実験 D:CPA 研修

2019/8/30

1　本研修の目的

CPA (Correlation Power Analysis , 相関電力解析) は, 暗号モジュールにおいて暗号化処理時に消費される電力と, 処理から推定した消費電力の相関により秘密鍵を解析する解析手法である. バイトごとに鍵を推定することができるため, 鍵の探索空間を大きく減らすことができるなどの利点がある. 本研修では AES-128 (鍵長が 128bit の AES) を対象として, 取得した消費電力波形及び暗号文から CPA を用いて鍵値を解析する手法の理解を目的とする. なお解説は,AES の基本的な知識があることを前提としている. AES のアルゴリズムについては参考文献 [1] を参照すると良い.

2　CPA による鍵の解析

本章では,CPA を用いた解析アルゴリズムについて解説していく. ただし研修を目的とするため, 具体的なソースコードは示さずアルゴリズムの説明のみ行う.

2.1　概要

本節では, AES に対する CPA の概要について述べる. まず始めに, CPA の大まかな流れを図 1 に示す.
本研修では攻撃の前提として, 以下の情報・データが得られているものとする.

得られているデータ

- 暗号モジュールの消費電力波形 (暗号化処理の一定のタイミングで計測したもの)
- 消費電力波形に対応した暗号文
- AES 暗号中の S-box テーブル

図 1 より,CPA による解析は次の 3 つのステップに大別できる. ただし本研修では既に波形は用意されているものを使用するため, ステップ 1 については省略しステップ 2 から解説していく.

CPA の手順

1. 消費電力波形の計測及び暗号文の取得
2. 暗号文から消費電力を推定
3. 相関係数の計算と鍵値の推定

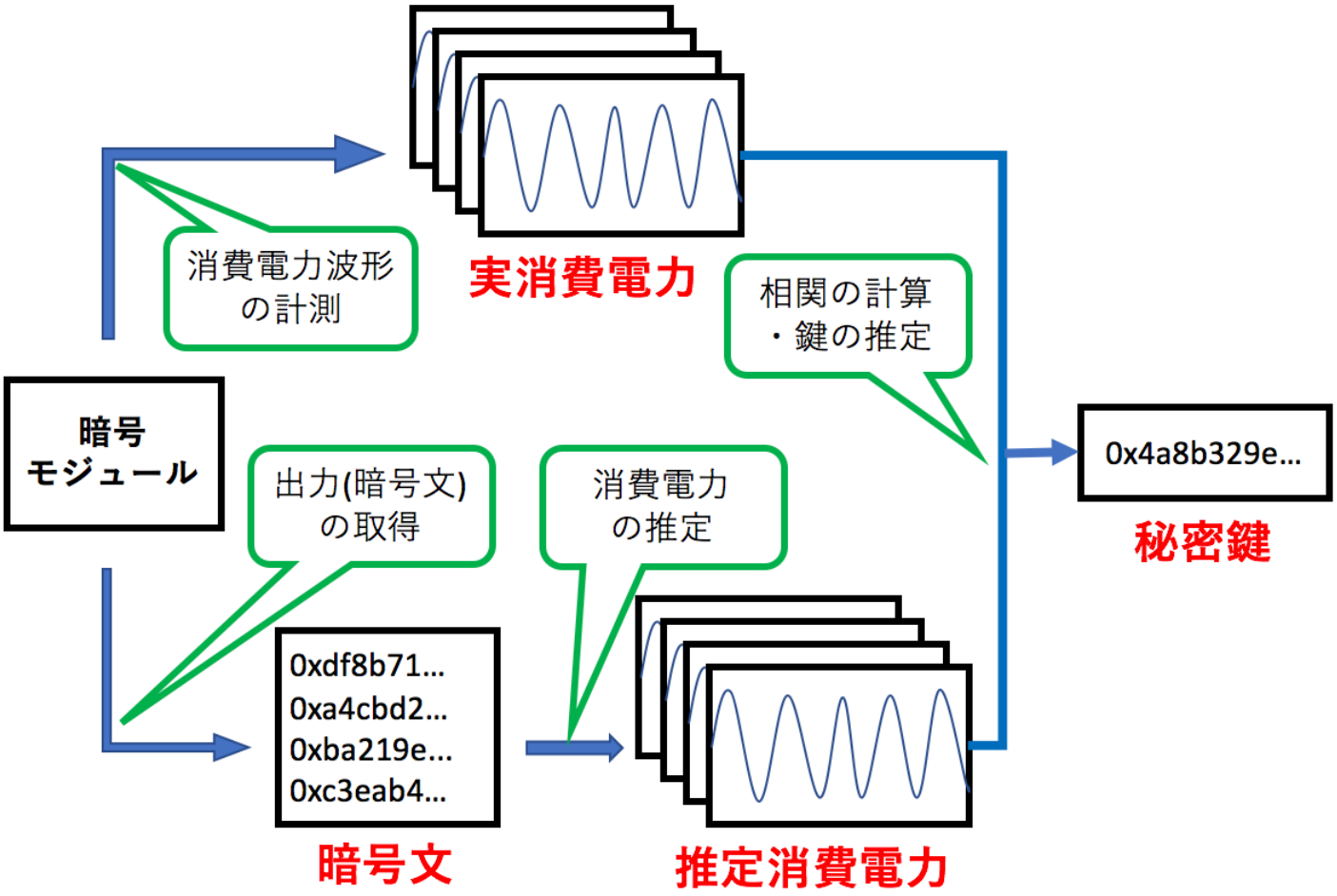


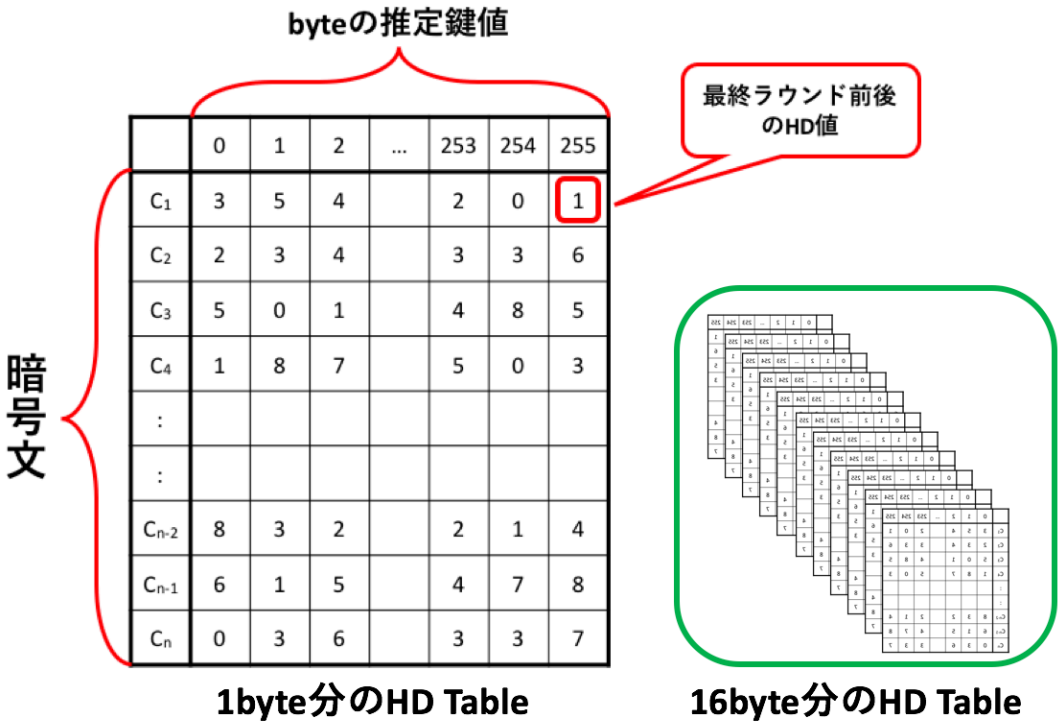
図 1: CPA の流れ (イメージ図)

2.2 消費電力の推定

本節では取得した暗号文をから消費電力を推定する手法について説明する. 消費電力の推定はどの処理が消費電力が大きいと仮定するかによって推定値が異なる. 本研修では各ビットの値の書き換えが消費電力が大きいと仮定し, バイトごとの最終ラウンド前後の値のハミング距離 (Hamming Distance, HD 値) を推定消費電力として使用する. ハミング距離は取得した暗号文を仮定したラウンド鍵を使って書き戻し, 暗号文自体との XOR をとることで求められる. 即ち, 暗号文の特定のバイトをそれぞれ c_x,c_y とすると,

$$\mathrm{HD}_x = \mathrm{InvSbox}(\mathrm{InvShiftRows}(\mathrm{AddRoundKey}(c_x))) \oplus c_y \tag{1}$$

ただし ShiftRows の処理によりバイトの位置がずれるため, 書き戻すバイトと XOR をとるバイトが異なる点には十分に注意が必要である. 推定消費電力は, 暗号文の全バイト・全鍵値について上のように求めた HD 値をテーブルとして扱う. 以後, このテーブルを **HD テーブル**と呼ぶ (図 2). HD テーブルは基本的に (暗号文数) $\times 16 \times 256$ の 3 次元テーブル, または (暗号文数) $\times$ 4096 の 2 次元テーブルとなる.



	0	1	2	...	253	254	255
C_1	3	5	4		2	0	1
C_2	2	3	4		3	3	6
C_3	5	0	1		4	8	5
C_4	1	8	7		5	0	3
:							
:							
C_{n-2}	8	3	2		2	1	4
C_{n-1}	6	1	5		4	7	8
C_n	0	3	6		3	3	7

図 2: HD テーブル

2.3 鍵値の推定

本節では前節で推定した HD テーブルと計測した波形から鍵値を推定する手法について説明する．本研修では計測した波形は csv 形式で保存されている．作成した HD テーブルは値の書き換えを行う瞬間の消費電力を推定したものであるため, 計測した波形からも値の書き換えが行われていると思われる時間を特定し値を抽出する必要がある．相関係数の計算には**ピアソンの相関係数**を使用する．各バイトで最も相関が大きくなったラウンド鍵の鍵値がそのバイトのラウンド鍵と推定できる．ただし実際の攻撃を考える際は, 波形によっては正しい鍵値でも相関係数が低くなるものや, 正しい鍵値と誤った鍵値の相関係数がほとんど変わらないものも存在するため, 鍵が推定できたと判断する基準については熟慮する必要がある．

2.4 鍵の書き戻し

AES において, ラウンド鍵は秘密鍵を拡張して生成する．反対に, ラウンド鍵の値がわかればそこから一定の操作を行うことで元々の秘密鍵を求めることも可能である. したがって, ラウンド鍵を解析できることは秘密鍵を解析できることと同義として扱うことができる．本書では鍵の書き戻しのアルゴリズムについては省略するが, 比較的容易に書き戻せるため研修ではラウンド鍵を書き戻し秘密鍵の値まで求めることとする．

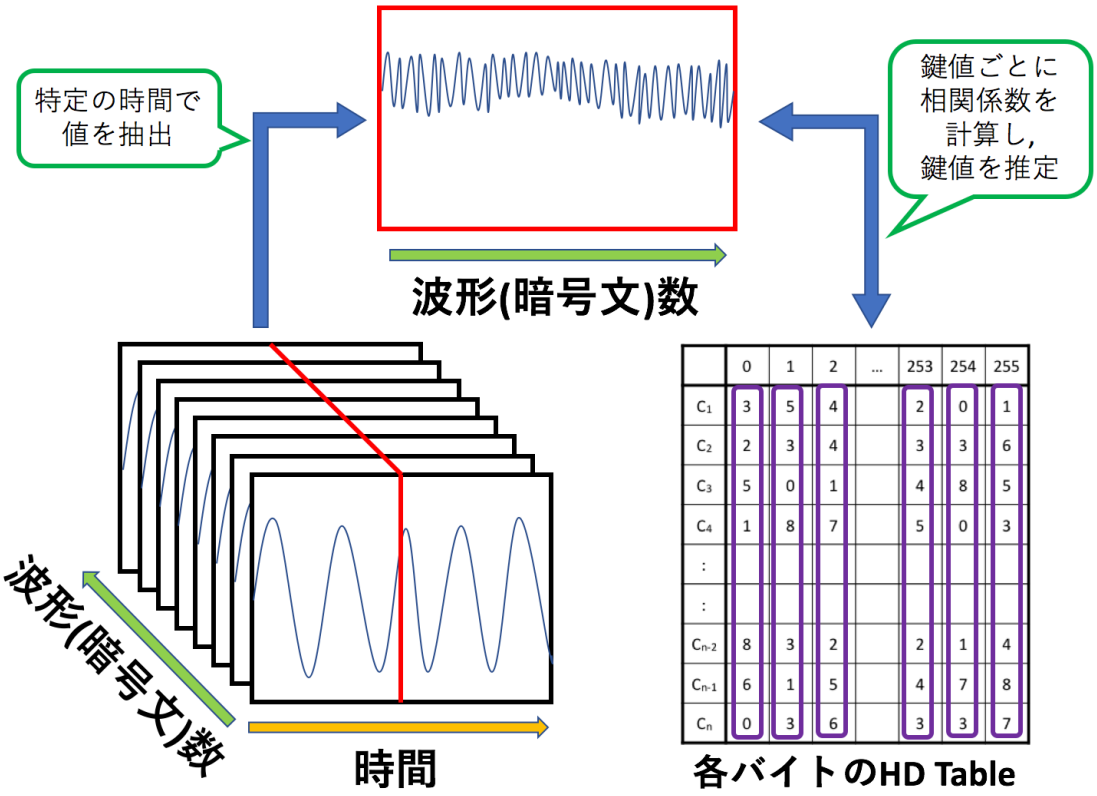


図 3: 鍵の推定

2.5 注意点・ヒント

- CPA はより少ない波形数で鍵を解析することが目標となるため, プログラムを書く際には波形数を変更しやすいように書くと良い.
- 使用する波形数に大きく左右されるが, プログラムの実行には数時間かかることも多いため, 探索範囲はなるべく絞って探索を行うと良い.
- HD テーブルの生成にも時間がかかるため, 一度作成したらテキストファイルに書き込むなどしておいて 2 度目以降はファイルを読み込む方が効率良く試行できる.
- 推定した鍵値が正しいかの判定法として, 各鍵値の波形数に対する相関係数のグラフを用いると判断しやすくなる (ただし, プログラムの実行にかかる時間は長くなるため注意が必要).

3 レポートについて

練習の一環として本研修のレポートは Tex により作成するものとする. 記述したプログラム, 推定された鍵値とその相関係数, 簡単な考察を書くこと.

参考文献

[1] AES nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf