暗号アルゴリズムの詳細評価

128bit-Block 暗号 SC2000

最大線形 / 差分確率、最大線形 / 差分特性確率

評価者: 青木和麻呂 (NTT)

平成 13 年 1 月 12 日

要約　SC2000 の差分解読法および線形解読法に対する安全性評価結果をまとめる。応募者は、3 段繰り返しおよび 4 段繰り返し的特性を用いて特性確率の上限を求めている。その結果、現在のところ SC2000 は差分解読法、および線形解読法に対して安全であると考えられる。

Abstract　This report verifies whether the SC2000 self-evaluation report is correct for differential cryptanalysis and linear cryptanalysis. The submitter computed the bound of the probability of 3 or 4 rounds iterative-like characteristic. As a result, SC2000 currently seems secure against differential cryptanalysis and linear cryptanalysis.

1　評価の方針 (はじめに)

以下の手順により評価を行なう。

1. **仕様書及び自己評価書全体の斜め読み**: SC2000 の概要を学ぶ
2. **本報告書の関係箇所の抽出**: 本評価書は差分解読法および線形解読法以外に関する記述も多数あるので差分解読法及び線形解読法に関する記述のみを選択
3. **仕様書及び自己評価書の関係箇所の熟読**: 自己評価内容の理解
4. **妥当性検証**: 自己評価内容の正当性検証
5. **既発表論文の調査**: WWW などを用い調査
6. **既発表論文のまとめ**: 前手順で調査した論文の要約作成
7. **報告書作成**: 全作業のまとめ

2　自己評価書の記述内容の解説 (妥当性検証)

2.1　記号

自己評価中などにある次の記号を利用する。

$$\mathrm{Hw} : \mathrm{GF}(2)^n \to \mathbf{Z} \qquad \text{ビット列のハミング重み}$$

$$\mathrm{t} : \mathrm{GF}(2)^n \to \mathrm{GF}(2); \qquad \mathrm{t}(x) = \begin{cases} 0 & \text{if } \mathrm{Hw}(x) = 0 \\ 1 & \text{if } \mathrm{Hw}(x) \neq 0 \end{cases}$$

$$\mathrm{Trunc} : \mathrm{GF}(2)^6 \times \mathrm{GF}(2)^5 \times \mathrm{GF}(2)^5 \times \mathrm{GF}(2)^5 \times \mathrm{GF}(2)^5 \times \mathrm{GF}(2)^6 \to \mathrm{GF}(2)^6;$$

$$\mathrm{Trunc}(x^{(0)}, x^{(1)}, x^{(2)}, x^{(3)}, x^{(4)}, x^{(5)}) = (\mathrm{t}(x^{(0)}), \mathrm{t}(x^{(1)}), \mathrm{t}(x^{(2)}), \mathrm{t}(x^{(3)}), \mathrm{t}(x^{(4)}), \mathrm{t}(x^{(5)}))$$

$$\delta_f(a, b) = \Pr_x[f(x) \oplus f(x \oplus a) = b]$$

$$\lambda_f(a, b) = \left(2 \Pr_x[x \bullet a = f(x) \bullet b] - 1\right)^2$$

2.2　応募者の主張

2.2.1　構成要素

S-box S_5 最大差分確率 2^{-4}、最大線形確率 2^{-4}

S-box S_6 最大差分確率 2^{-4}、最大線形確率 2^{-4}

M **関数** $\forall x \in \mathrm{GF}(2)^{32} \backslash \{0\}[\mathrm{Hw}(\mathrm{Trunc}(x)) + \mathrm{Hw}(\mathrm{Trunc}(Mx)) \geq 6]$
かつ $\forall x \in \mathrm{GF}(2)^{32} \backslash \{0\}[\mathrm{Hw}(\mathrm{Trunc}(x)) + \mathrm{Hw}(\mathrm{Trunc}({}^tMx)) \geq 6]$

L **関数** $\max(\mathrm{Hw}(a), \mathrm{Hw}(b)) \leq \mathrm{Hw}(\mathrm{Trunc}(c)) + \mathrm{Hw}(\mathrm{Trunc}(d)) \leq 2\min(\mathrm{Hw}(a) + \mathrm{Hw}(b), 6)$
但し、 $(c, d) = L(a, b)$

S-box S_4 最大差分確率 2^{-2}、最大線形確率 2^{-2}
かつ $\forall a, b \in \mathrm{GF}(2)^2[\delta_{S_4}((a, 0), (0, b)) = 0, \delta_{S_4}((0, a), (b, 0)) = 0]$
かつ $\forall a, b \in \mathrm{GF}(2)^2[\lambda_{S_4}((a, 0), (0, b)) = 0, \lambda_{S_4}((0, a), (b, 0)) = 0]$

B **関数** $\delta_B((a, b, c, d), (e, f, g, h)) \leq (2^{-2})^{w_d}$
かつ $\lambda_B((a, b, c, d), (e, f, g, h)) \leq (2^{-2})^{w_d}$
但し、

$$\begin{aligned} w_d &= \mathrm{Hw}(a \vee b \vee c \vee d) = \mathrm{Hw}(e \vee f \vee g \vee h) \\ w_l &= \mathrm{Hw}(a \vee b \vee c \vee d) = \mathrm{Hw}(e \vee f \vee g \vee h) \end{aligned}$$

で、

$$\begin{aligned} w_d &\geq \max(\mathrm{Hw}(a), \mathrm{Hw}(b), \mathrm{Hw}(c), \mathrm{Hw}(d)) \\ w_l &\geq \max(\mathrm{Hw}(a), \mathrm{Hw}(b), \mathrm{Hw}(c), \mathrm{Hw}(d)) \end{aligned}$$

も成立。

I **関数** 差分攻撃、線形攻撃等の安全性には全く影響がない。

2.2.2 n 段消去型攻撃

4 段以上は不可能で、 2 〜 3 段については状況によっては不可能との見積り (表 7)。

2.2.3 差分攻撃と線形攻撃

truncated vector を使った探索。

n 段消去攻撃の評価から 15 段の差分確率および線形確率の評価がされれば十分であることが分かる。次の場合のみ評価している。

1. B 関数をクロス接続に修正し、最良差分特性または最良線形特性を探索する。最良のものは「3 段周期の様なもの」であった。より具体的には、 active S-box の数が 0-m-n-0 であり、

<table>
<tr><th></th><th>R_5-R_5-R_3-R_3</th><th>R_3-R_3-R_5-R_5</th><th>R_5-R_3-R_3-R_5</th><th>R_3-R_5-R_5-R_3</th></tr>
<tr><td>差分</td><td colspan="2">$m+n=8$</td><td colspan="2">$m+n=7$ ($(m,n)=(2,5)$ または $(5,2)$)</td></tr>
<tr><td>線形</td><td>$m+n=8$</td><td colspan="3">$m+n=7$ ($(m,n)=(3,4)$ または $(4,3)$)</td></tr>
</table>

   というものであった。この結果に B 関数を当てはめて、 15 段の特性確率の上限を評価したところ

   差分特性確率 2^{-134} 以下

   線形特性確率 2^{-142} 以下

   であったので安全といえる。

2. B 関数で差分の半分が消失してしまう現象を利用し、 B 関数まで含めた 3 段繰り返し特性の最良のものを探索した。それを用いた 15 段の特性確率の上限を評価したところ

   差分特性確率 2^{-150} 以下

   線形特性確率 2^{-150} 以下

   であったので安全といえる。

これらの評価について応募者自身も

> なお、本方式による安全性評価では、可能な全ての差分、線形近似式を探索しつくしていることを証明しているわけではなく、また設計者らによって最良特性差分近似式、最良線形近似式が 2 段あるいは 3 段以下の周期を持つことを証明しているわけではないことをコメントしておく。本暗号の理論的な安全性保証については、今後の課題である。

と述べていることを付け加えておく。

2.3 評価者の解釈

応募者の主張は概ね妥当と思われるが、以下の問題点を発見した。

M 関数 仕様書の縦ベクトル、横ベクトルの使い方と異なる部分が自己評価書中多数あり、応募者が期待していると思われるように解釈可能な場合もあるが、期待と違うように解釈すると、評価が誤りになる部分もある。

I 関数 差分攻撃、線形攻撃等の安全性には特性確率の観点からは影響がないことは事実であるが、一般には影響がある。しかし、影響が無いことの証明は自己評価所中にはない。

n 段消去型攻撃 n 段消去した後の各ビットに影響する拡大鍵のビット数を評価している。しかし、完全に拡大鍵が独立として評価しているので、より厳密には拡大鍵の生成方法も考慮した評価が必要である。

差分攻撃と線形攻撃 1. 見つけた 3 段繰り返しのような差分特性や線形特性をどう R_3 と R_5 の繰り返しシーケンスに当てはめているのか不明である。

また、時間的な制約から下記問題点の妥当性検証、および以下の応募者の主張については、未評価である。

- S-box S_5 の最大差分確率、最大線形確率
- S-box S_6 の最大差分確率、最大線形確率
- M 関数の分岐数
- M 関数の truncated vector の入出力対応
- ${}^tM$ 関数の分岐数
- ${}^tM$ 関数の truncated vector の入出力対応
- L 関数の Trunc() の推移
- S-box S_4 の最大差分確率、最大線形確率
- S-box S_4 の差分分布表および線形分布表
- 具体的な truncated vector を使った探索

2.4　既発表論文の調査・まとめ

国内外でいくつかの発表があるが全て応募者によるものであり、その内容は自己評価書に含まれているので、改めて取り上げることはしない。

3　まとめ

応募者によりある程度、差分確率と線形確率の上限が評価されているが、応募者自身が述べているように現在の技術では全てを調べ尽くすことは困難であるので、いくつかの有望そうな攻撃に限って評価している。この結果からすぐに SC2000 が破れるということはまずないと考えられる。しかし、近い将来に理論的な差分解読や線形解読が成功するかもしれない。しかし、実用的な解読法が成功することはまずないだろうと考えられる。

全体概要

要約　SC2000 の差分解読法および線形解読法に対する安全性評価結果をまとめる。応募者は、3 段繰り返しおよび 4 段繰り返し的特性を用いて特性確率の上限を求めている。その結果、現在のところ SC2000 は差分解読法、および線形解読法に対して安全であると考えられる。

Abstract　This report verifies whether the SC2000 self-evaluation report is correct for differential cryptanalysis and linear cryptanalysis. The submitter computed the bound of the probability of 3 or 4 rounds iterative-like characteristic. As a result, SC2000 currently seems secure against differential cryptanalysis and linear cryptanalysis.