# 暗号 AES の実装と評価

福田恵子　(指導教員：萩田真理子)

## 1　研究背景

1997年アメリカ合衆国において，それまで共有鍵暗号方式の代表的な規格であったDESが，急速な計算機の処理速度の上昇によって安全ではなくなってきたことを理由に，新しい規格としてAES(Advanced Encryption Standard)が世界規模で公募された．そして2001年3月，J.DaemenとV.Rijmenが提案したRijndaelがAESとして採択され公表された．以降，AESはアメリカ合衆国のみだけでなく，欧州の暗号規格NESSIEや日本の暗号規格CRYPTRECにも採用され，今日の共有鍵暗号方式の代表的な規格の一つとして利用されており，新たな共有鍵暗号方式の規格を提案する際の速度や安全性の評価基準としても利用されている．本研究では，評価基準に用いられるAES自身の安全性を考察していく．

## 2　AES(Advanced Encryption Standard)

### 2.1　仕様

**ブロック長** 128bit, 192bit，256bitの中から選択可能

**鍵長** 128bit，192bit，256bitの中から選択可能

**ラウンド数** 鍵長に依存．鍵長128bit：10回，192bit：12回，256bit：14回

本研究ではブロック長128bit，鍵長128bitを使用する．

### 2.2　暗号化アルゴリズム

AES(ブロック長128bit)の暗号化アルゴリズムは以下の通り．

1. 入力された平文を8bit毎に区切り，4×4マス(state)に振り分ける．
2. 入力された鍵をKeyExpansion関数を用いて【規定ラウンド数+1】(11)個に拡張．
3. stateに対してAddRoundKey変換を施す．
4. stateに対し，SubByte変換，ShiftRow変換，MixColumn変換，AddRoundKey変換を【規定ラウンド数−1】(9)回繰り返し行う．
5. 最終ラウンドのみ，SubByte変換，ShiftRow変換，AddRoundKey変換だけを行う．

## 3　評価方法と結果

### 3.1　安全性の高い暗号の条件

安全性の高い暗号の条件の一つとして，類似性の高い平文の集合が類似性の低い暗号文の集合へと変換されることが挙げられる．これは，類似した平文から類似した暗号文が生成されてしまうと，解読したい暗号文に類似した暗号文を用いて平文を推測されてしまう恐れがあるからである．従って，暗号文と真性乱数が識別不可能であることが必要とされる．

### 3.2　評価方法

本研究は，4.1の条件をAESが満たしているかについていくつかの評価を行った．評価方法と条件については以下の通りである．

**評価方法１** 各暗号文の1のビットの数を数え，その分布と同数の乱数の1のビットの数の分布を比較．評価条件は以下の通り．

- **平文空間** 128bit中1のビットが1つまたは2つだけの類似した平文の集合
- **鍵** 0(全て0のビットのみ，鍵長128bit)
- **ラウンド数** 1〜10ラウンドまで1ラウンドずつ観測

**評価方法２** 各暗号文を4byte毎に区切って格納し，格納時に以前に等しい値を格納していた場合を衝突1としてその回数を計測．

- **平文空間** 128bit中1のビットが1つまたは2つだけの類似した平文の集合
- **鍵** 0(全て0のビットのみ，鍵長128bit)
- **ラウンド数** 1〜10ラウンドまで1ラウンドずつ観測

本研究において4byte毎に区切ったのは，AESアルゴリズムが1byte毎の演算を行うことが多く，かつ4byteで1つの変換を行うからである．

### 3.3　結果

#### 3.3.1　評価方法１の結果

図1は評価方法1に基づいて，1ラウンドのみ操作した各暗号文の1のビットの数を数え，同数のものがいくつあるかを示している．図2は同数の乱数を同様に1のビットの数を数え，各々の個数を示したものである．図1と図2を比較すると，1ラウンドのみ変換を施したものには偏りが存在し，本来多いはずの中心部分にはあまり存在していないことがわかる．しかし，図1のように，3ラウンド操作すると分布が乱数と比較しても差がなくなってしまっている．

よって，評価方法1においては，AESは乱数性が高いことがわかった．

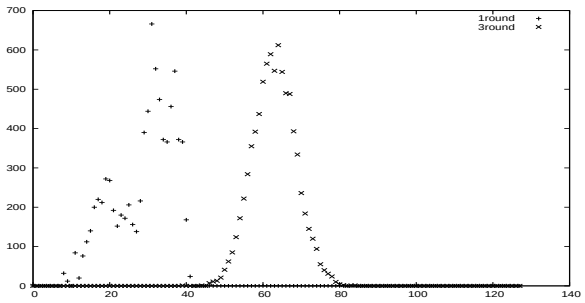

図 1: 1・3 ラウンド目の 1 の数の分布

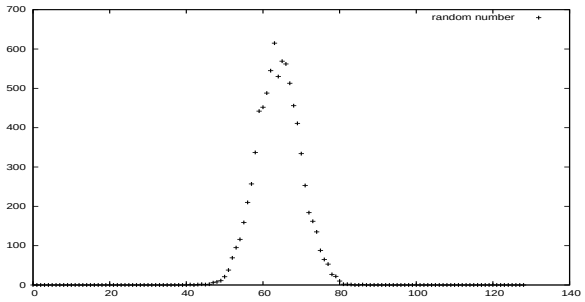

図 2: 同数の乱数の 1 の数の分布

### 3.4 評価方法 2 の結果

先に，衝突の発生する期待値を計算する．4byte 毎に取り出すことより，空間全体は $2^{32} = 4294967296$ 個の元が存在する．平文空間は ${}_{128}C_1 + {}_{128}C_2 = 128 + 8128 = 8256$ 個の元があり，これを 4byte 毎に区切るので，全体から 33024 個取り出したこととなる．$2^{32}$ の空間から 33024 個取り出した時の衝突回数の期待値は，多くとも $\sum_{k=1}^{33024} \frac{k-1}{2^{32}} = 0.126957$ となる．従って，真性乱数を同数取ってきた場合，衝突回数は 1 程度である．

ここで表 1 を見ると，1 ラウンドと 2 ラウンドでは衝突が確認されるが，3 ラウンド以降は衝突が確認されない．従って衝突回数の期待値が極めて小さいことから，評価方法 2 において，1 ラウンドと 2 ラウンドは乱数性が低いが，3 ラウンド以降は乱数性が高いことがわかる．

表 1: 各ラウンドでの衝突数

| Round | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| Number | 32495 | 25266 | 0 | 0 | 0 |
| Round | 6 | 7 | 8 | 9 | 10 |
| Number | 0 | 0 | 0 | 0 | 0 |

## 4 AES の各関数に対する評価

### 4.1 評価方法

3 節の結果より，本研究の評価方法においては，AES の乱数性は極めて高いことがわかった．ここでは，AES の 4 つの変換のうち，どの変換が重要な変換であるかを検証する．検証方法は以下の通りである．

**暗号化アルゴリズム** AES の SubByte 変換 (SB)，ShiftRow 変換 (SR)，MixColumn 変換 (MC)，AddRoundKey 変換 (ARK) の 4 つの変換のうち，どれか一つの変換を除いて暗号化を行う．

**評価方法** 各暗号文を 4byte 毎に区切り，3 節の評価方法 2 と同様の衝突を計測．

**平文空間** 128bit 中 1 のビットが 1 つまたは 2 つだけの類似した平文の集合

**鍵** 0(全て 0 のビットのみ，鍵長 128bit)

**ラウンド数** 1 〜 10 ラウンドまで 1 ラウンドずつ観測

### 4.2 結果

表 2 を見てわかるように，どの変換を抜いた場合においても衝突回数が格段に増加している．従って，AES の 4 つの変換は，どの変換を抜いた場合でも乱数性が非常に悪くなることがわかった．また，ShiftRow 変換と MixColumn 変換それぞれを除いた場合は等しい結果となり，これは各行 (列) に出現する種類の総数分を全体 (33024) から除いたものである．この原因は，同一のものは変換後も同一のものになるためである．

表 2: 除去した変換毎の衝突数

| Round | AES | 除去した変換 | | | |
|---|---|---|---|---|---|
| | | SB | SR | MC | ARK |
| 1 | 32495 | 32495 | 32495 | 32495 | 32495 |
| 2 | 25266 | 28706 | 31966 | 31966 | 29145 |
| 3 | 0 | 0 | 30908 | 30908 | 24770 |
| 4 | 0 | 14396 | 30908 | 30908 | 24768 |
| 5 | 0 | 14396 | 30908 | 30908 | 24768 |
| 6 | 0 | 0 | 30908 | 30908 | 24768 |
| 7 | 0 | 4496 | 30908 | 30908 | 24768 |
| 8 | 0 | 30908 | 30908 | 30908 | 24768 |
| 9 | 0 | 30908 | 30908 | 30908 | 24768 |
| 10 | 0 | 24388 | 30908 | 30908 | 24768 |

## 5 まとめと今後の課題

本研究を通して，AES の乱数性は高く，10 回のラウンド数は安全性を高めるために十分であることがわかった．そしてその安全性は 4 つの変換を全て組み合わせることに起因しており，全ての変換が不可欠であるという結果が得られた．

今後，4 節の結果を詳しく分析するために，各変換の特徴をさらに解析していきたい．また，変換の順序を入れ換えた場合の解析をしたい．

## 参考文献

[1] J. Daemen, V. Rijmen, ”AES Proposal: Rijndael”, AES submission, 1998.

[2] NIST, ”Advanced Encryption Standard (AES) ”, FIPS PUB 197, 2001.