コンピュータセキュリティ 10−14
(2000. 7. 25)

GOSTの差分解読(2)

関 春樹　金子 敏信†

通信・放送機構 横浜リサーチセンター
〒221-0031 横浜市神奈川区新浦島町1−1−32ニューステージ横浜

†東京理科大学 理工学部電気工学科
〒278-8510 千葉県野田市山崎2641

E-mail: hseki@yokohama.tao.go.jp, †kaneko@ee.noda.sut.ac.jp

あらまし ブロック暗号GOSTは、前のソビエト連邦で提案され、政府標準となっていた。著者等は99年3月のISEC研究会で、12ラウンドのGOSTに対する差分解読実験結果について報告した。今回はこの解読を拡張した結果について報告する。まず、平均で2^{51}個の選択平文を用いて13ラウンドのGOSTを解読出来、最も弱い鍵値では17ラウンドが解読出来る事を示す。次に、この差分解読をrelated-key attackと結合する事により拡張する。John Kelsey等は、GOSTにrelated-key attackを適用したが具体的な特性は示されていなかった。ここでは、具体的な特性を示す。平均で2^{56}個の選択平文で21ラウンドのGOSTを解読出来る。この解読は、Randomに生成されたS-boxの場合にも適用出来る。

キーワード ブロック暗号, GOST, 差分解読, Related-key attack

Differential Cryptanalysis of GOST(2)

Haruki SEKI　Toshinobu KANEKO†

Telecommunications Advancement Organization of Japan
1-1-32 Shin'urashima-cho, Kanagawa-ku, Yokohama 221-0031 Japan

†Department of Electrical Engineering, Science University of TOKYO
2641 Yamazaki Noda, Chiba, 278-8510 Japan

Abstract The block cipher GOST was proposed in former Soviet Union in 1989. In this paper we present differential cryptanalysis of reduced rounds of GOST. Introducing the idea of using a set of differential characteristics, which is a partitioning type, we can reduce the influence of the key value upon the probability as well as get high differential probability. Using 2^{51} chosen plaintexts the key of 13-rounds of GOST can be obtained. Next we expand the analysis with combining related-key attack. Using 2^{56} chosen plaintexts the key of 21-rounds of GOST can be obtained.

key words Block cipher , GOST , Differential attack , Related-key attack

1 はじめに

ブロック暗号GOSTは、前のソビエト連邦で提案され政府標準となっていた[8]。

本稿では、GOSTの差分解読について報告する。GOSTはFeistel型の構造を持ち、各ラウンドでの鍵演算が加算である。そのため、単一の差分特性を用いた解読は有効でない。その理由は、差分特性確率が入出力差分値のみでなく、サブ鍵の値によっても変わり、場合によっては0となってしまう。著者等は、文献[2]でこれを解決するための方法を示し、12ラウンドのGOSTに対する差分解読実験を行った。即ち、ある一定の条件に入る複数の入出力差分特性の集合を同時に利用する方法である。これは Truncated Differertial attack と同類であるが、S-boxの差分集合を用いるという点でPartitioning Type とも言える。この特性を用いる事により、鍵の値による特性確率への影響を減らすと共に、確率自体も大きく出来た。今回はこの解読を拡張する。

まず、平均で2^{51}個の選択平文を用いて13ラウンドのGOSTを解読出来、最も弱い鍵値では17ラウンドが解読出来る事を示す。

次に、この差分解読をrelated-key attack [6]と結合する事により拡張する。John Kelsey等は、GOSTにrelated-key attack を適用した[7]。しかし、具体的な特性は文献[7]の中で示されていなかった。本稿では、具体的な特性を示す。平均で2^{56}個の選択平文で21ラウンドのGOSTを解読出来る。

これらの解読はS-boxがRandomに生成された場合にも適用できる。

本稿は次の構成から成る。第2節では、GOSTのアルゴリズムを簡単に説明する。第3節では、単一の差分特性を用いた差分解読について述べる。第4節では、入出力差分特性の集合を同時に利用した差分解読について述べる。第5節では、related-key attack と結合した解読について述べる。第6節では、Randomに生成されたS-boxの場合について述べる。第7節でまとめる。

2 GOSTのアルゴリズム

図 1に示すように全体はFeistel型で、ラウンド数は32、ブロック長は64 bit、鍵長は256 bitである。

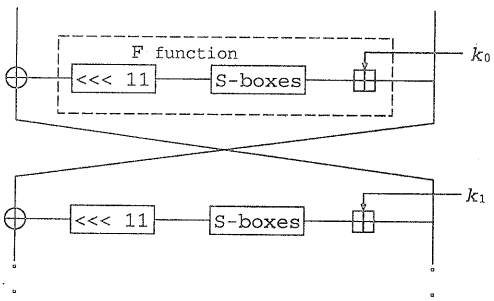

図 1: GOST round function

F関数は、次の演算から構成されている。

＋：2^{32}を法とする加算

S-box：8個の異なる4×4-bit S-box $S_1, S_2, \cdots, S_8$

<<< 11：11-bit左ローテーション

仕様ではS-Box の値は規定されていない。本稿では、The Central Bank of the Russian Federation で使用されていた[8]と言われる S-Box を対象として用いる(付録1参照)。

鍵スケジュールは単純である。256bitのマスタ鍵Kを8個の32bitブロック: $k_1, k_2, \cdot, k_8$ に分割する。各ラウンドでは表の様にサブ鍵を使う。

Round	1	2	3	4	5	6	7	8	9	10	～	15	16	17	18	19	20	21	22	23	24	25	26	～	31	32
key	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	k_1	k_2	～	k_7	k_8	k_8	k_7	k_6	k_5	k_4	k_3	k_2	k_1	k_8	k_7	～	k_2	k_1

3 単一差分特性を用いた解読

各ラウンドでの鍵演算は加算である。その様な暗号は、特性確率が入出力差分値のみでなく、サブ鍵の値によっても変わり、場合によっては0となってしまう(付録2参照)。図2は、最良の3-round 繰り返し特性の1つを示している。この特性は、1ラウンド当たり次の確率を持つ。

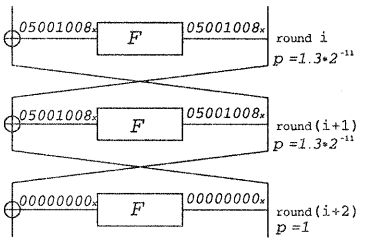

図 2: 最も確率の高い3ラウンド繰り返し特性の一つ

$$0 \leq Prob\{05001008_x \rightarrow 05001008_x\} \leq 1.5 \times 2^{-7} \tag{1}$$

ここで、X → Y は入力差分 X が出力差分 Y を生じる事を示す。全ての鍵値に対する平均確率は1ラウンド当たり 1.3×2^{-11}である。8ラウンドの特性確率は 2^{-53}である。2-R attack を用いると10ラウンドのGOSTが2^{56}個の選択平文で解読出来ると期待される。しかし、1/2以上の鍵空間でS-boxの差分確率は0になる(付録2参照)。8ラウンド特性では、確率が0にならない鍵値は 2×10^{-5}の割合でしか存在しない。

4 差分特性集合を用いた解析

差分特性確率の鍵依存性を小さくするために、ある一定の条件に入る複数の入出力差分特性の集合を同時に利用する方法を採用した。これは Truncated Differertial attack と同類であるが、S-boxの差分集合を用いるという点でPartitioning Type とも言える。この特性を用いる事により、鍵の値による特性確率への影響を減らすと共に、確率自体も大きく出来る。

4.1 差分特性集合

図3に示す様な差分特性集合を利用する。♯は、MSB(most significant bit) が0の4 bit差分である。この差分特性集合は active S-box の出力差分のLSB(least significant bit) が0の時に実現出来る。active S-box の数は、ラウンド番号が増えると共に1つずつ増え、ラウンド8以降は4に飽和する。

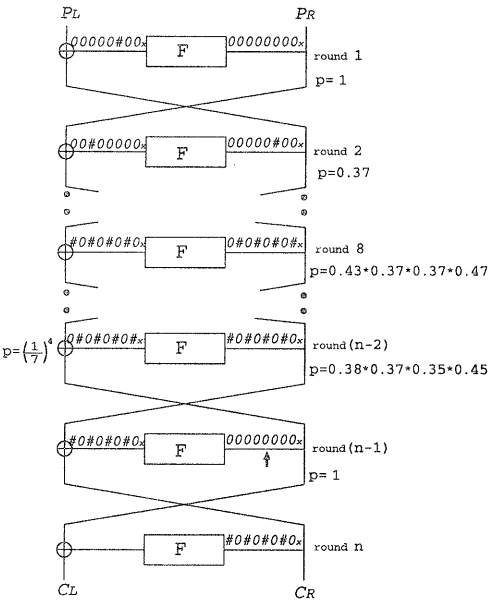

図 3: 差分特性集合

最初にS-boxの差分確率を見積もる。確率は、S-box番号と鍵値に依存して 0.30 から 0.75 まで変化する(詳細は付録3を参照)。p_{S_i}を全ての鍵値に対するS_iの平均確率とする。各ラウンドの平均確率は、active S-box のp_{S_i}の積である。例えば、ラウンド8,10の平均確率は$p_{S_1} \times p_{S_3} \times p_{S_5} \times p_{S_7} = .43 \times .37 \times .37 \times .47$。

4.2 GOSTの解読

最終ラウンドのサブ鍵を求めるために、図3に示す特性を利用する。最初に、$(n-1)$番目のF関数への32 bit入力差分を0に固定する。♯が1から7までRandomに分布すれば、これが成り立つ確率は$(\frac{1}{7})^4$である。nラウンドGOSTの特性確率p_nを見積もる。nが偶数の時、以下に示す値となる[1]。

$$p_n = p_{S_3}^{\frac{n}{2}-1} \times p_{S_6}^{\frac{n}{2}-2} \times p_{S_1}^{\frac{n}{2}-2} \times p_{S_4}^{\frac{n}{2}-3} \times p_{S_7}^{\frac{n}{2}-3} \times p_{S_2}^{\frac{n}{2}-4} \times p_{S_5}^{\frac{n}{2}-4} \times p_{S_8}^{\frac{n}{2}-5} \times \left(\frac{1}{7}\right)^4. \tag{2}$$

S/N比は以下で定義される[9]。

$$\begin{aligned} S/N &= \frac{2^k \times p}{\alpha \times \beta}. \\ k &= \text{解読対象の鍵ビット数} \\ p &= \text{差分特性確率} \\ \alpha &= 1\text{ペアから推定される鍵数} \\ \beta &= \text{Wrong apir の排除後に解析対象ペアが残る確率} \end{aligned}$$

[1]奇数の場合も同様に示される。

この解読では以下の値になる。

$$k = 32, \quad \alpha = 1, \quad \beta = 2^{-20}$$

よってS/N比は以下。

$$S/N = p_n \times 2^{52}. \tag{3}$$

表1はp、S/N、選択平文数の見積もりである。P_Lの3ビット(図3の♯)のみが異なる2^3個の平文のStructureを集めると、1つのStructureで28個の平文ペアを作れる。最も弱い鍵では、p_{17}が1.6×2^{-49}になり、17ラウンドのGOSTが解読出来る。

表 1: 攻撃に必要な平文ペアの見積もり

Rounds	Prob.	S/N	Chosen Plaintexts
12	1.2×2^{-44}	2^8	2^{45}
13	1.7×2^{-50}	7	2^{51}
14	1.5×2^{-55}	0.4	impossible

5 Related-key Differential Attack

Related-key attackは、最初文献[6]で示された。John Kelsey等は、GOSTにrelated-key attackを適用した[7]。しかし、具体的な特性は文献[7]の中で示されていなかった。本節では、4.2で述べた差分解読とrelated-key attackを結合し、具体的な特性を示す。2つの未知の鍵KとK^*を攻撃に用いる。その関係は以下である。

$$\begin{aligned} K &= (k_1, k_2, \cdot\cdot, k_8) \\ K^* &= (k_1 \oplus 80000000_x, k_2, \cdot\cdot, k_8) \end{aligned}$$

鍵Kに対する平文$P = (P_L, P_R)$と、鍵K^*に対する平文$P^* = (P_L \oplus 00000700_x, P_R)$を用いて、最初の8ラウンドを確率$\frac{1}{4}$でバイパス出来る[2]。図4はrelated-key attackを使った差分特性を示している。
9ラウンドの出力差分は、確率$\frac{3}{4}$で$00000\sharp00_x$となる。10ラウンド以降の特性は4.2で示したものと同じである。結果的に、nラウンドのGOSTの差分特性確率は$\frac{1}{4} \times \frac{3}{4} \times p_{n-8}$となる。ここで、$p_{n-8}$は式(2)から求められる。表2は$p$、S/N、攻撃に必要な平文数を示す。

表 2: Related-key attackに必要なペア数の見積もり

Rounds	Prob.	S/N	Chosen Plaintexts
20	1.8×2^{-47}	1.8×2^5	2^{49}
21	1.3×2^{-52}	1.3	2^{56}
22	1.1×2^{-57}	2^{-5}	impossible

[2] $(k_1 \oplus 80000000_x) + P_R = k_1 + (P_R \oplus 80000000_x)$。よってこの確率は$Prob\{8_x \rightarrow e_x\}$に等しい。全ての$k_1$について、$S_8$の確率は$\frac{1}{4}$である。

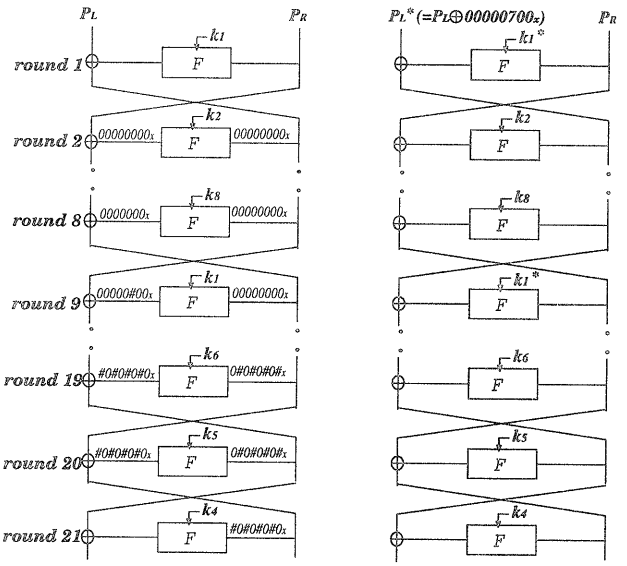

図 4: Related key による差分特性

6 Randomに生成されたS-boxの場合

GOSTではS-boxの値は規定されていない。そこで、本節ではRandomに生成されたS-boxの場合について検討する。

100,000個のS-boxをrandomに生成し、確率 $Prob\{$MSB=0の非零差分$\rightarrow$ LSB=0の非零差分$\}$ を求めた。表3は、確率と、それに対応するS-box数の割合、そして攻撃可能なラウンド数を示す。平均で、12ラウンドのGOSTが解読出来る。

表 3: Random S-box の場合の見積もり

Prob	0.34≤	0.38≤	0.42≤	0.47≤	0.50≤	0.54≤	0.625
Ratio(%)	62	27	8	2.3	0.5	0.4	
Rounds (differential)	12	13	14	15	16	17 ~ 20	20
Rounds (related-key)	19	20	21	22	23	24 ~ 26	27

次に、related-key attackと結合した解読について検討した。最初の8ラウンドをバイパスする最良の差分特性はS-boxの値により変わる。しかし、$\frac{1}{8}$以上の特性を常に見つける事が出来る。よって、ここではこの値を全てのS-boxに使う事にする。平均で19ラウンドのGOSTがrelated-key attackとの結合で解読出来る。

100,000個のS-boxの中で最大の確率は0.625である[3]。この場合には20ラウンドのGOSTが差分解読により、27ラウンドのGOSTがrelated-key attackとの結合により解読出来る。差分特性集合を用いた本解読はrandomに生成されたS-boxでも有効である。

[3]このS-boxは{9,7,5,1,11,15,3,13,0,4,12,10,14,8,2,6}。

7 まとめ

本稿では、差分特性集合を用いたGOSTの解読結果について述べた。The Central Bank of the Russian Federationで使われたS-boxの場合には、平均で2^{51}個の選択平文があれば、13ラウンドのGOSTが解読出来る。最も弱い鍵の場合、17ラウンドのGOSTが解読出来る。Related-Key attackとの結合により解読を拡張した。2^{56}個の選択平文を用いて21ラウンドのGOSTが解読出来る。

randomに生成されたS-boxの場合にもこの解読法が適用できる事も示した。平均12ラウンドのGOSTが差分特性集合を用いて解読出来、19ラウンドのGOSTがrelated-key attackとの結合により解読出来る。最も弱い鍵の場合、20ラウンドのGOSTが差分特性集合を用いて解読出来、27ラウンドのGOSTがrelated-key attackとの結合により解読出来る。

参考文献

[1] GOST, Gosudarstvennyi Standard 28147-89, *"Cryptographic Protection for Data Processing Systems "*, Government Committee of the USSR for Standards, 1989.

[2] 関 春樹, 金子 敏信, "差分解読法によるGOSTの解読実験," 信学会技術研究報告, ISEC98-80, pp.61–66, 1999.

[3] L.R.Knudsen, *"Truncated and higher order differentials"*, FSE'94, Lecture Notes in Computer Science , pp.196-211, Springer-Verlag, 1994.

[4] L.R.Knudsen,T.A.Berson, *"Truncated Differentials of SAFER"*, FSE'96, Lecture Notes in Computer Science , pp.15-26, Springer-Verlag, 1996.

[5] J.Borst,L.R.Knudsen,V.Rijmen, *"Two Attacks on Reduced IDEA"*, Eurocrypt'97, Lecture Notes in Computer Science , pp.1-13, Springer-Verlag, 1997.

[6] E.Biham, *"New Types of Cryptanalytic Attacks Using Related Keys"*, Eurocrypt'93, Lecture Notes in Computer Science , pp.398-409, Springer-Verlag, 1993.

[7] J.Kelsey, B.Shneier, D.Wagner, *"Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES"*, CRYPTO'96 Proceedings, Spring-Verlag, 1996, pp.237- 251.

[8] B.Shneier, *"Applied Cryptography"*, John Wiley & Sons, pp. 331-334.

[9] E.Biham, A.Shamir., *"Differential Cryptanalysis of DES-like Cryptosystems,"* Journal of Cryptology 1991.

付録1： S-Box

今回の解読に使用した8個の S-box の内容を以下に示す。表記は10進である。これらは、文献[8]に示されている値で、The Central Bank of the Russian Federation で使用されていたとされるものである。

S_8 = {1,15,13,0,5,7,10,4,9,2,3,14,6,11,8,12}
S_7 = {13,11,4,1,3,15,5,9,0,10,14,7,6,8,2,12}
S_6 = {4,11,10,0,7,2,1,13,3,6,8,5,9,12,15,14}
S_5 = {6,12,7,1,5,15,13,8,4,10,9,14,0,3,11,2}
S_4 = {7,13,10,1,0,8,9,15,14,4,6,12,11,2,5,3}
S_3 = {5,8,1,13,10,3,4,2,14,15,12,7,6,0,9,11}
S_2 = {14,11,4,12,6,13,15,10,2,3,8,1,0,7,5,9}
S_1 = {4,10,9,2,13,8,0,14,6,11,1,12,7,15,5,3}

付録2： S-Box の差分確率の鍵依存例

表はS_1の$Prob\{8_x \rightarrow 2_x\}$、$S_4$の$Prob\{1_x \rightarrow a_x\}$、$S_7$の$Prob\{5_x \rightarrow 1_x\}$の鍵依存性を示す。表中の鍵値は、それぞれのS-boxに対応する鍵の4ビットである。ここで、鍵加算による桁上がりが上位bitの差分値に影響を与える場合はカウントから除外した。これは今回用いた特性では上に位置する S-Box の差分値を 0 と規定しているからである。

表は鍵空間の半分以上について確率が0になる事を示している。

key	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
S_7	0	.13	0	.25	0	.13	0	0	0	.13	0	.25	0	.13	0	0
S_4	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0	.38	0
S_1	.13	0	0	0	0	0	0	0	0	.13	.13	.13	.13	.13	.13	.13

付録3： S-Box 入出力差分

表は各S-Boxの$Prob\{$MSB=0の非零差分 $\rightarrow$ LSB=0の非零差分$\}$を示している。ここで、鍵加算による桁上がりが上位bitの差分値に影響を与える場合はカウントから除外した。これは今回用いた特性では上に位置する S-Box の差分値を 0 と規定しているからである。

key	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f	average ps_i
S_8	.46	.46	.43	.43	.43	.46	.46	.46	.46	.46	.43	.43	.43	.46	.46	.46	.45
S_7	.75	.55	.43	.36	.39	.38	.43	.55	.75	.55	.43	.36	.39	.38	.43	.55	.47
S_6	.43	.39	.32	.30	.32	.32	.36	.39	.43	.39	.32	.30	.32	.32	.36	.39	.35
S_5	.46	.39	.36	.32	.32	.32	.36	.43	.46	.39	.36	.32	.32	.32	.36	.43	.37
S_4	.46	.38	.36	.32	.39	.32	.36	.39	.46	.38	.36	.32	.39	.32	.36	.39	.37
S_3	.43	.39	.32	.32	.32	.32	.43	.39	.43	.39	.32	.32	.32	.32	.43	.39	.37
S_2	.46	.43	.36	.36	.32	.38	.36	.38	.46	.43	.36	.36	.32	.38	.36	.38	.38
S_1	.57	.55	.43	.36	.39	.36	.36	.43	.57	.55	.43	.36	.39	.36	.36	.43	.43