CRYPTREC
Cryptography Research and Evaluation Committees

暗号技術調査WG(軽量暗号)
活動報告

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	国立大学法人東北大学
委員	青木　和麻呂	日本電信電話株式会社
委員	岩田　哲	国立大学法人名古屋大学
委員	小川　一人	NHK放送技術研究所
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	国立大学法人電気通信大学
委員	渋谷　香士	ソニー株式会社
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

2015年度 軽量暗号WG 活動内容

CRYPTREC
Cryptography Research and Evaluation Committees

- 「暗号技術ガイドライン(軽量暗号)」の作成に向けた検討
  - ガイドラインの作成方針の決定
  - ガイドラインに記載する軽量暗号アルゴリズムの選択
  - 実装詳細評価の方針決定
  - 軽量暗号WG活動の対外的アピールのあり方に関する検討

軽量暗号ガイドラインの作成目的

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、暗号技術ガイドラインを作成する。
- 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

軽量暗号ガイドラインの目次案(1/2)

CRYPTREC Cryptography Research and Evaluation Committees

I. はじめに

II. 軽量暗号の活用例

1. 軽量暗号とは
2. 軽量暗号はどこに使えるか？
3. どんな軽量暗号、パラメータを選べばいいか？
4. 軽量暗号を使う時の留意点
5. ユースケースごとの軽量暗号活用例と効果

軽量暗号ガイドラインの目次案(2/2)

CRYPTREC Cryptography Research and Evaluation Committees

III. 軽量暗号の性能比較

1. ハードウェア実装
   回路規模/消費電力量/レイテンシで比較
2. ソフトウェア実装
   必要メモリサイズで比較

IV. 代表的な軽量暗号

1. ブロック暗号
2. ストリーム暗号
3. ハッシュ関数
4. メッセージ認証コード
5. 認証暗号

ガイドラインに記載するアルゴリズム

CRYPTREC Cryptography Research and Evaluation Committees

- IV章に代表的な軽量暗号アルゴリズムを、ブロック暗号、ストリーム暗号、ハッシュ関数、メッセージ認証コード、認証暗号の技術分野ごとに記載

- 選択基準
  - IACR(国際暗号学会)主催の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
  - 破られていない
  - その他、技術分野ごとに検討

IV章に記載するアルゴリズム(案)

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.

IV章に記載するアルゴリズム(案)

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.

IV章に記載するアルゴリズム(案)

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.

IV章に記載するアルゴリズム(案)

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
SCREAM	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

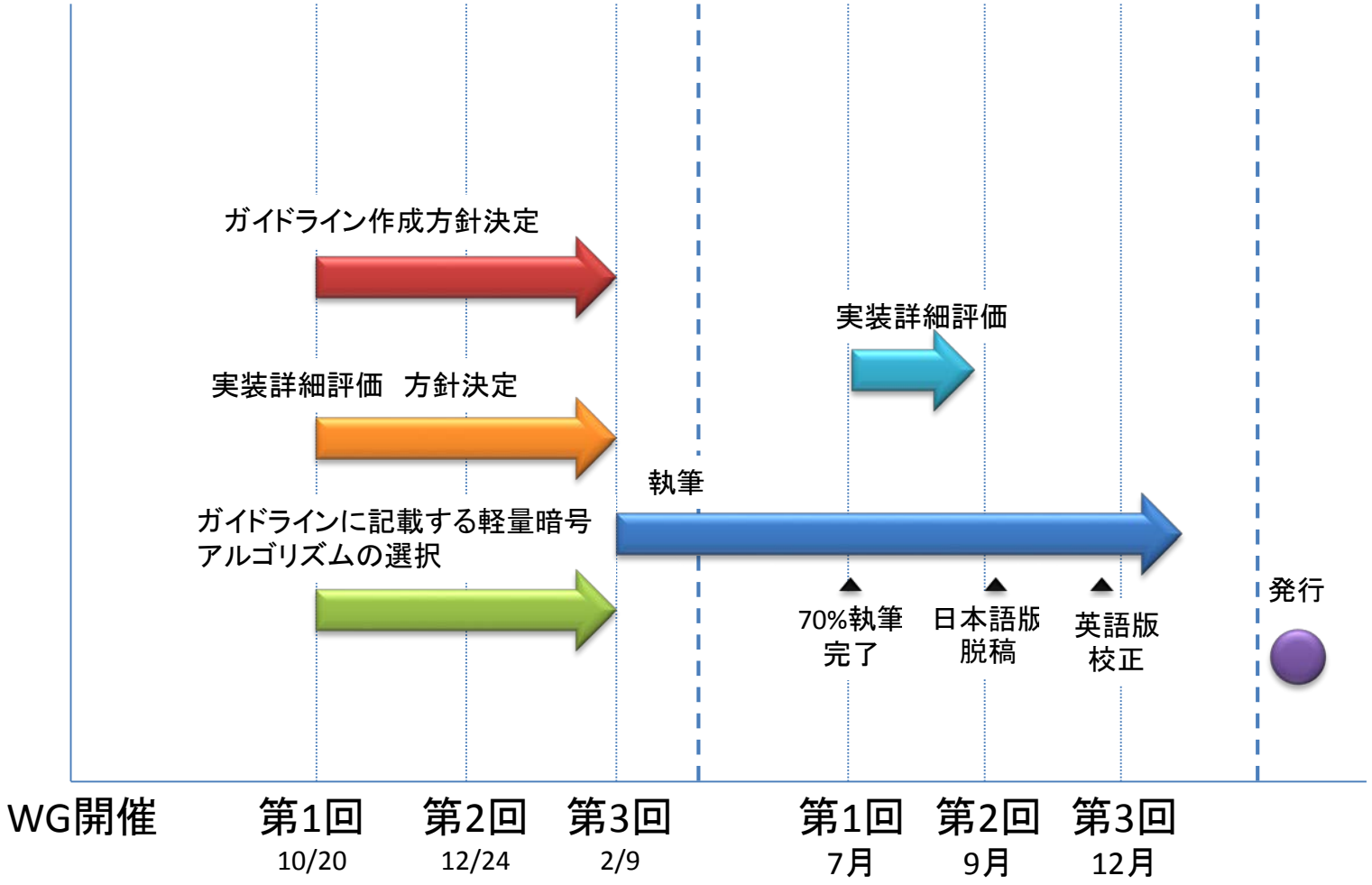
- ハードウェア実装評価
  - 標準的なCMOSセルライブラリ：NANGATE Open Cell Library (45nm CMOS)
  - アーキテクチャ：①各アルゴリズムの仕様に準じた標準的な実装,②処理速度を優先する実装,③回路規模を優先する実装
  - 測定指標：最大動作周波数、処理速度、ゲートカウント、回路遅延、消費電力、ピーク電流
- ソフトウェア実装評価
  - プロセッサ：ルネサスエレクトロニクス組み込みマイコン
  - 測定指標：処理速度、メモリサイズ(ROM, RAM)

実装詳細評価方針(3/3)

CRYPTREC
Cryptography Research and Evaluation Committees

- 実装対象分野およびアルゴリズム
  - 軽量認証暗号
    - P. 11記載のアルゴリズムから選択
    - ソフトウェア実装のみ
  - 軽量ブロック暗号
    - P.8記載のアルゴリズム
    - ハードウェア実装, ソフトウェア実装

ガイドライン作成スケジュール



軽量暗号WG活動の対外的アピール

CRYPTREC Cryptography Research and Evaluation Committees

- 「暗号技術調査WG(軽量暗号)報告書」の発行
  - 2013・2014年度の調査結果を報告 (134ページ)
  - CRYPTREC Report 2014内
- CRYPTREC軽量暗号WGの活動紹介
  - NIST Lightweight Cryptography Workshop 2015
  - IoTセキュリティフォーラム
- 「暗号技術ガイドライン(軽量暗号)」の発行
  - 日本語版・英語版を2017年度に発行