SCIS 2001 The 2001 Symposium on Cryptography and Information Security
Oiso, Japan, January 23-26, 2001
The Institute of Electronics, Information and Communication Engineers

有限状態カオス暗号系の暗号解析
Cryptanalysis of the Finite State - Chaotic Encryption System

星野 文学*
Fumitaka Hoshino

あらまし カオスを用いたブロック暗号が幾つか発表されている. 本論文では, 差分攻撃に耐え得るカオス暗号とされる FS-CES に対して暗号学的な解析を行い, FS-CES が差分攻撃ではない他の攻撃に対しては脆弱であることを示す.

キーワード カオス暗号, Slide Attack

1 はじめに

カオスを用いたブロック暗号が幾つか発表されている [1,2]. それらの多くは, 簡単な構造のラウンド関数を何段も繰り返し用いると云う意味で既存のブロック暗号と良く似ている. 従って既存のブロック暗号に対する安全性評価手法をそのままカオス暗号に用いることが可能である. 実際, 幾つかのカオス暗号に対し暗号学的評価が行われている [3]. また, そうした評価に基づき差分攻撃に耐え得るカオス暗号として有限状態パイコネ変換を用いたカオス暗号が発表された [1].

しかしながらブロック暗号の決定的な安全性評価手法は現状では確立されていない. 安全性を保証するには, 既知の全攻撃法に対して, 各個に鍵の全数探索より非効率であることを示す以外に手段はない. 従って実用的なブロック暗号の設計を目指すには, 少なくとも代表的な攻撃アルゴリズムに関しては全て考慮する必要がある. カオス暗号も例外ではない.

2 FS-CES

2.1 FS-CES の定義

[1] に従い, s bit の平文空間, s bit の暗号文空間, 及び約 s bit の鍵空間をもつ離散化変形テント写像に基づく暗号系 FS-CES を次のように定義する.

- $M = 2^s$ として, 平文 X を $X \in \{1, \ldots, M\}$ とする.
- 鍵 A を $0.4M < A < 0.6M$ の整数とする.
- 離散化変形テント写像 $F_A(X)$ を

$$F_A(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, & (1 \le X \le A) \\ \left\lfloor \frac{M}{M-A}(M-X) \right\rfloor + 1, & (A < X \le M) \end{cases}$$

  と定義する. $X \in \{1, \ldots, M\}$ の時 $F_A(X)$ の値域は $\{1, \ldots, M\}$ で, X と $F_A(X)$ は 1 対 1 に対応する [1].
- $F_A(X)$ の逆写像を $F_A^{-1}(X)$ とする.
- 整数 n に対して, 写像 $F_A^n(X)$ を

$$F_A^n(X) = \begin{cases} F_A(F_A^{n-1}(X)), & (n > 0) \\ X, & (n = 0) \\ F_A^{-1}(F_A^{n+1}(X)), & (n < 0) \end{cases}$$

  と定義する.
- n を十分大きな正整数とする. 平文 X ,鍵 A に対する FS-CES の暗号化は $Y = F_A^n(X)$ であり, 暗号文 Y, 鍵 A に対する FS-CES の復号は $X = F_A^{-n}(Y)$ である.

2.2 FS-CES の特長

上記定義よりすぐに分かる FS-CES のブロック暗号としての特長を列挙する.

- 鍵スケジュールが無い.
- ラウンド関数が鍵に依存しない不動変換

$$F_A(M) = 1$$

  を持っている.

* NTT 情報流通プラットフォーム研究所, 〒 239-0847 神奈川県横須賀市光の丘 1-1, NTT Information Sharing Platform Laboratories, 1-1 Hikarinooka, Yokosuka-Shi, Kanagawa 239-0847, JAPAN

3 Slide Attack

Slide Attack [4] は鍵スケジュール及びラウンド関数の弱点をを利用する攻撃法である. 簡単のため全ラウンド鍵が同じであるとする. ラウンドを m 段ずらした時 (図 1 では $m = 1$), 図 1 の斜線部のように各ラウンドが全く等価な処理を行うような, 2 つの平文 X_0 及び X_1 が探索できれば, 全ラウンドのアタックは m ラウンドのアタックに帰着出来るというのが基本的なアイディアとなる.

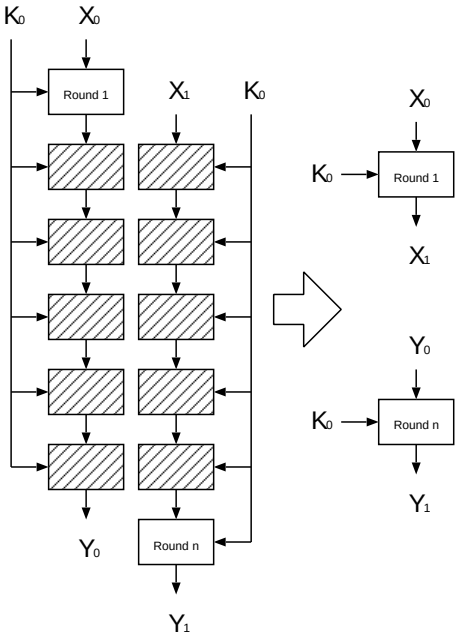

図 1: Slide attack

4 FS-CES に対する Slide Attack

- 攻撃の種類 : 選択平文攻撃
- 必要な平文-暗号文対の数 : 2 個
- 攻撃方法 : Encryption Oracle に平文 M, 及び平文 1 に対応する暗号文

$$\begin{aligned} Y_0 &= F_A^n(M) \\ Y_1 &= F_A^n(1) \end{aligned}$$

を問い合わせる. A に依らず $F_A(M) = 1$ であるから, $F_A(Y_0) = Y_1$ のはずである. 従って,

$$Y_1 = \left\lceil \frac{M}{A} Y_0 \right\rceil \quad (1)$$

または

$$Y_1 = \left\lfloor \frac{M}{M-A}(M - Y_0) \right\rfloor + 1 \quad (2)$$

である. (1) の場合,

$$\frac{M}{A} Y_0 \le Y_1 < \frac{M}{A} Y_0 + 1$$

より,

$$\frac{M}{Y_1} Y_0 \le A < \frac{M}{Y_1 - 1} Y_0$$

である. Y_1 が M と同等の大きさを持つ場合 (大抵の場合) A を探索する手間は極めて小さい. Y_1 が偶然にも十分小さいとき, Encryption Oracle に $Y_0' = F_A^n(Y_0), Y_1' = F_A^n(Y_1)$ を問い直せば十分である (平文-暗号文対 4 個の適応的選択平文攻撃). (2) の場合も同様に,

$$M - \frac{M}{Y_1}(M - Y_0) \le A < M - \frac{M}{Y_1 - 1}(M - Y_0)$$

である.

5 実験及び結果

128 bit($M = 2^{128}$), 321 段[1] ($n = 321$) の FS-CES に対して上記の Slide Attack を試みた (ランダムな鍵 1000 個に関して実験).

[実験環境] PentiumII 400MHz, Linux
[使用言語] GP/PARI CALCULATOR
[暗号化速度] 平均 34 msec/1 block
[攻撃速度] 平均 141 msec/1 key (問い合わせ含)
[攻撃成功率] 100 %

6 結論

FS-CES は全てのラウンドで同じラウンド鍵を用いるので, 暗号学的に安全ではない. 少なくとも Slide Attack 或は Related Key Attack [5] に耐え得るような鍵スケジュールの導入を検討すべきである.

7 参考文献

[1] 増田 直樹, 合原 一幸, "有限状態パイコネ変換を用いたカオス暗号," 電子情報通信学会論文誌 A Vol. J82-A No.7 pp.1038-1046 1999 年 7 月.

[2] Toshiki Habutsu, Yoshifumi Nishino, Iwao Sasase, Shinsaku Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map," EUROCRYPT'91, LNCS 547, pp.127-140, Springer-Verlag, 1991.

[3] Eli Biham, "Cryptanalysis of the Chaotic-Map Cryptosystem Suggested at EUROCRYPT'91," EUROCRYPT'91, LNCS 547,pp.532-534, Springer-Verlag, 1991.

[4] A. Biryukov, D.Wagner, "Slide Attacks," FSE'99, LNCS 1636, pp.156-170, Springer-Verlag, 1999.

[5] Eli Biham, "New Types of Cryptanalytic Attacks Using Related Keys," EUROCRYPT'93, LNCS 795, pp.398-409, Springer-Verlag, 1994.

[1] $n = 321$ の根拠は [1] の安全性解析に依る.