（26-4）

平成26年度「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発」の研究開発目標・成果と今後の研究計画
副題　プライバシ保護とセキュリティレベル切替えが可能なセキュアRFIDタグの実現

1. 実施機関・研究開発期間・研究開発予算

◆実施機関	株式会社サイバー創研（代表研究者）、国立大学法人電気通信大学、株式会社日立製作所
◆研究開発期間	平成24年度から平成26年度（3年間）
◆研究開発予算	総額183百万円（平成26年度　57百万円）

2. 研究開発の目標

「プライバシ保護とセキュリティレベルの切替え機構を実装した1チップパッシブRFIDタグ」の実装技術のフィジビリティを確認する。

3. 研究開発の成果

■背景

- ・任意のリーダでIDを取得可能であり、RFIDタグが貼付された物品の購入者の行動パターンや嗜好性などのプライバシが侵害される恐れ
- ・パッシブ型RFIDタグに対する暗号技術を活用したプライバシ保護に関する理論的な提案はあるが実装例なし

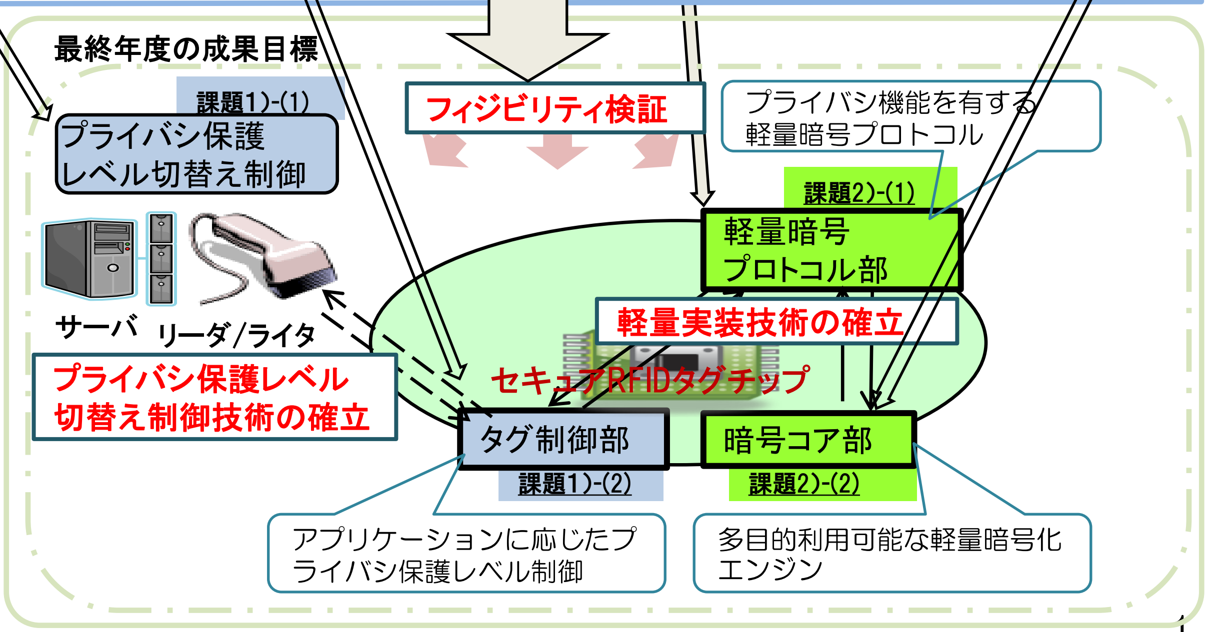
■狙い

- ・実現が極めて困難で世界でまだ実現例がなく、軽量暗号コアと軽量暗号プロトコルの実装によるプライバシ保護レベルの切替えが可能な、**1チップセキュアRFIDタグチップ**の機能の開発
- ・日本発の標準化推進に資する1チップ搭載技術に関するフィジビリティ検証

■成果

- ・プライバシ保護レベルを切替え利用可能なRFIDのフィジビリティを検証
- ・試作した1チップセキュアRFIDタグチップは、動作ピーク時の消費電力が約3.5mWであり、市販のリーダ/ライタからの給電で十分動作可能であることを検証

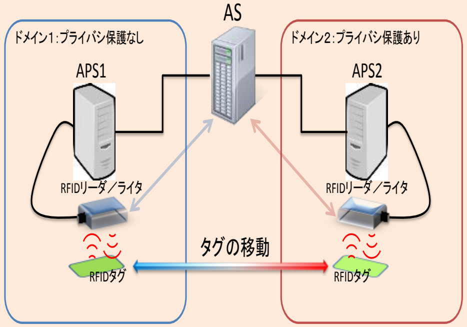
課　題	成　果
軽量暗号プロトコルの実装技術	軽量暗号プロトコルの選定、セキュリティパラメータの策定 デジタル回路の設計、RTLシミュレーションとFPGAを用いた基礎実験と機能検証
軽量暗号プロトコルの普及促進に資する機能の搭載技術	プライバシ保護機能を切替え可能とする制御方式、回路の設計、メモリ構成仕様と物理マッピングの策定、RF部アナログ回路、デジタル部を含めたレイアウトの設計とチップ作製、試作チップの性能および機能検証
暗号化方式の選定と実装技術	消費電力が最小な軽量ハッシュ関数SPONGENTを暗号プリミティブに選出し、チップ試作用の暗号コアを開発、暗号コアの制御やI/Oの機能を実現する回路を含めた省電力な実装アーキテクチャを考案
アプリケーションに応じたプライバシ保護レベルの制御技術	各ユースケースに適合する条件を明確化、電力評価によるフィジビリティ検証


最終年度の成果目標

課題1）アプリケーションを考慮した普及促進に資する技術

課題1）-(1)アプリケーションに応じたセキュリティレベルの制御技術

■認証サーバ構成による、プライバシ保護レベル切替えの実現



RFIDを活用したプライバシ保護を実現するアプリケーションにおいて、

- 利用者の移動範囲内（ドメイン）でプライバシ保護を実現・提供するためのアプリケーションサーバ（APS）と
- 新たな（別の）ドメインとのドメイン間移動を実現するための認証機能を一元的に管理する認証サーバ（AS）

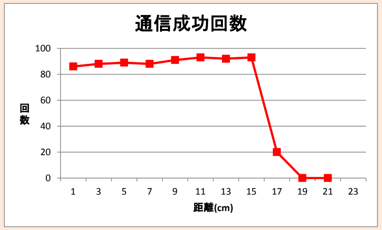
による二階層構成を提案

■プライバシ保護機能が有効な代表的な利用シーン並びに当該シーンでのRFIDに対する条件等の明確化

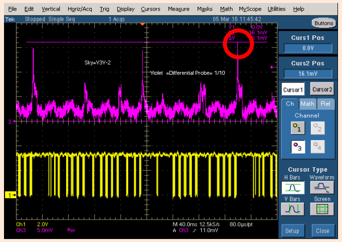
項　目		プライバシ保護が有効な利用シーン例		参　考
利用シーン		ブランド保証	家電のリコール	物　流　（倉庫）
保護の必要度		大	中	小
仕様条件	通常使用状況での RFID（物品）の移動	有	無	有
	RFID（物品）の移動速度	普通	ー	（比較的）速い
	R/W と RFID タグ間距離	短距離（～30cm）	短距離（～30cm）	中距離（～1m）
	R/W と RFID タグ間距離変動	（若干）有	無	有
	複数 RFID の同時混在	（若干）有	無	多数
	公共空間での保護レベル切替	有	有	無
	保護レベル切替許容時間	普通（～1 秒）	普通（～1 秒）	短時間（処理点数大、～10ms 程度）

R/W:リーダ/ライタ

■試作RFIDの利用する上での距離条件、電力条件の実証評価



距離測定例（100回実施）

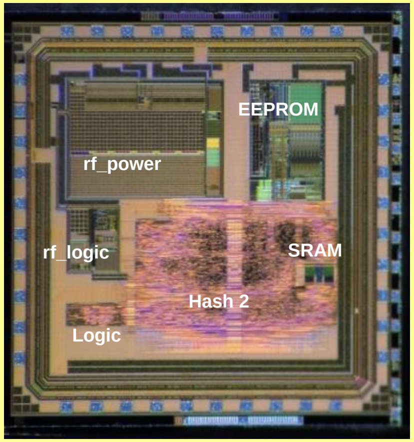


消費電力測定例

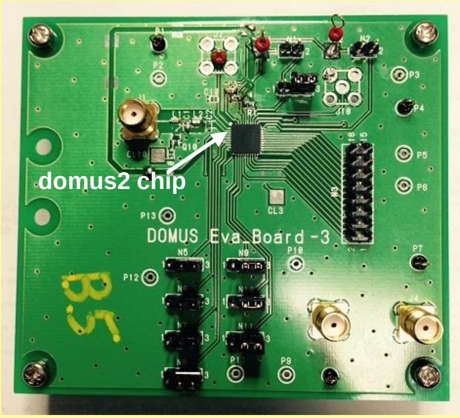
- 通信成功回数測定で約15cmでの動作を確認
- プライバシ保護レベル切替え機能を実装し動作を確認
- 電力を最も消費するのは、EEPROMであることを確認

課題1）-(2)セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術

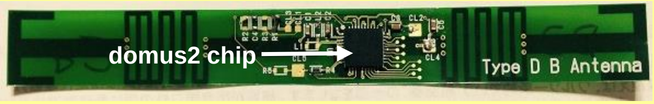
■プライバシ保護レベル切替えの制御方式と制御回路を設計　メモリの構成仕様とその物理マッピングを策定　RF部アナログ回路、デジタル部を含めたレイアウトの基本設計、詳細設計を完了し、RFIDチップを作製



H26年度（2回目）のRFID試作チップ

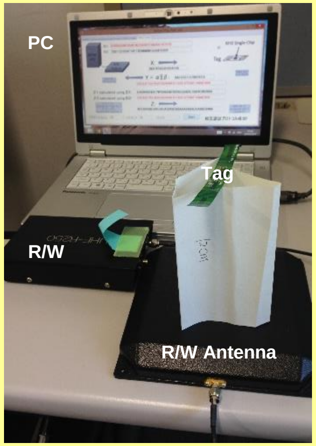


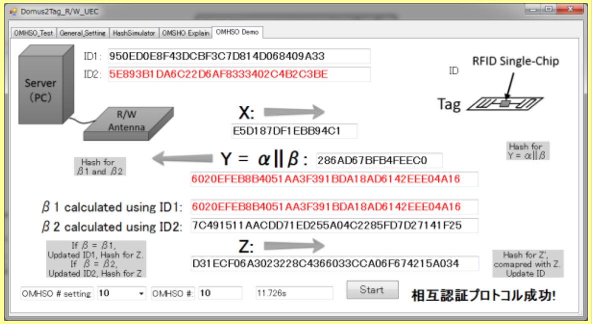
RFID試作チップ 評価ボード



RFID試作チップ
フレキシブルタグ

■アンテナと接続し、試作チップの性能および機能検証を実施　RF信号発生器と市販リーダ/ライタで正常動作を確認





ID1: 950ED0E8F43DCBF3C7D814D068409A33

ID2: 5E893B1DA6C22D6AF8333402C4B2C3BE

X: E5D187DF1EBB94C1

Y = α||β: 286AD67BFB4FEEC0

6020EFEB8B4051AA3F391BDA18AD6142EEE04A16

β1 calculated using ID1: 6020EFEB8B4051AA3F391BDA18AD6142EEE04A16

β2 calculated using ID2: 7C491511AACDD71ED255A04C2285FD7D27141F25

If β = β1, Updated ID1, Hash for Z. If β = β2, Updated ID2, Hash for Z

Z: D31ECF06A3023228C4366033CCA06F674215A034

OMHSO # setting: 10

OMHSO #: 10

11.726s

相互認証プロトコル成功!

市販リーダ/ライタを用いたデモのGUI

市販リーダ/ライタを用いたデモ環境

課題2） １チップ実装技術

課題2）-(1） 軽量暗号プロトコルの実装技術

■ OMHSOを軽量暗号プロトコルとして選定し、そのセキュリティパラメータを策定

Server: (ID_1,ID_2),　　Tag: ID

S1: Generate random number X

S2: Send X $\xrightarrow{X}$ T1: Generate random number α

T2: Computer $\beta \leftarrow H_0(ID||X||\alpha)$

S3: Compute $\xleftarrow{Y}$ T3: Send $Y \leftarrow \alpha||\beta$

Tag Authentication:
$\beta_1 \leftarrow H_0(ID_1||X||\alpha)$,
$\beta_2 \leftarrow H_0(ID_2||X||\alpha)$.
S4: If $\beta = \beta_1$
$Z \leftarrow H_1(ID_1||X||\alpha)$,
else if $\beta = \beta_2$
$Z \leftarrow H_1(ID_2||X||\alpha)$,
else
$Z \leftarrow random\ number$

S5: Send Z $\xrightarrow{Z}$ T4: Compute

$Z' \leftarrow H_1(ID||X||\alpha)$ Server Authentication

S6: If $\beta = \beta_1$

Server ID Updating:
$ID_{new} \leftarrow H_2(ID_1)$.
$ID_2 \leftarrow ID_1$,
$ID_1 \leftarrow ID_{new}$.

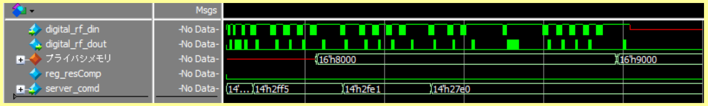
T5: if $Z = Z'$
$ID_{new} \leftarrow H_2(ID)$. Tag ID Updating

OMHSOプロトコルのシーケンス

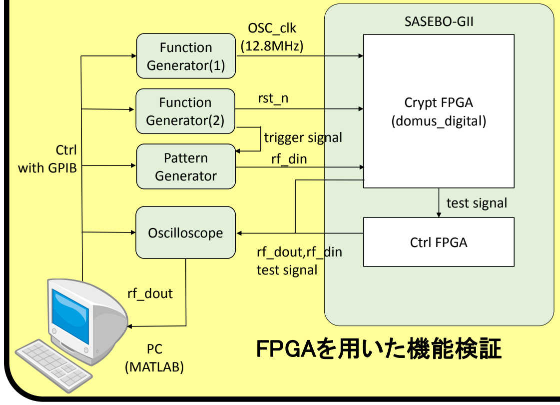
ID, ID₁, ID₂	128-bit
,β	64-bit
Z,Z’	160-bit
seed	80-bit

セキュリティ　パラメータ

■プロトコル部に対応するデジタル回路の基本設計を完了し、チップ試作前に、RTLシミュレーションとFPGAを用いた基礎実験と機能検証を実施



RTLシミュレーションを用いた機能検証



FPGAを用いた機能検証

	hash_sel = 0/1
デリミタ	800kHz,533kHz, 400kHz,320kHz
‘00’	-7.0% ~ 7.0%
‘01’	-9.4% ~ 4.7%
‘10’	-4.7% ~ 9.4%
‘11’	-9.4% ~ 4.7%

デジタル回路部のクロック周波数変動に対する許容範囲

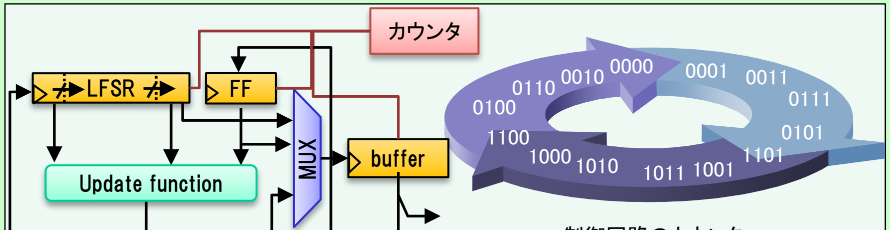
課題2)-(2） 暗号化方式の選定と実装技術

■ RFIDタグチップで利用可能な暗号コアを開発

- セキュリティ要件に合う暗号プリミティブをリストアップ
- 性能要件に合わせた実装アーキテクチャを決定
- 暗号プリミティブのハードウェア実装を行い、ハードウェア実装性能を評価
- 消費電力が最小な軽量ハッシュ関数SPONGENTをRFIDタグチップ向けの暗号プリミティブとして選出
- デジタル部の設計仕様に合う暗号コアを開発し、チップ試作用に暗号コアを提供

■ 暗号コア軽量実装技術に関する新たな知見を追加

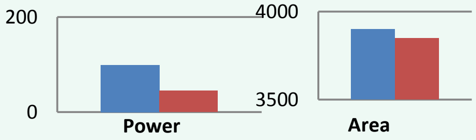
- 暗号コアのインタフェースの特徴を活用した実装アーキテクチャを考案し、ハードウェア実装と性能評価を実施
- 暗号コアの消費電力を削減可能な制御回路のカウンタを設計し、ハードウェア実装と性能評価を実施
- 暗号コアにハッシュ関数Keccakを用いる場合の、RFIDタグチップ全体の性能に対する影響を検証



実装アーキテクチャ

制御回路のカウンタ

制御回路のカウンタの構成方法による消費電力の削減効果の有効性を確認



ハードウェア実装性能

4. これまで得られた成果（特許出願や論文発表等）

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
軽量暗号プロトコルの省リソースデバイスに対する実装効率向上に関する研究開発	7 (5)	1 (1)	0 (0)	23 (10)	1 (1)	0 (0)	0 (0)

※成果数は累計件数、（ ）内は当該年度の件数です。

（1）報道発表

平成26年9月4日に「ID情報を秘匿したまま認証が可能なパッシブ型RFIDタグチップの試作に成功」と題して報道発表を行った。
その結果、日刊の全国紙を含む4種類の新聞で取り上げられた。また、インターネットの電子ニュースとしても多数が確認された。

（2）学会等での発表

IEEE INTERNATIONAL SYMPOSIUM ON ELECTROMAGNETIC COMPATIBILITYの国際シンポジウムでの“Software and Hardware Co-Verification for Privacy-Enhanced Passive UHF RFID Tag”と題する発表を含む23件の学会等の外部発表を行い、研究成果のアピール、技術普及への取組を実施した。今後、国際的なジャーナル等への投稿を計画しており、更なる学術的アピール、技術普及への取組を継続する予定である。

5. 研究開発成果の展開・普及等に向けた計画・展望

今後IoTの実用展開が盛んになると想定されるが、RFIDはIoT実現の有効なデバイスの一つとして捉えられており、また、その他のセンサ等も含めてプライバシ上の配慮が必要な情報を扱うことが多くなると考えられる。

プライバシに配慮したRFIDを利用するアプリケーションにおいては、複雑な暗号プロトコル処理をリーダ/ライタによる外部給電で動作させることが課題である。そこで本研究課題では、暗号プロトコルの軽量化を行い、さらにRFアナログ部と1チップ実装することで、低消費電力で動作するパッシブタグの実装技術を確立した。試作した1チップセキュアRFIDタグチップは、動作ピーク時の消費電力が約3.5mWであり、市販のリーダ/ライタからの給電で十分動作可能であることが検証できたことから、有効な技術であることが証明された。なお、プライバシ保護レベルは切替え可能であり、保護の必要のない状況では、既存のシステムと互換性を有しているため広範囲に適用可能である。

以上の結果、1チップセキュアRFIDタグの実現性が証明され、所期の目標は達成された。

1チップセキュアRFIDタグの実現性を更にアピールすると共に、本研究開発成果をNICTにおける自ら研究を含む今後の研究開発に資することができ、今後の軽量暗号プロトコルの実用化に向けての礎となることが期待できる。