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

最終ラウンド候補の認証機能付き軽量暗号に対する高位合成の評価
Evaluation of High-Level Synthesis for Finalists in Authenticated Lightweight Cryptography

竹本 修 * 池崎 良哉 * 野崎 佑典 † 吉川 雅弥 †
Shu Takmeoto Yoshiya Ikezaki Yusuke Nozaki Masaya Yoshikawa

キーワード ハードウェアセキュリティ，軽量暗号，認証付き暗号，高位合成

あらまし

Society5.0 の推進によって，小型デバイスの利用が拡大している．それに伴い，小型デバイスを指向し小面積実装や低遅延実装を実現する暗号アルゴリズムとして，軽量暗号が数多く提案されている．近年では軽量暗号の標準化を進めるため，アメリカ国立標準技術研究所（NIST）によって軽量な認証付き暗号（Lightweight Cryptography）に対するコンペティションが実施されている [1]．2021 年 3 月には最終ラウンド候補として表 1 に示す 10 方式の暗号アルゴリズムが選出されており，さらなる暗号性能やセキュリティの議論が求められている．

また，小型デバイスに関して，少量多品種展開が可能な FPGA が広く利用されている．そこで，FPGA へのハードウェア実装の開発工数短縮が可能な高位合成が注目を集めている．高位合成は C 言語等の高位プログラミング言語からハードウェアに実装するためのハードウェア記述言語（HDL）を自動的に生成する技術である．

そこで本研究では，軽量暗号のコンペティションにて最終ラウンド候補に挙げられた認証付き暗号に対し，高位合成を用いて FPGA 実装した場合の性能について評価する．これまでに我々は Elephant，GIFT-COFB，PHOTON-Beetle，TinyJAMBU の 4 方式について評価してきており [2,3]，本稿ではすべての暗号方式の比較評価について新たに示す．

表 1: 軽量暗号コンペティションの最終ラウンド候補

暗号アルゴリズム名	ナンス長 [bits]	タグ長 [bits]
ASCON	128	128
Elephant	96	64/128
GIFT-COFB	128	128
Grain-128AEAD	96	64
ISAP	128	128
PHOTON-Beetle	128	128
Romulus	128	128
SPARKLE	128/256	128
TinyJAMBU	96	64
Xoodyk	128	128

参考文献

[1] https://csrc.nist.gov/Projects/lightweight-cryptography/finalists

[2] 竹本修, 池崎良哉, 野崎佑典, 吉川雅弥,“軽量暗号に対する高位合成の評価,” 2021 年度電気・情報関係学会北陸支部連合大会講演論文集, E-6, 2021 年 9 月

[3] 竹本修, 池崎良哉, 野崎佑典, 吉川雅弥,“Elephant の高位合成に対する評価,” 令和 3 年度電気・電子・情報関係学会東海支部連合大会講演論文集, H1-7, 2021 年 9 月

* 名城大学大学院, 愛知県名古屋市天白区塩釜口一丁目 501 番地, Meijo University, 1-501 Shiogamaguchi, Tempaku-ku, Nagoya, Aichi 193426008@ccalumni.meijo-u.ac.jp
† 名城大学, 愛知県名古屋市天白区塩釜口一丁目 501 番地, Meijo University, 1-501 Shiogamaguchi, Tempaku-ku, Nagoya, Aichi