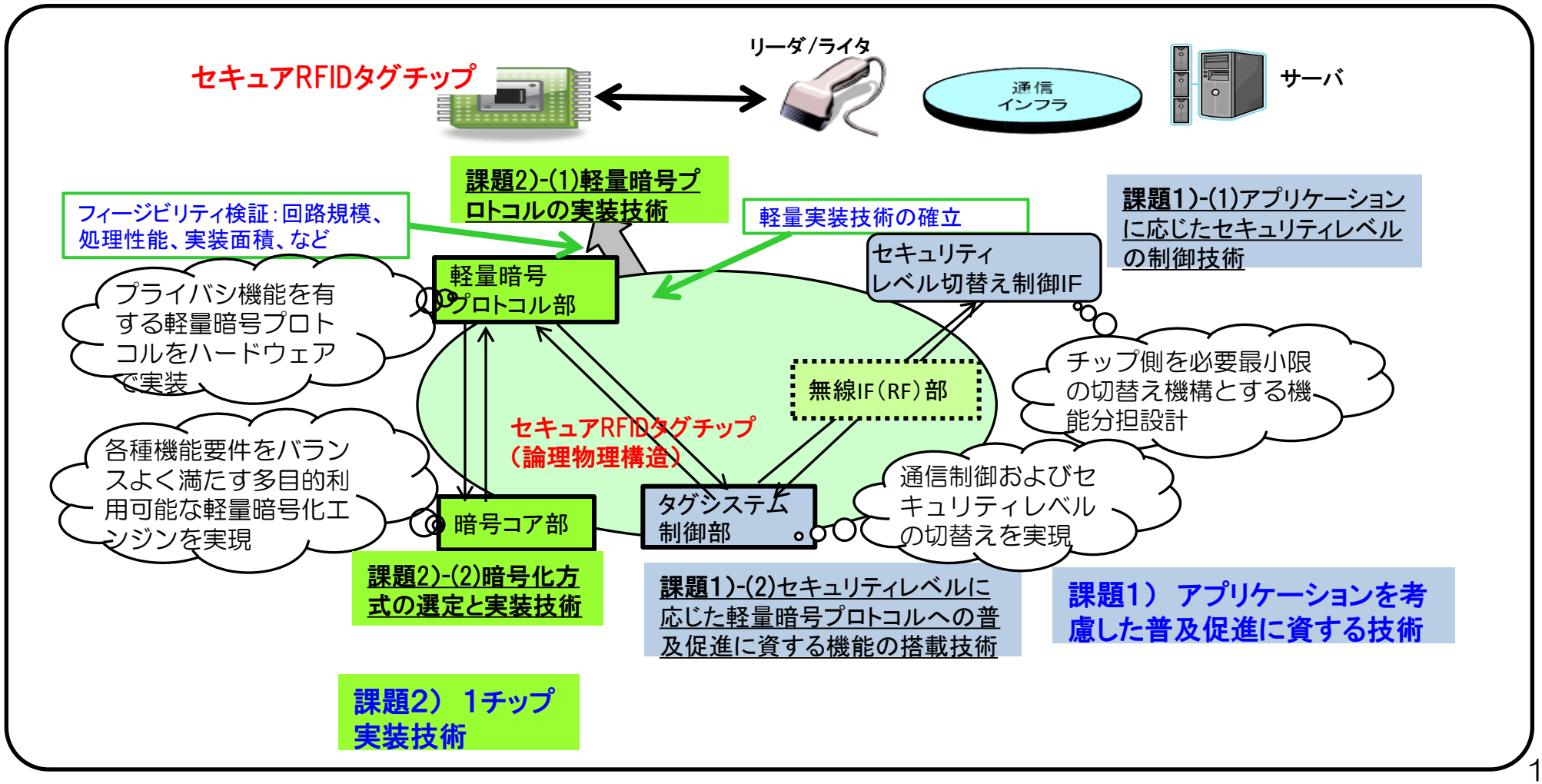
# 平成25年度「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上に関する研究開発」の研究開発目標・成果と今後の研究計画
## 副題　プライバシ保護とセキュリティレベル切替えが可能なセキュアRFIDタグの実現　　（その1）

1．実施機関・研究開発期間・研究開発費
- ◆実施機関　　株式会社サイバー創研（幹事者）、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185百万円（平成25年度　61百万円）

2．研究開発の目標

平成26年度末までに、「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」の実装技術のフィージビリティを確認する。

3．研究開発の成果（最終年度の成果目標）



# 平成25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に関する研究開発」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　　（その2）

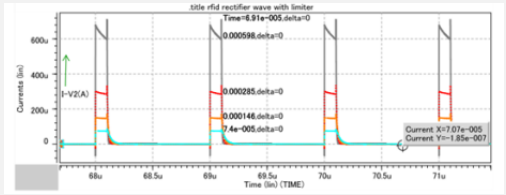
### 3．研究開発の成果（平成25年度の成果）
### 課題1）アプリケーションを考慮した普及促進に資する技術
### 課題1）-(1)アプリケーションに応じたセキュリティレベルの制御技術

今年度の研究開発成果：セキュリティレベル切替え制御インターフェース仕様確立及び電力解析シミュレーションによるチップのフィージビリティ検証
（課題）アプリケーションに応じたプライバシ保護あり／なし切替えすなわちセキュリティレベル切替えの制御技術
- ・セキュリティレベル切替え制御インターフェース仕様（詳細仕様）の確立
  - –安全性を確保して、タグのセキュリティレベルを切替えるためのサーバとタグとの間のメッセージシーケンスを設計した。
  - –プライバシ保護レベル切替え中の電力不足発生に対応するために、タグが保持すべき情報と情報の切替え条件を設計した。
- ・セキュアRFIDタグチップの軽量実装技術のフィージビリティ検証
  - –タグディジタル部の主要部分の消費電力をシミュレーションで検証した。
  - –負荷の違いが電力供給部に与える影響をシミュレーションで検証した。

●タグディジタル部の電力消費の一例（ネットリストの比較結果）

| 回路モジュール | クロックゲーティング無し(uW) | クロックゲーティング有り(uW) | 電療増減率(%) |
|---|---|---|---|
| Domus_digital | 324.0 | 258.0 | −20.37 |
| HASH | 20.7 | 3.2 | −84.40 |
| その他暗号部 | 9.7 | 6.8 | −.29.69 |
| IF部 | 283.0 | 238.0 | −15.90 |
| sram/Flash | 3.6 | 3.9 | 7.82 |

●電源回路の供給能力（負荷変動の一例）

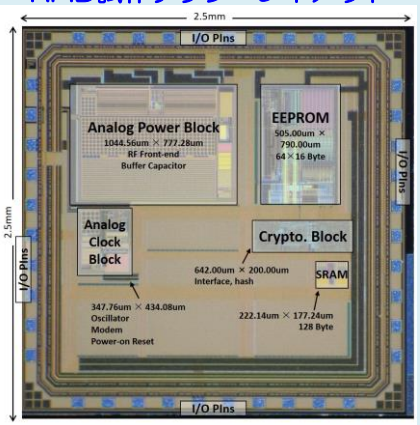



・黒田、西門、齋藤、波止元、清水
“RFIDタグ認証システム、RFIDタグおよびRFIDタグ認証方法”
2014年2月28日出願

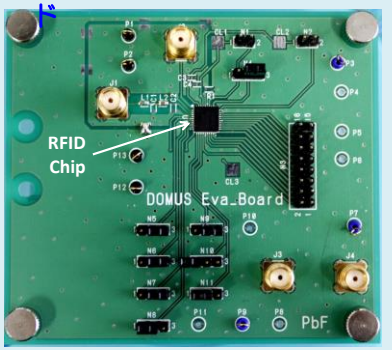
### 課題1）-(2)セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術

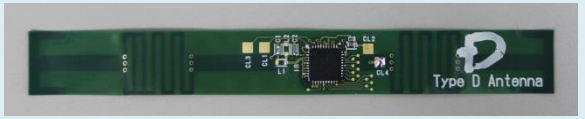
今年度の研究開発成果：1回目のRFIDタグを作製し、機能検証を行った
（課題）セキュリティレベルに応じた軽量暗号プロトコルへの普及促進に資する機能の搭載技術
- ・セキュアプログラマビリティ確保方式の軽量実装技術の確立
  - –メモリの物理マッピングの策定を行い、RTLシミュレーションで機能検証を完了した。
- ・セキュアRFIDタグチップの軽量実装技術の確立
  - –ディジタル部とアナログ部を含めたレイアウトの基本設計・詳細設計を完了した。
  - – 1回目の試作チップを外注により作製し、機能検証を行った。

RFID試作チップ　レイアウト




RFID試作チップ 評価ボード




試作RFIDタグ


・ Yang Li, Toshiki Nakasone, Kazuo Ohta, Kazuo Sakiyama, “Privacy-Mode Switching: Toward Flexible Privacy Protection for RFID Tags in Internet of Things,” In WiP Session of CCNC’14, IEEE.
・Yang Li, Toshiki Nakasone, Kazuo Sakiyama, “Toward Practically Secure and Flexible RFID Tags,” Hot Channel Workshop Apr. 2013.

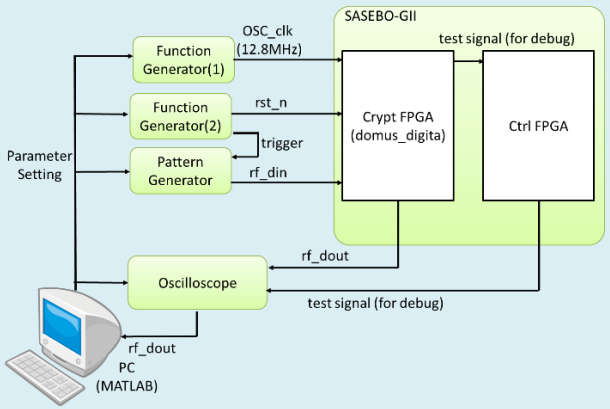
## 3. 研究開発の成果（平成25年度の成果）

### 課題2）1チップ実装技術

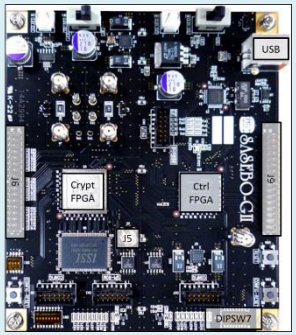
#### 課題2)-(1) 軽量暗号プロトコルの実装技術

今年度の研究開発成果：軽量暗号プロトコルのハードウェア実装による機能検証を行った
(課題) 軽量暗号プロトコルの選定、プロトコルの仕様策定
・軽量暗号プロトコルの軽量実装技術の確立
-昨年度策定した軽量暗号プロトコルの各種パラメータにもとづきハードウェアに実装した。
-FPGAを用いてディジタル部全体のハードウェア実装による基礎実験と機能検証を行った。

FPGA動作確認環境




機能検証に使った FPGAボード




クロック周波数変動時の動作範囲

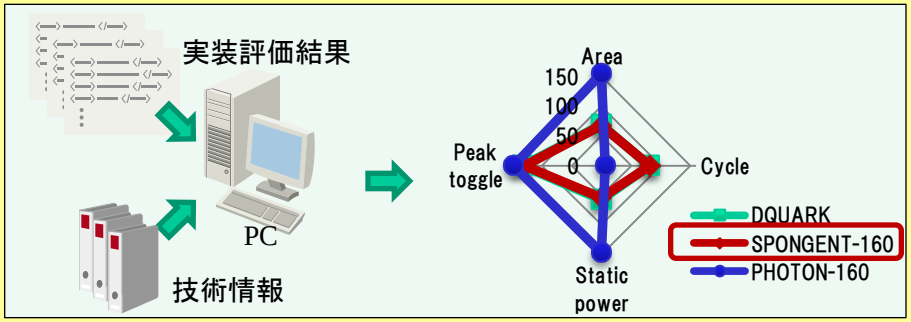
| Delimiter　Ctrl | 00 | 01 | 10 | 11 |
|---|---|---|---|---|
| Operational freq. range | -7% ～ 8.5% | -9% ～ 5.5% | -2.5% ～ 13% | -5% ～ 11.5% |

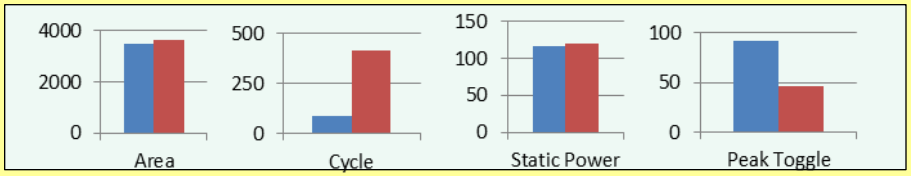
・Yang Li, Toshiki Nakasone, Kazuo Sakiyama, “Toward Applications of SRAM Retention Time as Battery-Less Timer for RFID Tags,” IWSEC 2013 Poster.
・Yang Li, Toshiki Nakasone, Kazuo Sakiyama, “Introduction to IAIK Demotag and Related Experiments on It,” Hot Channel Workshop Nov. 2013.

#### 課題2)-(2) 暗号化方式の選定と実装技術

今年度の研究開発成果：1回目チップ試作用の暗号コアの選定と暗号コアの最適実装に向けた基礎評価の完了
(課題) 暗号化方式の選定と実装技術
・暗号コアの選定
- 静的電力とピーク電力の評価を行った。
- 平成24年度実施の性能評価結果と電力評価結果にもとづき、暗号コアとしてハッシュ関数SPONGENT-160を選択した。
- デジタル部設計仕様に合った、1回目チップ試作用の暗号コアを開発し、仕様書をまとめた。

・暗号コアの軽量実装技術
- 消費電力と処理速度のトレードオフ関係を明らかにした。




・三上修吾、渡辺大、崎山一男、“OSKプロトコル向け軽量暗号アルゴリズムの実装評価、”Hot Channel Workshop 2013 April.
・Shugo Mikami, Dai Watanabe and Kazuo Sakiyama, “A Comparative Study of Stream Ciphers and Hash Functions for RFID Authentications,” RFIDsec’13 Asia.
・三上修吾、渡辺大、崎山一男、“バッファを用いた軽量擬似乱数生成器のハードウェア実装と評価”、SCIS2014.

4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数、（ ）内は当該年度の件数です。

| | 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 | 4<br>(2) | 0<br>(0) | 0<br>(0) | 13<br>(7) | 0<br>(0) | 0<br>0) | 0<br>(0) |

国内出願件数に関する補足説明

H24年度は、電通大　1件、サイバー創研　1件で合計2件
H25年度は、電通大　1件、サイバー創研　1件で合計2件
電通大のH24年度の出願1件は公知技術であることが判明したため，H25年度に取り下げた

5. 研究成果発表会等の開催について

・チップ試作の設計検証及び試作チップに対する実機検証で得られた結果を国内外の学会や会議の場での研究発表等を通して、研究成果を広く一般に周知、広報することを検討する。

6. 今後の研究開発計画

・H25年度のチップ試作で得られた知見を基に、H26年度は2回目のチップ試作を実施し、実現が極めて困難で世界でまだ実現例がない、軽量暗号コアと軽量暗号プロトコルの実装によるセキュリティレベルの切替えが可能な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ージビリティ検証