MISTY1の安全性に関する詳細評価

1　はじめに

MISTY1 はブロック長 64 ビット、鍵長 128 ビットの共通鍵ブロック暗号であり、データ攪拌部は Feistel 型に鍵依存線形変換 FL 関数を組み合わせた構造をしている。

本評価書では、最初に提案者による自己評価結果をまとめ、その後、データ暗号化部の安全性、鍵スケジュール部の安全性、実装に関連した攻撃法に対する安全性の各項目について検討を行なった。検討の結果、平文・暗号組の情報だけを用いた攻撃法に対し、データ暗号化部・鍵スケジュール部ともに目立った弱点は無かった。しかし、実装に関した攻撃では電力解析が脅威となり、対策が必要なことが明らかになった。

2　提案者による自己評価書の結果

MISTY1 の安全性に関し、提案者は次の 4 項目に分けて評価を行なっている。

a データ暗号化部の安全性

b 鍵スケジュール部の安全性

c 統計量情報による評価

d 実装に関した攻撃法に対する評価

各項目について評価を行なった結果、$a \sim c$ の項目については未解決な問題は有るものの、十分な安全性があると判断している。また、d の実装関連攻撃に対しても比較的小さなコストによって十分な安全性が確保できるとしている。

データ暗号化部の安全性　MISTY では、鍵全数探索以外の主要な攻撃法に対する安全性を評価している。最も重要な攻撃法と考えられる差分・線形解読法に対しては証明可能安全性の理論を利用し、安全性を確認している。その他の解読法も有効でないと判断している。

データ暗号化部の安全性に関する評価結果を表 1 に示す。

表 1: データ暗号化部の安全性の自己評価結果

攻撃方法	評価結果
差分解読法・線形解読法	証明可能安全性の議論などにより十分安全
短縮差分解読法	差分解読法に対する強度から十分安全
χ^2 解読法・分割解読法	構造に関する考察から十分安全
高階差分解読法	代数構造に関する考察から十分安全
不能差分解読法	鍵依存の FL 関数があるので十分安全
ブーメラン解読法	3 段で平均最大差分確率 2^{-56} 以下から十分安全
法 n 解読法	設計要素の特性の考察から、十分安全
非全射解読法	ラウンド関数の全単射性のため安全
Luby-Racoff 流ランダム性	S9 と S7 の安全性を仮定すれば、理論的な安全性が証明可能

鍵スケジュール部の安全性　MISTY1 では、鍵スケジュール部の特性に起因する攻撃法に対する安全性も評価している。

鍵スケジュール部の安全性に関する評価結果を表 2 に示す。

表 2: 鍵スケジュール部の安全性の自己評価結果

攻撃方法	評価結果
全数探索解読法	鍵長が 128 ビットなので現在の計算の技術に対しては安全
タイムメモリトレードオフ解読法	全数探索法と同様の計算量を要し安全
中間一致解読法	暗号化鍵の全ビットの影響が前段におよぶので安全
弱鍵・準弱鍵	FL 関数が有るので安全
関連鍵解読法	拡大鍵の制御が困難なため安全
スライド解読法	FL 関数があるので安全

統計量情報による評価　平文・暗号文間のビット相関やアバランシュ性は、必ずしも具体的な解読法に直結するとは限らないが、安全性の指標としては有効である。これらの指標を解析的に評価することは通常困難であり、計算機実験を利用して行なわれる。

提案者による統計量情報による評価結果を表 3 に示す。

表 3: 統計量情報による評価結果

攻撃方法	評価結果
アバランシュ効果	平文が 1 ビット変化したときの暗号文の変化を観測し、有意な偏りが存在せず
頻度検定	OFB モードで生成した擬似乱数列の分布を χ^2 検定と KS 検定で真性乱数と区別できず
衝突検定	OFB モードで生成した擬似乱数列の分布を χ^2 検定と KS 検定で真性乱数と区別できず

表 4: 実装に関した攻撃法に対する評価結果

攻撃方法	評価結果
タイミング攻撃	構成要素の処理時間が入力に依存せず、安全
電流解析攻撃・ 差分電流解析攻撃	S-box テーブルを動的に変更するなどの対策を取れば、かなりのレベルまで安全

実装に関した攻撃法に対する評価

3　データ暗号化部の安全性

3.1　差分解読法・線形解読法

MISTY1 は、3 段以上で最大平均差分確率と最大平均線形確率が 2^{-56} 以下で有ることが確認されている [2]。全体の段数が 8 段であり、1 段当たりの鍵ビット数も長いので、MISTY1 は差分解読法と線形解読法に対し、十分安全と考えられる。

3.2　短縮差分解読法

通常の差分解読法がビット単位で差分を分類したのに対し、短縮差分解読法ではそれより大きな単位、例えばバイト単位 (8 ビット単位) での差分の零／非零に注目した差分の波及確率を利用する [3]。

提案者は、短縮差分解読法の差分確率とは、通常の差分解読法における差分特性確率の和を考えることに相当すると述べていて、この表現自体は正しい。その次の、差分特性確率の和である平均差分確率の上界値が十分に小さいことから、短縮差分解読法に対して安全であるとするのは論理に若干の飛躍がある。しかし、実際に短縮差分解読法が MISTY1 に対して脅威となる可能性が低いと考えられる。

3.3 χ^2 解読法・分割解読法

χ^2 解読法や分割解読法は、平文と暗号文の部分情報間に統計的な相関性が存在するとき有効である。MISTY1 の構造を検討すると、等分割の単位である 32 ビット／16 ビット／8 ビットといった長さが検討対象となるが、最大平均差分・線形確率が十分に小さいことから、χ^2 解読法や分割解読法が有効である可能性は低い。

3.4 高階差分解読法

高階差分解読法では、中間出力の一部を GF(2) 関数の代数式で書き下し、その高階差分を求める選択平文を入力し、それに対する暗号文組が満たす代数方程式を解くことで拡大鍵の情報を推定する。MISTY1 の構成要素の代数次数は、S7 が 3 次、S9 が 2 次と低いので、高階差分解読法に対して有効であると予想された。実際、FL 関数抜きで 5 段まで攻撃できている [4]。しかし、これ以上攻撃可能段数を延ばすことは困難であると考えられ、FL 関数もあるので解読は困難と考えられる。

3.5 不能差分解読法

通常の差分解読法では、最も大きな差分特性確率を利用して拡大鍵の推定を行なった。不能差分解読法では逆に確率 0 の差分経路、つまり、起こり得ない差分波及パターンを利用して、拡大鍵の絞り込みを行なう [1]。ここで注意すべきは特性確率の意味で確率 0 となるパターンでなく、複数経路について足し合わせたものに対し、確率 0 となる必要があることである。一般にラウンド関数が全単射の Feistel 型暗号では、必ず 5 段まで不能差分解読法で解けることが知られている。よって、FL 関数抜きの MISTY1 では 5 段まで解読可能であるが、6 段以上の解読には成功していない。FL 関数の存在は不可能差分パターンを減らす効果があると考えられるので、8 段の MISTY1 に対しては、不能差分解読法は有効でないと考えられる。

3.6 ブーメラン解読法

ブーメラン解読法は、適応的選択平文攻撃を使った差分解読法の一種で、平文側と暗号文側の両方から真中の段に至る差分確率が大きいとき有効となる [1]。MISTY1 では 3 段で最大平均差分が 2^{-56} 以下なので、ブーメラン解読法は有効でないと考えられる。

3.7 法 n 解読法

法 n は、中間出力の n に対する剰余の分布に生じる偏りを利用した攻撃法であり、算術演算を基本とするアルゴリズムで有効である [1]。MISTY1 では算術演算が利用されておらず、最大平均差分・線形確率も十分小さいので、法 n 解読法は有効でないと考えられる。

3.8 非全射解読法

ラウンド関数が全射でない場合、出現しないバターンの存在を手がかりに拡大鍵の絞り込みを行なうのが非全射解読法である [1]。MISTY1 のラウンド関数は前者であるので、この解読法は適用できない。

3.9 Luby-Racoff 流ランダム性

非線形関数がランダムだと仮定したとき、アルゴリズム全体が擬似ランダムになることを理論的に示せるとき、Luby-Racoff 流ランダム性があると言い、アルゴリズムの構造に関する安全性の指標となる。ここで、擬似ランダムとは、非線形関数のサイズが無限大になる極限での漸近的性質である。擬似ランダム性は、安全であるための十分条件のようなもので、暗号アルゴリズムの構造はこの性質を満たすもので構成すべきである。MISTY1 では 5 段以上で擬似ランダムであることが示されている [7]。

4 鍵スケジュール部の安全性

4.1 全数探索解読法

全数探索法は、正しい平文／暗号文組を与える暗号化鍵をしらみつぶし的に探索する方式であり、いかなる暗号アルゴリズムにも適用可能である。3 節で取り上げた各種解読法が有効であるとは、暗号化鍵を特定するために必要とする計算量が全数探索に要するものより少なくて済むことを意味する。MISTY1 の暗号化鍵の長さは 128 ビットなので、2^{128} 回の暗号化の計算量が必要であり、現在の計算技術では困難である。

4.2 事前計算法

全数探索法の探索時間を削減するために、予め利用されることが分かっている平文での鍵と暗号文の対応表を作っておく方法。$64 * 2^{128}$ ビットの記憶容量を必要とし、現在の技術での適用は困難である。

4.3 タイムメモリトレードオフ解読法

事前計算法の記憶容量を削減するために、鍵／暗号文の適当な長さの系列を作り、系列の最初と最後だけ記憶しておく方法である [1]。劇的な記憶容量の削減には成功しておらず、鍵長 128 ビットの MISTY1 への適用は困難である。

4.4 中間一致解読法

アルゴリズムの前半で平文を順方向に暗号化したものと、アルゴリズムの後半で暗号文を逆方向に復号したものが一致することを利用した解読法である [1]。前半と後半に関与する鍵ビットの自由度が小さければ有効な解読法である。しかし、MISTY1 では任意の段の拡大鍵が暗号化鍵の全ビットに依存しており、有効ではないと考えられる。

4.5 弱鍵・準弱鍵

DES 暗号では、同じ鍵で平文を 2 回暗号化したとき、出力が平文に戻るとき、その暗号化鍵を弱鍵と呼ぶ。また、暗号化鍵を反転したもので暗号化したとき、暗号文が平文に戻る場合、準弱鍵と呼ぶ。これは、DES が Feistel 型であり、暗号化と復号の処理にある種の対称性が存在するために起こる現象である。MISTY1 では、準変換と逆変換の非対称性が大きい FL 関数を利用しているので、弱鍵・準弱鍵が存在する可能性は低いと考えられる。

ただし、弱鍵という用語は、攻撃が容易になる条件を満たす鍵の集合を指す場合が有る。MISTY1 の鍵スケジュールでは各段の拡大鍵が一致する暗号化鍵が 2^{16} 個存在することが知られている [6]。

4.6 関連鍵解読法

関連鍵解読法は、相互の関係式が分かっている 2 個の未知の暗号化鍵に対する平文・暗号文組が与えられ、それから暗号化鍵を推定する攻撃法である [1]。この攻撃が適用できるためには、2 個の鍵に対する中間データの多くが一致する状況が必要となる。MISTY1 の各段の拡大鍵は暗号化鍵の全ビットに依存しているので、そのような状況を作ることは用意ではないが、次に述べるスライド解読法のような例が見つかっており、有効性を否定しきることは出来ない。

4.7 スライド解読法

スライド解読法は、暗号の段を 1 段または複数段ずらしたときの中間データの系列が一致するような 2 個の平文を利用して、暗号化鍵を推定する解読法である [1]。FL 関数を除いた MISTY1 ではスライド解読法が有効である可能性が指摘されている [6]。しかし FL 関数の存在が、鍵パターンの周期性を壊すなど強度向上に寄与しているので、この解読が有効である可能性は低い。

5 実装に関する攻撃法の検討

MISTY1 自己評価書記載の内容を元に，実装に関する攻撃の詳細な検討を行う.

5.1 タイミング攻撃 (timing attacks)

タイミング解析 (タイミング攻撃) は、データ暗号化 (復号) の中間状態などが暗号鍵に依存して処理時間が異なる場合に、その相関性を利用して処理時間から直接拡大鍵の推定あるいは中間状態の推測を行い、鍵を推定する方法である。

タイミング解析は実装に依存した攻撃である為、ハードウェア、ソフトウェアいずれについても適用可能である。以下に MISTY1 の実装に際して対策の必要性の有無について検討する。

5.1.1 ハードウェア

ハードウェアにおいても、暗号利用の処理時間を詳細に観測することによりタイミング攻撃の適用は可能である。MISTY1 は小規模のテーブル参照あるいは論理回路で実装されるため、通常の実装においては鍵等に依存した処理時間の差異は考え難い。そのため、対策は必要ないかあるいは極めて容易であると考える。

5.1.2 ソフトウェア (PC)

PC で利用する CPU および OS は耐タンパーでないため、タイミング攻撃以外の実装に関係した攻撃方法も可能であることを考慮する必要がある。例えば実行されるコードや CPU 内部のレジスタの内容は比較的容易に観測可能である。このような直接的で強力な解析よりもタイミング解析のコストが大きければ、タイミング解析はその優位性を失うこととなる。

PC ソフトウェアは、OS 上で動作するため、OS に起因する処理時間の差異の影響を受ける。例えば、CPU のキャッシュヒットミスや、OS のメモリ管理により処理時間は変動する。この処理時間の変動よりも、鍵に依存した処理時間の変動が大きい場合にもに、タイミング攻撃は有意な情報量を取り出せるものと考える。

除算や乗算などの例外処理や処理の条件分岐の存在するとタイミング攻撃を適用できる処理時間の大きな変動が考えられるが、MISTY1 は小規模のテーブル参照あるいは論理回路で実装されるため、通常の実装においては鍵等に依存して処理時間の大きな差異が発生するとは考え難い。したがって、処理分岐を含まず、

処理時間がキャッシュミス程度の変動であり、タイミング解析に対して安全であると考えられる MISTY1 コードを作成することは可能である。

5.1.3 ソフトウェア (IC カード)

IC カードは耐タンパーデバイスであるため、IC カード内部のコードやレジスタの状態を観測することは極めて困難である。すなわち IC カードの内部を直接的に観測する手法の解析は適用に困難を伴う。

一方、IC カードでは搭載されているカード OS は PC のもの程高性能ではない。そのため、詳細な評価を行い、テスト環境を整えれば特定の処理のみの時間を外界から正確に測定することは可能である。このため、除算や乗算などの例外処理や処理の条件分岐による若干の処理時間の差異であってもタイミング攻撃の適用は可能である。

したがって、MISTY1 は小規模のテーブル参照あるいは論理回路で実装されるため、通常の実装においては鍵等に依存して処理時間の差異が発生するとは考え難い。処理分岐を含まず、処理時間が同じであり、タイミング攻撃に対して安全である MISTY1 コードを作成することは可能である。

5.2 電力解析

IC カード実装における電力解析を検討する。電力解析は、大きく分けて SPA(Simple Power Analysis) と DPA(Differential Power Analysis) に分類される。SPA は 1 回の暗号化処理における消費電力波形を利用し、鍵の導出を試みる。あるいは、SPA による、より詳細な評価を行うならば、複数の暗号化処理の消費電力波形を観測し、同一処理箇所における消費電力波形の差異に着目し、鍵の導出を試みる。また、DPA は複数回の暗号化処理における消費電力波形を統計処理し、鍵の導出を試みる。

IC カード実装においては、SPA および DPA に対して安全な暗号処理用コードあるいは電力解析に対する対策を施したハードウェアによる実装が必要である。MISTY1 は処理分岐を伴わずに実装可能であるため、タイミング解析や単純な SPA に対しては耐性が高い。

本評価では初歩的な SPA よりも一歩進んだ、複数データ間の消費電力波形の比較による SPA と DPA の適用可能性を検討する。

5.2.1 FO 関数

FI 関数の上位構造となる。従って、FI 関数において SPA 対策がなされるならば FO 関数は SPA に対して耐性を持つ。また、DPA に対しても同様に対策可能である。

5.2.2 FI 関数

FI 関数は S7, S9 と排他的論理和から構成される。FI 関数は任意の鍵入力に対して入出力が全単射となる。また各構成部品 (最小演算単位) は構成部品の入出力において全単射である。SPA により消費電力波形の差異を見つけることは難しい。また、自己評価書に述べるように文献 [8] の DPA 対策等を講じることにより、DPA についても消費電力波形と実際の処理データとの間の相関を除去し、かなりのレベルで DPA 対策を行えるものと考える。自己評価書では S7 のテーブルについて動的テーブル作成により 200 バイトの RAM 使用で対策可能との記述があるが、S9 についても同様の対策が必要である。S7 と S9 は交互に利用する為、S7 と S9 は別の RAM 領域にそれぞれ動的テーブルを作成する必要があると考える。この場合、少なく見積もっても RAM は 400 バイト必要である。IC カードの一般的な RAM 容量の制限から考えると、この対策は実施困難であり、より効率的な対策方法が望まれる。

5.2.3 FL 関数

FL 関数は論理積 (AND)、論理和 (OR)、排他的論理和 (XOR) から構成される。FL 関数は任意の鍵入力について全単射な写像となる。しかし、構成部品 (最小演算単位) レベルでは、拡大鍵との論理積あるいは拡大鍵との論理和演算において構成部品の入出力が全単射とならない。この特性を用いることにより、FL 関数に対して SPA/DPA による拡大鍵の推定が可能である。したがって、自己評価書には詳しい記述はないが、FL 関数においても SPA や DPA への対策が必要である。

以下に電力解析を用いた攻撃方法を具体的に考察する。

図 1 は MISTY の FL 関数である。拡大鍵との論理積あるいは拡大鍵との論理和演算は表 5 の真理値表に示すように全単射ではない。

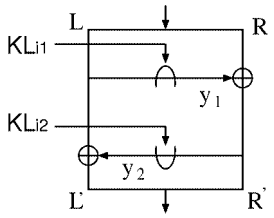

図 1: MISTY の FL 関数

表 5: 論理演算真理値表

論理積 ($y = k \cdot x$)

k	x	y
0	0	0
0	1	0
1	0	0
1	1	1

論理和 ($y = k \mid x$)

k	x	y
0	0	0
0	1	1
1	0	1
1	1	1

表 5 より、論理積 (AND) の出力においては 3/4 の確率で 0 が、1/4 の確率で 1 が出力される。論理和 (OR) の出力においても同様に 1/4 の確率で 0 が、3/4 の確率で 1 が出力される。

鍵が固定であるならば、電力解析を利用した選択暗号文攻撃が考えられる。まず暗号文すなわち FL 関数の出力 R' を

$$R' = (111\ldots)_2$$

とする。このとき、

$$L = L' \oplus (KL_{i2} \mid R') = L' \oplus ((111\ldots)_2) = \overline{L'}$$

ゆえに

$$\begin{aligned} y_1 &= KL_{i1} \cdot \overline{L'} \\ &= R' \oplus R = \overline{R} \end{aligned}$$

選択暗号文攻撃のため、FL 関数出力 R' が固定である。したがって y_1 と R の値 (0,1) のそれぞれの出現確率分布が同じである。また、y_1 の決定に用いる KL_{i1} と L のうち、拡大鍵 KL_{i1} は固定、$L = \overline{L'}$ である。

L' に一様にランダムな値を用いると、鍵との論理積出力 y_1 は表 5 に示す出現確率分布を持つ。拡大鍵 KL_{i1} が 0 か 1 かで異なる確率分布を持つ為、統計処理により DPA を用いた拡大鍵の推定は可能であると考えられる。

詳細は省略するが、同様に KL_i2 に対しても電力解析による拡大鍵の推定が可能である。

以上の解析により、自己評価書では S7 についてしか対策の必要性を述べていないが、FL 関数に対しても文献 [8] の 4.2 節 Bitwise Boolean Functions に述べる対策の実装が必要である考えられる。

5.3　実装に関する攻撃法のまとめ

MISTY1 の実装に関する攻撃法、タイミング攻撃 (Timing Attack), SPA(Simple Power Analysis), DPA (Differential Power Analysis) について検討を行った。MISTY1 は自己評価書でも述べているようにタイミング攻撃に対しては安全性が高い実装が可能な設計であり、万一脅威となる場合でも対策は容易である。

SPA や DPA といった消費電力解析に対しては、自己評価書に述べる S7 への対策実施以外にもさまざまな対策の実施が必要であり、IC カードへのソフトウェア実装においては IC カードのリソース上の制限から困難を伴うと思われる。ただし、この問題は消費電力解析に対して対策を行ったハードウェアの組み込みで解決可能である。

6　おわりに

平文・暗号文組のみを用いる攻撃について検討したところ、データ暗号化部・鍵スケジュール部ともに目立った弱点は無く、直接脅威になる解読法は存在しなかった。

しかし、実装に関する攻撃では、IC カードに対する電力解析が有効であることが明らかになった。自己評価書でも非線形関数 S7 についての対策が述べられているが、この他に S9 およびに鍵依存線形変換 FL の、合計 3 種類の構成要素に対する対策が必要である。ローエンドの IC カードの場合、ソフトウェアでの対応は困難で消費電力の推定を困難にするハードウェアの利用が現実的である。

参考文献

[1] 「共通鍵ブロック暗号の選択／設計／評価に関するドキュメント」, 通信・放送機構, 2000.

[2] 松井充. “ブロック暗号アルゴリズム MISTY”, 信学技報 ISEC 96-11, 1996.

[3] 松井充. “ブロック暗号 E2 の差分経路探索”, 信学技報 ISEC99-19, 1999.

[4] 田中秀麿, 久松和之, 金子敏信. “Fl 関数の無い MISTY1 に対する 6 階差分を用いた攻撃について”, 信学技報 ISEC98-37, 1988.

[5] 関春彦, 金子敏信. “CRYPTON の差分解読”, 信学技報 ISEC99-22, 1999.

[6] 古屋聡一, 宝木和夫. “既知平文攻撃を用いたスライド攻撃”, SCIS2000-A03, 2000.

[7] 杉田誠. “ブロック暗号 MISTY1 の擬似乱数性について”, 信学技報 ISEC97-19, 1997.

[8] Thomas S. Messerges, “Securing the AES Finalists Against Power Analysis Attacks”, FSE2000, 2000.