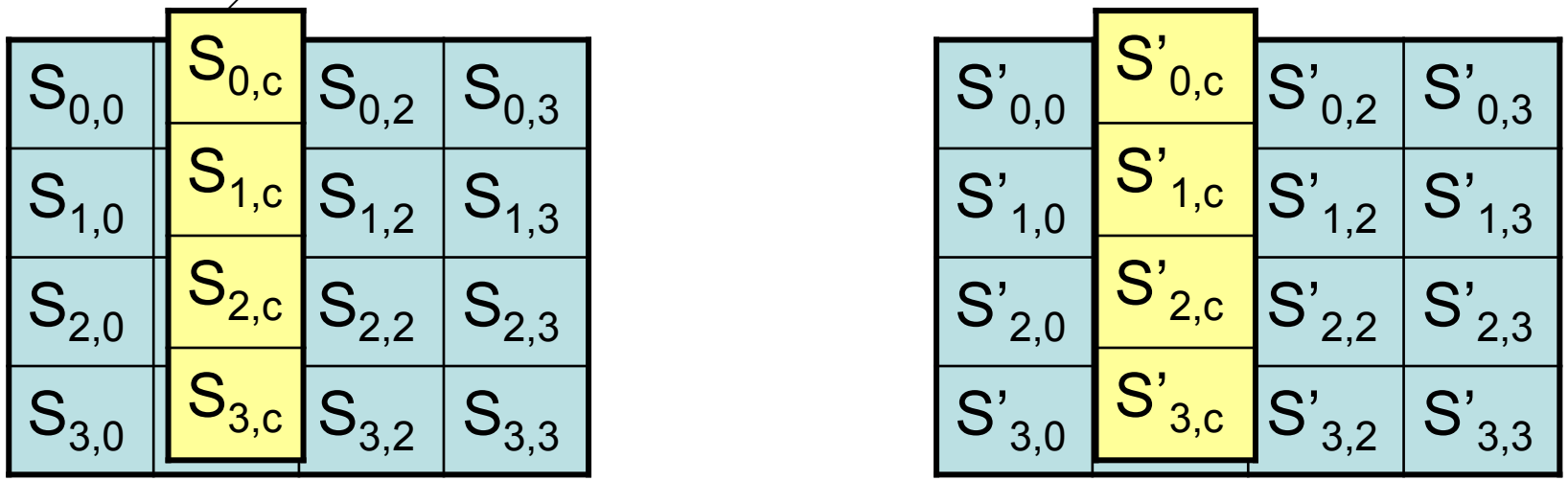


AES：MixColumsの処理

IPA

•4ブロックを1列として，列ごとに列ベクトルの変換。

$$\begin{pmatrix} S'_{0,c} \\ S'_{1,c} \\ S'_{2,c} \\ S'_{3,c} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} S_{0,c} \\ S_{1,c} \\ S_{2,c} \\ S_{3,c} \end{pmatrix}$$



DPAの例1

- 初期のDPA: DoM (Difference of Mean)

鍵の先頭1バイト=00と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	MSB
7d	21	0
7c	10	0
6a	02	0
da	57	0
17	f0	1
…	…	…

鍵の先頭1バイト=01と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	MSB
7d	10	0
7c	21	0
6a	7f	0
da	b9	1
17	47	0
…	…	…

1. 平文をランダムに変化させて暗号化を行い、消費電力を測定する
2. 中間値のあるビットに注目し、それが0か1かにとって電力波形を分類する。それを各鍵仮説(AES鍵の先頭1バイトの場合、256通り)に対して行う。
3. 2群に分けた電力波形について、それぞれ平均を取る
4. 誤った鍵仮説に対しては、平均値の差がゼロに近い値になるが、正しい鍵仮説に対しては、平均値の差が大きい値になると考えられるので、これによって正しい鍵の値が判明する

DPAの例2

- CPA (Correlation Power Analysis: 相関係数を使用する)

鍵の先頭1バイト=00と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	HW
7d	21	2
7c	10	1
6a	02	1
da	57	5
17	f0	4
…	…	…

鍵の先頭1バイト=01と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	HW
7d	10	1
7c	21	2
6a	7f	7
da	b9	6
17	47	4
…	…	…

1. 平文をランダムに変化させて暗号化を行い、消費電力を測定する
2. 中間値のhamming weightを計算する。それを各鍵仮説(AES鍵の先頭1バイトの場合、256通り)に対して行う。
3. 消費電力と、hamming weightとの間の相関係数を計算する
4. 誤った鍵仮説に対しては、相関係数の値がゼロに近い値になるが、正しい鍵仮説に対しては、相関係数の値が大きい値になると考えられるので、これによって正しい鍵の値が判明する

故障利用攻撃 (Fault Injection Attack)

- 暗号機能を実装したハードウェアの動作中に故意に故障(fault)を起こし、計算誤りを利用して解析を行う
  - クロックグリッチ
  - 電源グリッチ
  - レーザー攻撃
  - 電磁場印加
- 故障利用攻撃の例: RSA-CRT
  - $s=m^d \bmod n$ とする(正しい署名)
  - $s'_p=m^{dp} \bmod p$ (s_pの計算にfaultを入れる)
  - $s_q=m^{dq} \bmod q$
  - $s'=s_q+q(i_q(s'_p-s_q) \bmod p)$
  - このとき、$\gcd(s-s',n)=q$。また、$\gcd(m-s'^e,n)=q$ → 秘密の素因数が判明

最近の傾向

- Side Channel Analysisのdistinguisherが多彩になってきた
  - 例
    - Power Modelを使用
      - DPA (Difference of Mean)
      - CPA (Correlation Power Analysis)
    - Generic (Power Modelに依存しない)
      - MIA (Mutual Information Analysis)
      - KSA (Kolmogorov-Smirnov Analysis)
      - IKSA (inter-class KSA)
      - etc...

DPA (Differential Power Analysis)

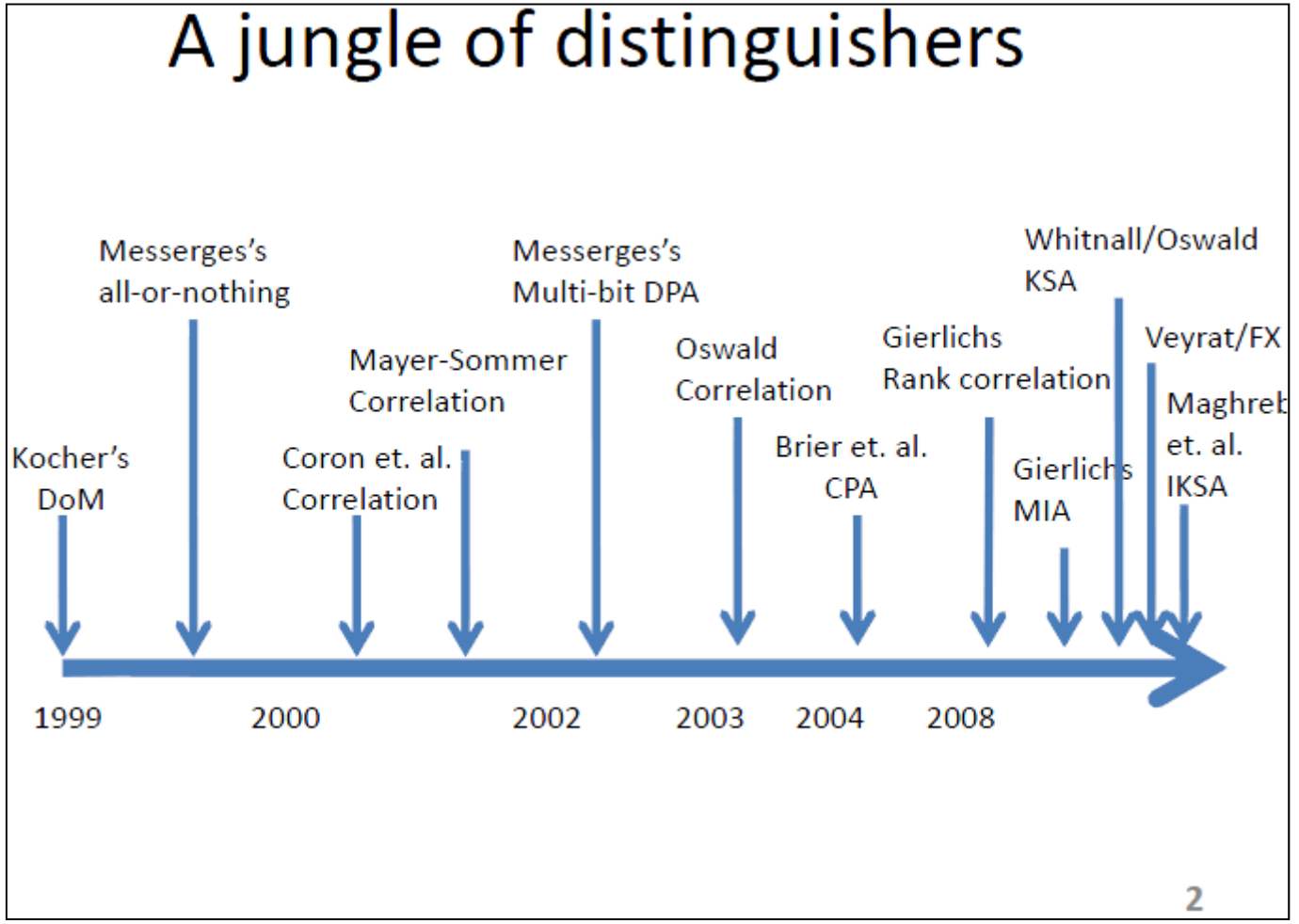
- 初期のDPA
  - Difference of Mean (DoM) (1999 P.Kocher. et al)
    - 中間値のある1ビットに注目する。
  - Correlation Power Analysis (CPA) (2004)
    - Pearson's correlation を使う。
    - Power Modelが判明している場合に強力
      - 例えば、消費電力とHamming Weight(HW)にlinearな相関がある場合

適切なPower Modelが不明の場合、攻撃は困難

“Generic” Power Analysis

- Power Modelを仮定しないPower Analysisの登場
  - Mutual Information Analysis (MIA)
  - Kolmogorov-Smirnov Analysis (KSA)
  - etc...
- linearなpower modelが見つからない場合(例えば、dual rail logicを採用したIC)には、CPAはうまくいかないが、MIAはうまくいく可能性がある

様々なdistinguishers



出典: Oscar Reparaz et.al., COSADE 2014

情報量 (Entropy)

- Shannon Entropy

$$H(X) = -\sum_{x \in X} P_X[X = x] \log_2 P_X[X = x]$$

- 条件付きShannon Entropy

$$H(X \mid Y) = -\sum_{x \in X, y \in Y} P_{X,Y}[X = x, Y = y] \log_2 P_{X|Y}[X = x \mid Y = y]$$

- 相互情報量 (Mutual Information)

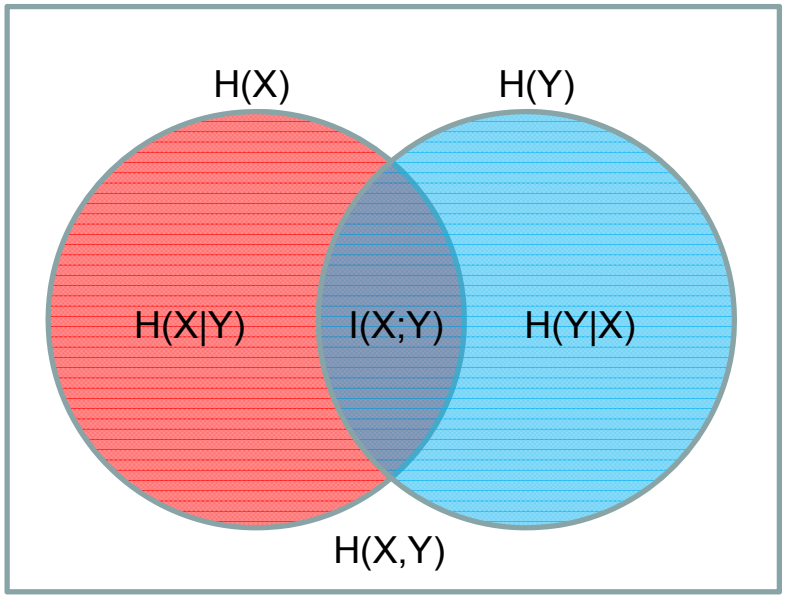
$$I(X;Y) = \sum_{x \in X, y \in Y} P_{X,Y}[X = x, Y = y] \log_2 \frac{P_{X,Y}[X = x, Y = y]}{P_X[X = x] P_Y[Y = y]}$$

  - 以下の定義も同値である

$$I(X;Y) = H(X) - H(X \mid Y)$$

相互情報量 (Mutual Information)

- 相互情報量とは、直観的には、Yを知ることによって得られる、Xに関する情報量である
  - 例: 情報Xを、通信チャネル(ノイズが乗るかも知れない)を通じて伝達する。受信される情報をYとする。
  - 通信チャネルが完全で、ノイズが全くないとすると、YはXによって完全に決定される。この場合、H(X|Y)=0, I(X;Y)=H(X)
  - 通信チャネルが完全に壊れていて、YにXに関する情報が全く伝わらない場合、XとYは独立になり、H(X|Y)=H(X), I(X;Y)=0



$$
\begin{aligned}
I(X;Y) &= H(X) - H(X|Y) \\
&= H(Y) - H(Y|X) \\
&= H(X) + H(Y) - H(X,Y) \\
&= H(X,Y) - H(X|Y) - H(Y|X) \\
&= I(Y;X)
\end{aligned}
$$

MIA (Mutual Information Analysis)

- W: 暗号処理中の状態変化 (bit flip等)
- L(W): Wによるleakage (HW, Id, etc)
- O: ノイズがあるかも知れない測定値(消費電力等)

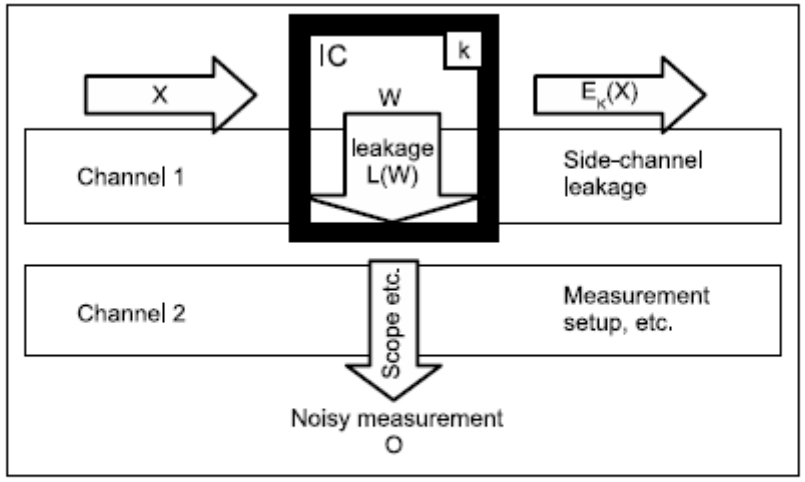


Fig. 1. Schematic illustration of the cascaded channels

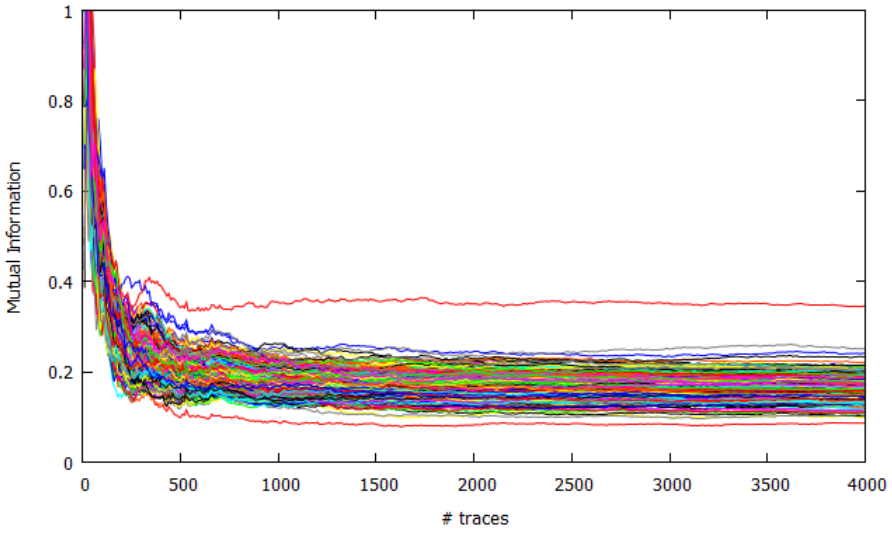
出典: B. Gierlichs et. al., Mutual Information Analysis - A Generic Side-Channel Distinguisher, CHES 2008

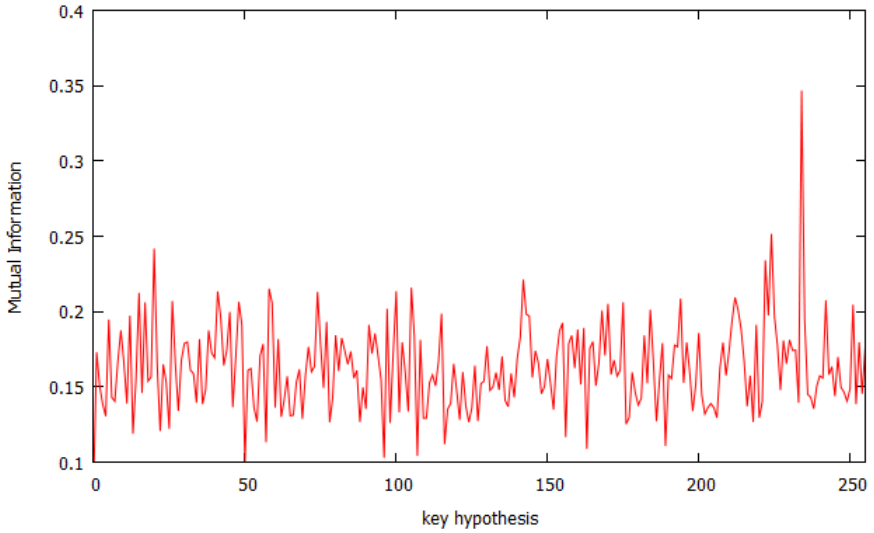
MIA (Mutual Information Analysis)

- ある中間値をターゲットにする (例: $W=S(P \oplus k)$)
- O: 消費電力を測定し、その分布を求める
- L_k: leakageに現れるpower model。ただし、power modelが不明なら、L_k=Id (恒等関数) としてもよい
  - ただし、ターゲットが単射の写像からの出力のときは注意が必要
- $H=L_k(W)$ を計算し、その分布を求める
- 各鍵仮説に対して、Mutual Information I(O;H)を計算する。
- 最も高いMutual Informationを与える鍵仮説を鍵と推定する。
  - 理論的には、正しい鍵仮説に対しては正のMutual Informationが得られ、誤った鍵仮説に対しては、OとHは独立となり、I(O;H)=0となるはずである。

MIAの実行例1

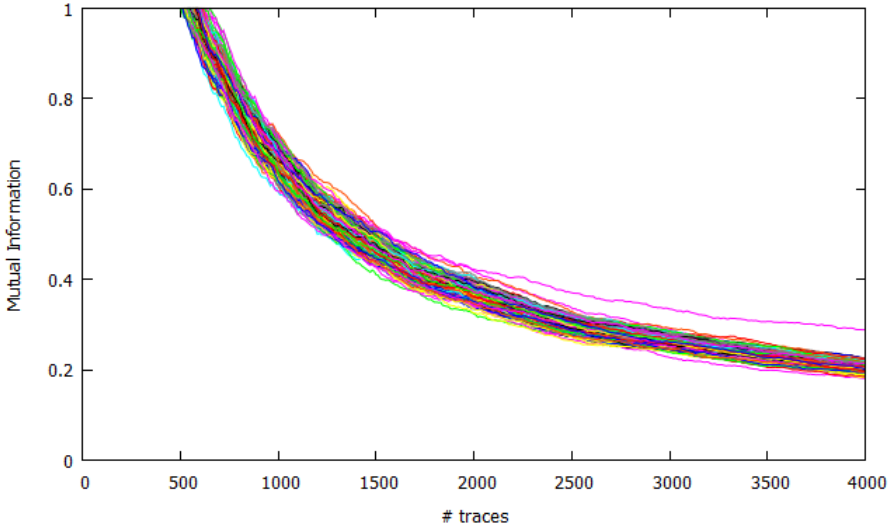
- MIA シミュレーション例 (AES)
  - ターゲットは第1ラウンドのSboxの出力
  - H=Sbox(P⊕k), L=LSB_3(H)
  - noiseなし

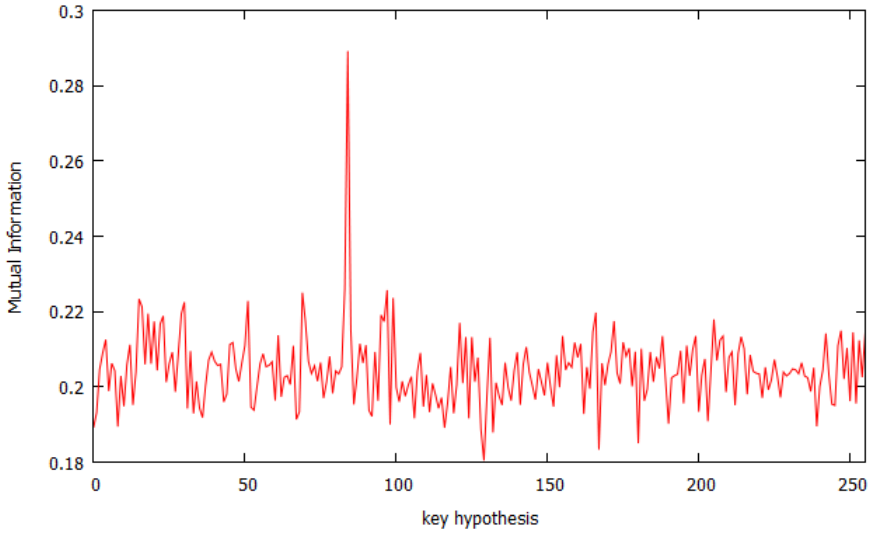




MIAの実行例2

- MIA シミュレーション例 (AES)
  - ターゲットは第1ラウンドのSboxの出力
  - H=Sbox(P⊕k), L=LSB_3(H)
  - gaussian noiseあり





MIAを実行する際の厄介なところ

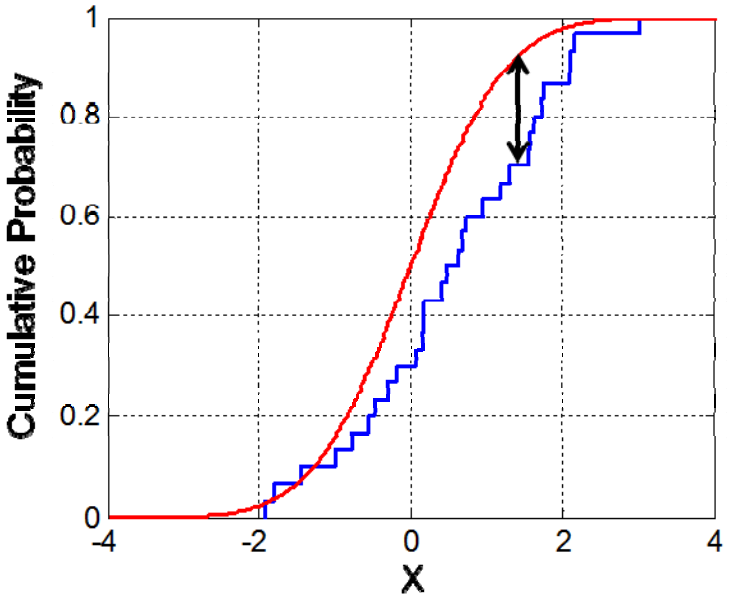
- 相互情報量を算出するために、確率密度関数(PDF: probability density function)を推定する必要がある
- 良いPDF推定器が重要

その方法は?

- ヒストグラム
  - 最も直観的で単純な方法
  - binの幅の選択が重要
- KDE (Kernel Density Estimation)
  - なめらかな分布が得られる
  - パラメタの選択が重要(Kernel Function, Query Points, Bandwidth)
- その他
  - b-spline, etc

KSA (Kolmogorov-Smirnov Analysis)

- Kolmogorov-Smirnov検定とは、有限個の標本に基づき、CDF(Cumulative Distribution Function: 累積分布関数)を比較して、母集団の確率分布が等しいかどうかを検定する手法
- Kolmogorov-Smirnov検定をサイドチャネル攻撃に応用



COSADE 2014の発表内容の概要

COSADE 2014

- COSADE: Constructive Side-Channel Analysis and Secure Design
- 開催日
  - 2014/4/14 ～ 4/15, Paris, France
- 主にサイドチャネル攻撃の研究に関するworkshopで、以下のようなトピックを対象としている
  - Constructive side-channel analysis and implementation attacks
  - Semi-invasive, invasive and fault attacks
  - Leakage models and security models for side-channel analysis
  - Cache-attacks and micro-architectural analysis
  - Decapsulation and preparation techniques
  - Side-channel based reverse engineering
  - Leakage resilient implementations
  - Evaluation methodologies for side-channel resistant designs
  - Secure designs and countermeasures
  - Evaluation platforms and tools for testing of side-channel characteristics

Study and Comparison of Side Channel Analyses

IPA

- A note on the use of margins to compare distinguishers, Oscar Reparaz, et. al.
- A Theoretical Study of Kolmogorov-Smirnov Distinguishers: Side-Channel Analysis vs. Differential Cryptanalysis, Annelie Heuser, et. al.
- Pragmatism vs. Elegance: comparing two approaches to Simple Power Attacks on AES, Valentina Banciu, et. al

A note on the use of margins to compare distinguishers

- Side Channel Analysisのdistinguisherの比較について
  - 近年、様々なdistinguisherが乱立している
    - DoM, Correlation, MIA, KSA,...
  - distinguisherの比較に、どういう尺度を使うか
    - 成功率 (最大のdistinguisher値を持つ鍵仮説が正しい鍵である確率)
    - マージン (正しい鍵仮説によるdistinguisher値と誤った鍵仮説によるdistinguisher値の最大値との差)
  - 同じ成功率でもマージンが違うことがある

IPA

- DPAやCPAのdistinguisherについてはよく研究されている
- “generic”なdistinguisherに関する振る舞いはあまり研究されていない
  - Kolmogorov-Smirnov distinguisherの振る舞いについての研究
  - SNRといったパラメタからの攻撃の成功率の理論的分析
  - closed-form expressionの導出

$$KSA(k) = \left(2\Phi(\sqrt{SNR-1}\right)\left|\kappa(k^*,k) - \frac{1}{2}\right|$$

Pragmatism vs. Elegance: comparing two approaches to Simple Power Attacks on AES

- AESに対するSPA
  - Mangardの攻撃 (pragmatic)
    - Key Scheduleで現れる値(各round key)の各バイトのhamming weight (HW) が漏れると仮定
    - 各HWの値を使い、鍵の候補を絞り込む
  - Algebraic Side-Channel Attack (elegant)
    - Algebraic cryptanalysisにside-channel情報を利用
    - SAT(satisfiability)問題(充足可能性問題)に帰着させ、SAT solverで解く。
  - これらの攻撃においては、中間値のHWが正確に判明するものと仮定していた
  - 現実には、消費電力測定にはノイズがつきものである。

Pragmatism vs. Elegance: comparing two approaches to Simple Power Attacks on AES

IPA

- AESに対するSPA
  - HW測定にノイズが入ると仮定して攻撃を評価
    - 各HWの候補を5つとすると、pragmaticな方法は現実的な範囲。Elegantな方法はうまくいかなかった。

Results

Previous results

Mangard's Attack (attacking 5 consecutive Round Keys, 1000 experiments)

HW used	100%	95%	50%
key space	11	16.5	$1.7 \cdot 10^{12}$
time	5m30s	5m	5h

ASCA Attack success rate (known PT and CT, 100 experiments)

# rounds	2	4	6
consecutive	0%	100%	100%
random	20%	60%	100%

Our results

(Using leaks from one encryption round and one round key. The PT is known. Averaged over 500 experiments)

	Encryption only		Key Schedule only		Combined	
Set size	Key space	Execution time	Key space	Execution time	Key space	Execution time
1	1	0.02 s	2^{58}	0.4 s	1	0.03 s
2	2^{20}	2.9 s	2^{74}	5 s	2^{12}	27 s
3	2^{48}	73.9 s	2^{95}	10 s	2^{13}	4 m
4	2^{84}	27 m	2^{106}	30 s	2^{52}	35 m
5	2^{116}	2.5 h	2^{115}	40 s	2^{60}	12 h

出典: Valentina Banciu et. al., COSADE 2014

Attacks and Countermeasures for Asymetric Cryptosystems

IPA

- Addition with Blinded Operands, Mohamed Karroumi, et. al.
- On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance, Christophe Giraud
- Common Points on Elliptic Curves: The Achilles' Heel of Fault Attack Countermeasures, Alberto Battistello

Addition with Blinded Operands

- サイドチャネル攻撃への対策
  - 中間値をランダム化する
  - masking (blinding)によってそれを行う
  - 2種類の主なmasking手法
    - Boolean masking: $x \rightarrow (X = x \oplus r_x, r_x)$
    - Arithmetic masking: $x \rightarrow (X = x - r_x, r_x)$
      - 両方のタイプの演算を使用するアルゴリズム に対しては、一方の種類のマスキングから別の種類のマスキングへのセキュアな変換が必要

Addition with Blinded Operands

- Secure Adder
  - $x \oplus r_x \qquad y \oplus r_y$ —Secure adder→ $s = (x + y) \oplus (r_x \oplus r_y)$
- マスキング変換なしで、リークなしで行う
  - AND-XOR-and-double method

On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance

IPA

- RSA-CRTの署名生成を、SCAやFAに耐性を持った実装で行う
  - アイディア: 署名生成は、通常は、秘密鍵*d*を使用するが、公開鍵*e*が利用可能な場合、それを利用して効率的にセキュアに計算するアルゴリズムを提案
  - eは、$2^{16}+1$のような小さい数であることが多い
    →計算時間が少なくて済む

IPA

- RSAの署名生成
  - $s=m^d \bmod n$
- RSA-CRTの署名生成
  - $s_p=m^{dp} \bmod p$
  - $s_q=m^{dq} \bmod q$
  - $s=s_q+q(i_q(s_p-s_q) \bmod p)$ (Garner's formula)
    $(iq=q^{-1} \bmod p)$

On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance

IPA

- Side Channel Analysis対策
  - Message masking: $s'_p=(m+k_0p)^{dp} \bmod 2^{64}p$
  - Exponent masking: $s'_p=(m+k_0p)^{dp+k_1(p-1)} \bmod 2^{64}p$
  - Square and Multiply Always, Montgomery Ladder,...
- Fault Injection対策
  - $s^e \bmod N \equiv m$ かどうかを検算する
  - …

On the Use of RSA Public Exponent to Improve Implementation Efficiency and Side-Channel Resistance

IPA

- 新しいアプローチ
  - Gauss Recombination
    - $S=pi_pS_q+qi_qS_p \bmod N$
      - ここで、$S_p=m^{dp} \bmod p$, $S_q=m^{dq} \bmod q$, $i_p=p^{-1} \bmod q$, $i_q=q^{-1} \bmod p$
  - 以下の式が成り立つ
    - $i_qS_p \equiv (mq^e)^{dp-1}mq^{e-2} \bmod p$
    - $i_pS_q \equiv (mp^e)^{dq-1}mp^{e-2} \bmod q$
  - これにより、
    - $S=pS1_q+qS1_p \bmod N$
      ここで、$S1_p= (mq^e)^{dp-1}mq^{e-2} \bmod p$
      $S1_q= (mp^e)^{dq-1}mp^{e-2} \bmod q$
  - この式を元にした、効率的なメッセージブラインディングのアルゴリズムを提案
    - 鍵長1024ビットで14.2%, 2048ビットで8.2%の効率向上

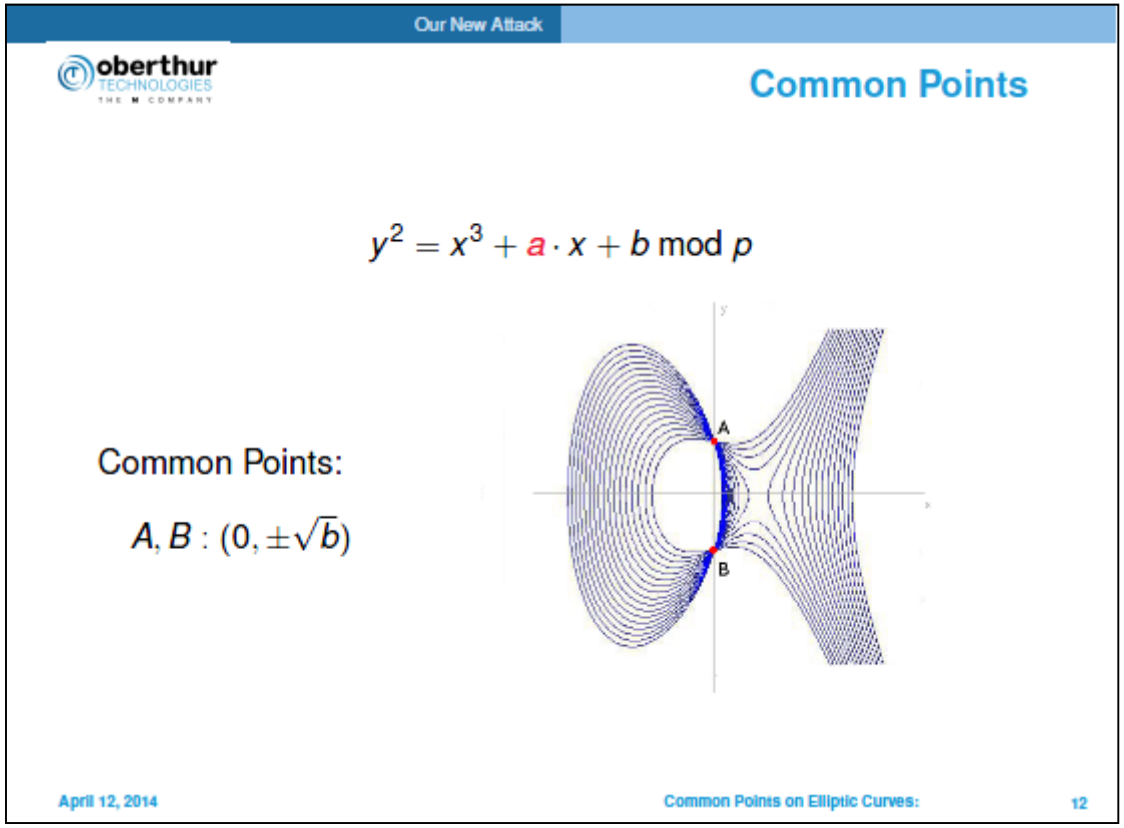
Common Points on Elliptic Curves:
The Achilles' Heel of Fault Attack Countermeasures

IPA

- 楕円曲線暗号に対するfault injection攻撃
  - 楕円曲線 $E(\mathbf{F}_p)$: $y^2=x^3+ax+b$, $P=(x_p,y_p)\in E(\mathbf{F}_p)$
  - 係数aにfaultを入れて、値を改変する。
  - 楕円曲線 $E'(\mathbf{F}_p)$: $y^2=x^3+a'x+b'$ 上の計算に改変する
  - $E'(\mathbf{F}_p)$上で、$P=(x_p,y_p)$が小さい位数を持っているかも知れない → 離散対数問題が解けてしまう
- 考えられる対策
  - 楕円曲線のパラメタチェック (CRCチェックなど)
  - $P=(x_p,y_p)$が楕円曲線上にあることのチェック (楕円曲線の方程式に代入して検算)
- これらの対策は、同等に見えるが…

Common Points on Elliptic Curves:
The Achilles' Heel of Fault Attack Countermeasures

- A=(0,±√b)は、aが変化しても楕円曲線上に乗っている (すべてのaに対する共通の点)
  - →楕円曲線上の点であることのチェックでは検出できない



2つの対策は同等ではない!

出典: Alberto Battistello, COSADE 2014

Generic Side Channel Analysis

IPA

- On Adaptive Bandwidth Selection for Efficient MIA, Mathieu Carbone, et. al.
- Generic DPA attacks: curse or blessing? Oscar Reparaz, et al.

On Adaptive Bandwidth Selection for Efficient MIA

- MIAは、相互情報量(Mutual Information)を計算することで、鍵を推測する。
- 相互情報量を計算するためには、確率密度関数(PDF)を見積もる必要がある。
- 確率密度関数の見積もりは、様々なチューニングパラメタがあり、単純ではない。
- Kernel density estimation(KDE)のチューニングパラメタ
  - Kernel Functions
  - Query Points
  - Bandwidth
- MIAの効率を最適化するための、これらのパラメタの選び方についての研究
- PDFの予測精度とMIAの攻撃成功率は必ずしも一致しないことを示唆している

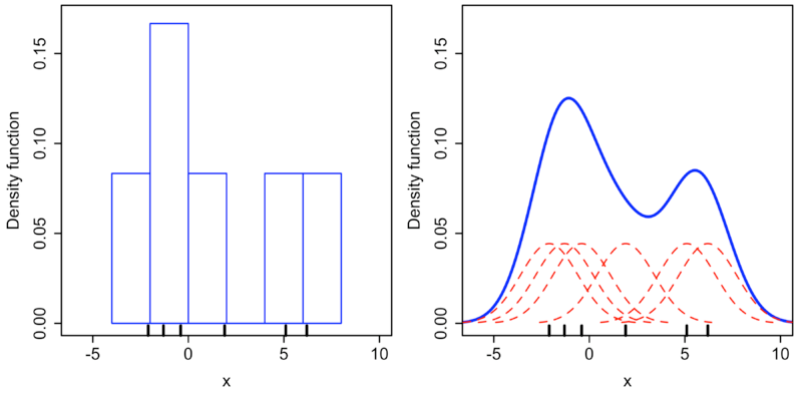
On Adaptive Bandwidth Selection for Efficient MIA

Kernel Density Estimation (カーネル密度推定)とは

- カーネル関数から決定される「コブ」を各標本に与えて、その総和をとる
- ヒストグラムと異なり、滑らかになる

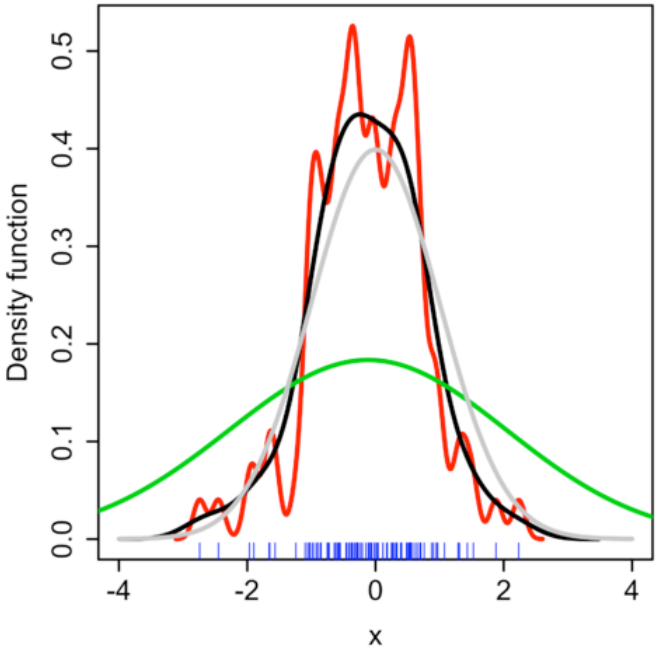
$$\hat{f}_h(x) = \frac{1}{Nh}\sum_{i=1}^{N} K\left(\frac{x - x_i}{h}\right)$$

K: カーネル関数
h: bandwidth (バンド幅、平滑化パラメータ)



ヒストグラムとKDEの比較

- バンド幅の選択による違い



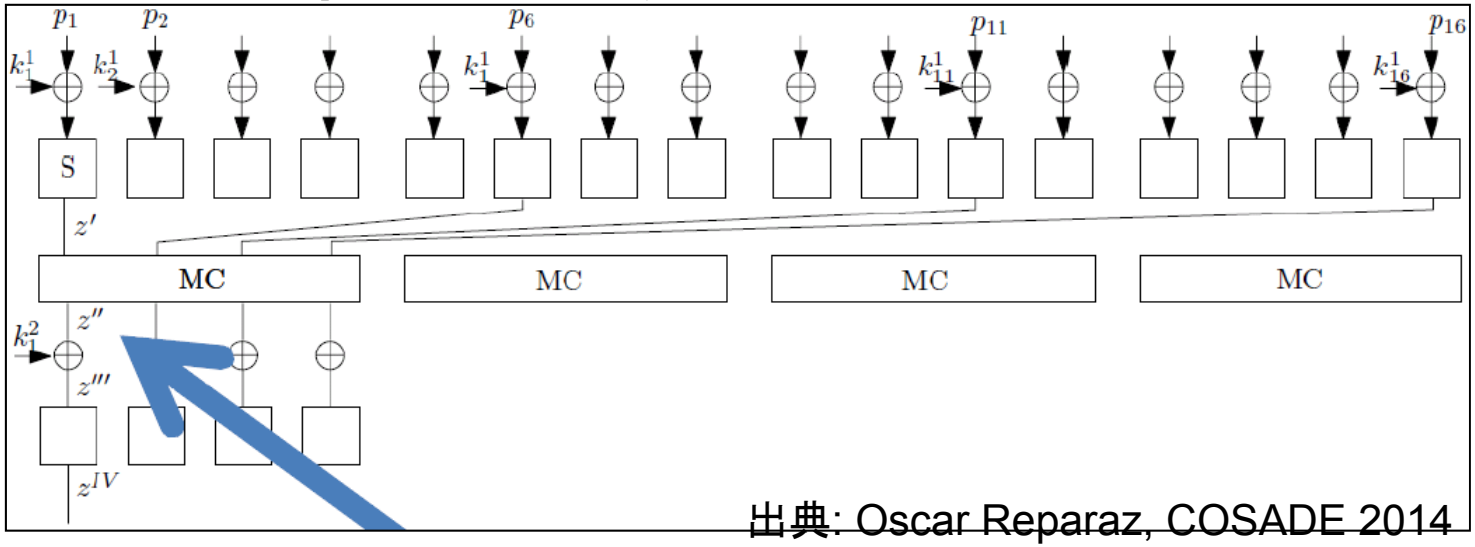
標本数: 100
Gray: 真の分布 (標準正規分布)
Red: h=0.05, Black: h=0.337, Green: h=2

Generic DPA attacks: curse or blessing?

- 単射のターゲット (例: $Z=S_{AES}(P \oplus K)$)に関する問題
  - AESのS-boxは全単射(したがって単射)な写像である。
  - 単射な写像に対して、genericなleakage model (H=Id(Z))を適用すると、鍵仮説によらず相互情報量が同じになるので、攻撃の効果がなくなる
  - bit drop techniqueの評価
    - Zから何ビットか落とし、injectiveでなくす
    - この論文のシミュレーションでは、5ビット落とすのが最適な結果をもたらしたが、SN比が高いとbit drop techniqueがうまくいかないケースもある

Generic DPA attacks: curse or blessing?

- AESにおける、non-injective targetの考察
  - $2S(p_1 \oplus k_1) \oplus 3S(p_6 \oplus k_6)$ (第1ラウンドのMixColumnsの一部)をターゲットにする
  - これは、16ビットの秘密情報と16ビットの既知情報から8ビットの値への写像なので、単射ではない
  - 鍵空間が大きくなる(k_1 とk_6の合成なので16ビット)が、MIAによる攻撃は可能である



出典: Oscar Reparaz, COSADE 2014

Generic DPA attacks: curse or blessing?

- バス暗号化がなされたハードウェアに対するMIA
  - 中間値が暗号化(バイトのpermutationによる)されていても、MIAのようなgeneric DPAは有効
    - permutationは、エントロピーの値に影響を与えず、したがって、相互情報量にも影響を与えないため

Fault Attacks and Software Security

IPA

- A Multiple-fault Injection Attack by Adaptive Timing Control under Black-box Conditions and a Countermeasure, Sho Endo, et. al.
- Adjusting laser injections for fully controlled faults, Franck Courbon, et. al.
- ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research, Colin O'Flynn, et. al.

A Multiple-fault Injection Attack by Adaptive Timing Control under Black-box Conditions and a Countermeasure

IPA

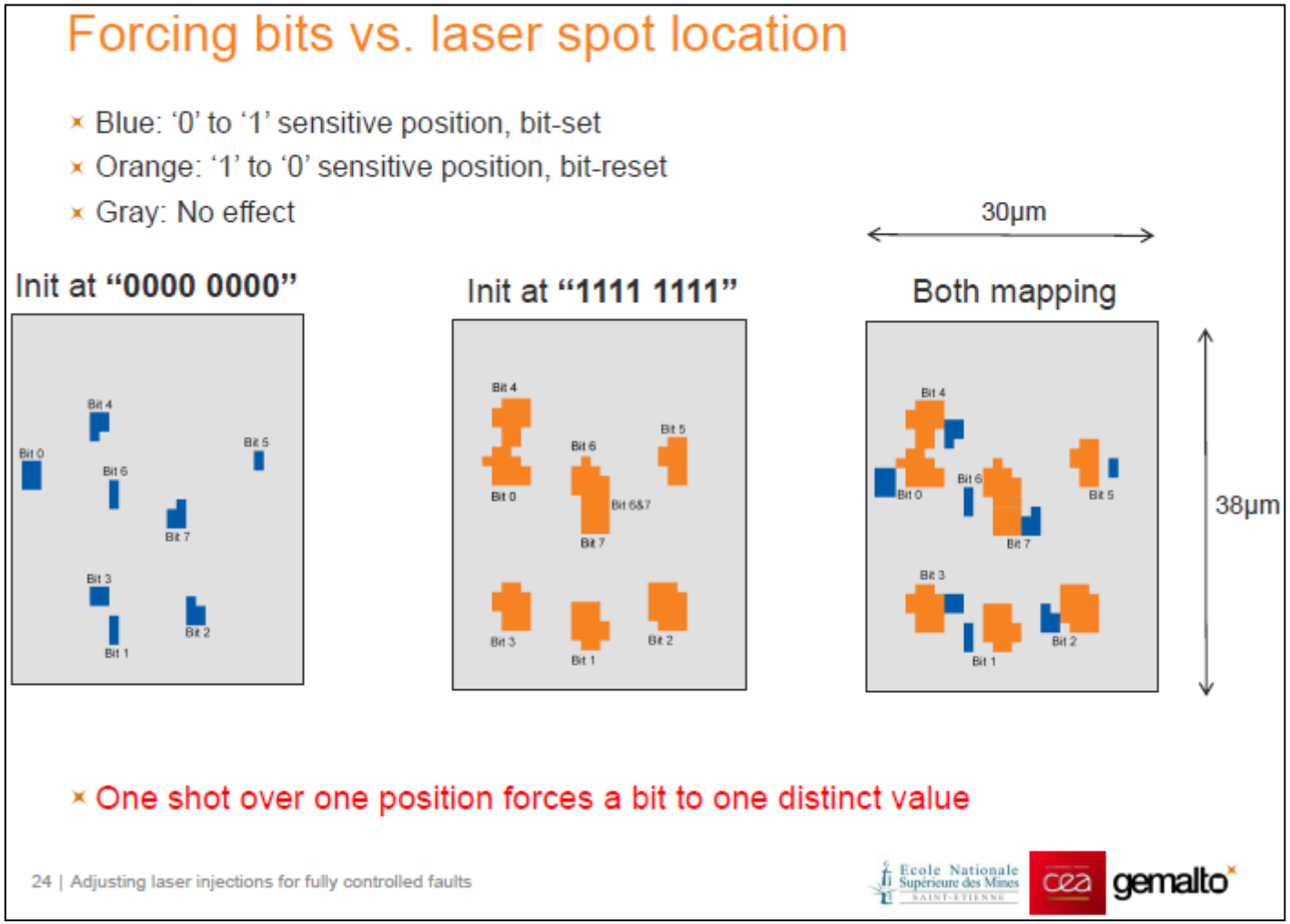
- ブラックボックス条件において、multiple-fault injection attackを成功させるための技法
  - 以下の条件を仮定
    - 実装されている暗号アルゴリズムは既知
    - 検算による対策が実装されていることが分かっている
    - 組み込みソフトウェアの実装の詳細は未知
  - 以下のステップでfault injectionを実行
    - Step 1: preliminary faultのタイミングを変化させ、エラーシグナルが得られるタイミングを探す
    - Step 2: Step 1で得られたタイミングでfault (clock glitch)を入れながら、2番目のfaultのタイミングを変化させ、重要な命令(条件分岐等)がスキップされるタイミングを探る (Fault Bのタイミングを探索)
    - Step 3: Fault Bを入れながら、DFAが可能になるようなfaulty ciphertextが得られるFault Aのタイミングを探索する
- この攻撃に対するcountermeasureの提案
  - Default fail, zero flag clear

Adjusting laser injections for fully controlled faults

IPA

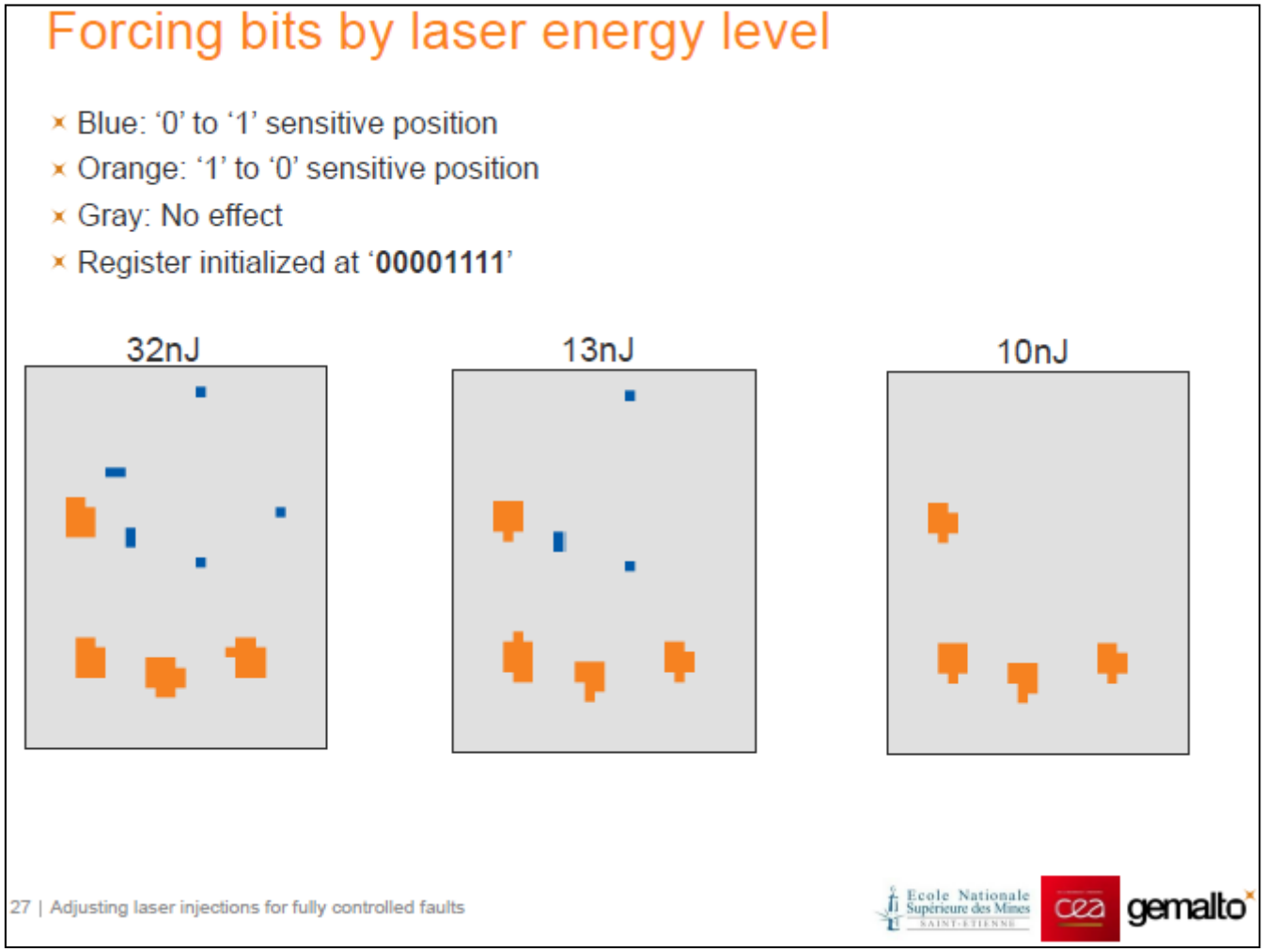
- レーザーによるfault injection攻撃
  - 何らかのfaultは起こせるが、faultの効果については、様々なfault modelが考えられる
    - Bit Set, Bit Reset, Byte Set, Random Byte, ...
  - レーザーの精密な制御 (位置、スポット径)
    - faultの起き方を制御できるか?
  - SRAMへの精密攻撃の結果
    - 特定のビットがセットされる箇所を特定
    - 特定のビットがリセットされる箇所を特定
    - レーザーの出力を調整すると、ビットリセットしか起こらないエネルギー領域があった
  - 1ビットセットやリセットといったfault modelは現実的と考えるべき

Adjusting laser injections for fully controlled faults



出典: Franck Courbon, COSADE 2014

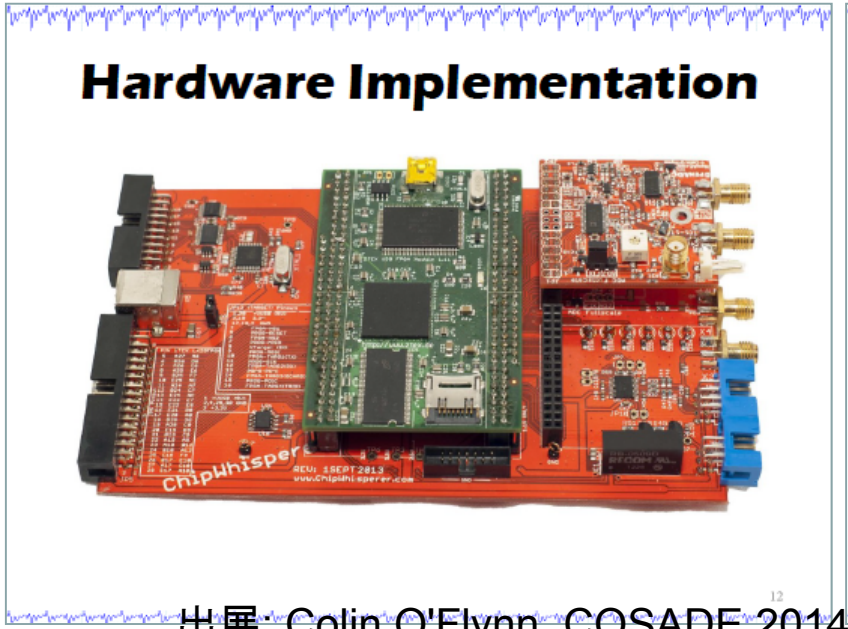
Adjusting laser injections for fully controlled faults

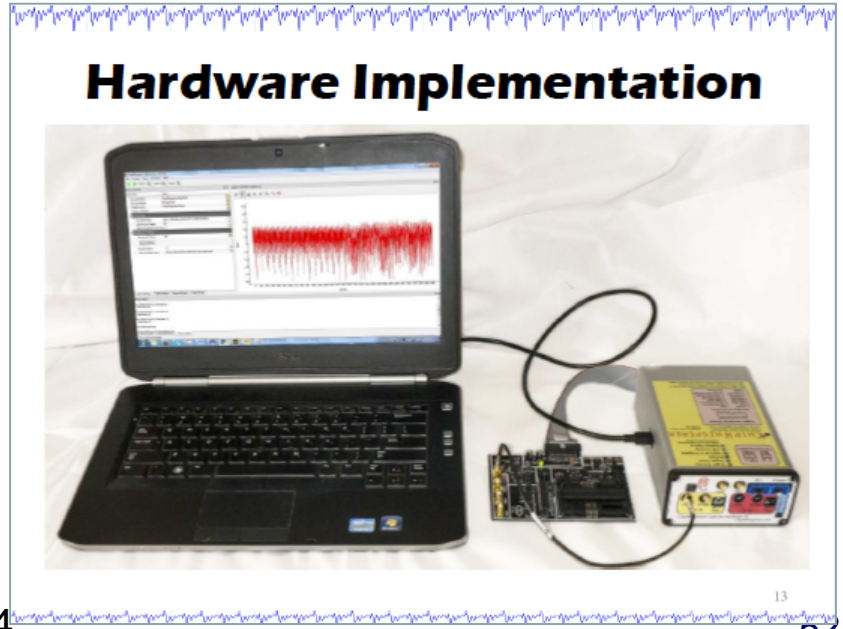


出典: Franck Courbon, COSADE 2014

ChipWhisperer: An Open-Source Platform for Hardware Embedded Security Research

- DPA用の完全なプラットフォームの紹介
- 以下のものをすべて含んでいる
  - Target device
  - Analog capture hardware
  - Capture software
  - Analysis software





出展: Colin O'Flynn, COSADE 2014

Attacks Against Countermeasures

- Collision-Correlation Attack against a First-Order Masking Scheme for MAC based on SHA-3, Luk Bettale, et. al.
  - First order maskingの対策を施したSHA3へのサイドチャネル攻撃
- Attacking Randomized Exponentiations Using Unsupervised Learning, Guilherme Perin, et. al.
  - 指数のランダム化の対策を施した実装に対する攻撃
  - RNS (Residue Number System) Montgomery Ladderがターゲット
- On the Security of RSM - Presenting 5 First- and Second-order Attacks, Sebastian Kutzner, et. al.
  - RSM masking scheme (DATE2012で発表された)に対する攻撃

Improvements in Side Channel Analysis

- On the Optimal Pre-processing for Non-Profiling Differential Power Analysis, Suvadeep Hajra, et. al.
  - DPAの成否はノイズに大きく左右される。ノイズに対抗するために、SN比を向上させるためのフィルタリングが行われる。
  - Matched filter(適合フィルター)を応用し“optimal” filter というフィルタを提案
- Template Attacks on Different Devices, Omar Choudary, et. al.
  - テンプレート取得を、攻撃対象と違うサンプルで行わなければならない状況でのテンプレート攻撃
  - 異なるサンプル間の違いの大部分はDCオフセットである
  - LDA (Fisher’s Linear Discriminant Analysis)やPCA (Principal Component Analysis) をうまく使う
- Using the Joint Distributions of a Cryptographic Function in Side Channel Analysis, Yanis Linge, et. al.
  - 普通のSCAでは、平文か暗号文の情報を必要とする
  - 内部データの分布からのリークを学習することで、平文や暗号文を必要としないSCAの手法を提案

Emerging Topics for Side Channel Analysis

- サイドチャネル解析の変わった応用
  - Studying Leakages on an Embedded Biometric System Using Side Channel Analysis, Maël Berthier, et. al.
    - 指紋比較アルゴリズムの実行中の消費電力を測定し、解析することで、内部のセンシティブな情報を復元する
    - さらに、内部の比較スコアを得る
    - ここから、reference fingerprint情報に迫る
    - このような攻撃に対する対策も提案
  - Support Vector Machines for Improved IP Detection with Soft Physical Hash Functions, Ludovic Gustin, et. al.
    - IP (Intellectual Properties) の不正使用防止への応用
  - Verifying Software Integrity in Embedded Systems: A Side Channel Approach, Mehari Msgna, et. al.
    - ソフトウェアのintegrityを、サイドチャネル情報からチェックする

まとめ

- 最新動向
  - 正確なpower modelに依存しない、”generic”なdistinguisherに関する論文が増えてきている
    - MIA, KSA, etc
  - Distinguisher以外のSCAの改良も研究されている
  - 精密なfault injection
  - 暗号鍵取得以外へのサイドチャネル解析の用途
- COSADE2014の発表スライドは、http://cosade.org/program.html から入手可能

IPAの取り組み

IPAの取り組み

- ハードウェア脆弱性評価に関する人材育成
  - 新しい攻撃への耐性を評価する最先端のツールを整備して、日本の半導体ベンダ、ICカードベンダ、評価機関、大学などの研究機関が利用できる評価環境の整備を進めている。
    - 最先端の評価ツール及びテストビークル(評価対象のIC)を使用し、脆弱性を評価することで新しい攻撃手法を修得
    - ICカードの開発過程で利用し、対抗策を検証することで、高い攻撃耐性を持った製品開発が可能
    - 将来的な攻撃手法の研究活動に活用
    - ここで紹介した攻撃についても、IPA所有の装置での再現を実施予定
  - セミナーの開催
    - 次回はCHES(9月)、CARTES及びCARDIS(11月)の後に開催予定

参考文献

- Stefan Mangard, Elisabeth Oswald, and Thomas Popp,
  Power Analysis Attacks: Revealing the Secrets of Smart Cards.
  Springer, December 2006. ISBN 0-387-30857-1
- B. Gierlichs, L. Batina, P. Tuyls, and B. Preneel,
  Mutual Information Analysis – A Generic Side-Channel Distinguisher.
  In E. Oswald and P. Rohatgi, editors, Cryptographic Hardware and Embedded Systems - CHES 2008, volume 5154 of Lecture Notes in Computer Science, pages 426–442
  http://link.springer.com/content/pdf/10.1007/978-3-540-85053-3_27.pdf
- Oscar Reparaz, Benedikt Gierlichs, and Ingrid Verbauwhede,
  Generic DPA attacks: curse or blessing?
  http://cosic.esat.kuleuven.be/publications/article-2425.pdf

ご清聴ありがとうございました。