



HITACHI
Inspire the Next



2014年9月4日

国立大学法人電気通信大学

株式会社日立製作所

株式会社サイバー創研

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

国立大学法人電気通信大学(学長：福田 喬／以下、電気通信大学)、株式会社日立製作所(執行役社長兼 COO：東原 敏昭／以下、日立)、株式会社サイバー創研(代表取締役社長：木下 研作／以下、サイバー創研)は、ID 情報を秘匿したまま認証を行うことで、プライバシーの侵害リスクを低減する UHF^{*1} 帯パッシブ型 RFID タグチップ^{*2} の試作に成功しました。従来の ID 秘匿認証(OMHSO)プロトコルは、タグチップ内で複雑な処理を実行するため、小型化および消費電力を抑えることが困難でした。今回試作した RFID タグチップは、アナログ信号とデジタル信号の処理回路を 1 つの回路に集積することで、回路規模が約 10 kGE^{*3}、消費電力は約 140 μ W^{*4} の小型化および省エネを実現しました。

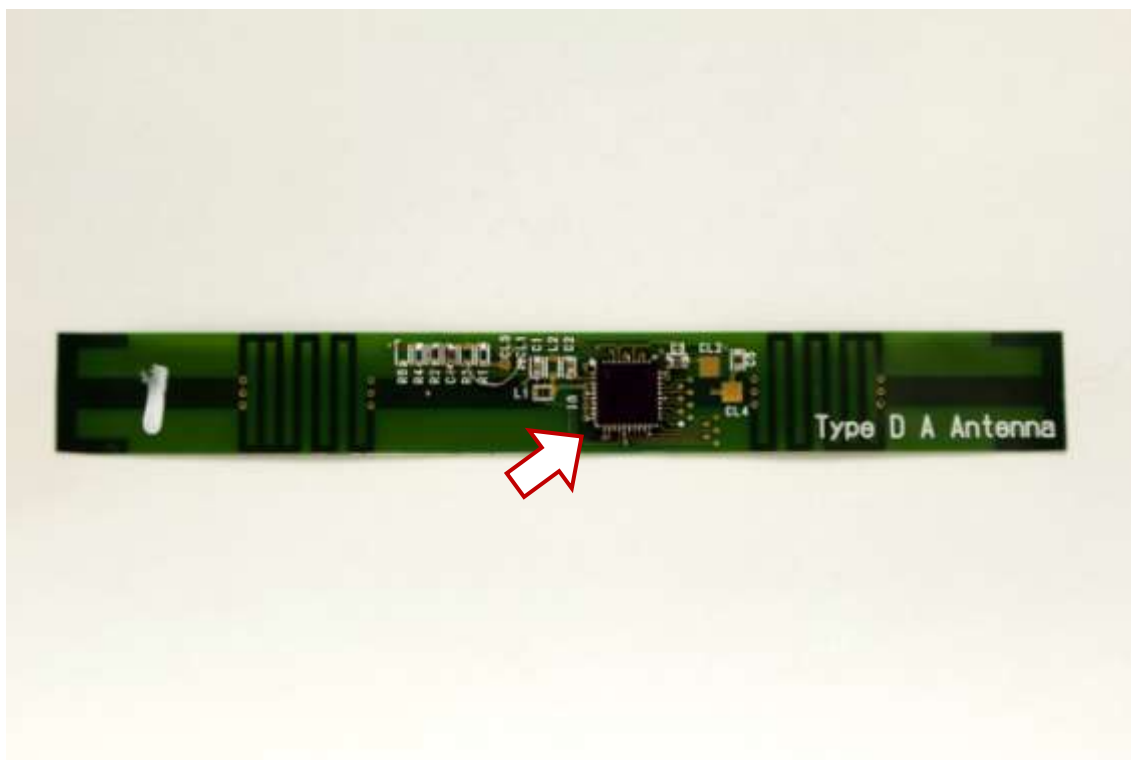
なお、本研究開発は、情報通信研究機構(理事長：坂内 正夫／以下、NICT)の委託研究「軽量暗号プロトコルの省リソースデバイスに対する実装効率向上の研究開発」により実施したものです。電気通信大学が RFID タグ全体の設計、日立が RFID タグに適した暗号技術の選定と実装、サイバー創研が RFID タグの電力評価を担当しました。

近年、RFID タグやセンサで収集された人や物の状態に関する情報(フィジカル情報)と、クラウドコンピュータ上に蓄積されるさまざまな情報(サイバー情報)を組み合わせ、快適なサービスを提供するサイバーフィジカルシステムが注目されています。例えばスマートシティの分野では、RFID タグを活用して人の位置や物の状態を把握し、日常生活に必要な電力量を調整するなど、利用者が所有する ID カードと組み合わせることで、効率的なサービスの提供が可能になります。一方、RFID タグはカードリーダーなどで容易に読み取ることができるため、その ID 情報を追跡されると個人のプライバシーを侵害されるリスクがあります。

このようなリスクを軽減するために、ID 情報の付け替えを行う仮名化技術や秘匿化技術の研究開発が進められています。NICT と電気通信大学の崎山一男教授、太田和夫教授らの研究グループでは、ハッシュチェーン^{*5}を用いて RFID タグが発信する ID 値^{*6}を毎回異なる値にすることで、ID 値の追跡を困難にする ID 秘匿認証(OMHSO)プロトコルを開発してきました。この方式は高い安全性を持つ認証方式ですが、RFID タグチップ内で複雑な処理を実行するため、小型化および消費電力を抑える効率的な実装方法の確

立が課題でした。

この課題を解決するために、アナログ信号処理回路とデジタル信号処理回路を1つの回路に集積することで、ID情報を秘匿したまま認証を行うために必要なデジタル信号を処理する部分の回路規模の小型化と電力の効率化を図り、新電波法の特定小電力無線局に対応したUHF帯(920 MHz帯)での動作確認に成功しました。これにより、ID値が固定である従来のRFIDタグを用いたシステムと比べて、よりプライバシー性の高いシステムの実現が期待されます。今後、本技術を活用し、フィジカル情報の安全な収集技術を確立して安心できるサイバーフィジカルシステムの構築に貢献していきます。



試作に成功したRFIDタグチップ

(電気通信大学 提供)

【用語】

- *1 UHF: Ultra High Frequency の略で、RFID で使われている無線周波数の一つ。
- *2 RFID: Radio Frequency Identification の略。RFID タグチップは、無線を利用して固体の識別に利用される IC チップで、パッシブ型 RFID タグは、電源を持たず、RFID リーダからの電磁波を利用して RFID タグチップの動作電力とする方式。
- *3 GE: Gate Equivalent の略で、回路面積を表す単位の一つ。試作した RFID タグチップでは、1 GE は約 $8.78\mu\text{m}^2$ に相当。数値は ID 秘匿認証プロトコルを処理するデジタル回路部分(揮発性メモリを除く)の評価結果。
- *4 電力を無線供給する環境で評価。ID 秘匿認証プロトコルの演算処理(揮発性メモリから必要なデータを読み出す/書き込む処理を含む)の評価結果。
- *5 ハッシュチェーン: データに対して暗号的ハッシュ関数を繰り返し適用する方法。
- *6 ID 値: RFID タグの認証に用いる情報。

■照会先

国立大学法人電気通信大学 情報理工学研究科 総合情報学専攻 [担当：崎山]

〒182-8585 東京都調布市調布ヶ丘 1-5-1

電話 042-443-5767

株式会社日立製作所 横浜研究所 企画室 [担当：吉田]

〒244-0817 神奈川県横浜市戸塚区吉田町 292 番地

電話 050-3135-3409

株式会社サイバー創研 [担当：黒田]

〒150-0002 東京都渋谷区渋谷二丁目 15 番 1 号 渋谷クロスタワー22 階

電話 03-3797-3183

以上

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL 等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
