MARS の最大差分 / 線形特性確率について

盛合 志帆
日本電信電話株式会社

2001 年 1 月 12 日

概要　本報告書は CRYPTREC にて公募された共通鍵ブロック暗号 MARS の安全性の詳細評価報告であり、(1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告するものである。本評価の結果、最大差分特性確率については、 keyed transformation（16 段の cryptographic core) の最大差分特性確率として、自己評価書に記述されている 2^{-156} という値を妥当と判断する。最大線形特性確率については、 keyed transformation の最大線形特性確率として、文献 [11] に記述されている 2^{-120} という値を妥当と判断する。しかし、 MARS の最大差分／線形特性確率のより妥当な評価結果を得るには、さらに詳細な評価が必要で、多くの時間を要すると考える。

1　評価の方針 (はじめに)

本稿は CRYPTREC にて公募した共通鍵ブロック暗号 MARS の安全性の詳細評価報告であり、(1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告する。本評価は、基本的に自己評価書の正式版とされている文献 [1] をもとにして行なったが、誤訳と見受けられるものについては、適宜、英語版の文献 [2] を参照して報告書を作成した。

MARS は、差分解読法や線形解読法に対する安全性の評価や保証が困難なアルゴリズムである。

まず第一の理由は、多種類の演算を用いた複雑な構造に起因する。 MARS では排他的論理和、加算、減算、 9 ビット入力 32 ビット出力の S-box、乗算、固定ビットローテーション、データ依存ローテーションが使われている。差分解読法や線形解読法に対する安全性を評価するには、まず、これらの個々の演算の差分特性や線形特性を明らかにする必要があり、さらにこれらを組み合わせた時の差分特性や線形特性を評価する必要があるが、この点について現在はほとんど未解決である。さらに最大線形 / 差分確率や最大線形 / 差分特性確率をもつ経路を探索することは、 32 ビット単位の算術演算や

9 ビット入力 32 ビット出力の S-box が主なネックとなって現実的に不可能である[1]。また、 MARS の構造上 (特に E 関数の中まで立ち入った場合)、各演算の入出力ビット長を短縮した簡易版を評価することによりもとの暗号の強度を評価する shrinking[6], truncated cryptanalysis[7] などの技術の適用も困難である。

第二の理由は、 MARS が “cryptographic core” と呼ばれる core 層と “forward mixing”, “backwards mixing” と呼ばれる wrapper 層の異なる構造からなることによる。異なる構造を組み合わせていても、 MISTY[8] や Camellia[9] のように最大線形 / 差分確率や最大線形 / 差分特性確率の評価に影響を与えないように工夫されているものもあるが、 MARS の場合はそうではない。

もちろん、これらの設計方針は、差分解読法や線形解読法のみならず、将来の未知の攻撃法に対する耐性を高めることを期待したものと記述されている。しかし、個別の解読法を一つ一つ試みるしか安全性を評価する方法がないという点で、安全性に対する信頼を確立するのに、より時間を要することは否定できないだろう。

自己評価書においても、差分解読法や線形解読法に対する安全性評価は、 forward mixing (平文側の 8 段) と backwards mixing (暗号文側の 8 段) を除いた cryptographic core の差分特性確率および線形特性確率の “crude (though conservative)” な限界 [2] を示すにとどまっている。 “conservative” は、自己評価書 [1] では「控えめな」と訳されているが、これは差分解読法や線形解読法が提案された当初示された、攻撃者の立場からなるべく高い差分／線形特性確率をもつ経路をヒューリスティックに探す手法と解釈すべきであろう。これはより高い差分／線形確率の存在の可能性を否定しておらず、設計者の立場からは十分な方法とは言えないことに注意する必要がある。

しかしながら、現時点では、 MARS に対してはこのような “conservative” な解析方法に頼らざるを得ず、本報告書でもこの手法に基づき最大差分／線形特性確率の検証を行なう。

2　自己評価書の記述内容の解説 (妥当性検証)

自己評価書では、 forward mixing (平文側の 8 段) と backwards mixing (暗号文側の 8 段) を除いた cryptographic core (=keyed transformation) の差分特性確率および線形特性確率の上限が評価されている。 forward mixing と backwards mixing を除くことは差分解読法および線形解読法において “16R-attack”[10] を仮定することと等価であると記述されている。

自己評価書に書かれている評価方法の概要は以下の通りである。まず、 MARS で使われている各演算についてのいくつかの差分特性および線形特性を調べ、それを利用して E 関数のいくつかの有用な差分特性および線形特性を構成し、それらを組み合わ

[1] 文献 [2] に記述されている MARS の S-box の最大線形確率さえ正確に計算されていなかったことが、AES 選定期間 (Round 2) 中に何人かの研究者により指摘されている [3, 4, 5]。

せて keyed transformation 全体で構成しうる差分特性および線形特性の確率の上限値を評価している。keyed transformation は E 関数をラウンド関数とみなした 16 段からなる type-3 Feistel network である。

2.1 最大差分特性確率の評価

差分特性確率の上限値の評価方法に関する自己評価書の記述内容を説明する。この差分解析では、差分オペレーションとして排他的論理和が用いられている。

E 関数の解析 まず、E 関数の解析では、乗算の入力差分値の最下位の “1” のビット位置により、3 つの差分特性を検討している。これらの差分特性は自己評価書の表 8 に示されており、タイプ 1, タイプ 2, タイプ 3 の順に確率 2^{-16}, 2^{-8}, 2^{-9} の値をとる。但し、多くの差分解析では鍵を固定した場合の全てのデータに対する確率 (data probability) が用いられるのに対し、ここで示されている確率は全ての鍵とデータの両方に対する確率である。但しその内訳である data probability と key probability (データを固定した場合の鍵に対する確率) も示されている。

keyed transformation の解析 次に keyed transformation の解析に入る。基本的なアイデアは、E 関数を S-box のようにみなして active S-box の数の下限を見積もることで全体の差分特性確率の上限を見積もるというものである。以下では自己評価書の用語に従って解説する。E 関数の入力差分が非零である段を active round、零である段を passive round と呼ぶ。また、連続する 4 段を “super-rounds” と呼び、線形解析においてもこれをモジュール化の単位として利用している。この連続する 4 段を単位として扱う点は、type-3 Feistel network の “conservative” な解析では妥当と考えてよいと思う。

各 super-rounds で active round 数の最小値を考えると、E 関数への入力差分が非零ならば出力差分も非零となることから、各 super-rounds で active round が 1 つの場合はありえない。よって active round 2 つの場合が最小である。そこで各 super-rounds で active round が 2 つになる場合を検討する。まず連続する 2 段が active となる場合 (4.2.3 章 第 1 の試み) を考えるが、このような場合は存在しないことが分かる。よって連続しない 2 段が active となる場合で、E 関数にタイプ 1 特性を利用する場合 (4.2.3 章 第 2 の試み) を考える。しかしこの場合もうまくいかないことが示せるので、連続しない 2 段が active となる場合で、E 関数にタイプ 3 特性を利用する場合 (4.2.3 章 第 3 の試み) を考える。これが MARS のもっともらしい (plausible) 差分特性ということで、この差分特性を利用して差分特性確率の上限が評価されている。これは自己評価書の図 11 に示されている差分特性を 2 回繰り返したものである。この図 11 の差分特性の確率の上限は $2^{-9} \cdot p \cdot q$ で示される。但し

- 2^{-9} は E 関数のタイプ 3 特性の確率

- p は差分値 z と b がキャンセルする (次の段が passive round となる) 確率
- q は差分値 y と c がキャンセルする (その次の段の入力差分が最初の active round への入力と同様のパターンとなる) 確率

である。$p \leq 2^{-16}$, $q = 2^{-5}$ より $2^{-9} \cdot p \cdot q \leq 2^{-30}$ となる。keyed transformation は super-rounds を 4 つつなげたもので、各 super-rounds には図 11 の差分特性が 2 つ含まれるので、keyed transformation 全体の差分特性確率は $2^{-30 \cdot 8} = 2^{-240}$ で押えられることが示される。

差分 (特性) 確率の上限の評価　自己評価書には差分 (特性) 確率の上限を評価する別の方法も示されている (4.2.3 章 最後の段落)。具体的には、以下の条件で構成できる差分特性の確率の上限を評価している。

- 各 super-rounds 当たり少なくとも 2 つの active round を含む。
- 各 active round の差分確率の上限は 2^{-12}。(この確率は全てのデータと鍵に対する確率である。)
  — 最も可能性の高い E 関数の差分特性 (タイプ 3 [2]) が 2^{-9} で、これに加えて 3 箇所の加算でそれぞれ最大 2^{-1} の差分確率をもつ。
- super-rounds を接続するために、4 箇所のデータ依存ローテーションにおけるローテートビット数を調整する必要がある。(確率 2^{-15})
  — 2 箇所はある特定の値に固定 (確率 $2^{-5} \times 2^{-5}$)、残りの 2 箇所の値は揃っていなければならない (確率 2^{-5})。

よって keyed transformation 全体で構成できる差分特性の確率の上限は以下で押えられる。

$$2^{-12 \cdot 8} \cdot 2^{-15 \cdot 4} = 2^{-156} \tag{1}$$

この方法は初めに示した評価方法よりも弱い仮定のもとで構成しうる差分特性の確率の上限を評価している。(例えば途中段の差分値を特定の値やパターンに固定していない。) 評価者 (設計者) の立場からは、この値の方が MARS の差分特性確率の上限値として示すのに適当と考える。

自己評価書の 4.2.4 章において、差分解析における mixing phase の効果についての記述があるが、差分特性確率の上限を導出するために forward mixing と backwards mixing の両方が考慮されているのか (片方だけなのか) 不明であり、かつ “active” な mixing round 1 段あたりの確率 (2^{-20}) の根拠が書かれていない。よって、本報告書で forward mixing と backwards mixing まで考慮した差分特性確率については論じない。

[2] タイプ 2 の差分特性の確率は 2^{-8} であるが、なぜかこれは評価に使われていない。

2.2 最大線形特性確率の評価

線形特性確率の上限値の評価方法に関する自己評価書の記述内容を説明する。

用語の定義 はじめに、関数 $f : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^n,\ x \mapsto y = f(x)$ の線形 (特性) 確率を次式のように定義する。

$$LP^f(\Gamma x, \Gamma y) = |2 \cdot \Pr[x \cdot \Gamma x = f(x) \cdot \Gamma y] - 1|^2 \tag{2}$$

但し、自己評価書では次式の定義と同義の「バイアス」 $bias^f$ を用いて評価されているため、具体的な評価の説明にはバイアスを用い、まとめなどでは適宜言い換えることにする。

$$bias^f(\Gamma x, \Gamma y) = \left|\Pr[x \cdot \Gamma x = f(x) \cdot \Gamma y] - \frac{1}{2}\right| \tag{3}$$

E 関数の解析 自己評価書では、まず各基本演算の線形近似の特性について解析した後、 E 関数で構成できる線形近似を分類し、その最大バイアスを表 7 に示している。これを本報告書では表 1に示す。

表 1: 自己評価書 [1] による E 関数の線形近似とそのバイアス

線形近似	最大バイアス
$\{L\}$	2^{-15}
$\{M\}$	2^{-20}
$\{L, M\}$	2^{-20}
$\{L, R\}$ $\{I, L\}$ $\{I, L, R\}$	2^{-8}
$\{M, R\}$	2^{-7}
$\{L, M, R\}$ $\{I, L, M\}$ $\{I, L, M, R\}$	2^{-13}
$\{I, M\}$ $\{I, M, R\}$	2^{-6}
$\{I, R\}$	2^{-1}

keyed transformation の解析 次に keyed transformation の解析に入る。ここでも差分解析と同様に、 “super-rounds” と呼ばれる 4 つの連続するラウンドを単位として解析される。自己評価書の図 6 に従って E 関数の入力を I, 出力を R, M, L と呼ぶことにする。 “super-rounds” 内で探索を行なった結果、 “super-rounds” 当たり少なく

とも 2 箇所で M が active, 1 箇所で L が active でなければならないことが分かる。表 1によると、 M を含む E 関数の線形近似のうち、最大バイアスをもつもののバイアスは 2^{-6} であり、 L を含む E 関数の線形近似のうち、最大バイアスをもつもののバイアスは 2^{-8} である。よって super-rounds 当たりの最大バイアスを Piling-up Lemma により計算すると、

$$2^2 \cdot 2^{-6} \cdot 2^{-6} \cdot 2^{-8} = 2^{-18} \tag{4}$$

となる。 keyed transformation には super-rounds が 4 つ含まれるので、 keyed transformation 全体の最大バイアスは

$$2^3 \cdot (2^{-18})^4 = 2^{-69} \tag{5}$$

となる。これより、 keyed transformation の最大線形特性確率は 2^{-136}(= 最大バイアス 2^{-69}) と示される。

自己評価書の記述内容の妥当性　自己評価書の評価内容の妥当性には疑問があり、例えば最大線形特性確率に関して、次のような結果が AES Round2 Public Comment として NIST に提出されている。

まず、 Knudsen らが [3] において、 S-box の線形近似のバイアスが設計者らによる推定値 2^{-3} を上回るケースを指摘した。その後青木が S-box の線形確率の完全な分布を計算し [5]、最大バイアスが $\frac{84}{2^9}$ であったことを示している。

線形解析については Robshaw らが、文献 [2] で示されている評価法では、最大バイアス 2^{-49} の線形特性 (線形特性確率で 2^{-96}) が存在する可能性を指摘している [4]。 (文献 [2] では最大バイアス 2^{-69} と評価されていた。) まず、 Robshaw らは E 関数の線形近似とその最大バイアスを計算機実験などにより検証し、実際は表 2のようになることを示した。次に、文献 [2] で示されている評価法では、 “super-rounds” 当たり少なくとも 1 箇所で M が active, もう 1 箇所で L が active の線形近似を構成できるので、super-rounds 当たりの最大バイアスは

$$2 \cdot 2^{-6} \cdot 2^{-8} = 2^{-13} \tag{6}$$

よって keyed transformation 全体の最大バイアスは

$$2^3 \cdot (2^{-13})^4 = 2^{-49} \tag{7}$$

となることを主張している。

しかし、 MARS の設計者らは Robshaw らの主張に対し、表 2の結果は認めたものの、最大バイアス 2^{-49} の線形特性については文献 [2] の拙い文章による解釈の相違によるものと否定した。その代わり、「より洗練された (“slightly more sophisticated”)」近似を用いてバイアスの上限を 2^{-61} に引き上げた [11]。これは線形特性確率で 2^{-120} に対応する。

表 2: Robshaw と Lisa[4] によって示された E 関数の線形近似とそのバイアス

線形近似	最大バイアス	コメント
$\{L\}$	2^{-15}	2% は 2^{-15} 以上のバイアスをもつ
$\{M\}$	2^{-20}	
$\{L, M\}$	2^{-12}	文献 [1] では 2^{-20}
$\{L, R\}$ $\{I, L\}$ $\{I, L, R\}$	2^{-8}	
$\{M, R\}$	2^{-7}	平均バイアス 2^{-7} の線形近似が 2 つ存在 subkey 空間の 1/2 に対しバイアス 2^{-7} 以上 subkey 空間の 1/8 に対しバイアス $2^{-6.2}$ 以上
$\{L, M, R\}$	2^{-12}	文献 [1] では 2^{-13}
$\{I, L, M\}$ $\{I, L, M, R\}$	2^{-13}	5% は 2^{-13} 以上のバイアスをもつ
$\{I, M\}$ $\{I, M, R\}$	2^{-6}	
$\{I, R\}$	2^{-1}	

3 まとめ

CRYPTREC にて公募された共通鍵ブロック暗号 MARS の安全性の詳細評価報告として、(1) ブロック暗号の検証評価 — (a) 最大線形 / 差分確率もしくは最大線形 / 差分特性確率について報告した。

本評価の結果、最大差分特性確率については、 keyed transformation (16 段の cryptographic core) の最大差分特性確率として、自己評価書に記述されている 2^{-156} という値を妥当と判断する。

最大線形特性確率については、 keyed transformation の最大線形特性確率として、文献 [11] に記述されている 2^{-120} という値を妥当と判断する。

しかし、 1 章でも述べたように、 MARS の最大差分／線形特性確率のより妥当な評価結果を得るには、さらに詳細な評価が必要で、多くの時間を要すると考える。

参考文献

[1] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charajit Jutla, Stephen M. Matyas Jr., Luke O'Connor, Mohammad Peyravian, David Safford, Nevenko Zunic, "MARS (AES 候補の暗号) 共通鍵暗号方式 技術仕様書", IBM Corpotaion, September 22, 1999 (改訂).

[2] Carolynn Burwick, Don Coppersmith, Edward D'Avignon, Rosario Gennaro, Shai Halevi, Charajit Jutla, Stephen M. Matyas Jr., Luke O'Connor, Mohammad Peyravian, David Safford, Nevenko Zunic, "MARS – a candidate cipher for AES", IBM Corpotaion, June 10, 1998.

[3] Lars Knudsen, Håvard Raddum, "Linear approximations to the MARS S-box," Public Comments on AES Candidate Algorithms – Round 2, April 6, 2000 (available at http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm).

[4] Matthew Robshaw, Yiqun Yin, "Potential Flaws in the Conjectured Resistance of MARS to Linear Cryptanalysis," Public Comments on AES Candidate Algorithms – Round 2, April 27, 2000 (available at http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm).

[5] Kazumaro Aoki, "The Complete Distribution of Linear Probabilities of MARS' s-box", Cryptology ePrint Archive 2000/033, June 29, 2000 (available at http://www.eprint.iacr.org/2000/033).

[6] Eli Biham, Alex Biryukov, Adi Shamir, "Cryptanalysis of Skipjack Reduced to 31 Rounds Using Impossible Differentials", Advances in Cryptology — EUROCRYPT'99, Lecture Notes in Computer Science 1592, pp.12–23, Springer-Verlag, 1999.

[7] Lars Ramkilde Knudsen, "Truncated and Higher Order Differentials," Fast Software Encryption — Second International Workshop, Lecture Notes in Computer Science 1008, pp.196–211, Springer-Verlag, 1995.

[8] Mitsuru Matsui, "New Block Encryption Algorithm MISTY," Fast Software Encryption — 4th International Workshop, FSE'97, Lecture Notes in Computer Science 1267, pp.54–68, Springer-Verlag, 1997.

[9] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita, "Camellia — A 128-Bit Block Cipher Suitable for Multiple Platforms," in preproceedings of Seventh Annual Workshop on Selected Areas in Cryptography (SAC2000)", pp.41-54, August 14-15, 2000.

[10] Eli Biham, Adi Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer-Verlag, 1993.

[11] The IBM MARS team, “Comments on MARS’s linear analysis,” Public Comments on AES Candidate Algorithms – Round 2, May 12, 2000 (available at http://csrc.nist.gov/encryption/aes/round2/pubcmnts.htm).