講演番号：18

軽量ブロック暗号 ELiF に対する中間一致攻撃

Meet-in-the-middle attack against lightweight block cipher ELiF

山本　貴大† 　五十嵐　保隆†
Takahiro YAMAMOTO† 　Yasutaka IGARASHI†
東京理科大学理工学研究科電気工学専攻
Graduate School of Science and Engineering, Tokyo University of Science

1.　概要

近年、セキュリティ耐性と暗号化効率の必要性がより重要になっている。各ブロック長に対して簡単な説明を持ち、柔軟な実装特性を持つよう Bogdanov の軽量ブロック暗号の構造に類似した極めて軽量なブロック暗号 EliF が 2016 年に Adnan Baysal 及び Ünal Kocabas によって提案された。これまでに EliF には差分攻撃及び線形攻撃で攻撃耐性評価が行われている[1]。本研究では極めて軽量で暗号化効率の高いブロック暗号 ELiF に注目した。本研究ではこの ELiF に対し中間一致攻撃を行うことで攻撃耐性評価を行う。

2.　ELiF の構造

ELiF の概要を図 1 に示す。ELiF は、ブロックサイズ bとラウンド数rによってパラメータ化され、$ELiF_{b,r}$と表す。$ELiF_{b,r}$のシリアルラウンド関数を図 1 に示す。

2.1 シリアルラウンド関数

$b > 2$、$r > 0$, $x_j^{(i)} \in GF(2)$、$j = 0$、1、…、$b-1$ はラウンドiの入力ビットとし、$k^{(i)} \oplus c^{(i)}$がi番目のラウンドキーと定数 XOR であるとする。$ELiF_{b,r}$のi番目のラウンド関数は、以下のように表される。

$$x_2^{(i)} = k^{(i)} \oplus c^{(i)} \oplus x_2^{(i)} \oplus x_1^{(i)} x_0^{(i)} \qquad (1)$$

2.2 ElIF 実装について

本実験ではブロック数を 64、鍵を 64bit とし、図 1 のシリアルラウンド関数を 64 個直列につなぎ、それぞれのシリアルラウンド関数に鍵をk^1、$k^2 \ldots k^{64}$と順に入れていったものを 1 ラウンドとする。

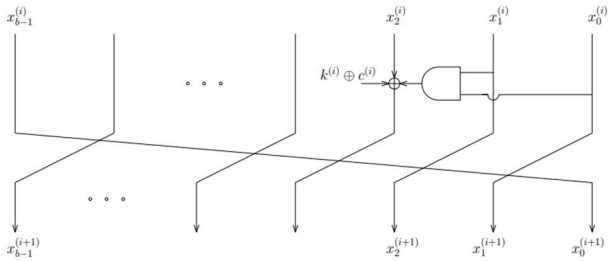

図 1 $ELiF_{b,r}$のシリアルラウンド関数[1]

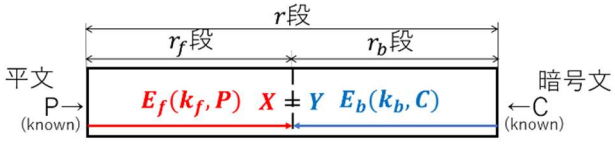

図 2 中間一致攻撃の概要

3.　中間一致攻撃の概要

中間一致攻撃は共通鍵暗号アルゴリズムに対する汎用的な解析手法であり、 1977 年に Diffie と Hellman が提案した。攻撃対象である暗号を 2 つの区間に分割し、それぞれの区間で秘密鍵を推定し、推定した鍵を用いて平文側から作成した暗号化されたデータと暗号文側から作成した復号化されたデータを手に入れ、データが一致するか調査を行うことで解析を行い、演算回数を総当たり攻撃よりも削減できる攻撃が中間一致攻撃である。図 2 に中間一致攻撃の概要を示す。E_fを暗号化関数、E_bを復号化関数、K_fを暗号化で推定する鍵、K_bを復号化で推定する鍵、r_fを暗号化できる段数、r_bを復号化できる段数とする。平文 P と暗号文 C を既知とし、全ての鍵候補K_fに対して$E_f(K_f, P)$を計算することでXを出し、 また全ての鍵候補K_bを使い$E_b(K_b, C)$暗号文の復号を行うことでYを出す。その結果、データが一致する$X = Y$かを調査し、真の鍵の値を特定する。

4.　ELiF に対する中間一致攻撃

中間値を決める際に、データが全て未知の値となってしまうと一致させるビット数がなくなり、演算回数を計算することができない。したがって, 本研究では中間一致攻撃では全てのデータが未知となる 1 ラウンド前を中間値とする。鍵に対して未知ビットを変えることで段数が一番伸びたものを調査する。これを暗号化方向と復号化方向に行い、中間値を手に入れる。また、暗号器はブロックサイズを 64、鍵サイズを 64 として暗号化を行うこととする。 1 個目から 64 個目までのシリアルラウンド関数は 1, 2, 3, …64 番目の鍵を用いてそこまでを 1 ラウンドとし、2 ラウンド目からは再び 1, 2, 3 …番目の鍵を用いるキースケジュールを行う。

5.　調査結果

中間一致攻撃 60 ラウンドの攻撃では総当たりでは鍵サイズが 64 であるため2^{64}回の攻撃が必要なのに対し中間一致攻撃では$2^{63.61}$回の攻撃が必要であることがわかった。

参考文献

[1] Adnan Baysal and Ünal Kocabaş, “ELiF : An Extremely Lightweight & Flexible Block Cipher Family and Its Experimental Security”, 752.pdf (iacr.org), 2016.