## １．文献情報

・発行年　　2003
・文献名　　SCIS2003
・タイトル　　S-box におけるキャッシュ遅延を利用した AES へのタイミング攻撃
・著者　　角尾 幸保、久保 博靖、茂 真紀、辻原 悦子、宮内 宏

## ２．攻撃対象

CPU キャッシュを搭載する PC にソフトウェア実装された、ブロック長/秘密鍵長ともに 128 ビットの Advanced Encryption Standard(AES)。

## ３．攻撃の原理・前提

原理

・２テーブルモデル

２つの S-box から構成される暗号では、S-box S0,S1 の入力値、P0⊕K0 と P1⊕K1 が等しいか等しくないかの状態を区別できれば、P0⊕P1 から鍵の差分値 K0⊕K1（鍵差分）を得ることができる。等しい場合は１文で正しい鍵差分を得ることができる。等しくない場合は P0,P1 を変えながら十分な量について計算を行えば､正しい鍵差分だけは一度も出現しないので、誤っている鍵差分と区別できる。

・n テーブルモデル

S-box が n 個の場合、与えられる文を S-box の入力幅で Pi に分割し、排他論理和する鍵を Ki とすると、任意の 2 個について以下のどちらかが成り立つ。

$Pi \oplus Ki = Pj \oplus Kj$　　(3)
$Pi \oplus Ki \neq Pj \oplus Kj$　　(4)
ただし $i \neq j,\ 0 \leqq i, j < n$

ほとんどの S-box の入力が等しい文、あるいは、ほとんど異なる文を多数用いて正しい鍵差分と誤った鍵差分を区別する。

・暗号化時間による平文の選択

現実に S-box の入力値を抽出するのは非常に困難なので、暗号化時間を観測することで文がどの状態であるか推定する。式(3)が成立することが多い文はキャッシュヒットすることが多いので暗号化時間が平均より短くなり、式(4)が成立することが多い文はキャッシュミスが多くなるので暗号化時間が平均より長くなる。

前提

・暗号アルゴリズム、暗号アルゴリズムの実装方法が既知
・秘密鍵は攻撃中不変
・正確な暗号化時間を測定できる

## ４．攻撃方法

4.1 NIST が提供している AES のサンプルプログラムへの適用

第 1 ラウンド SubBytes における S-box データのキャッシュミス回数と暗号化時間の相関を調べる。暗号化時間に対する平文数には複数のピークが見られた。原因はガロア体乗算への入力値によって処理時間が異なるためである。暗号化時間に対するキャッシュミス回数の平均値を見ると、予想に反してピーク毎に暗号化時間が長いほどキャッシュミス回数が少なくなっている。鍵差分を計算するためにキャッシュミス回数が少ない平文を収集したいが、実験環境の変更などによりピーク位置の移動があっても良い様に、既知平文集合の中から暗号化時間の長い平文を必要な量だけ選択する。

ランダムに与える既知平文集合 P から、暗号化時間が長い平文集合 P'を抽出する。P の文数を 2^(n+m)とし、暗号化時間の長い方から上位 2^-n の文を 2^m 文選択し、P'とする。収集時間を約 1 時間以内と定め、そのときに指定可能な n,m を選択する。暗号化時間はキャッシュをクリアした上で 3 回測定し、最速のものを暗号化時間とする。

P'を用いて鍵差分を計算する。S-box Si と Sj に挿入される鍵の鍵差分を以下で求め、ΔK(i,j)の値ごとに出現回数をカウントする。

$\Delta K(i,j) = Pi \oplus Pj \quad (i \neq j,\ 0 \leqq i,j \leqq 15)$

P'は式(3)が成立するケースが多い平文を多く含んでいると考えられることから、求めたΔK(i,j)の値のうち、最もカウントされた値を鍵差分 Ki ⊕ Kj の候補とする。

2^23 既知平文を用いて、暗号化時間の長い方から上位 2^-5 の文を、2^18 文収集することにより、成功確率 72%で 96 ビットの鍵差分を求めることができた。平文の収集には Pentium III 1GHz を用いて約 26 分を要した。残りの鍵 32 ビットの全数探索を行えば秘密鍵の全ビットを求めることができる。

4.2 ガロア体乗算を修正したプログラムへの適用

ガロア体乗算の結果をあらかじめ配列で保持し、mul 関数の入力値でその配列を参照する

ようにし、引数の値によって処理量に差が発生しないように修正したプログラムについて、サンプルプログラムと同様に調査した。
2^23 既知平文を用いて成功確率 60%で 80 ビットの鍵差分を求めることができた。平文の収集には Pentium III 1GHz を用いて約 20 分を要した。

## ５．可能な対策

記載されていない。

## ６．他の文献との関連

特に無し。