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

Elephant に対する鍵回復，識別及び偽造攻撃
Key Recovery, Distinguishing, and Forgery Attacks against Elephant

土生 亮 * 岩田 哲 *
Makoto Habu Tetsu Iwata

キーワード 共通鍵暗号，認証暗号，Elephant，鍵回復攻撃，識別攻撃，偽造攻撃

あらまし

認証暗号はデータの暗号化に加えて，認証の機能を持つ暗号化方式であり，平文，ナンス，付加データを入力とし，暗号文，タグを出力する．特に，回路やメモリが限られている状況での効率的動作を目的とした方式を軽量認証暗号方式という．米国 NIST は軽量認証暗号方式の標準化に向けて，暗号方式を公募する NIST Lightweight Cryptography Competition を行っている．

Elephant は暗号学的置換を利用した認証暗号方式であり [1]，本公募の最終ラウンド方式の一つである．暗号学的置換のサイズに応じて Dumbo, Jumbo, Delirium のバリエーションがあり，それぞれ証明可能安全性バウンドが示されている．提案論文 [1] の安全性定理は

$$\mathbf{Adv}^{\mathrm{ae}}_{\mathsf{Elephant}}(\mathcal{A}) \le \frac{0.5\ell q_e^2}{2^n} + \frac{1.5(q_e+q_d)^2}{2^n} + \frac{q_d}{2^t} + \frac{4\sigma^2+4\sigma p+4\sigma+p}{2^n} + \frac{p}{2^k}$$

であり，n はブロック長，ℓ はクエリの最大ブロック数，q_e は暗号化クエリの回数，q_d は復号クエリの回数，t はタグ長，σ はオンラインクエリの総ブロック数，p は暗号学的置換の呼び出し回数，k は鍵長である．本論文では，上記のバウンドのうち，$4\sigma p/2^n$，$0.5\ell q_e^2/2^n$，$1.5(q_e+q_d)^2/2^n$ の項が厳密であることを，それぞれ鍵回復攻撃，識別攻撃，偽造攻撃の手順を示すことにより明らかにする．それらは Dumbo, Jumbo, Delirium の全てに適用できる．

鍵回復では，平文を空列にすることで，Elephant を Even-Mansour 暗号 [3] と同等の処理とみなすことができる．そのため，Joan Daemen の手法 [2] を適用できる．ただし，Elephant が出力するタグは，置換のサイズよりも短いため，従来研究のチェック式を 6 式用意する必要があり，成功する場合はそのうちの 3 式を満たす．

識別攻撃では，Elephant の暗号化部分はナンスを入力とし，平文と暗号文の差分を出力する ℓ_M 個の異なる置換とみなせる（ℓ_M は平文ブロック数）．ナンスを変えて q_e 回暗号化をすると，現実世界では起こらない衝突が，理想世界では起こりうることを利用して識別を行う．

偽造攻撃では，タグが衝突している場合に置換の入力も衝突していることを期待する．Elephant が出力するタグは置換のサイズよりも短いため，3 回タグが衝突することを確認して，置換の入力が衝突していることを確認できる．その後，ナンスに適当な差分を加えてオラクルにクエリすることで，存在的偽造を行うことができる．

本論文で得られた結果を表 1 にまとめる．

表 1: 本論文の攻撃成功確率

鍵回復	識別	偽造
$O(pq_e/2^n)$	$O(\ell q_e^2/2^n)$	$O(q_e^2/2^n)$

参考文献

[1] T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink. Dumbo, Jumbo, and Delirium: Parallel authenticated encryption for the lightweight circus. *IACR Trans. Symmetric Cryptol.*, 2020(S1):5–30, 2020.

[2] J. Daemen. Limitations of the Even-Mansour construction. In *ASIACRYPT '91*.

[3] S. Even and Y. Mansour. A construction of a cipher from a single pseudorandom permutation. In *ASIACRYPT '91*.

* 名古屋大学大学院工学研究科 〒 464-8603 名古屋市千種区不老町． Nagoya University, Furo-cho, Chikusa-ku, Nagoya 464-8603, Japan. habu.makoto@f.mbox.nagoya-u.ac.jp, tetsu.iwata@nagoya-u.jp