MISTY の最大差分確率および最大線形確率について

評価者：NTT（神田　雅透）

2001 年 1 月 12 日

1　はじめに

1.1　MISTY の概要

MISTY は、1996 年に三菱電機株式会社より提案された 64 ビットブロック暗号であり、1996 年 11 月の ISEC 研究会 [9] ならびに第 4 回 Fast Software Encryption, FSE'97 [10] にて学会発表されている。MISTY の基本構造は、データブロック長 64 ビット、鍵長 128 ビットの N 段[1]Feistel 構造であり、2 段ごとに鍵依存線形変換関数である FL 関数が挿入されている。なお、推奨段数は $N = 8$ である。

MISTY の設計方針では、以下の 3 点が考慮され、安全性と実装性両面でのバランスを重視した設計が行われている。

- 安全性に関する何らかの数値的な根拠を持つこと
- プロセッサの種類によらずソフトウェアで実用的な性能を達成すること
- ハードウェア上で十分な高速性を実現すること

MISTY の設計方針として特筆すべき点は、設計時点において、差分解読法及び線形解読法に対する理論的安全性を保証する理論を構築し、それを実用暗号として始めて実現したことである。この理論は、後に「(差分解読法や線形解読法に対する) 証明可能安全性 (provable security)」の概念として、広く世界中に受け入れられた。これにより、MISTY が差分解読法及び線形解読法に対して安全であるとの評価が世界的にも認められている。

1.2　差分解読法及び線形解読法に対する安全性自己評価に関する記述

差分解読法及び線形解読法に対する自己評価は、自己評価書の第 2.1.1 節（差分解読法・線形解読法）に記述されている[2]。本レポートでは、自己評価書の記述内容および学会発表論文から、差分解読法及び線形解読法に対する安全性自己評価の妥当性を検証する。

1.3　差分解読法や線形解読法に対する安全性指標

差分解読法や線形解読法に対する安全性を示す指標として以下の 4 つが知られている。いずれの指標を用いて評価したのかによって、差分解読法や線形解読法に対する安全性評価の厳密性が異なることに注意されたい。最近では、以下に示す、“provable security” もしくは “practical security” を備えた暗号が望ましいとされている。

最大平均差分確率／最大平均線形確率　差分解読法や線形解読法に対する真の安全性を示す指標 [6, 12]。これらの確率が十分に小さいことが保証されれば、差分解読法や線形解読法に対して理論的に安全であることが証明される。しかし、全数探索並みの計算量が必要であるため、暗号全体についてこれらの確率を算出することは極めて困難である。

[1] N は 4 の倍数。

[2] さらに関連するところでは第 2.1.2 節、第 2.1.3 節、第 2.1.6 節、第 2.1.7 節がある。

最大差分特性確率／最大線形特性確率 攻撃者が、計算機などによって、差分解読法や線形解読法により暗号を実際に解読する場合の安全性を示す指標 [3, 7]。これらの確率は計算機実験などにより算出できることが多い。しかし、計算機能力の向上や探索アルゴリズムの改良等によって、これらの確率が変わることがあるので、評価時点での差分解読法や線形解読法に対する安全性の限界を示しているにすぎないと考えるべきである。したがって、これらの確率が十分に小さいことが差分解読法や線形解読法に対して安全であることの必要条件であって、十分条件ではない。

最大平均差分確率／最大平均線形確率の上界値 最大平均差分確率や最大平均線形確率の上界値を理論的に保証したことによって安全性を示す指標 [13]。これらの値が十分に小さいことが示されるのであれば、結果として最大平均差分確率や最大平均線形確率が十分に小さいことが保証される。この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）証明可能安全 (provable security)” という。

最大差分特性確率／最大線形特性確率の上界値 最大差分特性確率／最大線形特性確率の上界値を理論的に保証したことによって安全性を示す指標 [5, 14]。これらの値と最大平均差分確率や最大平均線形確率との間に理論的な関係はないため、これらの値が十分に小さいからといって、直接的に最大平均差分確率や最大平均線形確率が十分に小さいことが保証されるわけではない。しかし、実際の暗号の多くは、これらの値と最大平均差分確率や最大平均線形確率の値が極端に大きく離れているとは考えにくい。したがって、この指標により差分解読法や線形解読法に対して安全であると示すことを “（差分解読法や線形解読法に対する）実用的証明可能安全 (practical security)” という。実用的証明可能安全であることを証明するためには、64 ビットブロック暗号の場合、最大差分特性確率及び最大線形特性確率の上界値が 2^{-64} 以下となることが必要であるとされている。

2 自己評価書の妥当性検証

MISTY は、最初から差分解読法や線形解読法に対して十分な安全性を持つように設計されている。具体的には、拡大鍵が一様かつランダムに生成されると仮定して、**以下に示す差分解読法や線形解読法に対する証明可能安全性の理論をもとに設計**されている。なお、この理論については、FSE'96 [8] および IEICE 論文誌 [1, 11] に採録されており、**その正当性が第三者によっても確認されているものと考えられるので、その評価結果は十分に信頼できる**ものである。

定理 1（文献 [1]） 全単射ラウンド関数での最大差分（線形）確率を p_F とする。このとき[3]、r 段 ($r \geq 3$)Feistel 暗号での最大平均差分（線形）確率 P_r について、$P_r \leq p_F^2$ が成り立つ。

定理 2（文献 [8, 11]） n_1 ビット全単射関数 s_1 と n_2 ビット全単射関数 s_2 での最大差分（線形）確率をそれぞれ p_{s_1} と p_{s_2} であるとする ($n_1 \geq n_2$)。このとき、ラウンド関数が図 1に示すような l 階の入れ子構造であるとき、ラウンド関数での最大差分（線形）確率を p_F は、$p_F \leq (\max\{p_{s_1}p_{s_2}, 2^{n_1-n_2}p_{s_1}^2\})^l$ を満たす。

これに MISTY の仕様を当てはめると、2 階入れ子構造であり、また s_1 は 9 ビット s-box、s_2 は 7 ビット s-box に相当する。9 ビット s-box と 7 ビット s-box の最大差分確率及び最大線形確率はそれぞれ 2^{-8} と 2^{-6} であることが示されているので、定理 2 よりラウンド関数での最大差分確率及び最大線形確率はそれぞれ 2^{-28} 以下に、さらに定理 1 より（FL 関数無しの）3 段以上で最大差分確率及び最大線形確率はそれぞれ 2^{-56} 以下になることが示される。

64 ビットブロック暗号の場合、最大平均差分確率や最大平均線形確率は、理論上、2^{-62} まで小さくなることができることから、MISTY で示されている 2^{-56} 以下という値はまだ大きな値であると考えることもできなくはない。しかし、MISTY の推奨段数が 8 段であるうえ 2 段ごとに FL 関数が挿入されてること、さらに最大平均差分確率と最大平均線形確率はどちらも単調減少であることを考え合わせれば、3 段ですでに 2^{-56} 以下という値を達成しているので、実際の攻撃に利用するような 6 段あるいは 7 段での最大平均差分確率や最大平均線形確率

[3] 一般のラウンド関数のときの結果は文献 [13] に記述されている。

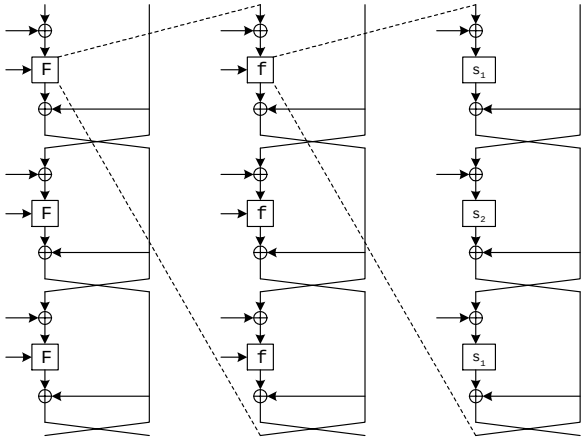

図 1: 入れ子構造

表 1: MISTY の最大差分（線形）特性確率の上界値

段数	1	2	3	4	5	6	7	8
上界値	1	2^{-28}	2^{-56}	2^{-56}	2^{-84}	2^{-112}	2^{-112}	2^{-140}

は理論限界の 2^{-62} に限りなく近いであろうと十分に期待できる。そして、何よりも、現在知られている世界中の実用暗号の中で、**差分解読法や線形解読法に対する証明可能安全を示し、かつ十分な実装性能を有しているのが MISTY しかないということは、64 ビットブロック暗号の分野における特筆されるべき事実**である。

また、以下では、特に自己評価書には記載されていないが、最大差分特性確率／最大線形特性確率の上界値の観点からも検証してみる。この評価手法は、多くの暗号における設計指針として、現在、最大平均差分確率／最大平均線形確率の上界値よりも広く使われているものである。したがって、この評価手法による結果は、他の暗号の安全性評価結果と比較する上で有用な情報を与えるものと思われる。MISTY のような全単射ラウンド関数を利用した Feistel 暗号に対して、SAC'98 に採録されている評価方法 [4] により最大差分特性確率や最大線形特性確率の上界値を示すことができる。

定理 3（文献 [4]） 全単射ラウンド関数での最大差分（線形）特性確率を p_F^* とする。このとき、R 段 Feistel 暗号での最大差分（線形）特性確率の上界値は、$(p_F^*)^{2r}$（$R = 3r, 3r+1$ のとき）もしくは $(p_F^*)^{2r+1}$（$R = 3r+2$ のとき）で表される。

定理 3 に MISTY の仕様を当てはめ、$p_F^* = 2^{-28}$ とおくと、表 1のように最大差分（線形）特性確率の上界値が得られる。この結果からは、MISTY が **5 段で（差分解読法や線形解読法に対して）実用的証明可能安全 (practical security) を満たしている**ことがわかる。したがって、この点からも、**提案者の推奨する 8 段 MISTY は、差分解読法及び線形解読法に対して十分に安全**であることの根拠となる。

3 まとめ — 妥当性の判定

本レポートでは、自己評価書の記述内容と学会発表論文から、差分解読法及び線形解読法に対する安全性自己評価の妥当性を検証した。

差分解読法及び線形解読法に対する安全性を数値的根拠を与えるために、**（差分解読法や線形解読法に対する）証明可能安全性 (provable security) の理論を構築し、それに基づいて設計されていることは従来の暗号にはない特徴**である。**この理論には、提案者だけでなく、第三者の立場にある暗号研究者らの結果も多数組み合わさっていることから、その正当性は十分に信頼できる**ものであると考えるべきである。したがって、3 段以上で最大平均

差分確率及び最大平均線形確率がそれぞれ 2^{-56} 以下になることを示すことによって、実際の攻撃に利用するような 6 段あるいは 7 段での最大平均差分確率や最大平均線形確率は理論限界の 2^{-62} に限りなく近いと十分に期待できるように設計されていることになる。

また、表 1で示したように、もう一つの有用な安全性評価指標である最大差分特性確率／最大線形特性確率の上界値の観点からも、**5 段で（差分解読法や線形解読法に対して）実用的証明可能安全 (practical security) を満たす**ことが示される。

これらの結果から、提案者の主張どおり、**推奨段数である 8 段 MISTY は差分解読法及び線形解読法に対して十分に安全**であることが導かれる。

なお、念のため付け加えるが、**提案者が利用した証明可能安全性の理論はあくまで差分解読法及び線形解読法に対してのみ有効なのであって、それ以外の解読法については別に検証する必要がある**。例えば、証明可能安全性の定理から、3 段以上であれば差分解読法及び線形解読法に対して安全であることを示している Feistel 暗号ならば、当然、6 段 Feistel 暗号は差分解読法や線形解読法に対して安全である。しかし、差分解読法から派生した不能差分利用攻撃 [2] において、全単射ラウンド関数を利用した Feistel 暗号には必ず 5 段の不能差分経路が存在することが知られており、この不能差分経路を利用すると（ラウンド関数の構成にもよるが）6 段 Feistel 暗号が解読できることがある。

このように、差分解読法や線形解読法に対して安全であることの証明が、即、別の解読法に対して安全であることの証明にはならない。特に、段数が非常に少ないの場合には、差分解読法や線形解読法に対する安全性証明と別の解読法に対する安全性証明は全く別のものであると考えたほうがよい。その意味において、MISTY の**推奨段数が 8 段であるのは適切な設定であると考えられると同時に、3 段以上で（差分解読法や線形解読法に対する）証明可能安全 (provable security) を満たしているからといっても 8 段より少ない段数（例えば 4 段）で利用することは避けるべき**である。

参考文献

[1] K. Aoki and K. Ohta, "Strict Evaluation of the Maximum Average of Differential Probability and the Maximum Average of Linear Probability," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E80-A, No.1, pp.2–8, 1997.

[2] E. Biham, A. Biryukov, and A. Shamir, "Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials," *Advances in Cryptology — EUROCRYPT'99*, LNCS **1592**, pp.12–23, 1999.

[3] E. Biham and A. Shamir, "Differential Cryptanalysis of the Data Encryption Standard," Springer-Verlag, 1993. (The extended abstruct appeared at CRYPTO'90 and Journal of Cryptology, Vol.4, No.1, 1991)

[4] M. Kanda, Y. Takashima, T. Matsumoto, K. Aoki, and K. Ohta, "A Strategy for Constructing Fast Round Functions with Practical Security," *Selected Areas in Cryptography — 5th Annual International Workshop, SAC'98*, LNCS **1556**, pp.264–279, 1999.

[5] L. R. Knudsen, "Practically secure Feistel ciphers," *Fast Software Encryption — Cambridge Security Workshop*, LNCS **809**, pp.211-222, 1994.

[6] X. Lai, J. L. Massy, and S. Murphy, "Markov Ciphers and Differential Cryptanalysis," *Advances in Cryptology — EUROCRYPT'91*, LNCS **547**, pp.17–38, 1991.

[7] M. Matsui, "Linear Cryptanalysis Method for DES cipher," *Advances in Cryptology — EUROCRYPT'93*, LNCS **765**, pp.386–397, 1994.

[8] M. Matsui, "New Structure of Block Ciphers with Provable Security aginst Differential and Linear Cryptanalysis," *Fast Software Encryption — Third International Workshop*, LNCS **1039**, pp.205–218, 1996.

[9] 松井充, "ブロック暗号アルゴリズム MISTY," 信学技報 *ISEC96-11*, 1996.

[10] M. Matsui, "New Block Encryption Algorithm, MISTY," *Fast Software Encryption — 4th International Workshop, FSE'97*, LNCS **1267**, pp.54–68, 1997.

[11] M. Matsui, "On a structure of Block Ciphers with Provable Security aginst Differential and Linear Cryptanalysis," *IEICE Transactions Fundamentals of Electronics, Communications and Computer Science*, Vol.E82-A, No.1, pp.117–122, 1999.

[12] K. Nyberg, "Linear Approximation of Block Ciphers," *Advances in Cryptology — EUROCRYPT'94*, LNCS **950**, pp.439–444, 1991.

[13] K. Nyberg and L. R. Knudsen, "Provable Security against a Differential Attack," *Journal of Cryptology*, Vol.8, No.1, pp.27–37, 1995.

[14] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, and E. DcWin, "The Cipher SHARK," *Fast Software Encryption — Third International Workshop*, LNCS **1039**, pp.99–112, 1996.