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

組み合わせ AONT の安全性に関するエントロピー解析
Entropy Analysis on Security of Combinatorial AONT

赤尾　奏名汰 *　　顧　玉杰 †　　櫻井　幸一 †
Akao Sonata　　Gu Yujie　　Sakurai Kouichi

キーワード 組み合わせ AONT、安全性、perfect security、weak security、条件付きエントロピー

あらまし

AONT（All-or-Nothing Transform, 悉無律を満たす変換）は、鍵の総当り攻撃を困難にするために、計算量的安全性を根拠に、データの暗号化の前処理技術として Rivest[1] によって提案された。AONT は現在まで暗号と情報セキュリティにおいて多くの応用がなされている。

後に、無条件に安全な AONT や、組み合わせ AONT が Stinson によって発表された [2]。Stinson は無条件に安全な (s, v)-AONT を以下のように表現している。

有限集合 Γ として、関数 $\phi : \Gamma^s \to \Gamma^s$ とする。ただし、$|\Gamma| = v$、$s > 0$ である。ϕ を入力列 $(x_1, x_2, \cdots, x_s)$ から出力列 $(y_1, y_2, \cdots, y_s)$ への写像としたとき、ϕ が AONT であるとは、以下を満たすことである。ただし、$x_i, y_i \in \Gamma (1 \leq t \leq s)$。

(1) ϕ が全単射である。

(2) 出力 $y_1, y_2, \cdots, y_s$ のうち、任意の 1 つの y_j が失われたら、任意の x_i についての情報を得ることは不可能である。

組み合わせ AONT は、unbiased という特徴を持つ行列で表現したものであるが、安全性は入力の確率分布によって異なる。Esfahani と Stinson は、全ての平文の入力が等確率ならば完全な安全性 (perfect security) を持ち、すべての入力が非ゼロ確率であるならば弱い安全性 (weak security) を持つことを示した [3]。perfect security では、出力が与えられた下での入力の確率と、入力の確率が等しいことを表している。つまり、入力について事前分布と事後分布が等しい。weak security は出力が与えられた下での入力の確率が非ゼロであることを表している。

本論文では、組み合わせ AONT における、perfect secuirty と weak security の違いをより詳細に述べる。方法として、入力がそれぞれ独立であるもとで、出力の一部が与えられたときの、入力の一部に対する情報量、つまり条件付きエントロピーを定量的に分析した。その結果、上限や下限に関する関係式を新たに示し証明することが出来た。また、入力の確率が全て等しい時、上限と下限が等しくなることも示すことが出来た。

今回の研究では入力をそれぞれ独立であるとしたが、今後の課題として、各入力が依存する場合とではどのような違いが生じるのか、ということが挙げられる。

謝辞

本研究は、JSPS 科研費 若手研究 21K13830 の助成を受けたものです。

参考文献

[1] R. Rivest, “All-or-nothing encryption and the package transform,” in Fast Software Encryption 1997, Lecture Notes in Computer Science, 1267 (1997) pp. 210-218.

[2] D. Stinson, “Something about all-or-nothing (transforms),” Designs, Codes and Cryptography, vol. 22, pp. 133–138, 2001

[3] N. Esfahani and D. Stinson, “On security properties of all-or-nothing transforms,” arXiv: 2103.05697.(2021)

* 九州大学大学院　システム情報科学府, 福岡県福岡市西区元岡 744 , Graduate School of Information Science and Electrical Engineering, Kyushu University, Motooka Nishi-ku, Fukoka-shi, Fukuoka-ken

† 九州大学大学院　システム情報科学研究院, 福岡県福岡市西区元岡 744, Faculty of Information Science and Electrical Engineering, Kyushu University, Motooka Nishi-ku, Fukoka-shi, Fukuoka-ken