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 CHAM に対する Bit-based Division Property Using Three Subsets を用いた Integral 攻撃

Integral Attack with Bit-based Division Property Using Three Subsets on lightweight block cipher CHAM

中曽根　彰人 *　　五十嵐　保隆 *
Akito Nakasone　　Yasutaka Igarashi

キーワード CHAM, MILP, Bit-based Division Property Using Three Subsets, Integral 特性

あらまし

CHAM は 2018 年に Koo らによって提案された ARX 型の軽量ブロック暗号で、ブロック長/鍵長の値によって CHAM-64/128、CHAM-128/128、CHAM-128/256 の 3 種類が存在する。提案論文では、(ブロック長/4)階差分で 16 段の CHAM において Integral 特性を持つと評価されているが、鍵回復攻撃については言及されていない。この評価に対し本稿では、CHAM-128/128、CHAM-128/256 に対して混合整数線形計画法(Mixed Integer Linear Programming: MILP)を用いた Bit-based Division Property Using Three Subsets によってより詳細に Integral 特性を探索し、鍵回復攻撃を行った。その結果、114 階差分で 19 段の CHAM において Integral 特性を持つことが明らかとなった。そしてこの特性を利用し平文-暗号文組を 2^{114} 組用いて、20 段の CHAM-128/128 に対して $2^{127.00}$、24 段の CHAM-128/256 に対して $2^{255.00}$ の暗号化回数で鍵回復攻撃が成功することが分かった。

軽量ブロック暗号 CHAM

CHAM の種類ごとの各パラメータを表 1 に、2 段分の段関数を図 1 に示す[1]。

表 1　CHAM の各パラメータ

暗号	ブロック長	鍵長	段数
CHAM-64/128	64	128	88
CHAM-128/128	128	128	112
CHAM-128/256	128	256	120

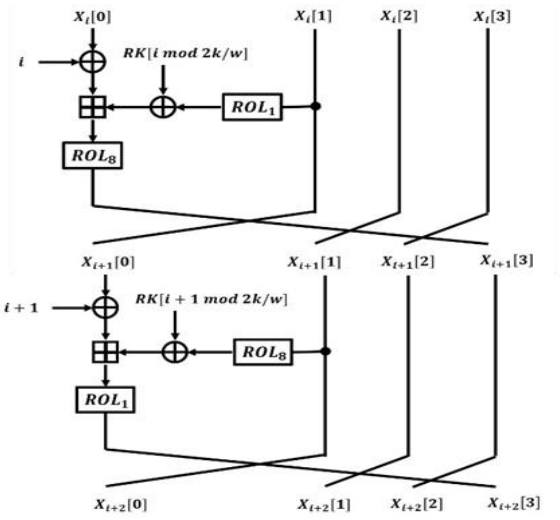

図 1　CHAM の段関数(2 段分)

Integral 特性探索の結果

MILP を用いた Bit-based Division Property Using Three Subsets による Integral 特性探索の結果、19 段の CHAM-128/128,CHAM-128/256 に対して以下の Integral 特性を得た。

入力集合(114 階差分):
(AAAAAAAA,AAAAAAAA,AAAAAAAA,AAAAaaccCCC)
⇒19 段目出力:
(UUUUUUUuubu,UUUUUUUU,UUUUUUUU,UUUUUUUU)

参考文献

[1] Dongyoung Roh, Bonwook Koo, Younghoon Jung, Il Woong Jeong, Dong-Geon Lee, Daesung Kwon, and Woo-Hwan Kim," Revised Version of Block Cipher CHAM", ICISC 2019, LNCS 11975, pp. 1–19, 2020.

* 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