SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

軽量ブロック暗号 CRAFT のハッシュ関数への応用に関する考察
research on application of block cipher CRAFT for hash function

西尾　明日駆 *　　五十嵐　保隆 *
Nishio Asuku　　Igarashi Yasutaka

キーワード　ブロック暗号　CRAFT　等価鍵　ハッシュ関数　第二原像計算困難性　衝突計算困難性

あらまし

CRAFT は FSE2019 で提案された軽量 Tweakable ブロック暗号である。CRAFT に関する他の論文では、差分攻撃[2]や関連鍵攻撃などに対する強度について分析が行われた。提案論文[1]では不能差分攻撃への強い耐性が主張されると同時に、ある単純な条件を満たす複数の鍵と tweak の組の集合は、平文と暗号文に対し同じ入出力関係を与えることが示されている。本論文では平文と暗号文に対し同じ入出力関係を与える複数の鍵と tweak の組の集合に関するより詳細な説明と、その危険性に関して記述する

等価な鍵とツイークの危険性

等価な鍵と tweak の組

ブロック暗号 CRAFT は以下の式（1）を満たす異なる鍵$(\boldsymbol{K}_0 \| \boldsymbol{K}_1)$とツイーク T を用いて暗号化を行ったとき、段鍵の値が一致し、入出力関係も一致する。[1]

$$\Delta \boldsymbol{K}_0 = \Delta \boldsymbol{K}_1 = \Delta \boldsymbol{T}$$
$$= [\,\Delta\alpha, \Delta\alpha, \cdots, \Delta\alpha, \Delta\alpha] \cdots (1)$$

ここで$\Delta\alpha$は 0 でない任意の 1nibble(4bit)の値である。また、$\boldsymbol{K}_0$、$\boldsymbol{K}_1$、Tはそれぞれ任意の 64bit の値であり 1nibble の成分を 16 個持つベクトルとする。

等価な鍵とツイークの危険性[2]

ブロック暗号の使用用途の一つに暗号学的ハッシュ関数への応用が挙げられる。暗号学的ハッシュ関数は第二原像計算困難性と衝突計算困難性を満たさなければならない。

ハッシュ関数の構造の一つである Merkle–Damgård 構造を図 1 に示す。Mはハッシュ関数への入力であり、$M_i (0 \leq i \leq n)$は M を f 関数の上部の入力と同じビット数になるように分割したものである。必要に合わせてパディングを行う。この時の f 関数の構造の一つに Davies-Meyer 構造が挙げられる。Davies-Meyer 構造を図 2 に示す。

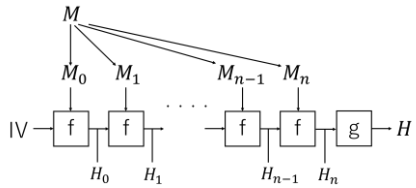

図 1　Merkle–Damgård 構造

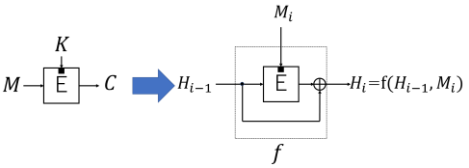

図 2　Davies-Meyer 構造

このハッシュ関数の E に CRAFT を用い、M_iに(1)式を満たす鍵とツイークを入力した場合、最終的な出力は一致する。したがって、このような構造を持つハッシュ関数に CRAFT を用いた場合、容易に第 2 原像計算および衝突計算を行うことができる。

参考文献

[1] Christof Beierle, Gregor Leander, Amir Moradi and Shahram Rasoolzadeh “CRAFT: Lightweight Tweakable Block Cipher with Efficient Protection Against DFA Attacks” IACR Transactions on Symmetric Cryptology 2019(1), pp.5–45, 2019

[2] Yuki Asano, Shingo Yanagihara, Tetsu Iwata “Cryptanalysis of 256-bit Key HyRAL via Equivalent Keys” LNCS Lecture Notes in Computer Science book series volume 7341,　pp 257-274　2012

* 東京理科大学 〒278-8510　千葉県野田市山崎 2641.
Tokyo University of Science, 2641 Yamazaki, Noda, 278-8510