メッセージ認証符号 $Chaskey$ に対する新しい差分型攻撃法

高橋 勇介　　金子 敏信
東京理科大学理工学部電気電子情報工学科

1　序論

$Chaskey$[1] は 2014 年 8 月に SAC2014 で日立製作所が提案した 32-bit Microcontroller 向けメッセージ認証符号である。$Chaskey$ は、制作者の自己評価で差分攻撃に対する安全性が確認されている [1]。そのため、本稿では新しい差分型攻撃法を用いて π 関数 3 段時の $Chaskey$ に対する攻撃計算量の調査を行った。

2　$Chaskey$ の構造

単一鍵 $Even-Mansour$ ブロック暗号と見なす。π 関数と平文側、暗号文側の鍵加算からなる。入力として、鍵長 256bit、入力平文 128bit を持つ。出力の認証符号の bit 長は 128bit として考える。

2.1　π 関数

算術加算、巡回シフト、排他的論理和で構成されており、8 段分繰り返される構造になっている。本稿では 3 段分繰り返される構造を対象とする。

3　新しい差分型攻撃

3.1　π 関数 1 段分のアルゴリズム解析

非線形演算である算術加算で生じる桁上がり bit を D_i とする。i bit 目出力 Z_i は 2 つの入力 S_i、T_i と桁上がりの線形和である。

$$Z_i = S_i \oplus T_i \oplus D_i \tag{1}$$

この関係式を π 関数全体に適用することにより π 関数の出力は入力と桁上がりの線形和で表せる。算術加算の場合、桁上がりは下位 bit から上位 bit に影響し、次数が上昇する。桁上がり D_i は次式で表せる。

$$D_i = (S_{i-1} \oplus T_{i-1})D_{i-1} \oplus S_{i-1}T_{i-1}\ ,\ D_0 = 0 \tag{2}$$

3.2　3 段の π 関数に対する差分型攻撃の準備

π 関数 1 段あたり 4 箇所の算術加算がある。π 関数 3 段を考え、入出力から離れた箇所の桁上がり変数が影響しない方程式を導出する。(2) 式の両辺に $(S_{i-1} \oplus T_{i-1} \oplus 1)$ を掛算する。

$$D_i(S_{i-1} \oplus T_{i-1} \oplus 1) = (S_{i-1} \oplus T_{i-1} \oplus 1)S_{i-1} \tag{3}$$

D_{i-1} の影響を受けない桁上がりの式が得られる。この関係を利用し、なるべく次数の低い式を手に入れる。(3) 式において $S_{i-1} \oplus T_{i-1} = 0$ であれば、

$$D_i = S_{i-1} \tag{4}$$

となる。

3.3　3 段の π 関数に対する差分型攻撃

前述の方法で次数上昇を抑えた式を求める。π 関数 3 段に関して適用すると、6bit の仮定を行えば次数を抑えた

$$R = 0 \tag{5}$$

の式が得られる。R は平文側 bit の 4 次式、暗号文側 bit の 3 次式の和である。これは恒等式であり、これは平文 P 及び P^* に対して成立する。P^* に対する式を次式で表す。

$$R^* = 0 \tag{6}$$

R 内の平文側 bit の 2 次項以上に関係のない bit に差分を入れて P^* とする。(5) 式 (6) 式の差分を取れば (7) 式となる。

$$\Delta R = R \oplus R^* = 0 \tag{7}$$

ΔR は暗号文側 bit の 3 次式の差分である。平文 P に対して 6bit 仮定が成立しているならば P^* においても成立しているような平文差分、暗号文差分を選択する。解析によれば、選択平文として $2^6 \times 16$ 組の平文を用意すれば、各 6bit の仮定に対応する ΔR が 15 個得られる。ΔR は暗号文側 bit の 14bit が関係している。この 14bit を総当たりするならば、正しい鍵は常に生き残り、偽の鍵は確率 $\frac{1}{2}$ で生き残る。したがって、ΔR の式が 15 個程度あれば、この 14bit は確定する。この時の攻撃計算量は

$$2^{14} + 2^{13} + \cdots \simeq 2^{15} \tag{8}$$

である。前述の 6bit 仮定が正しければ 14bit の総当たり鍵の生き残りとして正しい鍵候補が得られる。正しくない場合は、全ての 14bit 鍵の生き残りはなくなってしまう。6bit 仮定を含めた攻撃計算量は次式である。

$$2^6 \times 2^{15} = 2^{21} \tag{9}$$

4　解析結果と結論

3 段の π 関数に対する新しい差分型攻撃の攻撃計算量は 2^{21}、必要平文数は $2^6 \times 16 = 2^{10}$ 組となった。尚、参考文献 [1] の差分確率を用いた既存の差分攻撃の攻撃計算量は 2^{69} 程度で、必要平文数は $2^{5.58}$ 組程度である。したがって、この新しい差分型攻撃は $Chaskey$ に対して既存の差分攻撃よりも必要平文数は増えるが、攻撃計算量は少ない。

参考文献

[1] Nicky Mouha, Bart Mennink, Anthony Van, Herrewege, Dai Watanabe, Bart Preneel, and Ingrid Verbauwhede "Chaskey: An Efficient MAC Algorithm for 32-bit Microcontrollers", SAC2014