軽量暗号 Ascon などに関わる標準化動向調査

GMO サイバーセキュリティ by イエラエ株式会社

2023 年 9 月

エグゼクティブサマリー

本報告書では、NIST 軽量暗号コンペティションで 2023 年 2 月 7 日に選定された Ascon について標準化動向の調査を行った。Ascon の選定に関連する情報については、文献 [1]に詳しく記載されているため、この文献を中心に調査を行った。

Final Round では、最終候補として 10 のアルゴリズムが選択され、以下に示すような選考プロセスにおいて評価が行われた。

- 選考プロセスでのポイント
  - 様々な評価基準（安全性、ソフトウェアおよびハードウェアの性能、設計の成熟度、第三者による安全性評価の量、知的財産権の有無など）に異なる重み付けを割り当てて実施
  - 異なるセキュリティ要件、異なる機能性、異なる複雑性を持った攻撃などを踏まえた評価の実施
  - 限られたリソースにおける安全性評価および性能評価の実施

最終候補となったアルゴリズムの中から NIST が Ascon を選定したポイントについて整理を行うと以下の項目が挙げられる。

- 安全性
  - 高いセキュリティーマージン
  - 多数の第三者による安全性評価の数
- 設計/実装
  - 設計の微調整を行わないという設計の成熟度
  - 軽量暗号コンペティションである CAESAR プロジェクトにおいて軽量暗号の最終的なポートフォリオに選択されている実績
  - 漏えいに対するモードレベルでの保護メカニズムを有すること
  - 実装と設計の柔軟性
  - サイドチャネル攻撃に対する対策を行うための追加コストが低いこと
- 機能性
  - ハッシュに加えて XOF や MAC などの追加機能を有すること
- 性能
  - ソフトウェアおよびハードウェア環境において、現行の NIST 標準である AES-GCM や SHA-2 を上回る性能を有すること

また、NIST 以外の標準化団体における検討については、2023 年 9 月現在では大きな動きは見られなかったが、2023 年後半に予定されている NIST が発行する標準仕様の公開を受けて、本格的に様々な団体での検討が行われるものと考える。また、標準化された暗号技術が利用できる環境としてソフトウェアやハードウェア実装が公開されることが重要であるが、CAESAR プロジェクト等の実績などから実装がいくつか公開されているケースが見受けられた。これは Ascon の設計が成熟しており、NIST 軽量暗号コンペティションにおいて設計の微修正が行われていないことが背景にあると考える。

目次

1. はじめに

2017 年 3 月に公開された CRYPTREC 暗号技術ガイドライン（軽量暗号）（以下、「2016 年度ガイドライン」という） [2]では、「実装性能と安全性のトレードオフを勘案した上で、従来の暗号技術に対して特定の性能指標で優位性（軽量性）を持つように設計された共通鍵暗号技術」をスコープとし、軽量暗号の活用例、代表的な軽量暗号の性能比較、代表的な軽量暗号に関する基本情報について紹介している。しかしながら、暗号方式に対する安全性評価技術は日進月歩であり、2016 年度ガイドラインの公開から 5 年以上が経っているため、2016 年度ガイドラインには記載されていない。そのため、軽量暗号の安全性を脅かす新たな脅威が生じている可能性は十分に考えられる。そこで、2016 年度ガイドラインで紹介された暗号方式を中心とした代表的な軽量暗号の安全性評価に関する動向調査を行うことを目的とし、2021 年 9 月の時点における軽量暗号に対して現実的な脅威に繋がる脆弱性が指摘されているか否かを明らかにするための報告書として「CRYPTREC 暗号技術ガイドライン（軽量暗号）」掲載の暗号方式に関する安全性評価の動向調査 [3]が公開された。

また、2019 年度量子コンピュータ時代に向けた暗号の在り方検討タスクフォースにおいて、「CRYPTREC において、軽量暗号は CRYPTREC 暗号リストに組み込まず、別途ガイドラインという形で取り扱う」ことが決定された。この決定を踏まえて 2020 年度第 2 回暗号技術検討会において、2016 年度に作成した「CRYPTREC 暗号技術ガイドライン（軽量暗号）」について 2023 年度中を目処に更新することが承認された。そこで本報告書では、2020 年度第 2 回暗号技術検討会の承認内容を踏まえて、「NIST Lightweight コンペティション最終選考で採択された軽量暗号方式」や「軽量暗号として ISO/IEC 等で近年採録されたもしくは採録される予定の方式」に関する標準化動向について状況を整理した調査報告として、「軽量暗号の評価指標、標準化動向に関する調査（NIST 軽量暗号コンペティションファイナリストなど）」 [4]が報告された。しかしながら、調査報告は 2022 年 12 月であったため Lightweight Cryptography Project の結果を含めた内容にすることができなかった。Ascon が選出された。

本調査報告書では、前回の報告書の調査期間以降である 2023 年 2 月 7 日に選定された Ascon を中心とした標準化動向調査を行い、「CRYPTREC 暗号技術ガイドライン（軽量暗号）」の更新に向けた標準化動向調査結果を執筆する。

2. NIST 軽量暗号コンペティション

2016 年度ガイドラインの発行後、NIST*による軽量暗号コンペティション（以下、NIST 軽量暗号コンペティションとする。）[5]が開催された。前回の報告書 [4]の執筆時には「最終評価は 2022 年末に終了する予定である」と告げられていたが、2023 年 2 月 7 日に Ascon を選定したことがアナウンスされた。

なお、NIST 軽量暗号コンペティションの Web サイトでは、図 1 のような構成となっており、各 Round に関する情報や軽量暗号 Workshop に関する情報、制約のある環境下での実装性能など有益な情報へのリンクが整理されている。

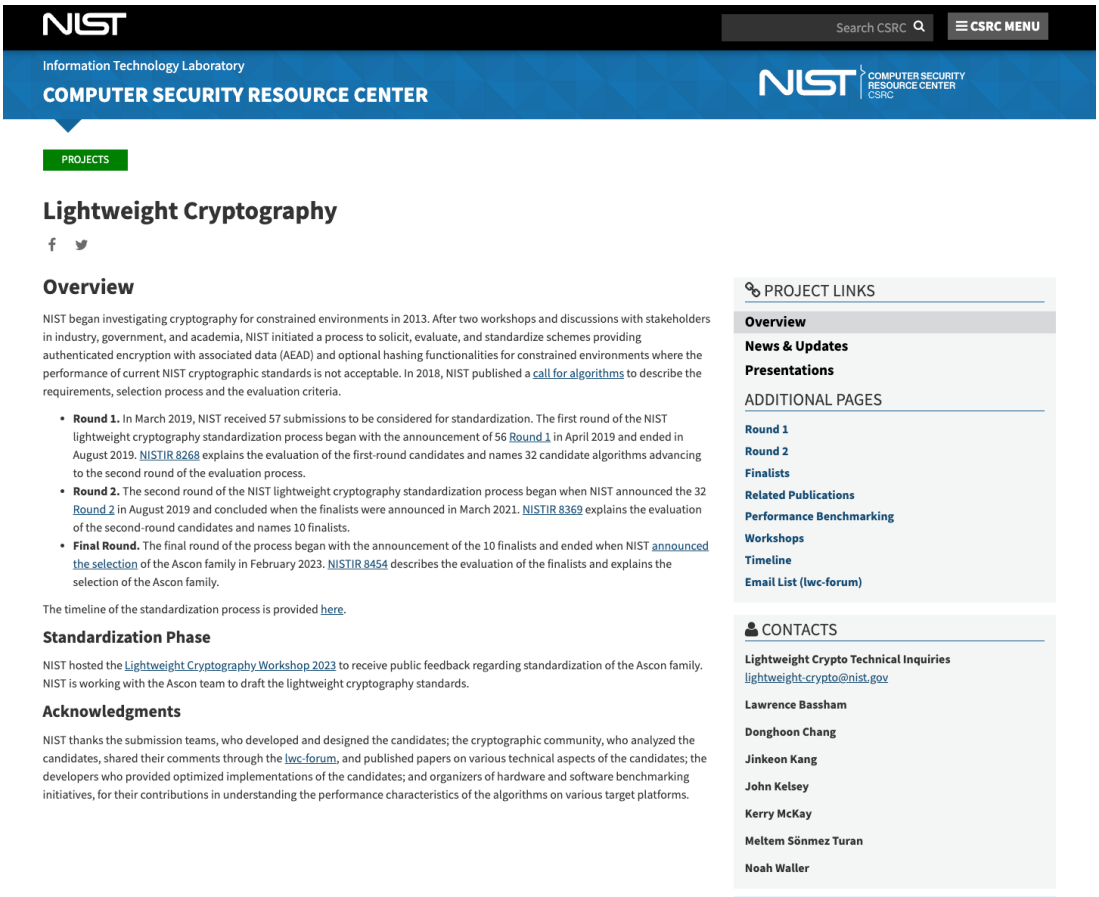

図 1　NIST 軽量暗号コンペティション

---

* NIST の正式名称は、National Institute of Standards and Technology であり、日本語では米国立標準技術研究所と呼ばれるアメリカの政府機関である。科学技術分野における計測と標準に関する研究が行われている。
URL： https://www.nist.gov/

以下に、2023 年 9 月現在の NIST 軽量暗号コンペティションにおける標準化動向に関する状況を整理する。NIST 軽量暗号コンペティションでは選定プロセスにおける Round 1 から Final Round の 3 回の選定が実施されている。それぞれの選定プロセスにおいて、どのような軽量暗号アルゴリズムが提案され、採択されたかについては表 1 を参照することで全体像を把握することができるように情報整理を行なっている。

	Round1	Round2	Final Round	Final Selection
#	候補アルゴリズム名	候補アルゴリズム名	候補アルゴリズム名	候補アルゴリズム名
1	ACE	ACE	ACE	ACE
2	ASCON	ASCON	ASCON	ASCON
3	Bleep64	Bleep64	Bleep64	Bleep64
4	CiliPadi	CiliPadi	CiliPadi	CiliPadi
5	CLAE	CLAE	CLAE	CLAE
6	CLX	CLX	CLX	CLX
7	COMET	COMET	COMET	COMET
8	DryGASCON	DryGASCON	DryGASCON	DryGASCON
9	Elephant	Elephant	Elephant	Elephant
10	ESTATE	ESTATE	ESTATE	ESTATE
11	FlexAEAD	FlexAEAD	FlexAEAD	FlexAEAD
12	ForkAE	ForkAE	ForkAE	ForkAE
13	Fountain	Fountain	Fountain	Fountain
14	GAGE and InGAGE	GAGE and InGAGE	GAGE and InGAGE	GAGE and InGAGE
15	GIFT-COFB	GIFT-COFB	GIFT-COFB	GIFT-COFB
16	Gimli	Gimli	Gimli	Gimli
17	Grain-128AEAD	Grain-128AEAD	Grain-128AEAD	Grain-128AEAD
18	HERN & HERON	HERN & HERON	HERN & HERON	HERN & HERON
19	HYENA	HyENA	HyENA	HyENA
20	ISAP	ISAP	ISAP	ISAP
21	KNOT	KNOT	KNOT	KNOT
22	LAEM	LAEM	LAEM	LAEM
23	Lilliput-AE	Lilliput-AE	Lilliput-AE	Lilliput-AE
24	Limdolen	Limdolen	Limdolen	Limdolen
25	LOTUS-AEAD and LOCUS-AEAD	LOTUS-AEAD and LOCUS-AEAD	LOTUS-AEAD and LOCUS-AEAD	LOTUS-AEAD and LOCUS-AEAD
26	mixFeed	mixFeed	mixFeed	mixFeed
27	ORANGE	ORANGE	ORANGE	ORANGE
28	Oribatida	Oribatida	Oribatida	Oribatida
29	PHOTON-Beetle	PHOTON-Beetle	PHOTON-Beetle	PHOTON-Beetle
30	Pyjamask	Pyjamask	Pyjamask	Pyjamask
31	Qameleon	Qameleon	Qameleon	Qameleon
32	Quartet	Quartet	Quartet	Quartet
33	REMUS	REMUS	REMUS	REMUS
34	Romulus	Romulus	Romulus	Romulus
35	SAEAES	SAEAES	SAEAES	SAEAES
36	Saturnin	Saturnin	Saturnin	Saturnin
37	Shamash & Shamashash	Shamash & Shamashash	Shamash & Shamashash	Shamash & Shamashash
38	SIMPLE	SIMPLE	SIMPLE	SIMPLE
39	SIV-Rijndael256	SIV-Rijndael256	SIV-Rijndael256	SIV-Rijndael256
40	SIV-TEM-PHOTON	SIV-TEM-PHOTON	SIV-TEM-PHOTON	SIV-TEM-PHOTON
41	SKINNY-AEAD/SKINNY-HASH	SKINNY-AEAD/SKINNY-HASH	SKINNY-AEAD/SKINNY-HASH	SKINNY-AEAD/SKINNY-HASH
42	SNEIK	SNEIK	SNEIK	SNEIK
43	SPARKLE (SCHWAEMM and ESCH)	SPARKLE (SCHWAEMM and ESCH)	SPARKLE (SCHWAEMM and ESCH)	SPARKLE (SCHWAEMM and ESCH)
44	SPIX	SPIX	SPIX	SPIX
45	SpoC	SpoC	SpoC	SpoC
46	Spook	Spook	Spook	Spook
47	Subterranean 2.0	Subterranean 2.0	Subterranean 2.0	Subterranean 2.0
48	SUNDAE-GIFT	SUNDAE-GIFT	SUNDAE-GIFT	SUNDAE-GIFT
49	Sycon	Sycon	Sycon	Sycon
50	Thank Goodness It's Friday (TGIF)	Thank Goodness It's Friday (TGIF)	Thank Goodness It's Friday (TGIF)	Thank Goodness It's Friday (TGIF)
51	TinyJambu	TinyJambu	TinyJambu	TinyJambu
52	Triad	Triad	Triad	Triad
53	TRIFLE	TRIFLE	TRIFLE	TRIFLE
54	WAGE	WAGE	WAGE	WAGE
55	Xoodyak	Xoodyak	Xoodyak	Xoodyak
56	Yarará and Coral	Yarará and Coral	Yarará and Coral	Yarará and Coral

表 1　NIST 軽量暗号コンペティション選定アルゴリズム（最終決定）

【Round 1】

2019 年 3 月に NIST は、NIST 軽量暗号コンペティションの Round 1 として 57 件の提出物を受け取り、“Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process”[6]で示した要件に基づき完全性と妥当性の観点から提出された軽量暗号アルゴリズムから Round 1 の候補アルゴリズムとして 56 個のアルゴリズム選定を 2019 年 4 月に行い、2019 年 8 月に Round 1 を終了した。

なお、Round 1 に関する詳細なステータスについては、“Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process”[7]を参照してほしい。

なお、Round 1 で使用された評価基準は [7]において要約されているので、概要について整理を行う。この Round での評価基準として最重要なものは、「提出された暗号アルゴリズムの安全性」と言える。軽量暗号であることを評価するために制約のある環境下での実装特性（性能とコスト）も重要な基準となっていたことがわかる。また、実装での安全性の観点からは、サイドチャネル攻撃への対策に適しているかどうかについても評価されていた。

【Round2】

NIST 軽量暗号コンペティションの Round2 は、NIST が 2019 年 8 月に 32 個の候補アルゴリズムを発表し、2021 年 3 月に Finalist を公表したことで Round2 が終了した。なお、Round2 における選定に関する詳細なステータスについては、“Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process”[8]を参照してほしい。

[8]において Round2 で使用された評価基準が要約されているので、概要について整理を行う。この Round での評価基準は、前回の Round 1 と同様の評価観点である「第三者による分析や広く理解された設計原理と安全性証明に基づく要求」および「制約のあるデバイスを用いたアプリケーションにおける候補アルゴリズムの性能（制約のある環境における候補アルゴリズムのハードウェアおよびソフトウェアの性能)」というものであり、Round を経ることにより評価基準が詳細化されたという理解をした。なお、Round 1 と同様に候補アルゴリズムのサイドチャネル耐性についても評価基準となっていた。

【Final Round】

NIST 軽量暗号コンペティションの Final Round は、2021 年 3 月に Round2 での評価を踏まえて Ascon、Elephant、GIFT-COFB、Grain-128AEAD、ISAP、PHOTON-Beetle、Romulus、SPARKLE、TinyJAMBU、および Xoodyak の 10 個のアルゴリズムを選定し

た。当初は、NIST 軽量暗号コンペティションにおいて制約のある環境に適した AEAD とハッシュ機能として 1 つまたは複数の方式を選択するために標準化プロセスを開始したが、結果として 2023 年 2 月 7 日に Ascon ファミリーを選定したことを発表した。

なお、Final Round における選定に関する詳細なステータスについては、“Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process”[1]を参照してほしい。このドキュメントの目的は標準化プロセスとして Final Round の公開記録を提供し、選定された最終候補のアルゴリズムの評価について説明することである。

各 Round での候補アルゴリズムが選定されなかった理由については、NIST が公開している Status Report において示されているが、次の Round に進めなかった理由について概要を整理する。

【Round 1】

- 第三者による安全性に対する評価が公開されていないことや提出資料において、安全性の要求を裏付ける情報が不十分である提案については除外された。
- 第三者評価によって、Forgery Attacks、Length-extension Attacks や Distinguishing Attacks が存在する方式が整理された。
  - なお、指摘された懸念を払拭するために設計者が提案した修正は、評価時には考慮されなかったが、実装のバグによる実用的な攻撃（例えば、Forgery Attacks）は排除の理由とはされなかった。NIST の研究者は実装の更新をチェックし、元の仕様と整合性が取れているかを確認した。

【Round 2】

- Round 1 と同様に第三者による安全性評価が行われていることや安全性の要求を裏付ける情報が十分に情報公開されていること。
- 制約のあるデバイスを使用するアプリケーションにおける性能（制約のある環境におけるハードウェアおよびソフトウェアでの性能）がよいこと。
  - さまざまな性能とコストの指標で評価・比較され、現在の NIST 標準（特に AES-GCM [9]と SHA-2 [10]）より著しく性能がよいものが選定時に優遇されていた。
- 追加検討事項として、以下の項目について評価されている。
  - Side-Channel Resistance、Nonce-Misuse Security、RUP Security、Impacts of State Recovery および Post-Quantum Security

3. Ascon の選定に関する評価基準や評価観点

NIST 軽量暗号コンペティションの最終選考アルゴリズムとして Ascon が選定されたが、Final Round[†]における評価基準と選考プロセスについての概要を整理し、Ascon が選定された理由について調査結果を示す。詳細については、文献 [1]の「2. Evaluation Criteria and Selection Process」を参照することでより詳しく情報を得ることができる。

3.1. NIST 軽量暗号コンペティションにおける評価基準や評価観点

NIST 軽量暗号コンペティションにおける評価基準について、まとめると以下に示す 4 つが主な基準となっていると考えられる。また、重要度という観点から評価基準を見ると、最も重要な基準は「安全性」である。それに次ぐ重要な基準は「制約のある環境下におけるソフトウェアおよびハードウェアでの性能」であると考えられる。

- 暗号学的安全性
- 制約のある環境下におけるソフトウェアおよびハードウェアでの性能
- サイドチャネル攻撃や故障攻撃への耐性
- 知的財産

それぞれの評価基準について、具体例を挙げて詳しく解説を行う。

- 暗号学的安全性

  評価対象アルゴリズムにおける安全性は、提出された閲覧可能な自己による安全性解析結果、設計者による安全性に対する要求、安全性証明、広く閲覧可能な第三者による安全性評価などの情報を幅広く評価している。

  なお、明示的に提出が要求されていないが、Nonce-misuse シナリオや Releasing Unverified Plaintext (RUP) シナリオ、状態回復への影響、耐量子暗号としての安全性などが追加の考慮事項として挙げられている。

  なお、最終候補として選定されたアルゴリズムに対する安全性評価については、文献 [1]の「3. Finalists」に整理されている。

[†] 文献 [1]において、Final Round が Round 3 として明記されていることに注意されたい。

・ 制約のある環境下におけるソフトウェアおよびハードウェアでの性能

様々な性能やコストに関する測定基準において、Final Round に選定されたアルゴリズム同士や NIST 標準である AES-GCM [11] [12]（AEAD としての比較対象）と SHA-2 [13]（ハッシュ関数としての比較対象）との比較・評価が行われる。なお、現行アルゴリズムとして広く採用されている AES-GCM や SHA-2 に対しては大幅に優れた性能を発揮することが期待されている。

なお、最終候補として選定されたアルゴリズムの性能比較結果は、文献［1]の「4. Benchmarking Results」および「B. NIST Software Benchmarking Results」に整理されている。

・ サイドチャネル攻撃や故障攻撃への耐性

サイドチャネル攻撃への耐性を提供する必要はないと示されているが、簡単かつ低コストで実現できることが強く要望されている。

なお、最終候補として選定されたアルゴリズムのサイドチャネル攻撃や故障攻撃に関する結果は、文献［1]の「4.3. Resistance to Side-Channel and Fault Attacks」に整理されている。

・ 知的財産

知的財産について、特許請求の使用を必要とする可能性のあるアルゴリズムや実装に反対はしないが、技術的な理由によりこのアプローチが正当化される場合、評価プロセスでの選定を妨げる可能性のある要因であると示されている。

なお、知的財産に関する声明については、文献［1]の「2.2. Selection Process」に整理されている。

3.2. NIST 軽量暗号コンペティションにおける評価プロセス

最終候補を公正に評価し、標準化されたのちに長期にわたって利用されるアルゴリズムを選択することが困難な作業であることが示されており、困難な作業である理由として、以下の項目が挙げられている。

・ 最終候補の機能

- セキュリティの要求
- ベースとなる構成要素
- サポートされるパラメータサイズ
- 設計アプローチ
- バリエーションの数
- 利用可能な第三者による安全性評価の数
- 最適化された実装物の数

また、NIST 軽量暗号コンペティションの初期段階において、ターゲットアプリケーションに関して、一般からのフィードバックを踏まえて 2 つのプロファイル（図 2）を決定した。この部分が NIST 軽量暗号コンペティションにおいて 1 つまたは複数のアルゴリズムが選定される可能性が出た要因である。

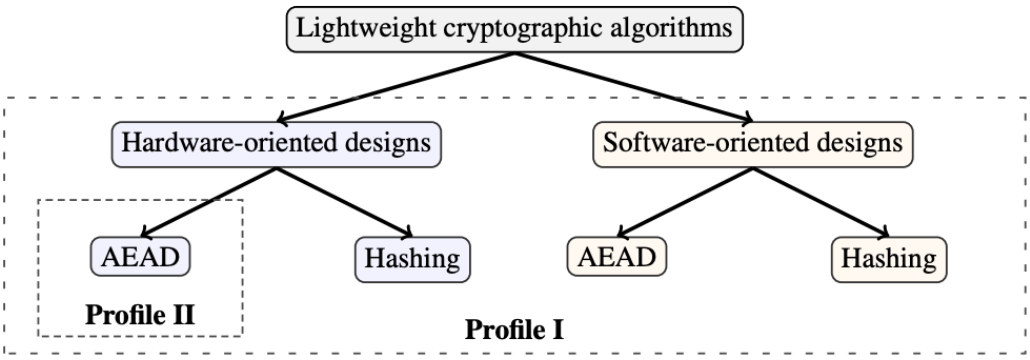

図 2 軽量暗号アプリケーションにおけるプロファイル

2 つのプロファイルが定められており、以下のとおりである。

- プロファイル 1
  - 制約のある環境でのソフトウェアとハードウェアのための AEAD およびハッシュ
- プロファイル 2
  - 制約のある環境でのハードウェアのための AEAD

最終候補に対する評価プロセスとして、第三者によるセキュリティ評価、バリエーション、設計の微調整、ベンチマーク、耐量子安全性、知的財産に関する声明の 6 つの観点から状況を整理し、まとめる。

・ 第三者によるセキュリティ評価

最終候補のアルゴリズムは、多くの第三者によるセキュリティ評価が行われた。それぞれの最終候補に対する評価結果は、文献 [1]の「3. Finalists」にまとめられている。また、単一鍵および Nonce-respecting において最終候補における安全性の要求を無効にするような評価はなく、ほとんどの候補は安全性のマージンがある状況であった。

・ バリエーション

AEAD とハッシュについては、異なる入出力サイズをサポートし、かつ／または異なるベースとなる構成ブロックを持つ、複数のバリアント（最大 10 個）の提出が許可されたが、NIST は公正な比較を行えるようにするため特定の入出力サイズを持つ AEAD とハッシュのバリエーションを各チームに求めた。この要望に対して、いくつかのチーム（Ascon、SPARKLE、Xoodyak など）には eXtendable Output Function (XOF)の亜種が含まれていたが、これらは正式なバリエーションとは考慮されなかったが、XOF 機能を提供できる柔軟性は選考過程において設計における有利な点としてみなされた。

・ 設計の微調整

Final Round の初期段階において、安全性や実装性能を向上させるための軽微な設計変更（NIST は以前に実施されたセキュリティ評価を無効にしない範囲を想定）が許可されたが、Ascon、GIFT-COFB、ISAP、PHOTON-Beetle および SPARKLE については、設計上の微調整は実施されなかった。一方、その他の候補については、性能向上や安全性改善のために設計が修正された。

・ ベンチマーク

NIST 標準である AES-GCM と SHA-2 よりも大幅に優れた性能を発揮することが期待されている。また、軽量暗号の重要な要素の 1 つとして、実装者が特定の用途に最適な実装を行うためのトレードオフ（コストと性能）を行えることである。

ソフトウェアでのベンチマーク結果として Ascon、GIFT-COFB、SPARKLE、TinyJAMBU および Xoodyak が、様々なプラットフォームで性能における優位性を示めした。詳細な情報については、文献 [1]の「4.1. Software Benchmarking」および「Appendix B. NIST Software Benchmarking Results」にまとめられている。また、ハードウェアでのベンチマーク結果として、Ascon、Xoodyak および TinyJAMBU が

最も優れた性能を示した。詳細な情報については、文献 [1]の「4.2. Hardware Benchmarking」にまとめられている。

また、サイドチャネル攻撃や故障攻撃への耐性やそのような攻撃を軽減させるための必要な実装オーバーヘッドについても評価が行われ、Ascon、ISAP、Xoodyak および TinyJAMBU はとても良い評価を示した。詳細な情報については、文献 [1]の「4.3.1. Protected Implementations and Side-Channel Security Evaluations」にまとめられている

- 耐量子安全性

軽量暗号の標準化プロセスにおける主要な関心事の一つではないが、量子コンピュータによる脅威に対する安全性の提供は長期利用の観点からも必要であるため、評価時には量子的な脅威に対するセキュリティも考慮された。一般的に共通鍵暗号関連の耐量子安全として、最も一般的な攻撃は Grover アルゴリズム [14]であり、網羅的な鍵探索(または、ハッシュ関数における衝突の発見)を 2 次関数的に高速化することが知られている。この攻撃を回避するためには、より大きな鍵サイズ（または、より大きなダイジェストサイズ）を持たせることになる。

これを踏まえると、3 つの候補が 128 ビットより長い鍵をサポートしている結果となった。特に SPARKLE ファミリーと TinyJAMBU ファミリーは 192 ビットと 256 ビットの鍵を持つ AEAD バリエーションを含み、また Ascon のバリエーションの 1 つが 160 ビットの鍵をサポートしている。

- 知的財産に関する声明

NIST は、最初のアルゴリズム提出時に、選択されたアルゴリズムに対して全世界でロイヤリティなしで利用できるようにするという目標が述べられていた。NIST は、アルゴリズム提出者に対し、候補アルゴリズムの実装によって侵害される可能性のある既知の知的財産をすべて特定するよう要求しており、結果として、最終候補の中で、該当する特許が特定されたのは PHOTON-Beetle のみという結果となった。しかしながら、この知的財産に関する事項は選考プロセスの決定には影響はなかったことが示されている。

3.3. Ascon に関する評価

NIST 軽量暗号コンペティションで行われた評価として、上記の基準に従って最終候補を評価した結果、NIST は Ascon ファミリーを標準化として選定した。Ascon ファミリーは、AEAD とハッシュ関数、そして追加された XOF を含むものとなっている。これにより、幅広いアプリケーションのニーズを満たすことができる。また、Permutation ベースの設計であるため追加機能を実装する際に追加コストが少なく済むことが期待されている。最終候補の中でも Ascon は、安全性という側面から見ると最終候補の中で最も成熟していると考えられている。理由としては、他の最終候補のいくつかは NIST 軽量暗号コンペティションの前から発表されていなかったが、Ascon ファミリーの AEAD バリエーションは CAESAR コンペティションの一環として発表され、安全性等について分析が行われていた。この CAESAR コンペティションでは、軽量認証暗号化を含む 3 つのプロファイルが作成されており、最終的に Ascon の AEAD バリエーションは、最終的な CAESAR ポートフォリオにおける軽量アプリケーションの主要な選択肢として選定された実績もある。Ascon の成熟度は、Final Round で行われた設計の微調整にも現れており、バリアントが追加されたが、Round 2 のバリエーションには設計の変更が行われていない状況であった。この事実を踏まえると、評価・分析で行われた攻撃に対処するために設計の微調整を行った他最終候補とは異なり、Ascon の高い成熟度を認識することができる事象と言える。

Ascon は公開されてから長い歴史があるため豊富な評価・分析が行われており、第三者による評価と実装が最も多いアルゴリズムであると言える。また、Ascon は暗号解析攻撃で先行しているにもかかわらず、高い安全性を維持している。さらに、Ascon ファミリーの AEAD バリエーションは、nonce-misuse resilience など AEAD におけるいくつかの高いセキュリティ機能を有する。

専用ハードウェアや組み込みシステムなど制約の多い環境での性能という基準は、最終選定の重要な要因となったと記されている。Ascon はソフトウェアおよびハードウェアで非常に優れた性能を発揮した。コストと性能の間のさまざまなトレードオフをサポートする実装の柔軟性を実証し、制約のあるリソース環境のさまざまなソフトウェアおよびハードウェアで、現在の NIST 標準である AEAD（AES-GCM）およびハッシュ（SHA-2）よりも優れた性能を示した。Ascon はまた、サイドチャネル攻撃等に対する対策が行われた保護された実装において、保護されていない実装よりも追加コストが低いことも示された。最終候補の 1 つである ISAP も、Ascon の Permutation に依存する AEAD のバリエーションを 2 つ持っていたが、最終的に Ascon よりも実装がより大きく、より遅くなるため実現性が低いと判断された。

軽量暗号の標準化プロセスで研究されたAsconのバリエーションの重要な制限事項の1つは、「256 ビット鍵のオプションがない」ことである。これは、量子アルゴリズムによる攻撃に対する 128 ビットのセキュリティが必要な場合に問題となる。しかしながら、この点に対して NIST は、この選定プロセスの主な目的を「軽量な AEAD とハッシュである」と強調している。もし仮に耐量子対策として 256 ビット鍵が必要な場合には、AES-GCM を使用することができると考えているようである。必要に応じて、より高い耐量子安全性を実現する追加のバリエーションの検討する可能性もあることが示唆されている。

なお、NIST の見解として、当面、Ascon ファミリーは制約のある環境下において十分なセキュリティを提供できると考えており、Ascon の性能はターゲット・デバイスやアプリケーションで許容されると予想されるため、現時点では第二候補のアルゴリズムは必要ないと判断しているとのことである。

4. 他標準化団体における軽量暗号 Ascon への検討状況

NIST 軽量暗号コンペティションにおいて、2023 年 2 月に Ascon が選定された結果を受けて、Ascon そのものや軽量暗号に関する採用に向けた検討が行われているかについて、NIST 以外の組織で標準化が行われているかを調査した。調査方法については以下のとおりである。

- 調査対象 標準化団体
  - IETF、W3C、ISO/IEC、ITU-T、Global Platform
- 調査方法
  - 調査手段：検索エンジン
  - 検索キーワード：Ascon、Light weight Crypto
  - 検索期間：2023 年 2 月 7 日 ～ 9 月 15 日

調査結果は以下のとおり[†]。

- IETF
  - Internet Draft “Secure UAS Network RID and C2 Transport” [15] の「5.3. Ciphers for Secure Transport」において、無人航空機で Ascon を選択するのが最善であることが示されている[‡]。その際には、ESP [16]や DTLS [17]の拡張が必要であるとも記述されている。
  - Internet Draft “Properties of AEAD algorithms” [18]の「4.4.2. Lightweight」において、NIST 軽量暗号コンペティションに関する参照が行われている。
  - IETF 117 で開催された TLS WG の発表である「New Post-Quantum Signatures on the Horizon」 [19]において、Ascon-Sign（SPHINCS+ with Ascon）が取り上げられていた。
- W3C
  - 調査した範囲では該当なし
- ISO/IEC
  - 調査した範囲では該当なし

[†] 2024 年 3 月 3 日現在、調査結果に関して追加情報が無いことを確認した。

[‡] Internet Draft 内では「NIST has selected a new lightweight cipher, Ascon, that may be the best choice for use on a UA. Work will be needed to develop full support for Ascon in both ESP and DTLS.」と記述されている。

- ITU-T
  - 調査した範囲では該当なし
- Global Platform
  - 調査した範囲では該当なし

以上のことから、標準化団体での検討状況については、大きな動きはあるように感じられなかった。しかしながら産業界において NIST 軽量暗号コンペティションの結果を受けて利用可能な環境を提供するような動向を把握したのでいくつか紹介する。NIST による最終的な標準化仕様が公開されることで、他標準化団体や産業界での活動が活性化されることが期待される。

- IP コア関連
  - Rambus 社 「Ascon-IP-41 暗号エンジン」 [20]
  - Xiphera 社 「XIP2201B: Ascon」 [21]
  - CAST 社 「Ascon-F」 [22]
- 暗号ライブラリ関連
  - Bouncy Castle 1.7.3 以降 [23]
  - CIRCL[§] [24]

[§] GitHub 上には記述されていないが、”https://pkg.go.dev/github.com/cloudflare/circl@v1.3.3/cipher/Ascon”には仕様が公開されている。

5. Ascon に関する考察

これまでの調査結果を踏まえて Ascon が選定されたことについて考察を行う。ポイントとなるのは、文献 [1]で示されている以下のような評価基準において、全体的に高い評価を得ることができている点であると考えられる。

- 暗号学的安全性
- 制約のある環境下におけるソフトウェアおよびハードウェアでの性能
- サイドチャネル攻撃や故障攻撃への耐性
- 知的財産

特に「暗号学的安全性」と「制約のある環境下におけるソフトウェアおよびハードウェアでの性能」が高く評価されているのではないかと考える。

5.1. 安全性

安全性については、Ascon のバリエーションが CAESAR コンペティションの最終ポートフォリオに含まれていることから、発表からの長い歴史があるため、第三者からのセキュリティ評価の数もかなり多い結果となっている。また、NIST 軽量暗号コンペティションにおいても Round 2 以降に設計を変更しないくらい設計が枯れていることも評価ポイントになっていたと考えられる。なお、文献 [1]の「3.1.2. Security Analysis」において、Ascon ファミリーに対するセキュリティ評価の概要がまとめられているので、具体的な内容を把握したい方は参照のこと。

5.2. 性能

制約のある環境下におけるソフトウェアおよびハードウェアでの性能については、ソフトウェアベンチマークおよびハードウェアベンチマークのそれぞれについて考察を行う。なお、文献 [1]の「4. Benchmarking Results」に注意点として、最終候補の特定の指標における最適化の可能性を完全に示すものでなく、すべての実装が同じ仮定や目標で設計されているわけではないことが示されている、さらに、注意点として、最終候補のより効率的な実装は実施可能であり、厳密な順位付けではないことに注意し一般的な指針として考慮することが示されている。

＜ソフトウェア・ベンチマーク＞

マイクロコントローラ上のソフトウェア性能は、最終候補の評価基準として重要である。評価実施については、複数の評価主体によって性能評価が行われた。評価主体とマイクロコントローラの環境については表 2 のとおりである。この評価では、メモリに制限のある 8 ビットマイコンから 32 ビットおよび 64 ビットマイコンまで幅広いターゲットプラットフォームを対象としている。

表 2 評価主体とベンチマークに使用したマイコンの仕様

Initiative	*Microcontroller*	*Processor*	*Word size*	*Clock speed*	*Flash*	*RAM*
NIST [253]	ATmega328P	AVR	8-bit	16 MHz	32 KB	2 KB
	ATmega4809	AVR	8-bit	16 MHz	48 KB	6 KB
	SAMD21G18A	ARM Cortex-M0+	32-bit	48 MHz	256 KB	32 KB
	nRF52840	ARM Cortex-M4	32-bit	64 MHz	1 MB	256 KB
	PIC32MX320F128H*	MIPS32 M4K	32-bit	80 MHz	128 KB	16 KB
	PIC32MX340F512H	MIPS32 M4K	32-bit	80 MHz	512 KB	32 KB
	ESP8266	Tensilica L106	32-bit	80 MHz	4 MB	80 KB
	AT91SAM3X8E	ARM Cortex-M3	32-bit	84 MHz	512 KB	96 KB
Renner et al. [254]	ATmega328P	AVR	8-bit	16 MHz	32 KB	2 KB
	STM32F103C8T6	ARM Cortex-M3	32-bit	72 MHz	64 KB	20 KB
	STM32F746ZG	ARM Cortex-M7	32-bit	216 MHz	1 MB	320 KB
	ESP32 WROOM	Tensilica Xtensa LX6	32-bit	240 MHz	4 MB	520 KB
	Kendryte K210	RISC-V (Dual Core)	64-bit	400 MHz	16 MB	8 MB
Weatherley [255]	ATmega2560	AVR	8-bit	16 MHz	256 KB	8 KB
	AT91SAM3X8E	ARM Cortex-M3	32-bit	84 MHz	512 KB	96 KB
	ESP32	Tensilica Xtensa LX6	32-bit	240 MHz	4 MB	520 KB

*PIC32MX340F512H microcontroller used with PlatformIO's PIC32MX320F128H board profile

以下に、NIST と Renner らによる評価結果の概要を示す。

- NIST による評価結果の概要
  - 評価環境での性能と PlatformIO でのコンパイルに成功した時に使用されたフラッシュサイズ（単位: バイト）で評価された。
  - AEAD 機能のサイズにおいて、Ascon は一貫してトップ・パフォーマーであり、AES-GCM よりもコンパクトな実装を実現した。
  - ハッシュ機能のサイズにおいて、Ascon はすべてのプラットフォームで一貫して SHA-256 より小さかったが、すべての環境で最速だったのは SHA-256 であった。
- Renner らによる評価結果の概要

- マイクロコントローラ上の AEAD アルゴリズムの性能を評価するためのベンチマークフレームワークを開発しており、この評価では、実行時間（マイクロ秒、テストベクタの平均生成時間)、コンパイル済みバイナリのサイズおよび RAM 使用量（STM32F7 のみ）を得ることができる。
- Arduino Uno の環境において、SPARKLE 、GIFT-COFB 、Xoodyak がトップ 3 であり、Ascon はかなり近接するような速度であったことから、この環境ではトップ集団でないことがわかる。ただし、コードサイズの観点では Ascon は最小サイズに達していると報告されている。

以上のことから、ソフトウェア・ベンチマークにおいて、Ascon は全体的にすべての環境で実行速度およびコードサイズにおけるトップ・パフォーマーであることが選定の決め手になったと考えられる。

＜ハードウェア・ベンチマーク＞

ハードウェア・ベンチマークにおいて、Round 2 で実施されたサイドチャネル攻撃対策が行われていない実装の性能評価結果の多くは Final Round に流用可能であることが示されていた。特に NIST は、ジョージ・メイソン大学（GMU）の暗号研究グループである CERG の評価結果に注目した。また、GMU はサイドチャネル攻撃等の対策を行った実装評価を行うには膨大な時間と専門知識が必要であり、単一グループが単独で行うことが困難であることを踏まえて、複数グループのリソースと専門知識を集結させるなどの貢献を行なっている。

GMU チームによる評価は、ベンチマーク環境として Xilinx 社 Artix-7 プラットフォームを使用した。保護された実装と保護されていない実装の両方が評価された。保護されていない実装と保護された実装のスループットや面積、あるいはマスキングに必要なランダム・ビット数などの性能比較により、保護されていない実装に保護手法を適用するコストに関する知見が得られたとされている。その評価結果として、非保護の AEAD 実装において Ascon は AES-GCM よりも平文を高速に処理した。サイズについて Ascon はトップ集団と比較するとよい結果は出ていない。なお、スループットから評価すると Ascon は最もスループットが高い結果となった。また、ハッシュ処理では、Ascon の非保護実装が最も高いスループットを示したが、サイズについて Ascon はトップ集団と比較するとよい結果は出ていない。

以上のことから、ハードウェア・ベンチマークにおいて、Ascon は全体的にすべての環境で実行速度においてはトップ・パフォーマーであるが、サイズの観点からは Ascon は最小

の実装を実現できていないが、GMU 以外の評価主体の評価によりエネルギー効率がよいことが報告されていることから選定の決め手になったと考えられる。

上記で考察した結果や文献 [1]で議論されている内容を踏まえると、Ascon は NIST 軽量暗号コンペティションの評価基準において高い評価結果を示していることから順当な判断によって選定されたと考える。

5.3. 標準化

NIST 軽量暗号コンペティション終了後である 2023 年 6 月 21～22 日にオンライン開催であったが、NIST 主催による 6th Lightweight Cryptography Workshop[**]が開催され、選定プロセスや軽量暗号の標準化に関する様々な側面について議論が行われた。18 個の発表が行われたが、その中から NIST 所属の Meltem Sönmez Turan 氏によって発表された「Evaluation of the Finalists and the Selection of Ascon」 [25]において、Ascon の標準化ドキュメントが公開されるタイミングに関する情報について言及されているためである。その標準化ドキュメントの公開時期として 2023 年後半（図 3）と共有されている。本報告書の 2023 年 9 月現在、標準ドキュメントの草案は公開されていない。

図 3 資料" Evaluation of the Finalists and the Selection of Ascon"

[**] https://csrc.nist.gov/Events/2023/lightweight-cryptography-workshop-2023

6. まとめ

本報告書では、NIST 軽量暗号コンペティションで 2023 年 2 月 7 日に選定された Ascon について標準化動向の調査を行った。Ascon の選定に関連する情報については、文献 [1]に詳しく記載されているため、この文献を中心に調査を行った。

Final Round では、最終候補として 10 のアルゴリズムが選択され、以下に示すような選考プロセスにおいて評価が行われた。

- 選考プロセスでのポイント
  - 様々な評価基準（安全性、ソフトウェアおよびハードウェアの性能、設計の成熟度、第三者による安全性評価の量、知的財産権の有無など）に異なる重み付けを割り当てて実施
  - 異なるセキュリティ要件、異なる機能性、異なる複雑性を持った攻撃などを踏まえた評価の実施
  - 限られたリソースにおける安全性評価および性能評価の実施

最終候補となったアルゴリズムの中から NIST が Ascon を選定したポイントについて整理を行うと以下の項目が挙げられる。

- 安全性
  - 高いセキュリティーマージン
  - 多数の第三者による安全性評価の数
- 設計/実装
  - 設計の微調整を行わないという設計の成熟度
  - 軽量暗号コンペティションである CAESAR プロジェクトにおいて軽量暗号の最終的なポートフォリオに選択されている実績
  - 漏えいに対するモードレベルでの保護メカニズムを有すること
  - 実装と設計の柔軟性
  - サイドチャネル攻撃に対する対策を行うための追加コストが低いこと
- 機能性
  - ハッシュに加えて XOF や MAC などの追加機能を有すること
- 性能
  - ソフトウェアおよびハードウェア環境において、現行の NIST 標準である AES-GCM や SHA-2 を上回る性能を有すること

また、NIST 以外の標準化団体における検討については、2023 年 9 月現在では大きな動き

は見られなかったが、2023 年後半に予定されている NIST が発行する標準仕様の公開を受けて、本格的に様々な団体での検討が行われるものと考える。また、標準化された暗号技術が利用できる環境としてソフトウェアやハードウェア実装が公開されることが重要であるが、CAESAR プロジェクト等の実績などから実装がいくつか公開されているケースが見受けられた。これは Ascon の設計が成熟しており、NIST 軽量暗号コンペティションにおいて設計の微修正が行われていないことが背景にあると考える。

参考文献

[1] NIST, “Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process:,” NIST, 2023.

[2] CRYPTREC 軽量暗号ワーキンググループ, “CRYPTREC 暗号技術ガイドライン（軽量暗号),” 3 2017.. Available: https://www.cryptrec.go.jp/report/cryptrec-gl-2003-2016jp.pdf.

[3] 伊藤竜馬, “「CRYPTREC 暗号技術ガイドライン（軽量暗号)」掲載の暗号方式に関する安全性評価の動向調査,” 2021. . Available: https://www.cryptrec.go.jp/exreport/cryptrec-ex-3101-2021.pdf.

[4] GMO サイバーセキュリティ by イエラエ株式会社, “軽量暗号の評価指標、標準化動向に関する調査（NIST 軽量暗号コンペティションファイナリストなど）,” 17 4 2023. . Available: https://www.cryptrec.go.jp/exreport/cryptrec-ex-3206-2022.pdf.

[5] National Institute of Standards and Technology, “Lightweight Cryptography,” . Available: https://csrc.nist.gov/projects/lightweight-cryptography.

[6] NIST, “Submission Requirements and Evaluation Criteria for the Lightweight Cryptography Standardization Process,” NIST.

[7] K. M. Ç. Ç. D. C. ,. L. B. Meltem Sönmez Turan, “Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process,” 10 2019. . Available: https://csrc.nist.gov/publications/detail/nistir/8268/final.

[8] NIST, “Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process,” NIST, 2021.

[9] M. Dworkin, “NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC,” 11 2007. . Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

[10] National Institute of Standards and Technology, "FIPS PUB 180-4 Secure Hash Standard (SHS)," 2015. . Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[11] U.S. Department of Commerce , "Advanced Encryption Standard (AES)," 2001. . Available: https://doi.org/10.6028/NIST.FIPS.197- upd1.

[12] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," 11 2007. . Available: https://doi.org/10.6028/NIST.SP.800-38D.

[13] U.S. Department of Commerce , "Secure Hash Standard (SHS)," 8 2015. . Available: https://doi.org/10.6028/NIST.FIPS.180-4.

[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," 1996.

[15] R. Moskowitz, "Secure UAS Network RID and C2 Transport," 3 2023. . Available: https://datatracker.ietf.org/doc/draft-moskowitz-drip-secure-nrid-c2/.

[16] P. Jokela, "Using the Encapsulating Security Payload (ESP) Transport Format with the Host Identity Protocol (HIP)," 4 2015. . Available: https://www.rfc-editor.org/rfc/rfc7402.html.

[17] E. Rescorla, "The Datagram Transport Layer Security (DTLS) Protocol Version 1.3," 4 2022. . Available: https://www.rfc-editor.org/rfc/rfc9147.html.

[18] A. Bozhko, "Properties of AEAD algorithms," 3 2023. . Available: https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/.

[19] T. W. Bas Westerbaan, "New Post-Quantum Signatures on the Horizon," 7 2023. . Available: https://datatracker.ietf.org/meeting/117/materials/slides-117-tls-new-post-quantum-signature-algorithms-on-the-horizon-00.

[20] Rambus, "Rambus IP Solution Supports New NIST Lightweight Cryptography Algorithm," 22 2 2023. . Available: https://www.rambus.com/blogs/rambus-ip-solution-supports-new-nist-lightweight-cryptography-algorithm/.

[21] Xiphera, “XIP2201B: ASCON, A Lightweight Cryptographic Suite for AEAD and Hashing,” 1 8 2023. . Available: https://xiphera.com/products/pdf/XIP2201B_PB.pdf.

[22] CAST, “ASCON-F, ASCON Authenticated Encryption & Hashing Engine,” 11 9 2023. . Available: https://www.cast-inc.com/security/encryption-primitives/Ascon-f.

[23] Bouncy Castle, “The Legion of the Bouncy Castle,” 8 4 2023. . Available: https://www.bouncycastle.org/releasenotes.html#r1rv73.

[24] Cloudflare, “CIRCL (Cloudflare Interoperable, Reusable Cryptographic Library),” . Available: https://github.com/cloudflare/circl.

[25] Meltem Sönmez Turan - NIST, “Evaluation of the Finalists and the Selection of Ascon,” 21 6 2023. . Available: https://csrc.nist.gov/Presentations/2023/evaluation-of-the-finalists-and-the-selection.

[26] “CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness,” . Available: https://competitions.cr.yp.to/caesar.html.

[27] “FELICS - Fair Evaluation of Lightweight Cryptographic Systems,” . Available: https://www.cryptolux.org/index.php/FELICS.

[28] “CAESAR submissions,” . Available: https://competitions.cr.yp.to/caesar-submissions.html.

[29] T. A. &. A. Luykx, An Account of the ISO/IEC Standardization of the Simon and Speck Block Cipher Families, Springer.