5705

AES 暗号に対する線形解読法の理解と実装

Understanding and implementation of linear cryptanalysis for AES cipher

08548 三品佑一
指導教員 清水哲也

1. はじめに

AES 暗号とは米国政府が設定した次期米国政府標準暗号の名称であり、最も広く利用されていた暗号アルゴリズムである DES(Data Encryption Standard)の後継として規格化された。
この DES 暗号が近年のコンピュータ処理能力の向上により、線形解読法を用いて解読された[4]。これに伴い米国政府は DES に代わる共通鍵ブロック暗号を公募しアルゴリズムに必要とされる条件・評価基準や選定スケジュールを 1997 年 9 月に発表した[1]。そして 2001 年に安全性や処理速度等の評価基準から Rijndael アルゴリズム[5]が採用された。Rijndael とは SPN 構造を用いたブロック暗号であり、鍵が可変長であることが特徴である。

また鍵長が 128bit の AES 暗号は現在まで関連鍵不可能差分攻撃によって10ラウンドの内7ラウンドまでの解析実績がある[3]。

2. 研究目的

本研究では、文献[2]に基づき AES 暗号に対してブロック暗号で最も適用される線形解読法について理解し、AES 暗号に対する線形解読法を C 言語で実装することを目的とする。

3. 研究のアプローチ

線形解読法を実装するにあたって、線形解読法を理解し解読をシミュレーションする必要がある。シミュレーションする際に AES 暗号に対して解読を行うと複雑であり時間がかかるため、鍵長を 16bit とした暗号アルゴリズムに縮小し簡略化した上で解読をシミュレーションする。そしてその縮小版 AES 暗号のプログラムを作成し解読できる環境を整え解読をシミュレーションする。
シミュレーション環境を表 1 に示す。

表 1 シミュレーション環境

開発環境	VisualStudio2010
OS	Windows7 Professional 32bit
プロセッサ	Intel Core2Quad Q8400 2.66GHz
メモリ	4.00GB
開発言語	C++ Ver.16.00.30319.01

4. 結 果

本研究では文献[2]より4×4の S-box を導入した16bit(ブロック長)に縮小した AES 暗号のプログラミングを実行した。
擬似コードを図1に記し、実行結果を図2に示す。

```
Cipher(byte in[4*Nb], byte out[4*Nb], word w[Nb*(Nr+1)])
begin
  byte state[4,Nb]
    start=clock()
    state = in
    for round = 1 step 1 to Nr-1
      AddRoundKey(state, w[round*Nb, (round+1)*Nb-1])
      SubBytes(state)
      ShiftRows(state)
    end for
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    SubBytes(state)
    AddRoundKey(state, w[Nr*Nb, (Nr+1)*Nb-1])
    out = state
    end=clock()
end
```

図 1 16bit 縮小版 AES 暗号の擬似コード

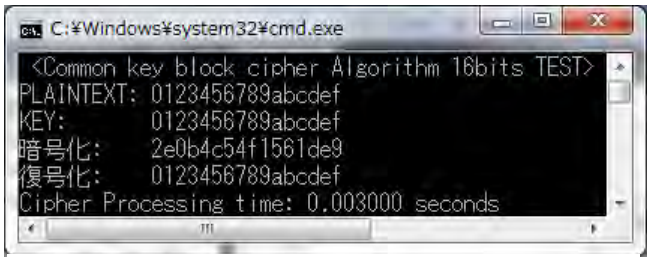

図 2 縮小版 AES 暗号プログラムの実行結果

5. おわりに

今回の研究では線形解読法の理解と線形解読法の解読対象である縮小版 AES 暗号のプログラムしか作成することができなかった。原因は線形解読法の理解に時間がかかってしまったためである。

今後は文献[2]より線形解読法のシミュレーションを行い、現状では求められていない全ての部分キービットに対しての線形近似式を求め、それらを実装することで、解読に必要な平文・暗号文や処理回数が判明し線形解読法を評価することが見込める。

文 献

[1] National Institute of Standards and Technology (2001), “fips-197”
[2] Howard M
“A Tutorial on Linear and Differential Cryptanalysis”
[3] Hadi Soleimany,Alireza Sharifi,Behnam Bahrak,Mohammadreza Aref “Cryptanalysis of 7-Round AES-128”
[4] Matsui Mitsuru (1994). “Linear Cryptanalysis Method for DES Cipher”
[5] Joan Daemen,Vincent Rijmen(2002)
”The design of Rijndael” Springer