3-5　64ビットブロック暗号KASUMIに対する高階差分攻撃

3-5 A Study on Higher Order Differential Cryptanalysis of 64 Bit Block Cipher KASUMI

田中秀磨　杉尾信行　金子敏信
TANAKA Hidema, SUGIO Nobuyuki, and KANEKO Toshinobu

要旨

本論文では第三世代携帯電話標準暗号である128ビット鍵64ビットブロック暗号KASUMIの高階差分攻撃に対する強度評価について述べる。KASUMIは線形解読法や差分解読法に対して証明可能安全性を有するMISTY1の派生型である。本論文で示す攻撃は選択平文攻撃の一つであり高階差分特性を利用する。本研究の結果、KASUMIを攻撃するのに効果的な平文の選択法を計算機実験によって発見した。この効果的な選択平文を用いると5段KASUMI（元は8段構成）が2^{22}個の選択平文と2^{63}の計算量によって攻撃可能である。

In this paper, we show the strength of 128 bit secret key - 64 bit block ciipher KASUMI which is the standard cipher algorithm in the third generation mobile phone system, against higher order differential attack. KASUMI is a variant of MISTY1 which has provable security against linear and differential cryptanalysis. Our attack algorithm is a chosen plaintext attack and uses higher order differential property. We found the effective choice of plaintexts for the attack by computer simulations. When the effective chosen plaintexts are used, 5 round KASUMI (original has 8 round) can be attacked by 2^{22} chosen plaintexts and 2^{63} computational cost..

[キーワード]
選択平文攻撃，ブロック暗号，高階差分攻撃，確率的高階差分，3GPP
Chosen plaintext attack, Block cipher, Higher order differential cryptanalysis, Probabilistic higher order differential, 3GPP

1　はじめに

64ビットブロック暗号KASUMI[3]は三菱電機によって開発されたMISTY1[7]をベースに3GPPで開発された。MISTY1の持つ線形解読法と差分解読法に対する証明可能安全性の性質を継承しつつ、MISTY1の弱点であった代数的解読法に対する安全性を高めたと主張されている。また、第三世代携帯電話での使用を目的に開発されているため、小型実装が可能であり高速な処理を実現している。

安全性は提案元の3GPPで示されているが、例えば文献[1][9]のような強度評価結果も示されている。文献[1]は、Related-key攻撃による強度評価である。これは利用者AとBが使用している秘密鍵間にある関係が存在した場合、差分解読法によって秘密鍵の特定が可能になるという攻撃方法である。携帯電話における利用を前提としているため、場合によってはこのような攻撃が可能になり得るが攻撃者に非常に有利な条件が与えられている。Blundenらは5段のKASUMIと6段のKASUMIに対して攻撃を行い、5段の場合は2^{33}の計算量で、6段の場合2^{112}の計算量で攻撃が可能であると主張している。文献[9]は、本論文と同じ代数的解読法の一つである高階差分攻撃によるFL関数を省いた変

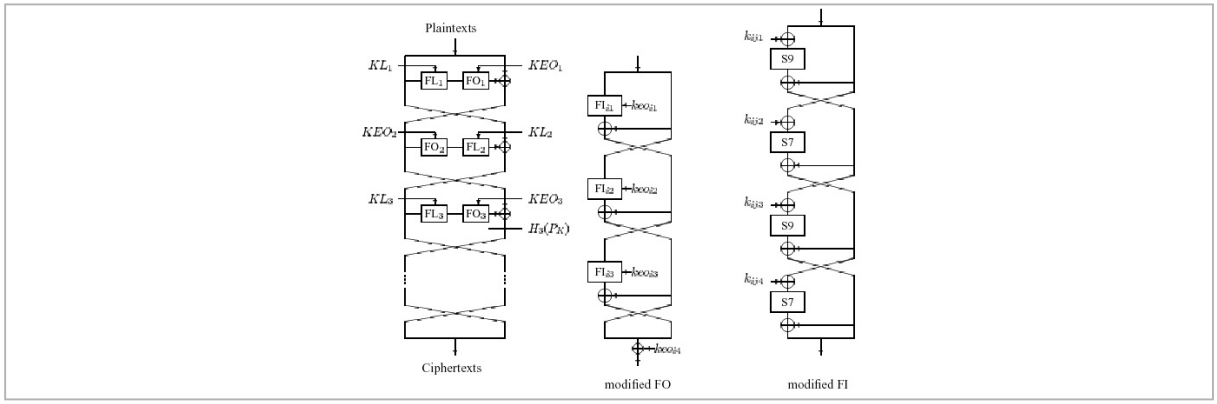

図1 変形 KASUMI

形 KASUMI に対する強度評価である。この結果、4 段のFL関数なし KASUMI が 1,416 の選択平文と 2^{22} の計算量で攻撃可能であることが示されている。

本研究では、文献[9]の攻撃方法を改良し FL 関数がある場合について 5 段 KASUMI の攻撃に成功した。選択平文攻撃による攻撃結果としては最高の結果である。これは平文サブブロック単位による選択平文について、最も効果的な選択法の発見が基になっている。さらに導出した攻撃方程式において、一部の未知数を全数探索で定めることによって、代数的解法における独立未知数の爆発的増加を防ぐことを可能にした。その結果、5 段 KASUMI が 2^{22} 個の選択平文と 2^{63} の計算量で攻撃可能であることが分かった。**2** において KASUMI の構造を示し、**3** において高階差分攻撃を簡単に示す。特に代数的解法については **3-4** を参照のこと。**4** で KASUMI の高階差分攻撃について、**5** でまとめを述べる。

2 64 ビットブロック暗号 KASUMI

KASUMI は 128 ビット鍵の 64 ビットブロック暗号である。図 1 に変形 KASUMI の構造を示す。変形 KASUMI は、以下で述べる攻撃方程式の表現を容易にするために、各段で用いられる拡大鍵の等価鍵を用いて位置をずらしたものである。基本構造は MISTY と似た Feistel 型の入れ子構造となっている。格段は 32[bit] 入出力の FO 関数と FL 関数で構成されている。仕様では 8 段である。FO 関数は 3 段の FI 関数で構成され、FI 関数は 2 種類の非線形関数 S-box は S7

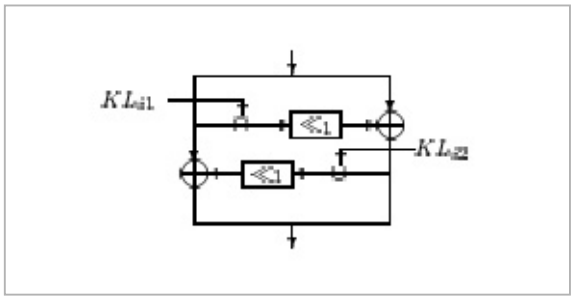

図2 FL 関数

と S9 で構成される。S7 と S9 はそれぞれ 7[bit] 入出力と 9[bit] 入出力であり、非対象 Feistel 型構造となっている。次数はそれぞれ 3 次と 2 次である。FL 関数は図 2 に示す線形関数である。ただし、鍵は非線形演算である OR で用いられている箇所があることに注意する。

3 高階差分攻撃

3.1 高階差分

$F(X;K)$ を $GF(2)^n \times GF(2)^s \rightarrow GF(2)^n$ の関数とする。

$$Y=F(X;K)$$
$$X \in GF(2)^n,\ Y \in GF(2)^n,\ K \in GF(2)^s \quad (1)$$

$(a_0, a_1, \cdots, a_{N-1})$ を線形独立な $GF(2)^n$ のベクトルとし、これらによって張られる部分空間を $V[a_0, a_1, \cdots, a_{N-1}]$ とする。ここで、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$ を $F(X;K)$ の X に関する N 階差分とすると、これは以下のように計算できる。

$$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X;K) = \sum_{A \in V_{[a_0,a_1,\ldots,a_{N-1}]}} F(X+A;K) \quad (2)$$

以下では $V[a_0, a_1, \cdots, a_{N-1}]$ が明らかなとき、$\Delta^{(N)}_{V_{[a_0,a_1,\ldots,a_{N-1}]}}$ を $\Delta^{(N)}$ と略記する。もし、$\deg_X\{F(X;K)\}=d$ であるならば、以下の性質が成立する。

性質 1

$$\deg_X\{F(X;K)\}=d \rightarrow \begin{cases}\Delta^{(d+1)}F(X;K)=0\\ \Delta^{(d)}F(X;K)=\text{const.}\end{cases} \quad (3)$$

3.2 攻撃方程式

図 3 は r 段 Feistel 型ブロック暗号の最終段を示している。$(r-2)$ 段目からの出力である $H^{(r)}(X)$ は以下のように計算できる。

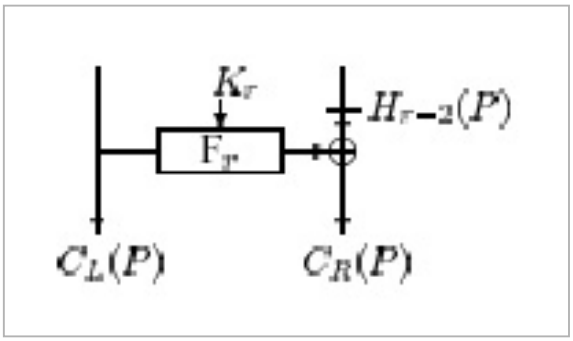

図3 r 段 Feistel 構造の最終段

$$H^{(r)}(X)=\tilde{F}(X;K^{(1,2,\ldots,(r-2))}) \quad (4)$$

ただし $\tilde{F}(\cdot)$ は $GF(2)^n \times GF(2)^{s\times(r-2)} \rightarrow GF(2)^n$ の関数であり、$K^{(1,2,\cdots,(r-2))}$ は 1 段目から $(r-2)$ 段目までの鍵とする。このように、$H^{(r)}(X)$ は平文側から計算できる一方で、暗号文側からも最終段の鍵 $K^{(r)}$ を推定することによって以下のように計算できる。

$$H^{(r)}(X)=F(C_L(X);K^{(r)})+C_R(X) \quad (5)$$

もし $\deg_X\{H^{(r)}(X)\}=d$ であるならば、以下の式が成立する。

$$\Delta^{(d)}\tilde{F}(X;K^{(1,2,\ldots,(r-2))})=\text{const} \quad (6)$$

式 (4) (5) (6) より、以下の式が導ける。

$$\sum_{A\in V_{[a0,a1,\ldots,ad-1]}}\{F(C_L(X+A);K^{(r)})+C_R(X+A)\}=\text{const} \quad (7)$$

もし const の値が定まれば、この方程式を解くことにより $K^{(r)}$ の値を定めることができる。それゆえ、以下ではこの方程式を攻撃方程式と呼ぶ。

3.3 全数探索による攻撃方程式の解法

全数探索を用いて攻撃方程式(7)を解く場合は、可能性のある $K^{(r)}$ の値すべてに対して式 (7) が成立するかを確認する。s[bit] の拡大鍵に対して N 階差分を用いている場合、計算量は最低でも $2^n\times 2^s$ 回の F 関数計算が必要となる。これは一般的に最も計算量を必要とする方法であるが、必要な選択平文数は最小である。

3.4 代数的解法による攻撃方程式の解法

文献[8]で示される代数的解法を適用することを考える。これは攻撃方程式を線形方程式へ変形することにより、計算量を大幅に削減する方法である。詳細は **3-4** に譲るが、線形化によって新たに再定義された独立未知数の総数を L とし、攻撃方程式の幅を H とすると、$\left\lfloor\frac{L}{H}\right\rfloor\times 2^N$ 個の選択平文と $\left\lfloor\frac{L}{H}\right\rfloor\times 2^N\times L$ 回の F 関数計算が必要となる。全数探索と比較すると、必要とする選択平文数が大幅に増加するが、計算量は無視できるほど小さくなる。

4 変形 KASUMI の高階差分特性

4.1 効果的な平文の選択法

高階差分攻撃に必要となる階数は、F 関数の次数によって決定される。しかしながら効果的に入力の値を決定することにより、F 関数の見かけの次数を引き下げることができる。高階差分攻撃に必要となる階数は、選択平文数や計算量の増加に大きく影響を与えるので、最小のものを探索する必要がある。

KASUMI の FO 関数の構造から、平文は以下のようなサブブロックに分割できる。

$$P=(X_7,X_6,X_5,X_4,X_3,X_2,X_1,X_0)$$
$$X_i\in\begin{cases}GF(2)^7, i=even\\ GF(2)^9, i=odd\end{cases} \quad (8)$$

本研究では、サブブロック単位で変数サブブロックと定数サブブロックに割り当て、効果的な選択平文の探索を行った。その結果、以下のような 16 階差分の場合、3 段目出力の一部のサ

ブブロックの 16 階差分値が 0 となることを計算機探索実験の結果発見した。

$$P_K = (0,0,0,0,X_3,X_2,0,0)$$
$$X_3,X_2 : \text{variable} \quad 0 : \text{fixed} \tag{9}$$

$H_3(P_K)$ を以下のような 3 段目からの出力とする。

$$H_3(P_K) = (h_3,h_2,h_1,h_0)$$
$$\begin{cases} h_3,h_1 \in GF(2)^7 \\ h_2,h_0 \in GF(2)^9 \end{cases} \tag{10}$$

発見した性質は $\Delta^{(16)} h_2(P_K)=0$ と表せる。

4.2 5 段 KASUMI に対する攻撃方程式の導出

発見した性質を図 4 に示す。これから、以下の攻撃方程式が導出できる。

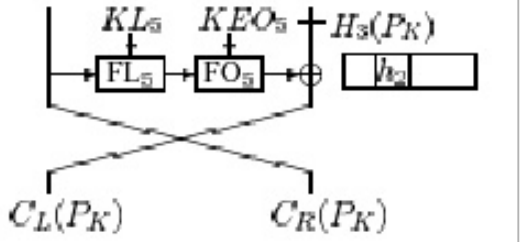

図4 5 段変形 KASUMI の最終段

$$\Delta^{(16)}\{FO_5(FL_4(C_R(P_K);KL_5);KEO_5)+C_L(P_K)\}=\Delta^{(16)}h_2(P_K)=0 \tag{11}$$

この式に含まれる未知数は以下のとおりである。

$$\begin{cases} KL_5 = \{KL_{51},KL_{52}\} : 32[bit] \\ KEO_5 = \{k_{511},k_{512},k_{513},k_{521},k_{522},k_{523},\} : 50[bit] \end{cases} \tag{12}$$

図 5 にこれらの関係図が示す。式 (11) を解くことにより 32+50 [bit] の拡大鍵を決定できる。

4.3 必要な選択平文数と計算量

本攻撃では、32 [bit] の未知数の決定に全数探索を、50 [bit] の未知数の決定に代数的解法を適用する。

代数的解法によって決定される拡大鍵による独立な未知数の総数を見積もる。S9 の次数が 2 次、S7 の次数が 3 次であることに注意し、また一部の拡大鍵は複数の S-box に入力されることを考慮しながら次数を解析する。その結果、k_{511}, k_{521} の次数は 4 次、k_{512}, k_{522} は 3 次、k_{513}, k_{523} は 2 次であることが分かった (図 5 参照)。その結果、独立未知数の総数 L は以下のように算出できる。

$$L = 2\times({}_9C_3+{}_9C_2+{}_9C_2)+2\times({}_7C_2+{}_7C_1)+2\times{}_9C_1$$
$$= 494$$

全数探索で未知数を決定する場合、未知数の大きさよりも方程式の幅が小さい場合、偽の値でも方程式を成立させるので、そのような偽鍵を排除するために複数の方程式を用意しなければならない。今、m 個の方程式を用意したと仮定すると 32 [bit] の真の値を定めるためには $2^{32}\times 2^{-m}<1$ が成立するだけの m を設定すればよい。$m=33$ とすれば十分偽鍵を排除できるので、$L=494$ と合計することにより 494+33=527 個の方程式が必要である。

攻撃方程式は 9 [bit] 幅の $h_2(P_K)$ を基に導出されているので、一組の 16 階差分から 9 個の方程式が得られる。従って、$\left\lfloor\frac{527}{9}\right\rfloor\times 2^{16}\approx 2^{22}$ 個の選択平文と $\left\lfloor\frac{527}{9}\right\rfloor\times 2^{16}\times 494\approx 2^{63}$ 回の F 関数計算が必要となる。

5 まとめ

本研究結果により、5 段 KASUMI が 2^{22} 個の選択平文と 2^{63} の計算量で攻撃可能であることが分かった。本攻撃は高階差分攻撃をベースに全数探索と代数的解読法を組み合わせた攻撃方法である。この結果、従来の攻撃結果を大幅に上回ることが可能となった。KASUMI は第三世代携帯電話の標準暗号であるが、小型実装が可能であるため、それに限らない利用も計画されている。本攻撃結果から仕様どおりの実装であれば、十分に汎用な攻撃方法である線形解読法、差分解読法、高階差分攻撃法に対して強度を持つといえるので、データ通信量に制限がある携帯電話以外での利用も問題ないと考えられる。

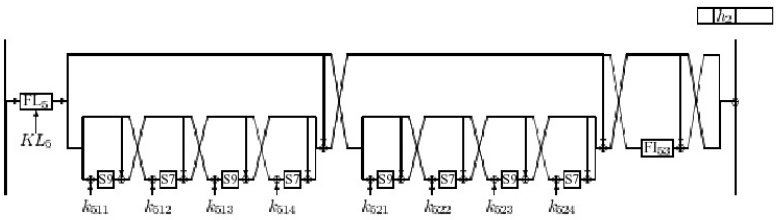

図5　5段目における拡大鍵

参考文献

1. Blunden, Escott, "Related key attack on reduced round KASUMI", FSE2001, LNCS2355, pp.289-297, Springer-Verlag, 2001.
2. Jakobsen, Knudsen, "The interpolation attack on block cipher", 4th Fast Software Encryption LNCS1267, pp.28-40, Springer-Verlag, 1997.
3. KASUMI, http://www.etsi.org/dvbandca/3gpp/3gppspecs.htm
4. Knudsen, "Truncated and higher order differentials", 2nd Fast Software Encryption LNCS1008, pp.196-211, Springer-Verlag, 1995.
5. Kuhn, "Cryptanalysis of reduced round MISTY", Eurocrypt2001, LNCS2045, pp.325-339, Springer-Verlag, 2001.
6. Lai "Higher order derivatives and differential cryptanalysis", Communications and Cryptology, pp.227-233, Kluwer Academic Publishers, 1994.
7. Matsui, "New structure of block ciphers with provable security against differential and linear cryptanalysis", 3rd Fast Software Encryption LNCS1039, pp.205-218, Springer-Verlag, 1996.
8. Shimoyama, Moriai, and Kaneko, "Improving the higher order differential attack and cryptanalysis of the KN cipher", 1997 Information Security Workshop LNCS 1396, pp.32-42, Springer-Verlag, 1997.
9. Tanaka, Ishii, and Kaneko, "On the strength of KASUMI without FL functions against higher order differential attack", ICISC2000, LNCS.2015, pp.14-21, Springer-Verlag, 2000.

田中秀磨（たなかひでま）
情報通信部門セキュリティ基盤グループ
博士（工学）
暗号理論、情報セキュリティ

杉尾信行（すぎおのぶゆき）
東京理科大学
暗号理論、情報セキュリティ

金子敏信（かねこしのぶ）
東京理科大学教授　博士（工学）
暗号理論、情報セキュリティ