2L－2

FEAL暗号における暗号化関数の解の導出実験

西條 良輔　小島 丈幸　乾 伸雄　野瀬 隆　小谷 善行
（東京農工大学工学部情報コミュニケーション工学科）

1　はじめに

FEAL暗号における，暗号化関数がF関数である．F関数は，S関数と呼ばれる関数を四つ組み合わせ，一度の処理で32bitのデータを8bitの鍵を二つ用いて暗号化する．

現在まで，既知平文状況下でF関数を線形近似して FEAL 暗号を解読した例が多く報告されている．[1][2][3] F関数を別の関数で置きかえるのは，F関数そのものを解くには，非常に多くの計算が必要だからである．

ここでは，このF関数の方程式を利用し，FEAL暗号の鍵を得ることを検討した．一つの平文と暗号文のペアから鍵を得るまで要した時間を，鍵の総当り攻撃の場合と比較する．

2　F関数

F関数 $Y=F_K(X)$は，入出力がそれぞれ32bitのデータであり，それぞれ8bitのデータ四つずつに(X_1,X_2,X_3,X_4), および(Y_1,Y_2,Y_3,Y_4)に分けられる．そうすると，F関数は，次式で表わされる．ただしF関数のパラメータである鍵は，16bitであり，8bitのデータ二つに分けられる．$K=(K_1,K_2)$

$$Y_1=S_0(X_1,Y_2)$$
$$Y_2=S_1((X_1\oplus X_2\oplus K_1),(X_3\oplus X_4\oplus K_2))$$
$$Y_3=S_0((X_3\oplus X_4\oplus K_2),Y_2)$$
$$Y_4=S_1(X_4,Y_3)$$

S関数は，次の式で表すことができる．

$$S_i(x,y)=ROL2((x+y+i)\bmod 256)$$

A Solution of F function for FEAL Cipher.
SAIJO Ryosuke, KOJIMA Takeyuki, INUI Nobuo,
NOSE Takashi, KOTANI Yoshiyuki
Dept of Computer, Tokyo Univ of Agric and Tech.

3　S関数からの鍵の導出

S関数において，入力をx,y，出力をz，またdを桁上がりとする．未知数はyとdであり，yには鍵成分が含まれている．nを第n桁とすると，次の式が成立する．ただし，n=1のとき，$d_1=i$である．

$$y_{ROL2(n)}=z_n\oplus x_n\oplus d_n$$
$$d_{n+1}=(x_n\times y_{ROL2(n)})\oplus\{d_n(x_n\oplus y_n)\}$$
$$(n=1,2,\cdots,8)$$

ただし，ROL2(n)=n+2 (n≦6),n-6 (n＞6)

すべてのnについてyを求めると，鍵を得ることができる．

4　F関数からの鍵の導出実験

4.1　実験1：一つのF関数

ランダムに生成された鍵を用いて，ランダムに生成された平文を暗号化する．総当りでは，正しい鍵が見つかるまで鍵の総当りを繰り返す．

方程式を利用する方法では，3節の方法を用いて，方程式を解き，鍵を導出する．

4.2　実験2：直列につないだ二つのF関数

二つのF関数を直列につなげたものを考える．このとき，各F関数は，一つのF関数の場合と異なり，入力および出力いずれか一方しか既知ではない．したがって，両方のF関数に3節の方程式を応用させることはできないので，最初のF関数に適当な鍵を与える．最初のF関数の出力を二つ目のF関数の既知の入力として，方程式を解く．導出された二つ目の鍵は，一つ目の鍵が正しくなければ，正しいものではないので，平文を用いて検算を行い，正しい鍵であるかどうかの判定を行う．

5 結果の評価

5.1 実験 1[表 1]

総当りでは，方程式に比べ平均約 2700 倍の時間が必要である．総当りは鍵により実行時間が左右されるが[表 3]，方程式では計算量が一定なので，実行時間はどの鍵でもほぼ同じである．

5.2 実験 2[表 2]

実験 1 と同じく，一つの F 関数について総当りを行っているので，実行時間 t は次のようになる．

$t=1.42\times10^{-5}\times[KEY1]$

[KEY1]は，総当りで KEY1 になるまでの鍵候補の変更回数．

二つの鍵の総当りは，平均で次の式で表される実行時間が必要である．総当りである鍵が出現するまでの平均鍵候補変更回数は 34952 である．また，一つの鍵について，全ての総当りを行うのに，$3.84\times10^{-2}\times2$ の時間を要する．したがって，平均実行時間 t は，次の式になる．

$t=34952\times7.68\times10^{-2}$

6 まとめ

本論文では FEAL 暗号の F 関数に着目して，鍵鍵を得る方法を示した．一組の平文と暗号文があれば鍵が得られる．

しかし，総当り攻撃と同じく，多段の FEAL に関しては計算量が多く解読が困難である．

この問題を解決するような，有効な方法の考案，併用が今後の課題である．

表 1：一つの F 関数での実験結果

	実行回数	平均実行時間
総当り	1000	3.84×10^{-2}
方程式	1000	1.42×10^{-5}

表2:直列につないだ二つのF関数での実験結果

	実行回数	平均実行時間
方程式	1000	0.264

表3:一つのF関数での総当りの実行結果

IN	OUT	KEY	実行時間
56777774	70c63096	4b45	2.20×10^{-2}
fd3809da	37d099d1	5845	2.58×10^{-2}
68993dd6	77758571	8107	3.77×10^{-2}
b3923e08	fb4b4a4d	ab71	5.00×10^{-2}
502bb852	ed2b2bf9	5175	2.39×10^{-2}
804129cf	6b5ae1c6	b6f8	5.34×10^{-2}
b4bd5948	f20836fd	7594	3.43×10^{-2}
73ee2268	a4b643b2	0f50	4.48×10^{-3}
ddc7e7c3	3eb226ab	cef3	6.04×10^{-2}

表4: 直列につないだ二つのF関数での方程式を用いた鍵導出の実行結果

IN	OUT	KEY1	KEY2	実行時間
56777774	9cb74e97	4b45	a67a	0.152
b9195575	3296adac	2a56	3d41	8.55×10^{-2}
c9e55218	f052d41b	b8ad	ab71	0.373
502bb852	42a3b8ca	5175	9a59	0.164
757d1dc8	755d4567	aeee	e97c	0.353
e5c30544	dc163534	2888	0f50	8.18×10^{-2}
ddc7e7c3	8523970d	cef3	894f	0.420
6f32c60c	a89e1f0c	bb8c	4521	0.379
896d8aaa	c2be9c19	eb9c	847f	0.476

参考文献

[1]松井 充：" 暗号安全性の最近の動向，5．暗号の攻撃・解読法：線形解読法"，情報処理，June 1996，pp516-520

[2]太田 和夫，青木 和麻呂："暗号安全性の最近の動向，6．暗号の攻撃・解読法：差分攻撃法"，情報処理，June 1996，pp521-525

[3]Mitsuru MATSUI,Atsuhiro YAMAGISHI："A New Cryptanalytic Method for FEAL Cipher.".IEICE TRANS FUNDAMENTALS VOL.77-A,NO.1 JANUARY 1994,pp2-7