CRYPTREC
Cryptography Research and Evaluation Committees

軽量暗号ガイドライン紹介

暗号技術評価委員会
軽量暗号WG主査
（東北大学 教授）
本間 尚文

軽量暗号WG　委員構成

CRYPTREC
Cryptography Research and Evaluation Committees

主査	本間　尚文	東北大学
委員	青木　和麻呂	日本電信電話株式会社
委員	岩田　哲	名古屋大学
委員	小川　一人	日本放送協会
委員	小熊　寿	株式会社トヨタIT開発センター
委員	崎山　一男	電気通信大学
委員	渋谷　香士	ソニーグローバルマニュファクチャリング＆オペレーションズ株式会社
委員	鈴木　大輔	三菱電機株式会社
委員	成吉　雄一郎	ルネサスエレクトロニクス株式会社
委員	峯松　一彦	日本電気株式会社
委員	三宅　秀享	株式会社東芝
委員	渡辺　大	株式会社日立製作所

軽量暗号WG（2013～2017）

CRYPTREC
Cryptography Research and Evaluation Committees

- 活動目的
  - 軽量暗号WGは，軽量暗号技術が求められるサービスにおいて，電子政府のみならず利用者が適切な暗号方式を選択でき，容易に調達できることをめざして設置された

- 活動概要
  - 軽量暗号技術に関する検討
  - 軽量暗号技術に関する現状調査（サーベイ）
  - アプリケーションに関する調査
  - 実装評価
  - 今後の活動方針に関する議論（→ガイドライン発行）

CRYPTREC暗号技術ガイドライン（軽量暗号）の作成目的

CRYPTREC
Cryptography Research and Evaluation Committees

- 作成目的
  - IoT等の次世代ネットワークサービスにおいて軽量暗号の活用が期待されることから，方式を選択・利用する際の技術的判断に資すること，今後の利用促進をはかることを目的として，当該暗号技術のガイドラインを作成
- 想定する読者
  - システム設計時に暗号技術の選択・利用の判断に関わるセキュリティや暗号の技術者

CRYPTREC暗号技術ガイドライン（軽量暗号）

- 2017年6月発行（日本語版・英語版）

CRYPTREC Webサイト（http://www.cryptrec.go.jp）からダウンロード可能

ガイドラインの目次(1/2)

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドラインの目次(2/2)

CRYPTREC
Cryptography Research and Evaluation Committees

ガイドラインに記載したアルゴリズム

CRYPTREC
Cryptography Research and Evaluation Committees

- 第4章に代表的な軽量暗号アルゴリズムを技術分野ごとに記載（2016年7月時点で決定）

- 選択基準
  - IACR(国際暗号学会)等の主要国際会議で発表されている
  - 国際標準となっている　または　検討中
  - 有力な攻撃法が発見されていない
  - その他，技術分野ごとに検討

記載されたアルゴリズム

CRYPTREC
Cryptography Research and Evaluation Committees

- ブロック暗号

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
LED	CHES 2011
Piccolo	CHES 2011
TWINE	SAC 2012
PRINCE	Asiacrypt 2012
Midori	Asiacrypt 2015
PRESENT	CHES 2007, ISO/IEC 29192-2
CLEFIA	FSE 2007, ISO/IEC 29192-2
SIMON	Cryptology ePrint Archive (Report 2013/404)
SPECK	Cryptology ePrint Archive (Report 2013/404)

✓ 主要国際会議で近年発表されており、現段階で有力な攻撃法が発見されておらず、かつ十分な実装性能をもつものを選択.
✓ 軽量暗号国際標準 ISO/IEC 29192-2 記載 または 検討中のものを選択.

記載されたアルゴリズム

CRYPTREC
Cryptography Research and Evaluation Committees

- ストリーム暗号

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
Grain v1/-128A	eStream portfolio, ISO/IEC 29167-13
MICKEY 2.0	eStream portfolio
Trivium	eStream portfolio, ISO/IEC 29192-3
Enocoro	ISO/IEC 29192-3
ChaCha20	RFC 7539

✓ 安全性評価が十分に行われたと考えられられる eStream portfolio 選定暗号 および ISO/IEC 標準から選択.
✓ 2015年にRFC化されたChaCha20も選択.

記載されたアルゴリズム

CRYPTREC
Cryptography Research and Evaluation Committees

- ハッシュ関数

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
PHOTON	CRYPTO 2011, ISO/IEC 29192-5
SPONGENT	CHES 2011, ISO/IEC 29192-5
QUARK	CHES 2010
KECCAK	SHA-3 competition, FIPS 202

- メッセージ認証コード

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
SipHash	Indocrypt 2012, DIAC

✓ MACは軽量ブロック暗号をCMACで使うか軽量ハッシュ関数をHMACで使うのが一般的であろうと考えられる.
✓ SipHashは短いメッセージに対しても高速なMACであり、Python, Rubyの連想配列用ハッシュ関数として利用されており、今後用途が広がる可能性あり.

記載されたアルゴリズム

CRYPTREC
Cryptography Research and Evaluation Committees

- 認証暗号

アルゴリズム名	発表された国際会議, 採録/提案されている標準等
ACORN	DIAC 2014, DIAC 2015
Ascon	DIAC 2014, DIAC 2015, CT-RSA 2015(analysis)
AES-JAMBU	DIAC 2014, DIAC 2015
AES-OTR	EUROCRYPT 2014, DIAC 2015
CLOC and SILC	FSE 2014 (CLOC), DIAC 2014 (SILC), DIAC 2015
Deoxys	Asiacrypt 2014 (TWEAKEY), DIAC 2014, DIAC 2015
Joltik	Asiacrypt 2014 (TWEAKEY), DIAC 2014, DIAC 2015
Ketje	DIAC 2014, (SHA3)
Minalpher	DIAC 2014, IEEE GCCE 2015(Hw)
OCB	ACM CCS 2001, Asiacrypt 2004, FSE 2011
PRIMATES	FSE 2014 (APE), Asiacrypt 2014 (RUP,bound), DIAC 2014, DIAC 2015

実装詳細評価方針(1/3)

CRYPTREC
Cryptography Research and Evaluation Committees

- 実装詳細評価の目的
  - 複数の軽量暗号アルゴリズム及び比較対象となる代表的な既存暗号技術を、同一プラットフォーム上で、統一的な実装ポリシーにより実装し、統一的な評価環境で比較を行う

実装詳細評価方針(2/3)

CRYPTREC
Cryptography Research and Evaluation Committees

- ハードウェア実装評価
  - 標準的なCMOSセルライブラリ：NANGATE Open Cell Library (45nm CMOS)
  - アーキテクチャ：①各アルゴリズムの仕様に準じた標準的な実装,②処理速度を優先する実装,③回路規模を優先する実装
  - 測定指標：最大動作周波数、処理速度、ゲートカウント、回路遅延、消費電力、ピーク電流
- ソフトウェア実装評価
  - プロセッサ：ルネサスエレクトロニクス組み込みマイコン
  - 測定指標：処理速度、メモリサイズ(ROM, RAM)

実装詳細評価方針(3/3)

CRYPTREC
Cryptography Research and Evaluation Committees

- 実装形態とアルゴリズム
  - 軽量ブロック暗号
    - 第4章のアルゴリズム
    - HW実装, SW実装
  - 軽量認証暗号
    - 第4章のアルゴリズムから選択
    - SW実装

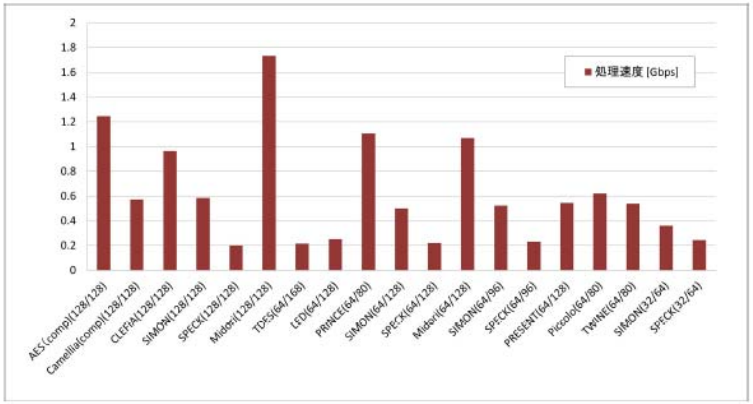
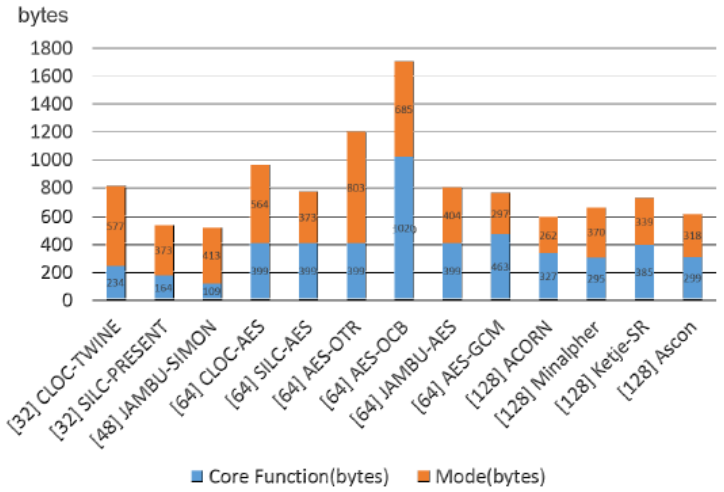


図 3.15　Enc/Dec,Round 実装の処理速度



軽量暗号の優位性

CRYPTREC
Cryptography Research and Evaluation Committees

回路規模	・ 軽量暗号とAESの差(数kgate)は，50μm角クラスの小さなチップや180nmなど古いプロセスではcriticalで，暗号機能の搭載可否に影響を与えうる
消費電力量	・ 回路規模が小さいほど消費電力(量)は小さくなる傾向．軽量暗号により消費電力(量)に関する設計条件を緩和できる効果が期待できる
レイテンシ	・ AESの2倍の応答速度をおよそ1/10の回路規模で実現できる軽量暗号が存在（20kgateで10ns以下での演算が可能）．産業向けI/Oデバイス制御などμsオーダーのリアルタイム性が求められる用途で活用可能
メモリサイズ	・ AESのおよそ1/4のROMサイズで実装可能な軽量暗号が存在．軽量暗号なら追加できるケースやチップ単価を下げられるケースあり

軽量暗号の留意点

CRYPTREC
Cryptography Research and Evaluation Committees

- 軽量暗号で達成可能な安全性
  - 軽量暗号は特定の性能指標で優位性をもつように設計されており，従来の暗号技術より安全性が低くなる傾向にある
    - 例えば、64ビットブロック暗号を用いて同じ鍵で2^32ブロック以上暗号化した場合、現実的な脅威になりうることがACM CCS2016で発表された。
    - CRYPTRECでも64ビットブロック暗号利用時の安全な利用方法（同じ鍵での暗号化上限回数）について指針を示す予定
  - 電子政府推奨暗号でもリスクなしの運用は困難であり，軽量暗号でも利用に応じたリスクを考慮しながらの運用が必要

まとめ

CRYPTREC
Cryptography Research and Evaluation Committees

- 軽量暗号の適切な利用を支援するため「CRYPTREC暗号技術ガイドライン(軽量暗号)」が発行された
  - CRYPTREC Webサイトで公開中

- 同ガイドラインにより，軽量暗号に対する正しい理解が広まり，必要とされる応用において活用が促進されることを期待したい