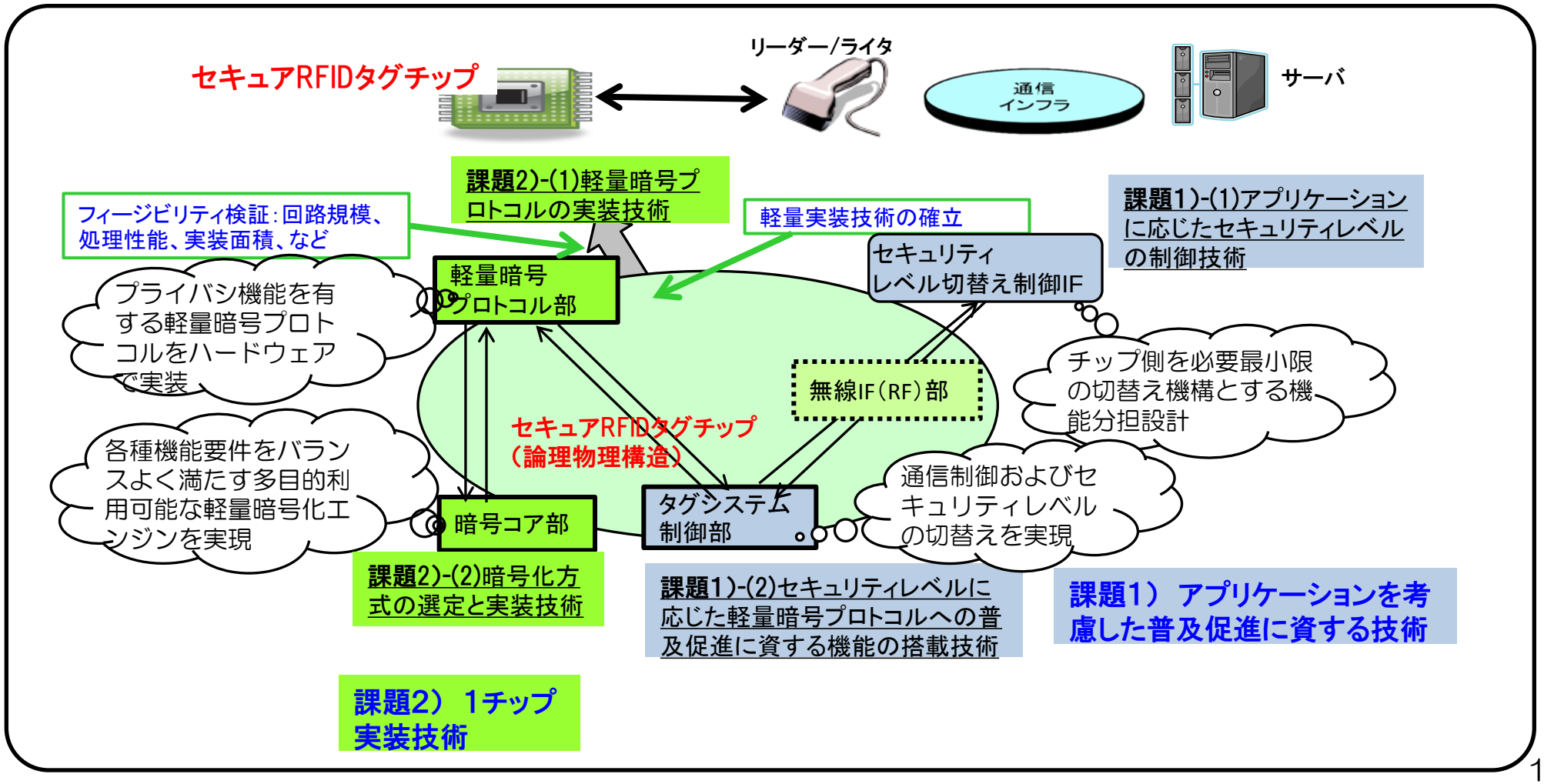
平成24年度「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上に関する研究開発」の研究開発目標・成果と今後の研究計画
副題　プライバシ保護とセキュリティレベル切替えが可能なセキュアRFIDタグの実現　　（その1）

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24年度　65百万円）

2. 研究開発の目標

   平成26年度までに、「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24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）

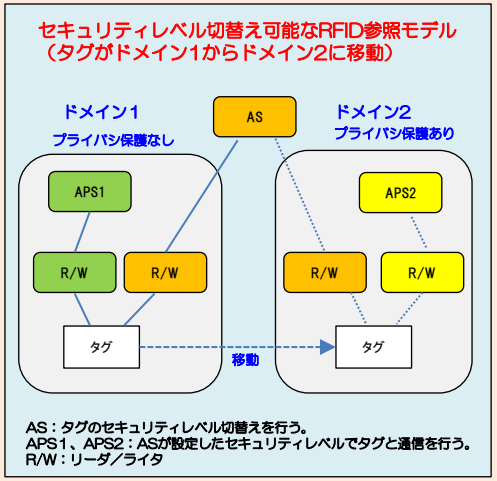
3. 研究開発の成果（平成24年度の成果）

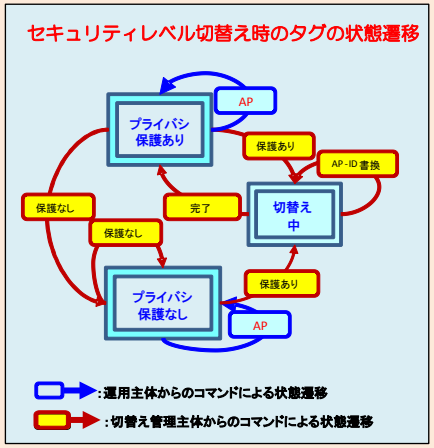
課題1）アプリケーションを考慮した普及促進に資する技術

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方式の確立
(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方式の確立
- 典型的なユースケースを想定して、セキュリティレベル切替え可能なRFID参照モデルを策定した。
- 策定した参照モデルについて、セキュリティレベル切替えを中心にタグの状態遷移図を作成した。

・セキュリティレベル切替え制御インターフェース仕様（基本仕様）の確立
- タグのセキュリティレベル切替え時のタグとセキュリティレベル切替え主体（AS)との間のメッセージシーケンスを分析し、タグが保持すべき情報を明確にした。
- 1チップ化の観点から、タグが満たすべき条件を整理した。





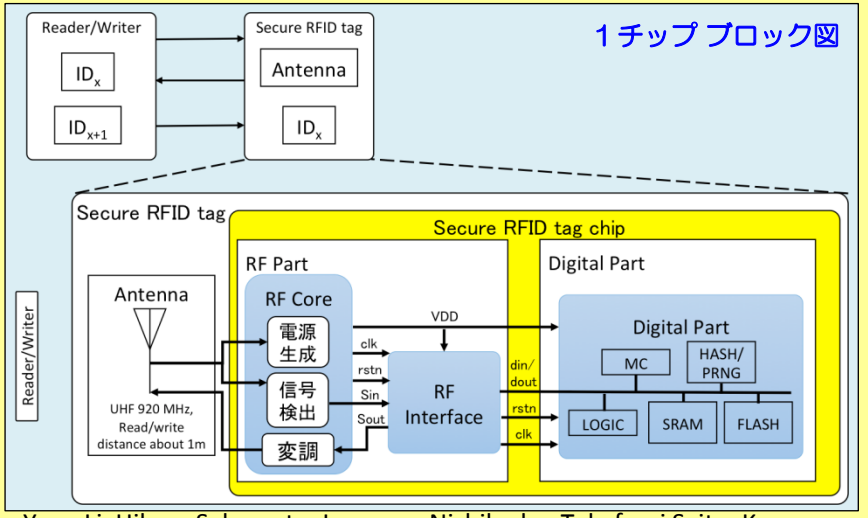
・西門、齋藤、波止元、清水
“セキュリティレベル切替え可能なRFIDタグ認証システム及びRFIDタグ”
2013年3月22日出願

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：軽量暗号プロトコルの制御方式,実装技術の確立
(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
・用途拡大を実現するタグシステム制御方式の確立
- -セキュリティレベルに応じてプライバシ保護機能を切替え可能とする制御方式を確立した。
- プライバシ保護機能の切替えに必要な制御回路を設計した。

・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（SRAMとEEPROM）の構成の仕様策定を行った。

・セキュアRFIDタグチップの軽量実装技術の確立
- 1チップ化を考慮したRF部とアナログ部の基本設計を完了した（汎用IPコアの詳細設計を外注し、設計スケジュールを加速）。
- RF部のインターフェース回路仕様を策定した（SRAMバスによるシステムメモリの共有によるコンパクト実装）。



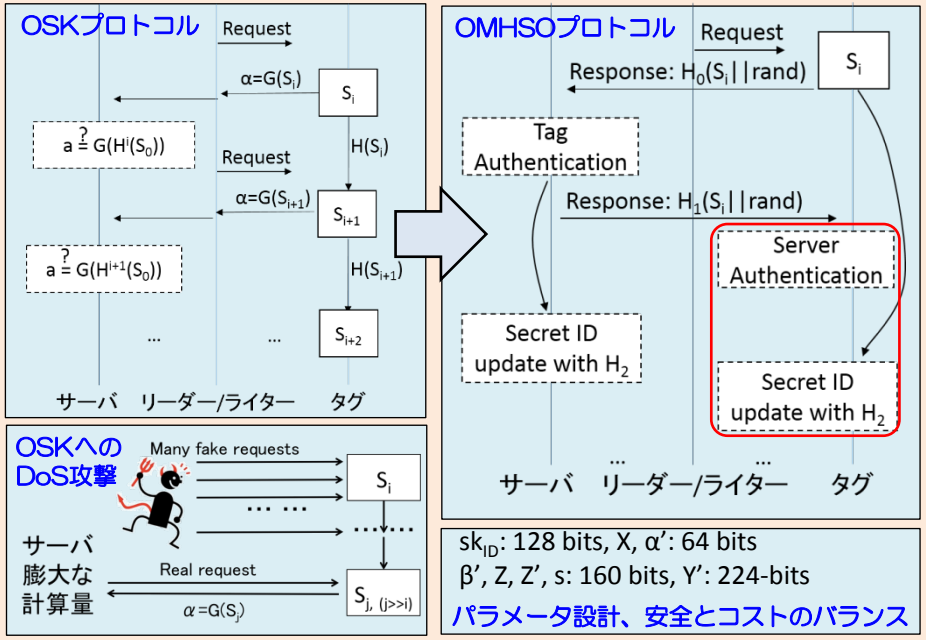
・Yang Li, Hikaru Sakamoto, Iwamasa Nishikado, Takafumi Saito, Kazuo Ohta, Kazuo Sakiyama “Toward Flexible Privacy Protection for RFID Tags Using Privacy-Mode Switching” 2013年総合大会
・李 陽, 崎山 一男, “Two Topics in Cryptographic Hardware: Coupon DFA and Secure RFID” 2013年2月暗号理論ワークショップ

平成24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3）

3．研究開発の成果（平成24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仕様策定、実装技術の確立
(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仕様策定
- OSKプロトコルのDoS攻撃耐性に関する技術調査にもとづき、OMHSOプロトコルを軽量暗号プロトコルとして選定した（OMHSOプロトコルは相互認証方式であるため、DoS攻撃耐性を有する）。
- 軽量暗号プロトコルOMHSOのセキュリティパラメータを策定した

・軽量暗号プロトコルの軽量実装技術の確立
- プロトコル部に対応するディジタル回路の基本設計を完了した。



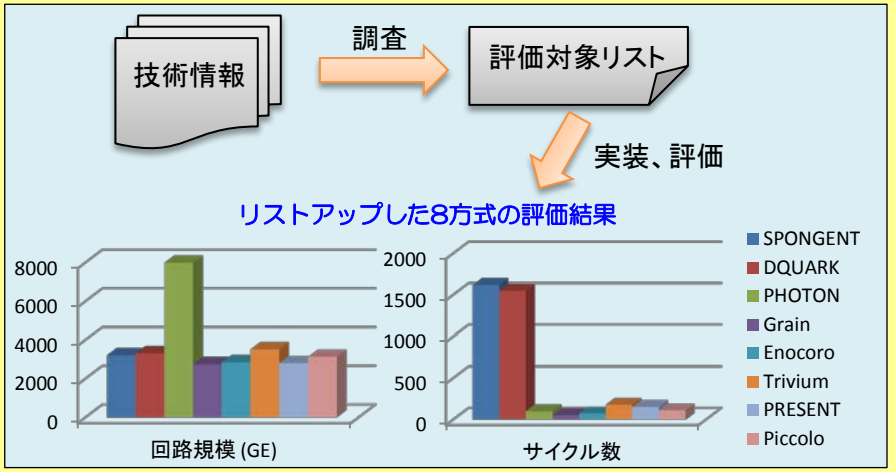
sk_ID: 128 bits, X, α': 64 bits
β', Z, Z', s: 160 bits, Y': 224-bits
パラメータ設計、安全とコストのバランス

・崎山一男, 李 陽, 中曽根俊貴, 山本晃裕 “電源遮断時間判定装置及び無線タグ 特願2013－038790
・中曽根俊貴, 李　陽, 崎山一男 “システム上にあるSRAMの電荷保持時間とPUF特性を利用したDoS攻撃対策” IEICE 2013年総合大会
・崎山一男, “暗号とプライバシーとRFIDシステム,” 近代科学社, 2013年3月

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：暗号コアの選定に向けた技術情報の調査と基礎評価の完了
(課題)　暗号化方式の選定と実装技術
・暗号コアの選定
- セキュリティ強度と機能要件（タグ長など）の関係を明確化した。
- ハッシュ関数の他に擬似乱数生成器が対象プロトコルの機能要件を満たすことを確認した。
- プロトコルの機能要件に適合する8方式(ハッシュ関数、擬似乱数生成器を含む)を実装評価対象としてリストアップした。

・暗号コアの軽量実装技術
- リストアップした8方式(ハッシュ関数3種類、擬似乱数生成器3種類、ブロック暗号2種類)のハードウェア実装し、評価した。
- 回路規模とサイクル数の評価を実施した。



・三上修吾、渡辺大、”プライバシ保護を配慮したRFID向けセキュリティ要件と軽量暗号アルゴリズムに関する一考察”、 Hot Channel Workshop 2012.
・三上修吾、渡辺大、崎山一男、“RFID認証プロトコル向け軽量暗号アルゴリズムの実装評価”、2013年暗号と情報セキュリティシンポジウム SCIS 2013.

4. これまで得られた成果（特許出願や論文発表等）　※成果数は累計件数と（ ）内の当該年度件数です。

	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	2(2)			6(6)			

5. 研究成果発表会等の開催について

・今年度は研究初年度であり、次年度以降の研究状況を踏まえ、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

本研究開発は、セキュアRFIDタグのフィージビリティ検証であり、NICTの自ら研究へ検討状況、検討結果を引き継ぎ、今後の方向性の判断に貢献する。