軽量暗号と標準化動向

2024年9月2日

菅野　哲
GMOサイバーセキュリティ byイエラエ株式会社

自己紹介

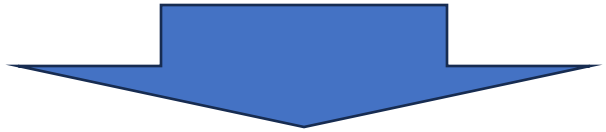
- 名前
  - 菅野 哲（かんの さとる）
- 所属
  - GMOサイバーセキュリティ byイエラエ株式会社
    - 常務取締役 CTO of Development
- どんなことやっていた／やっているの？
  - 暗号技術と標準化活動
    - 暗号ライブラリや情報セキュリティ関連のシステム開発
    - IETFなどでブロック暗号Camelliaに関する標準化活動
  - 外部活動
    - CRYPTREC 暗号鍵管理ガイダンスWG 委員
    - Trusted Computing Group Invited Expert（2018年10月～）
    - 公正取引委員会 デジタルアナリストとして活動（2024年5月1日 ～）

なぜ、新たな共通鍵暗号を必要としたのか？

新たな応用　X　新たな要求

背景

- バッテリー駆動などのより制約のある環境での需要が想定
- 省電力で暗号化を使いたいという要望
- 現行暗号（AES等）では、省電力性やフットプリントサイズなどがネックとなるケースを想定



「軽量暗号」の選定をしようぜ！

軽量暗号

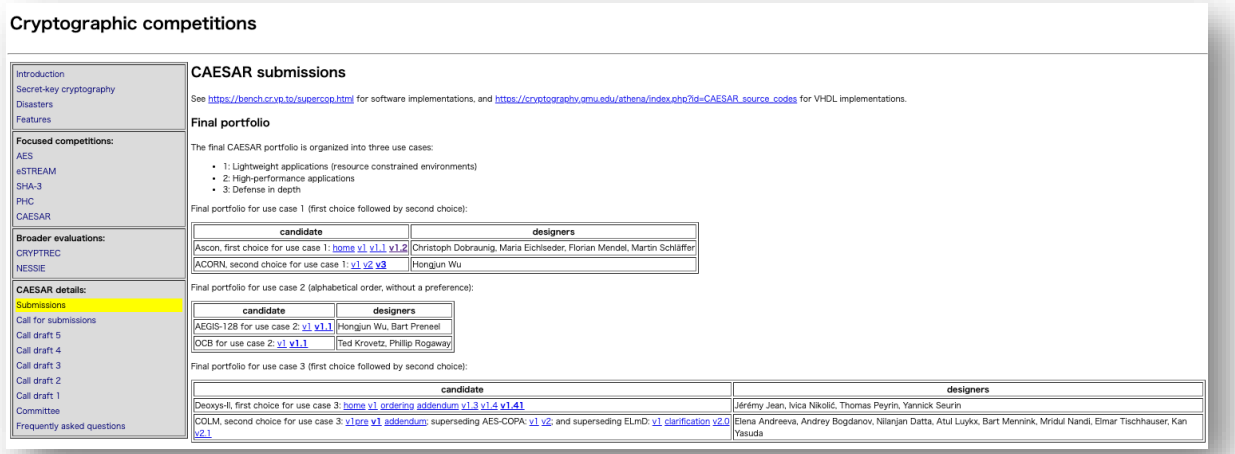
X

標準化動向

軽量暗号に関するコンペティション

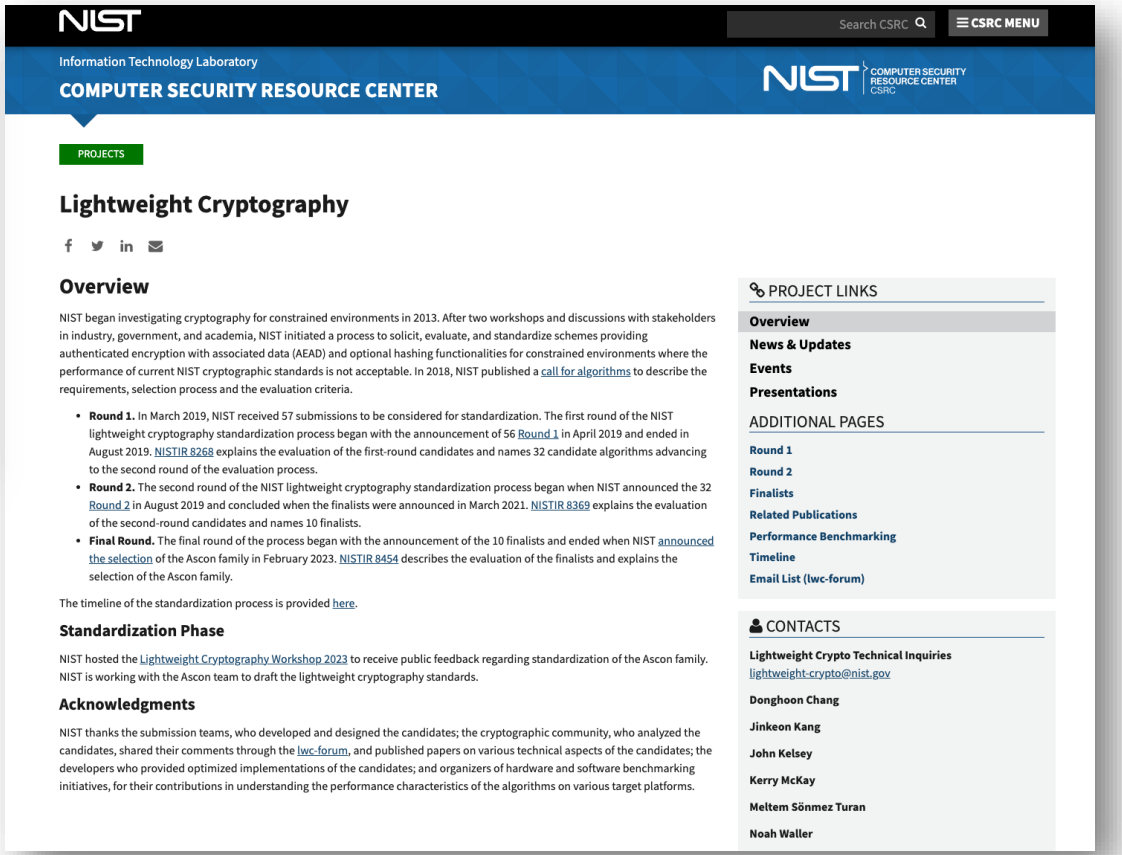
- メジャーな軽量暗号に関するコンペティションは2つあります。

【CAESARコンペティション】



https://competitions.cr.yp.to/caesar-submissions.html

【NIST軽量暗号コンペティション】



https://csrc.nist.gov/projects/lightweight-cryptography

軽量暗号に関するコンペティション

- メジャーな軽量暗号に関するコンペティション比較すると...

	CAESARコンペティション	NIST軽量暗号コンペティション
概要	認証付き暗号化（AEAD）の設計を促進 2013年に発表、2019年に最終ポートフォリオを決定	IoT機器などのリソースが制約された環境で使用するための軽量暗号 2019年に開始、2023年にASCON選定
目的	認証付き暗号化スキームの設計と評価 ・軽量アプリケーション ・高性能アプリケーション ・深層防御 (Defense in depth)	リソース制約のある環境での効率的な暗号化を提供するための方式の選定 特にエネルギー効率とセキュリティのバランスを重視
注目すべき成果	軽量暗号: ASCON、高性能アプリケーション向けとしてAEGIS-128などがある	AEADに加え、ハッシュ関数や拡張出力関数（XOF）などの機能を提供
気になる2つの違い	ターゲット: CAESARは主にAEADに焦点、NISTは軽量暗号全般に焦点 評価基準: CAESARは主に暗号化のセキュリティと適用性、NISTはエネルギー効率やリソース制約環境での実用性を重視	

NIST 軽量暗号コンペティション

- NISTによるAESやSHA-3などの実績のあるコンペティションのプロセスを踏襲

情報収集に向けたワークショップの開催
- 第1回 軽量暗号ワークショップ（2015年7月20日～21日）
- 第2回 軽量暗号ワークショップ（2016年10月17日～18日）

⇨ 軽量暗号の要件整理
ターゲットとする応用、業界ニーズについて広くフィードバックを収集

- 成果物
  - NIST IR 8114 Report on Lightweight Cryptography（初版: 2018年8月）
    - https://csrc.nist.gov/pubs/ir/8114/final

NIST 軽量暗号コンペティション

2018年8月に ”Submission Requirements and Evaluation Criteria for Lightweight Cryptography Standardization Process”を投稿（期限: 2019年2月）

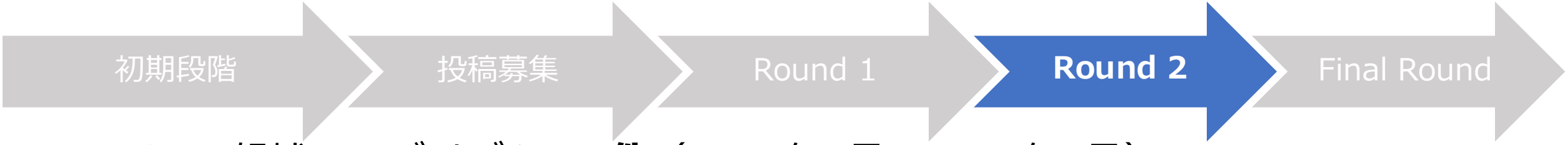
- セキュリティ要件
  - 安全性: 少なくとも112bit security
    （処理可能なデータ量上限 2^50バイト かつ nonce respecting setting）
  - 鍵長：少なくとも128bit
- 設計要件
  - NIST標準（AES-GCM、SHA-2）よりも高性能
  - 短いメッセージに最適化（IoT機器でのユースケースを想定）
- 実装要件
  - リファレンス実装、最適化実装、NISTが定義した標準APIとの互換性など

NIST 軽量暗号コンペティション

4ヶ月！

- Round 1の候補アルゴリズム **56件**（2019年4月～2019年8月）
- 3つの評価基準（セキュリティ、SW/HWパフォーマンス等）に基づいて評価
  - セキュリティに関する具体例：識別攻撃、実用的なタグ偽造、ドメイン分離に関する問題、独立した第三者による安全性評価
- 評価結果
  - 候補アルゴリズム **32件**が通過
- 成果物
  - NIST IR 8268 “Status Report on the First Round of the NIST Lightweight Cryptography Standardization Process”
    - https://csrc.nist.gov/pubs/ir/8268/final

NIST 軽量暗号コンペティション



- Round 2の候補アルゴリズム **32件**（2019年8月～2021年3月）
  20ヶ月！
- ワークショップ開催
  - 第3回 軽量暗号ワークショップ（2019年11月4日～6日）
  ⇨ 32候補の紹介＆議論、軽量暗号の研究成果共有、産業界からのフィードバック、評価基準や選定プロセスに関する議論
  - 第4回 軽量暗号ワークショップ（2020年10月19日～21日）
  ⇨ Round 2候補の分析結果、次Roundに進むべき候補に関する議論 等
- 評価結果
  - 最終候補アルゴリズム **10件**が通過
- 成果物
  - NIST IR 8369 “Status Report on the Second Round of the NIST Lightweight Cryptography Standardization Process” / https://csrc.nist.gov/pubs/ir/8369/final

NIST 軽量暗号コンペティション

- Final Round 候補アルゴリズム **10件**（2021年3月～2023年2月）

24ヶ月！

- **ASCON**
- **Elephant**
- **GIFT-COFB**
- **Grain-128AEAD**
- **ISAP**
- **Photon-Beetle**
- **Romulus**
- **Sparkle**
- **TinyJambu**
- **Xoodyak**

- 第5回 軽量暗号ワークショップ（2022年5月9日～11日）開催
- 困難を極めたFinalistの評価 ⇨ 包括的かつ透明性のある評価を重視(?)
  - 評価基準の重み付の難しさや各候補のセキュリティレベルや特性の差異
  - 安全性評価やベンチマークに向けたリソース制限 / 公開情報の偏り
- 成果物
  - NIST IR 8454 “Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process”（2023年6月）/ https://csrc.nist.gov/pubs/ir/8454/final

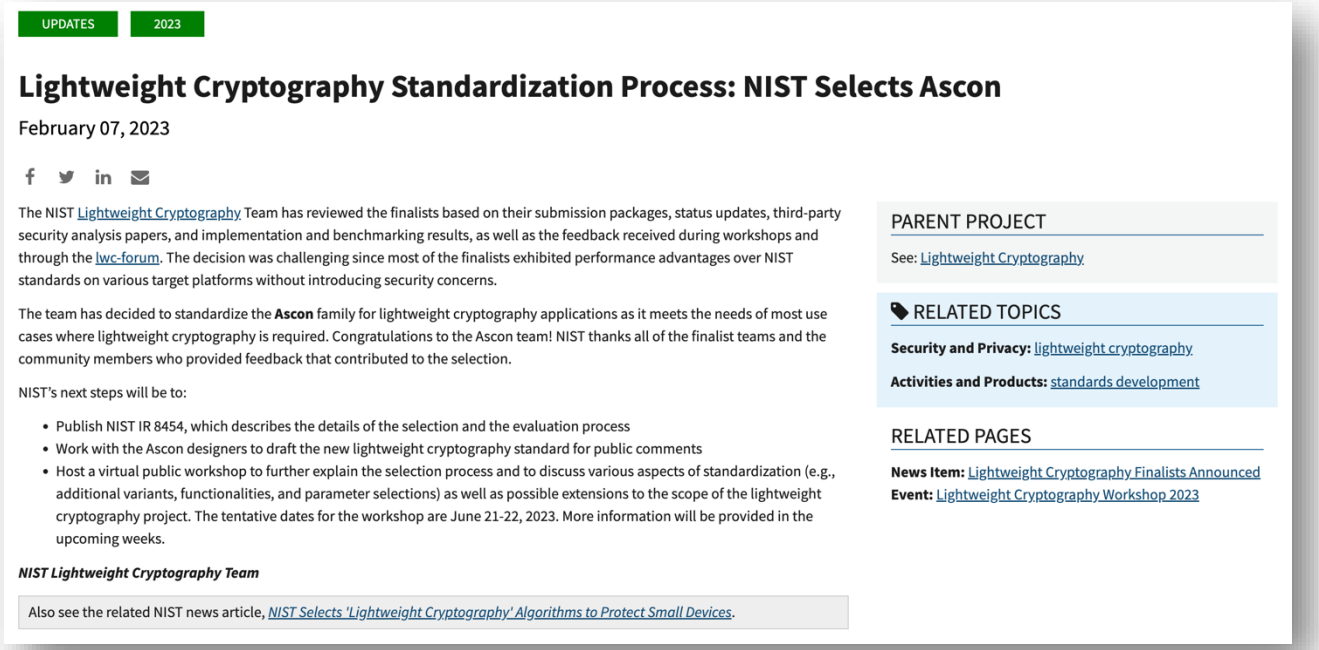
NIST軽量暗号としてASCONを選定

開始から
91ヶ月！

NISTは2023年2月に「ASCON」を勝者として選定とアナウンス！

気になるASCON選定理由！

- 豊富な実績
  - 2014年の設計以来、
    第三者評価実績多数
  - CAESEARコンペでの実績
  - アルゴリズム設計の安定性
- 高パフォーマンス
  - NIST標準よりSW/HWで高性能
- SCA耐性 / 対策の実装が容易
- 追加機能のサポート
  - XOFやMACなど高い汎用性



UPDATES 2023

Lightweight Cryptography Standardization Process: NIST Selects Ascon

February 07, 2023

The NIST Lightweight Cryptography Team has reviewed the finalists based on their submission packages, status updates, third-party security analysis papers, and implementation and benchmarking results, as well as the feedback received during workshops and through the lwc-forum. The decision was challenging since most of the finalists exhibited performance advantages over NIST standards on various target platforms without introducing security concerns.

The team has decided to standardize the **Ascon** family for lightweight cryptography applications as it meets the needs of most use cases where lightweight cryptography is required. Congratulations to the Ascon team! NIST thanks all of the finalist teams and the community members who provided feedback that contributed to the selection.

NIST's next steps will be to:

- Publish NIST IR 8454, which describes the details of the selection and the evaluation process
- Work with the Ascon designers to draft the new lightweight cryptography standard for public comments
- Host a virtual public workshop to further explain the selection process and to discuss various aspects of standardization (e.g., additional variants, functionalities, and parameter selections) as well as possible extensions to the scope of the lightweight cryptography project. The tentative dates for the workshop are June 21-22, 2023. More information will be provided in the upcoming weeks.

NIST Lightweight Cryptography Team

Also see the related NIST news article, *NIST Selects 'Lightweight Cryptography' Algorithms to Protect Small Devices*.

PARENT PROJECT

See: Lightweight Cryptography

RELATED TOPICS

Security and Privacy: lightweight cryptography

Activities and Products: standards development

RELATED PAGES

News Item: Lightweight Cryptography Finalists Announced

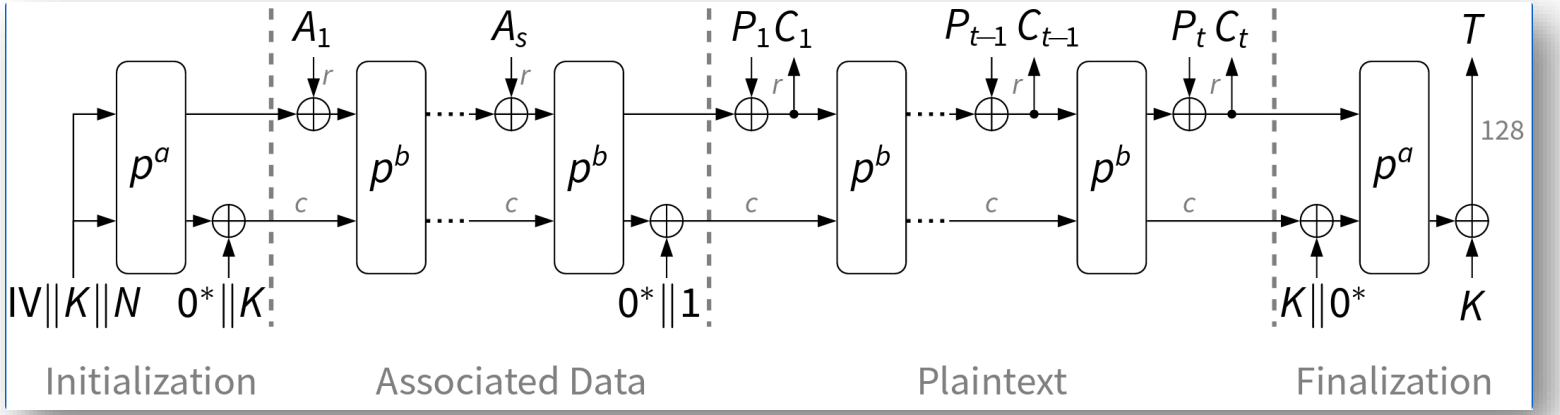
Event: Lightweight Cryptography Workshop 2023

https://csrc.nist.gov/news/2023/lightweight-cryptography-nist-selects-ascon

軽量暗号ASCONのご紹介（1/2）

- 主な機能
  - AEAD および Hash (固定 / 可変出力長)
- ASCON Permutation
  - 320bitの置換を異なる定数とラウンド数でインスタンス化
- AEAD：鍵による初期化/終期化を行うMonkeyDuplexモード
- Hash：スポンジ構造

https://ascon.iaik.tugraz.at/specification.html



ASCONでのAEAD（MonkeyDuplexモード）

軽量暗号ASCONのご紹介（2/2）

ASCONの品揃えと現状判明している標準化方針（暫定）および追加検討事項

- AEADとしてASCON-128 or 128a もしくは両方
  - ASCON-80pqは標準化対象としない
- ハッシュ関数ではなくXOFを標準化の対象として選択
- 追加検討として追加機能（PRF、MAC、KDFなど）や より短いTag（64/96bit）等

	品揃え	パラメータ
AEAD	ASCON-128	128-bit key/nonce/tag
	ASCON-128a	128-bit key/nonce/tag
	ASCON-80pq	160-bit key/128-bit nonce/tag
ハッシュ関数	ASCON-Hash	256 bit 出力
	ASCON-Hasha	256 bit 出力
拡張出力関数（XOF）	ASCON-XOF	任意の出力
	ASCON-XOFa	任意の出力

NIST 軽量暗号コンペティション

初期段階 → 投稿募集 → Round 1 → Round 2 → Final Round

Lightweight Cryptography Workshop 2023

NIST hosted the Sixth Lightweight Cryptography Workshop (virtual) on June 21-22, 2023 to explain the selection process and to discuss various aspects of lightweight cryptography standardization.

Agenda

Call for Papers

On-Demand Videos - June 21, 2023 (Day 1)

- Opening Remarks / Evaluation of the Finalists and the Selection of Ascon
- SCA Evaluation and Benchmarking of Finalists in the NIST Lightweight Cryptography Standardization Process
- ***Invited talk***: The Ascon Family: Lightweight Authenticated Encryption, Hashing, and More
- Hardware Implementation of ASCON
- FPGA Implementations of Message Authentication Codes based on Ascon-p
- A New Leakage Exploitation Framework and Its Application to Authenticated Encryption
- Efficient Second-Order Masked Software Implementations of Ascon in Theory and Practice
- Root-cause Analysis of the Side Channel Leakage from ASCON implementations
- Quantum Implementation of ASCON Linear Layer (was not presented)

On-Demand Videos - June 22, 2023 (Day 2)

- ***Invited talk***: Security of Permutation-Based Modes and its Application to Ascon
- Exact Security Analysis of ASCON
- Differential-Linear Cryptanalysis of ASCON: Theory vs. Practice
- A Closer Look at the S-box: Deeper Analysis of Round-Reduced ASCON-HASH
- Cryptanalysis of Ascon – An Information Theoretic Perspective – A Position Paper
- Lightweight Usable Cryptography - A usability evaluation of the Ascon 1.2 family
- Efficient Implementation of Permutation-Based Hash Functions for the RISC-V Architecture
- Proposals for Standardization of the Ascon Family
- Additional modes for Ascon
- Open Discussion

- ASCONを選定後に第6回 軽量暗号ワークショップ（2023年6月21日～22日）を開催

- ワークショップのサマリー
  - 選定プロセスの解説や標準化について様々な角度から講演を実施

https://csrc.nist.gov/events/2023/lightweight-cryptography-workshop-2023

軽量暗号

X

標準化動向

軽量暗号ASCONの標準化動向（NIST）

- 現在、ASCONに関する標準仕様は公開されていない状況
  - 当初の予定では「**2023年後半に公開予定**」とあるので難航していると予想

- 気になる文書形式は？
  - 現在の暫定的な決定として、**FIPSではなくSpecial Publication (SP) シリーズ**として公開予定
  - CNSA 2.0では ASCONは選択されない方針で想定されている（FAQ参照）

https://media.defense.gov/2022/Sep/07/2003071836/-1/-1/0/CSI_CNSA_2.0_FAQ_.PDF

正式な仕様を待つのみ…

Q: Will NSA be adopting the standards from NIST's Lightweight Cryptography effort?

A: NSA does not intend to add the ciphers resulting from NIST's Lightweight Cryptography effort to CNSA. The Lightweight Cryptography effort resulted in the selection of symmetric primitives based on the Ascon family. Their targeted security is substantially less than AES-256, rendering them generally unsuitable for NSS use cases. If CNSA 2.0 algorithms do not meet mission system performance requirements, early consultation with NSA is required.

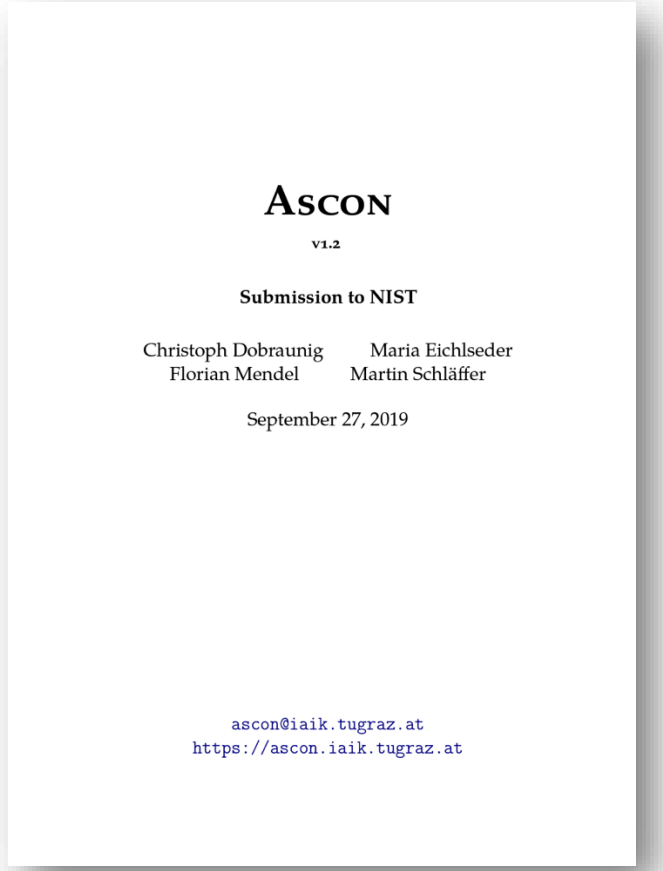
CNSA Suite 2.0 and Quantum Computing FAQ

軽量暗号ASCONの実装状況

正式な標準仕様が公開されていないが実装はチラホラ

- ASCONチームによって収集されている実装情報
  - リファレンス実装を含む情報が整理
    - https://github.com/ascon/ascon_collection
  - こちらのWebサイトの方が情報が充実 ☺
    - https://ascon.iaik.tugraz.at/implementations.html

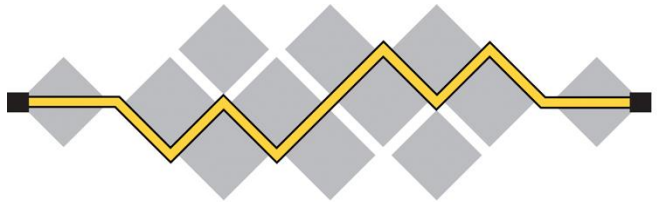
暗号ライブラリやIP coreなど製品は存在


ASCON
v1.2
Submission to NIST
Christoph Dobraunig Maria Eichlseder
Florian Mendel Martin Schläffer
September 27, 2019
ascon@iaik.tugraz.at
https://ascon.iaik.tugraz.at

ASCON v1.2準拠となっており
「正式な仕様で**仕様変更される可能性あり**」という事実に要注意！

https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ascon-spec-round2.pdf

軽量暗号ASCONの標準化動向（IETF）

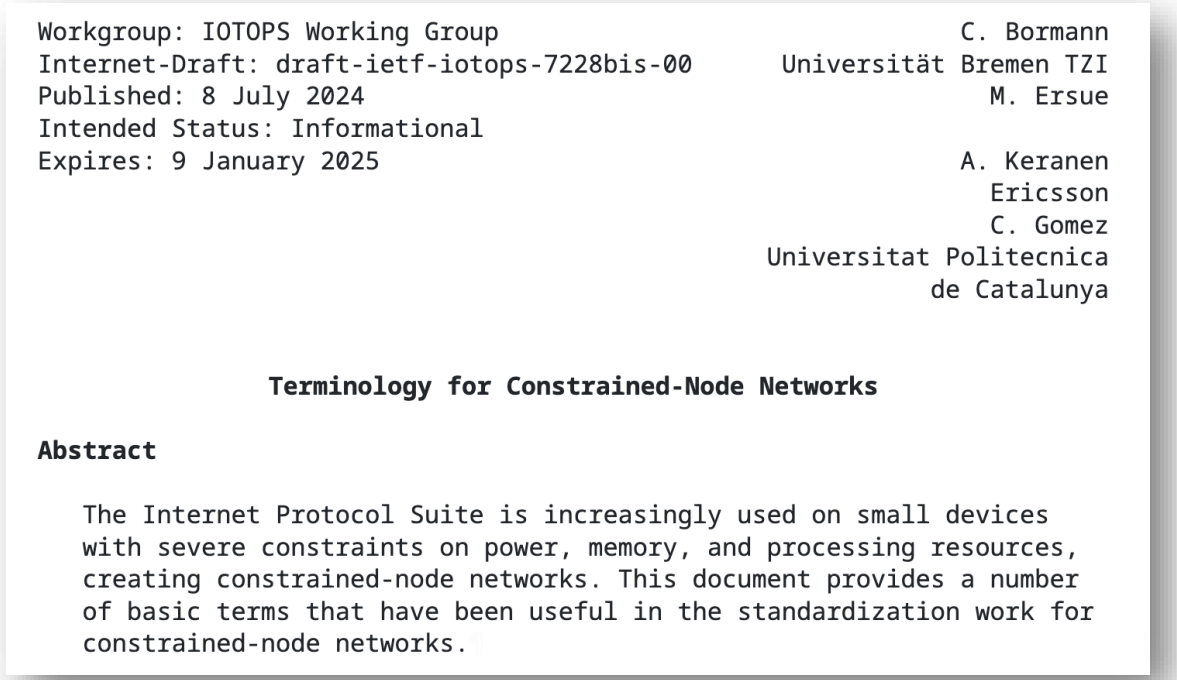


- IETFにおけるASCONに関する検討状況を整理
  - ASCON に関するInternet DraftやRFCは存在せず

- ASCONに関連する技術動向や議論されていたトピックス
  - Properties of AEAD Algorithms (Internet-Draft)
    - 発展著しいAEADに関するプロパティを整理
    - https://datatracker.ietf.org/doc/draft-irtf-cfrg-aead-properties/
  - Secure UAS Network RID and C2 Transport
    - Uncrewed Aircraft System (UAS) Network Remote ID通信規格
    - https://datatracker.ietf.org/doc/draft-moskowitz-drip-secure-nrid-c2/
  - COSE Hash Envelope
    - シグナリング用の新しいCOSEヘッダーパラメータ定義
    - https://datatracker.ietf.org/doc/draft-ietf-cose-hash-envelope/
  - SCA耐性のあるASCONを用いたEd25519 variant に関する議論 など

※ IETF （Internet Engineering Task Force）インターネットに関する技術の国際標準を策定する組織

IETF IOTOPS WGでのInternet Draft (1/2)



Workgroup: IOTOPS Working Group
Internet-Draft: draft-ietf-iotops-7228bis-00
Published: 8 July 2024
Intended Status: Informational
Expires: 9 January 2025

C. Bormann
Universität Bremen TZI
M. Ersue

A. Keranen
Ericsson
C. Gomez
Universitat Politecnica
de Catalunya

Terminology for Constrained-Node Networks

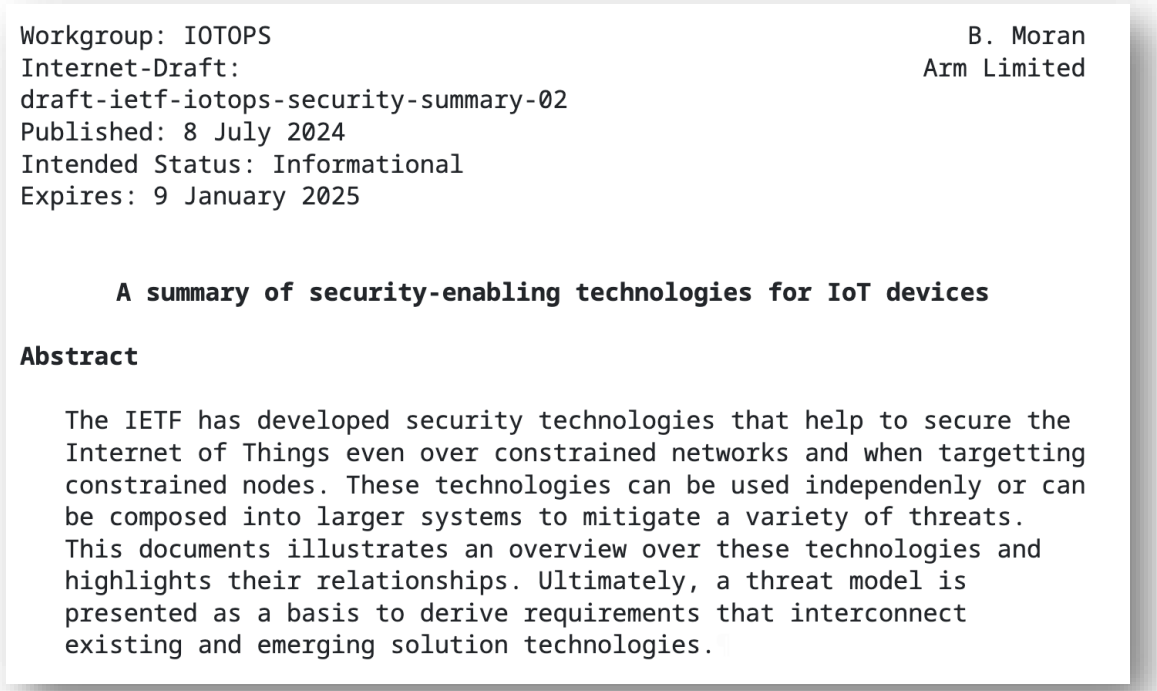
Abstract

The Internet Protocol Suite is increasingly used on small devices with severe constraints on power, memory, and processing resources, creating constrained-node networks. This document provides a number of basic terms that have been useful in the standardization work for constrained-node networks.

https://datatracker.ietf.org/doc/draft-ietf-iotops-7228bis/

- 概要
  - 電力、メモリ、および処理リソースに厳しい制約がある小型機器使用され、制約ノードネットワークの標準化作業で有用であった基本的な用語を整理する目的
- ポイント
  - 2014年5月に発行されたRFC7228を振り返り実用的な点を更新
    - 機器のクラス分類を拡張
      - 19段階で細かに表現
    - 電力関連の詳細化
    - ネットワーククラス分類 など

IETF IOTOPS WGでのInternet Draft (2/2)



Workgroup: IOTOPS
Internet-Draft:
draft-ietf-iotops-security-summary-02
Published: 8 July 2024
Intended Status: Informational
Expires: 9 January 2025

B. Moran
Arm Limited

A summary of security-enabling technologies for IoT devices

Abstract

The IETF has developed security technologies that help to secure the Internet of Things even over constrained networks and when targetting constrained nodes. These technologies can be used independenly or can be composed into larger systems to mitigate a variety of threats. This documents illustrates an overview over these technologies and highlights their relationships. Ultimately, a threat model is presented as a basis to derive requirements that interconnect existing and emerging solution technologies.

https://datatracker.ietf.org/doc/draft-ietf-iotops-security-summary/

- 概要
  - IETFによるセキュリティ技術が、制約のあるネットワークやデバイスを保護するためにどのように役立つかを説明
- ポイント
  - IoT機器/ネットワークで利用可能な技術を整理
  - IoT設計者のモヤモヤを解決するのに役立つ知見を発見できる（？）
  - 脅威モデルなども示されている など

軽量暗号ASCONの標準化動向（IEEE）

- IEEE 802.15.4 **LR-WPAN** (Low Rate Personal Area Network /低速無線個人エリアネットワーク) という規格が存在
  - バッテリー駆動なデバイス間における短距離通信を実現するための規格

2024年7月末にIEEE 802.15.4ae “**Ascon cryptographic algorithms**” という提案が行われた！

- 提案時の訴求ポイント
  - 802.15.4 はAES-CCMを想定しているが、さらに効率的である点
    - ASCON-128 or 128a のどちらかを想定
  - ハードウェア実装においてAESよりフットプリントが小さい
  - NIST軽量暗号コンペでの実績および複数の実装が存在

今後、想定される
軽量暗号ASCON

- 現行暗号技術では搭載が困難な機器や応用の登場が見込める！
- リソースの制約のあるIoT機器と言えば、センサーや通信デバイスを駆動させるための「電力供給」が課題
  - 無電源で駆動するIoT機器 ⇨ **環境発電 / エナジーハーベスティング**
- 環境発電 / エナジーハーベスティングの代表例
  - 太陽光や室内光（照明）、振動、廃熱、体温、電磁波等のエネルギー変換
  - 電力量は μW～mWオーダーと**極端に小さい**…

打開策として「軽量暗号」への期待が高まる

CRYPTREC 外部評価報告書

- ASCONを含む軽量暗号に関する情報が盛りだくさん！

2023年度暗号技術関連の調査報告

年度	報告書名	著者名	報告書文書番号
2023	軽量暗号Asconの実装性能に関する調査及び評価	崎山 一男	CRYPTREC-EX-3301-2023
2023	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	CRYPTREC-EX-3302-2023

2021年度暗号技術関連の調査報告

年度	報告書名	著者名	報告書文書番号
2021	「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	伊藤 竜馬	CRYPTREC EX-3101-2021
2021	ディジタル署名アルゴリズム EdDSAの実装性能調査	株式会社インフォーズ	CRYPTREC EX-3102-2021

2022年度暗号技術関連の調査報告

年度	報告書名	著者名	報告書文書番号
2022	軽量暗号の安全性に関する調査及び評価（Photon-Beetle,Sparkle,Tsudik's keymode）	岩田 哲	CRYPTREC EX-3201-2022
2022	軽量暗号の安全性に関する調査及び評価（GIFT-COFB,Xoodyak）	内藤 祐介	CRYPTREC EX-3202-2022
2022	軽量暗号の安全性に関する調査及び評価（Ascon,Grain-128AEAD,TinyJambu）	藤堂 洋介	CRYPTREC EX-3203-2022
2022	軽量暗号の安全性に関する調査及び評価（Elephant,ISAP,Romulus）	井上 明子	CRYPTREC EX-3204-2022
2022	軽量暗号の実装性能に関する調査及び評価（NIST軽量暗号コンペティションファイナリスト）	崎山 一男	CRYPTREC EX-3205-2022
2022	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）	GMOサイバーセキュリティ byイエラエ株式会社	CRYPTREC EX-3206-2022

https://www.cryptrec.go.jp/ex_reports.html

まとめ

- 軽量暗号と標準化動向というテーマとして、NIST軽量暗号コンペティションに注目しASCONに注目しお話しさせていただきました。
- 標準化動向として、NIST、IETFやIEEEでの話題に注目してポイントをお話しさせていただきました。
  - 所感として、NISTの正式な標準仕様が未公開な点が起因してゆっくりとした世の中への広がりとなっています
  - 一方で軽量暗号への興味や応用例は多いので今後が楽しみです！

何か気になることなどあれば～

- E-mail
  - satoru.kanno@gmo-cybersecurity.com
  - kanno@satokan.tech
- SNS
  - X (旧Twitter)
    - https://twitter.com/satorukanno
  - Facebook
    - https://www.facebook.com/satoru.kanno

お気軽にご連絡ください！

すべての人にインターネット