様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　４ 年　 ６ 月 ２５ 日現在

機関番号：３４４１６
研究種目：基盤研究(B)（一般）
研究期間：2018～2020
課題番号：１８Ｈ０３２４１

研究課題名（和文）低計算資源で実現可能なセンサ機器認証技術の研究開発

研究課題名（英文）Research of authentication schemes available to low computational resource sensor devices

研究代表者
桑門　秀典（KUWAKADO, Hidenori）

関西大学・総合情報学部・教授

研究者番号：３０２８３９１４

交付決定額（研究期間全体）：（直接経費）　　13,300,000円

研究成果の概要（和文）：低計算資源で実現可能なセンサ機器で認証プロトコルを実行できるように、PUF、Fuzzy extractor、認証プロトコルの三つを統合的に検討した。センサに必要なアナログフロントエンド回路を実装するプログラマブルアナログICがPUFとして利用可能であることがわかった。Fuzzy extractorでの利用を想定して、整数環上で秘密分散法を考案し、公開鍵暗号の一つであるNTRU暗号を用いたFuzzy extractorを構成した。認証プロトコルに必要な軽量ブロック暗号をC言語プログラムから高位合成によってFPGA実装を行い、C言語による記述と消費電力の関係を調べた。

研究成果の学術的意義や社会的意義
アナログ回路の設計開発の効率化のために開発されたプログラマブルアナログICがPUFとして利用できることはアナログフロントエンド回路を必要とするセンサに都合がよい。Fuzzy extractorは雑音除去のために誤り訂正符号を使った構成法がよく知られているが、NTRU暗号を利用すると、雑音除去だけでなく、固有情報の機密性が暗号学的に保証できる長所がある。

研究成果の概要（英文）：PUF, Fuzzy extractor, and authentication protocol were comprehensively examined so that the authentication protocol can be executed by sensor devices with low computational resources. Programmable analog ICs on which analog front-end circuits for sensors are implemented can be used as PUF. We proposed a secret sharing method on an integer ring as a tool for Fuzzy extractors, and showed Fuzzy extractors using NTRU public-key cryptosystem. The lightweight block cipher required for authentication protocols was implemented in FPGA from C language programs by high-level synthesis, and the relationship between the description in C language and power consumption was investigated.

研究分野：暗号理論

キーワード：物理的複製不可能関数　Fuzzy Extractor　プログラマブルアナログ回路

１．研究開始当初の背景

(1) センサ機器は Internet of Things (IoT)の重要な"Things"であり、米国起業家Ｊ．Brysek は１兆個のセンサを活用して社会的課題を解決する"Trillion Sensors Universe"というビジョンを提唱している。センサ機器の効果的な活用が進めば進むほど、センサ機器が発信するデータの真正性を保証するセンサ機器認証の技術が重要になる。センサ機器認証を実現するための有用な技術として、物理的複製不可能関数(Physical Unclonable Function: PUF)がある。PUF は、その機器に内在する複製困難な物理的構造に依存した、その機器固有の値を出力するハードウェアである。PUF の出力値は、機器固有かつランダムな値なので、認証等に使う秘密情報に利用できる。秘密情報を製造後に不揮発性メモリに書き込むことと比較して、PUF の利点は、秘密情報を保存するための不揮発性メモリが不要であること、機器ごとに秘密情報を生成する工程が不要であることが挙げられる。PUF の実現法として、LSI のシリコンの微細加工の不均一性、SRAM の動作の不均一性、リング・オシレータの動作の不均一性など、さまざまな物理現象に基づく方式が報告されているが、安価には実現できない PUF も少なくない。PUF をセンサ機器認証に利用する場合、センサ機器は安価なものが多いため、安価に実装できる PUF が必要である。

(2) Fuzzy Extractor は、バイオメトリクスデータ等のノイズが多いデータから機器認証で使用可能な秘密情報を生成するアルゴリズムである。PUF の出力値も測定や環境に依存したノイズを含むので、Fuzzy Extractor を使って PUF の出力値を安定化させて認証用秘密情報を定める。認証用秘密情報を定めた後は、原理的には任意の認証プロトコルが使用可能であるから、使用する認証プロトコルに言及している従来研究はない。しかし、センサ機器は計算資源が貧弱なものが多いため、低計算資源で実行できる認証プロトコルが必要である。認証プロトコルは数多く提案されているが、乱数生成器やメモリなど、認証プロトコルを実行するために追加の計算資源を必要とする認証プロトコルが多い。そこで、本研究では、低計算資源で認証プロトコルを実行できるように、PUF、Fuzzy extractor、認証プロトコルの三つを統合的に検討する。

２．研究の目的

本研究の目的は、IoT のセンサ機器のセキュリティ向上のために必要な低計算資源で実現できるセンサ機器認証技術を創出することである。具体的には、「プログラマブルアナログ IC を利用した PUF 用の特徴量の特定」と「低計算資源で実行可能な認証プロトコルの設計」に取り組む。

(1) プログラマブルアナログ IC を利用した PUF 用の特徴量の特定

センサ機器認証に PUF を利用する場合、PUF を実装する部品が必要である。一般に、アナログ素子から構成されるアナログ回路の特性は個々のアナログ素子の特性に依存するので、アナログ回路の動作特性を PUF に利用できる可能性がある。通常、センサと一緒に用いられるアナログフロントエンド回路は、ディスクリート部品やモジュールを組み合わせて設計・製造される。しかし、最近、複数のアナログ回路素子から成る回路ブロックの結線をソフトウェアで変更できるプログラマブルアナログ IC が開発・商品化され始めた。アナログフロントエンド回路を実装する場合もプログラマブルアナログ IC を利用すれば、その設計・製造の工程を削減できることが見込める。 本研究では、プログラマブルアナログ IC 内の回路ブロックの動作を検討し、PUF 用の特徴量を特定することを目指す。

(2) 低計算資源で実行可能な認証プロトコルの設計

センサ機器自身の真正性を検証する「身元認証」、センサ機器が送出したデータの真正性を検証する「メッセージ認証」の二種類の認証の総称として「センサ機器認証」という言葉を用いている。これら二種類の真正性を検証する「軽量」な認証プロトコルの従来研究は数多くある。従来研究の「軽量」とは、その意味は必ずしも同じではない。例えば、演算回数の少なさを意味する場合、消費電力の少なさを意味する場合、回路のゲート数の少なさを意味する場合などがある。本研究では、暗号処理ハードウェアの実装に関する論文によれば、演算回路のサイズよりレジスタ（メモリ）のサイズの方が全体の回路規模への影響が大きいことに着目した。IoT のセンサ機器での利用を想定すれば、回路を実装した場合の消費電力も重要である。

PUF の出力を認証に用いるためには、PUF の出力から測定などに起因する雑音を除去する必要がある。このため、従来は、誤り訂正符号を用いることで誤りを除去していた。一般的に、優れた誤り訂正能力を有する誤り訂正符号ほど、符号化と復号（誤り訂正）に多くの計算資源が必要である。また、真正性を検証するために用いる情報の機密性を保証するため、PUF の出力をそのまま真正性検証の情報として用いることはできない。つまり、認証プロトコルは誤り訂正符号だけでは実現できず、機密性を保証する何らかの仕組みが必要である。そこで、本研究では、機密性を保証しつつ、誤りも訂正できる方法を検討する。

３．研究の方法

(1) プログラマブルアナログ IC を利用した PUF 用の特徴量の特定

プログラマブルアナログ IC の製造時に生じる動作のばらつきを PUF の特徴量として利用するため、その誤差が特徴量として安定して取得できる回路ブロックの候補として、IC 内のオペアンプ素子とコンパレータ素子の入出力動作を調査する。これは、センサの出力信号を増幅・フィルタリングするアナログフロントエンド回路には、オペアンプ素子やコンパレータ素子がしばしば利用されるため、さらに、センサを内蔵する回路には、回路的に近い所にオペアンプ素子やコンパレータ素子が存在するためである。つまり、センサとオペアンプ素子等が回路的に近ければ、センサとオペアンプ素子等の間に偽の信号を混入することが、攻撃者にとって物理的に困難になる。次に、安価に市販されているディスクリートなオペアンプ素子について、PUF の特徴量として利用するため、入出力動作特性を調査する。

(2) 低計算資源で実行可能な認証プロトコルの設計

PUF の出力は、測定や環境に起因する雑音を含んでいるので、雑音を除去することが必要である。さらに、PUF の出力から個体識別情報を秘匿する必要がある。これらを実現するために、Fuzzy extractor が用いられる。Fuzzy extractor の代表的な実現法として、誤り訂正符号を用いた方式が知られている。そこで、低メモリ化を目指した Fuzzy extractor の別の構成法として、秘密分散と格子暗号の一つである NTRU 暗号の利用を検討する。また、認証プロトコルの省電力化のため、軽量ブロック暗号の FPGA 実装を行う。その際、最近開発された高位合成の技術を用いる。

４．研究成果

(1) プログラマブルアナログ IC を利用した PUF 用の特徴量の特定

プログラマブルアナログ IC の回路ブロックの製造時に生じる動作の誤差を PUF に利用することを検討し、その誤差が特徴量として安定して測定できる回路ブロックを調査した。最初に、プログラマブルアナログ IC 内のオペアンプ素子とコンパレータ素子の回路ブロックへの入力電圧を変化させたときの出力電圧に生じる誤差を特徴量として利用できるか否かを調査した。入力電圧が 1V 程度単位で制御する場合には、出力電圧に誤差が生じる場合はあるものの、同じ動作をする場合が多いことがわかった。プログラマブルアナログ IC 内にこれらの回路ブロック数は多くないので、プログラマブルアナログ IC を識別できない場合が無視できず、識別するためには多数のプログラマブルアナログ IC が必要である。

次に、プログラマブルアナログ IC の回路ブロックのコンパレータに着目し、コンパレータの製造時に生じる動作のばらつきとして、入力電圧を一定として、電源電圧（駆動電圧）の変化による出力値の変化を特徴量として利用の可否を調査した。その結果、駆動電圧の変化を利用すれば、入力電圧の変化よりも、特徴量として利用できる、つまり識別に利用できる情報量を増加することがわかった。プログラマブルアナログ IC 内に含まれるオペアンプ素子やコンパレータ素子の数は多くないので、特徴量の情報量を増やすためには、現在のところ、プログラマブルアナログ IC の個数を増やす必要がある。

そこで、ディスクリートなオペアンプ素子を補助的に使うことを想定して、市販されている安価なオペアンプ素子に対して同様の特徴量を調査した。その結果、使用したディスクリートなオペアンプ素子の製造時のばらつきは、プログラマブルアナログ IC 内のオペアンプ素子のばらつきよりも大きく、入力電圧の変化に対する出力電圧の個体差は市販の安価な LED を点灯・消灯する程の差があり、目視で識別可能な特徴量であることがわかった。

本課題を遂行中に、スマートフォンのセンサの校正情報を PUF として用いる方式が他の研究者により発見された。具体的には、スマートフォンに内蔵されている加速度センサの校正情報をセンサの測定値から推測し、それをスマートフォンの個体識別に用いる。本課題と類似性があるので、その追試を行い、同様の結果を得ることができた。さらに、加速度センサだけでなく、地磁気センサでも同様に校正情報を用いて、スマートフォンの個体識別ができる可能性を明らかにした。ただし、現在は、メーカーが提供した修正プログラムにより、加速度センサや地磁気センサを含め、スマートフォンに内蔵されているセンサの校正情報を取得する（あるいは推測する）ことが難しい状況になっている。

(2) 低計算資源で実行可能な認証プロトコルの設計

認証プロトコルの低計算資源化のために、メモリのサイズを小さくすることを目指した。Fuzzy extractor の省メモリ化のために、有限体ではなく、整数環上で秘密分散法の可能性を検討し、それが実現可能であることを示した。次に、Fuzzy extractor の前処理として、アナログ情報を利用することを検討した。これは、前述「(1) プログラマブルアナログ IC を利用した PUF 用の特徴量」の結果により、アナログ情報を取得できる見込みを得たからである。Fuzzy extractor では、識別するための固有情報を得るために誤り訂正符号がしばしば用いられる。アナログ情報を利用すれば、Fuzzy extractor で利用する誤り訂正符号の訂正能力をさらに有効に使えるが、メモリのサイズを大きくするので、本研究の目的に合致しないことがわかった。次に、本研究では、Fuzzy extractor では、測定時の雑音を除去するだけでなく、識別するための固有情報の機密性も保証する必要があることに着目した。固有情報の機密性を保証するために加えた雑音を復号時に訂正する能力がある NTRU 暗号の利用を検討した。NTRU 暗号を用いて Fuzzy extractor

を構成でき、測定時の雑音が想定内であれば、暗号学的な安全性が固有情報の秘匿性を保証できることを確認した。しかし、NTRU 暗号を用いて Fuzzy extractor を構成した場合、従来の Fuzzy extractor とのメモリのサイズを含めた計算機資源の厳密な比較が今後の課題として残った。

本研究では、認証プロトコルの低計算資源化のために、省電力化も目指した。認証プロトコルの省電力化のために軽量ブロック暗号を利用することを検討し、FPGA を使って実装した。通常、FPGA 実装の際には、ハードウェア記述言語 Verilog HDL などを用いる。しかし、軽量ブロック暗号の仕様は C 言語などのソフトウェア言語で記述されているので、ハードウェア記述言語へ変換するための能力（人材）が必要である。一般に、ソフトウェア言語記述からハードウェア記述言語への変換は、開発効率を悪くする原因であるため、C 言語等から回路の配置配線情報を記述したファイル(ビットストリーム)を生成する高位合成の技術開発が進んでいる。本研究では、軽量ブロック暗号のアルゴリズムの C 言語による記述から、Xilinx 社の Vivado、Vitis を用いて Zynq-7010 用ビットストリームを高位合成した。その結果、動作周波数 144MHz で約 1.4W の消費電力で動作できる FPGA 回路が高位合成により作成できることがシミュレーションで明らかになり、さらにそれらの値がアルゴリズムの C 言語による記述の仕方に依存することがわかった。低消費電力なビットストリームを生成するような、軽量ブロック暗号のアルゴリズムの C 言語による一般的な記述法を明らかにすることが今後の課題である。

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Hidenori Kuwakado	４．巻 -
２．論文標題 Secret Sharing Schemes Using Modulo-2^{m} Arithmetic Operations	５．発行年 2018年
３．雑誌名 The 2018 IEEE Conference on Dependable and Secure Computing	６．最初と最後の頁 -
掲載論文のDOI（デジタルオブジェクト識別子） 10.1109/DESEC.2018.8625126	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計0件

〔図書〕　計0件

〔産業財産権〕

〔その他〕

－

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	堀井　康史 (HORII Yasushi) (00268335)	関西大学・総合情報学部・教授 (34416)	
研究分担者	小林　孝史 (KOBAYASHI Takashi) (90268334)	関西大学・総合情報学部・准教授 (34416)	

７．科研費を使用して開催した国際研究集会

〔国際研究集会〕　計0件

８．本研究に関連して実施した国際共同研究の実施状況

共同研究相手国	相手方研究機関