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

単一鍵の Tweakable ブロック暗号を用いたブロック暗号の安全性
Security of Block Cipher Based on Single Key Tweakable Block Cipher

辻 健斗 * 岩田 哲 *
Kento Tsuji Tetsu Iwata

キーワード ブロック暗号，tweakable ブロック暗号，単一鍵，証明可能安全性

あらまし

Feistel 構造は Luby と Rackoff によって安全性解析がなされ，DES や Camellia を始めとして様々なブロック暗号に採用されている [2]．4 段の繰り返し構造をもとにした $2n$ ビットブロック暗号 $\Psi_4[F_1, F_2, F_3, F_4]$ は，強擬似ランダム置換であると数学的に証明がされている．各 F_i が n ビットの擬似ランダム関数のとき，識別利得は敵のクエリ回数 q を用いて $O(q^2/2^n)$ と示されている．これは，$q \ll 2^{n/2}$ のときに安全であることを意味する．

Patarin は Feistel 構造で使われる関数を単一にしたときの安全性を解析した [3]．単一の擬似ランダム関数 F，1 ビットシフト ζ により構成され，4 段の構造 $\Psi_4[F, F, F, F \circ \zeta \circ F]$ が強擬似ランダム置換であり，識別利得は複数鍵を用いた構造と同等の $O(q^2/2^n)$ であることを証明した．

Coron らは (n, n) ビット tweakable ブロック暗号を繰り返し構造にもつ $2n$ ビットブロック暗号を提案した [1]．2 段の構成 $\Phi_2[E_1, E_2]$ が強擬似ランダム置換であり，識別利得が $O(q^2/2^n)$ であると示した．

本稿では，Coron らの構成をもとに tweakable ブロック暗号の鍵を単一の鍵に変更したブロック暗号の安全性を解析する．図 1 に示す 3 段の構造 $\Phi_3[E]$ が，強擬似ランダム置換であり，識別利得が $O(q^2/2^n)$ であることを証明し，あわせて安全性の上界を与える攻撃を示す．また 2 段の構造 $\Phi_2[E]$ に対する効率的な識別攻撃を示す．

本稿で解析する構成は，2 段の Coron らの構成と同等の安全性を得られる．単一の鍵のみ用いることにより鍵の共有，管理，処理，更新に必要なコストを削減でき，関連鍵攻撃の脅威を低減することができる．Patarin の構成は関数に加えシフトを必要としたが，本稿で解析する構成は tweakable ブロック暗号のみで構成可能である．

表 1 に従来手法と本稿の構成との比較をまとめる．

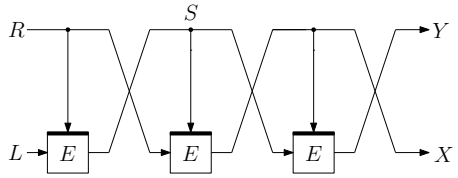

図 1: 本稿の解析対象

表 1: 従来手法との構成，安全性の比較．PRF は擬似ランダム関数，TBC は tweakable ブロック暗号．

要素技術	複数鍵	単一鍵
PRF	$\Psi_4[F_1, F_2, F_3, F_4]$ $O(q^2/2^n)$ [2]	$\Psi_4[F, F, F, F \circ \zeta \circ F]$ $O(q^2/2^n)$ [3]
TBC	$\Phi_2[E_1, E_2]$ $O(q^2/2^n)$ [1]	$\Phi_3[E]$ $O(q^2/2^n)$ [本稿]

謝辞

本研究は JSPS 科研費 JP20K11675 の助成を受けたものです．

参考文献

[1] J. Coron, Y. Dodis, A. Mandal, and Y. Seurin. A domain extender for the ideal cipher. In *TCC 2010*.

[2] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM J. Comput.*, 17(2):373–386, 1988.

[3] J. Patarin. How to construct pseudorandom and super pseudorandom permutations from one single pseudorandom function. In *EUROCRYPT '92*.

* 名古屋大学工学部 〒 464-8603 名古屋市千種区不老町．Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan. tsuji.kento@k.mbox.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.ac.jp