様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　１１　日現在

機関番号：　８２６２６
研究種目：　若手研究(B)
研究期間：　2013～2014
課題番号：　２５７３００３４

研究課題名（和文）複製困難な物理特性を用いたセキュアな動的再構成システムの実現

研究課題名（英文）Development of a secure dynamic reconfiguration system using a Physically Unclonable Function

研究代表者

堀　洋平（Hori, Yohei）

独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員

研究者番号：６０５３０３６８

交付決定額（研究期間全体）：（直接経費）　　3,100,000円

研究成果の概要（和文）：PUFとFuzzy Extractorを用いて暗号鍵を生成・共有するPUF-KEY回路のFPGA実装を行った。Fuzzy Extractorは誤り訂正符号を利用して不安定なPUF出力から暗号鍵を生成する機構である。今回、誤り訂正符号としてReed-Solomon (RS)符号を使用し、符号化器および復号器の回路開発にはMatlab HDL Coderによる高位合成を利用した。PUF-KEY回路の回路規模や速度について評価を行った。また、3枚のSASEBO-G3ボードにPUF-KEY回路を実装し、それぞれから異なる鍵が生成され、後に同じPUFを用いて復元できることを実機により確認した。

研究成果の概要（英文）：I have implemented a PUF-KEY circuit on a Kintex-7 FPGA that consists of a physically unclonable function (PUF), fuzzy extractor and AES circuits. A fuzzy extractor generates a cryptographic key from noisy PUF outputs by applying an error correcting code. In this study, I used (255, 239) Reed-Solomon (RS) codes for the fuzzy extractor. For the development of an RS encoder and decoder, I used Matlab HDL Coder, which is one of the popular high-level synthesis tools available. In this study, I show the speed and area performance of the PUF-KEY circuit. I also experimentally show the effectiveness of the PUF-KEY circuits by using three SASEBO-G3 FPGA boards. I confirmed that each PUF-KEY circuit on the boards generates a unique key, and then the same key is regenerated from the same PUF.

研究分野：　情報学

キーワード：　リコンフィギャラブルシステム　ハードウェアセキュリティ　PUF　暗号

１．研究開始当初の背景

近年，組み込み機器においても画像処理やネットワーク処理等の負荷の高い処理が要求されており，高速性と省電力性の両立のためには ASIC (Application-Specific IC) 等の専用回路を使うのが通常である．しかし，ASIC は製造後に回路を変更できず，アルゴリズムの更新や不具合の修正ができない．

一方，FPGA (Field-Programmable Gate Array)は「回路構成データ」をデバイスに書き込むことで回路を変更できる LSI である．特に，FPGA の動作を止めることなく特定領域のみを動的に書き換える「動的再構成」技術は，多様化・高品質化するサービスやコンテンツを高速に処理し，高い信頼性で利用するために極めて有用である．動的再構成技術により，Java アプレットや ActiveX などのソフトウェアのような感覚で，利用したいコンテンツに応じて専用回路をダウンロードしたり, Windows アップデートのような感覚で，出荷後に専用回路を修正したりすることが可能である．申請者は国内で他に先駆けて，動的再構成システムの研究開発を行ってきた．

しかし，FPGA の回路構成データは，常に盗聴，改ざん，トロイの木馬回路の混入等の危険に曝されている．これらを防ぐために，FPGA ベンダは暗号技術を用いた対策を提供しているが，FPGA 上に回路を安全に構築する手法は確立されていない．これは，消費電力や電磁波を解析する先進的なサイドチャネル攻撃等によって，暗号鍵を特定できるからである．実際に，Xilinx 社やマイクロセミ社の FPGA の暗号鍵の特定に成功した研究報告がある[1][2].

このような先進的攻撃の下でも，安全な回路構築を実現できると期待される技術が物理複製不能回路（Physical Unclonable Function. 以下 PUF）である．PUF は，デバイスのばらつき（ゲート長，しきい値電圧，不純物濃度等のばらつき）を利用する．同じ構造の PUF であっても，ばらつきの影響でゲート遅延や配線遅延，あるいは電源投入直後のメモリの初期値はチップごとに異なるため，チップに固有の出力を得ることができる．PUF はチャレンジ・レスポンス手続きによってその都度暗号鍵を生成できるため不揮発性メモリは必ずしも必要でなく，鍵の変更も容易で，サイドチャネル攻撃が困難となる．

Pappu [3] 以降，これまでに様々な PUF が提案されてきた．例として，信号遅延を利用する Arbiter PUF 等が挙げられる．しかし，遅延ベースの PUF はどれも（ア）スループットが極端に低い．これは，チャレンジが 64~256 bit なのに対し，出力が 1 bit 程度であるためである．一方，メモリベースの PUF はチャレンジ空間が小さいという問題がある．また，単純な PUF は（イ）機械学習で出力を予測可能[4] でセキュリティ用途に使えない．さらに，PUF はノイズに弱く，暗号鍵生成に用いるにはに誤り訂正技術が必須だが，既存の（ウ）誤り訂正・鍵生成の手法は必ずしも効率的でない[5]．また，既存の PUF の応用研究[6]では，PUF 単体とシステムのプロトコルが別々に評価されており，（エ）実システム中に実装された PUF の挙動の評価は行われていない．ごく最近「疑似 PUF」と呼ばれる回路を搭載した FPGA が発表されたが（SmartFusion2，マイクロセミ社，発売時期や詳細は不明），メモリベースなためチャレンジ空間が小さい問題がある．さらに，誤り訂正・鍵生成回路の有無も不明で，高ノイズな実システム中での評価もされていない．

[1] A. Moradi 他，“On the Vulnerability of FPGA Bitstream Encryption against Power Analysis Attacks −Extracting Keys from Xilinx Virtex-II FPGAs,” Cryptology ePrint Archive, 2011.
[2] S. Skorobogatov and C. Woods, “Breakthrough Silicon Scanning Discovers Backdoors in Military Chip", CHES2012, pp.23-40, 2012.
[3] S. R. Pappu, "Physical One-Way Functions", PhD Thesis, MIT, 2001.
[4] U.Rührmail 他,"Modeling Attacks on Physical Unclonable Functions", CCS2010, pp.237-249, 2010.
[5] R. Maes 他，"PUFKY: A Fully Functional PUF-based Cryptographic Key Generator", CHES2012, pp.302-319, 2012.
[6] J. Guajardo 他,"FPGA Intrinsic PUFs and Their Use for IP Protection", CHES2007, pp.63-80, 2007.

２．研究の目的

本研究は，（1）高スループットで（2）機械学習困難な PUF を，（3）高効率な誤り訂正技術によって暗号鍵生成に利用し，これを動的再構成システムに応用することで（4）安全に FPGA の回路を構築する手法を確立するとともに（5）実システム中の PUF の性能を評価する．動的再構成システムを用いる理由は，回路構成データの保護のために暗号鍵生成が必須となることに加え，動的再構成による高ノイズ下での鍵生成のテストができるからである．申請者は既に，高スループットで機械学習攻撃に強い Pseudo-LFSR PUF (PL-PUF)を開発しており, (1)(2)は実現されている．これに加えて本研究では(3)~(5)を以下のように実施し，上述の(ア)~(エ)の問題が全て解決される．

(3) PL-PUF 単体だけでなく誤り訂正部を含めた鍵生成部（以下，PUF-KEY 回路）を開発し，その回路規模とスループットの既存研究に対する優位性を示す．

(4) PUF-KEY 回路をセキュリティの根源とし，動的再構成システム中で安全に回路構築ができるプロトコルを確立する．先進的攻撃の下でも安全に FPGA の回路が構築できる手法を確立する．
(5) ランダム性，安定性，ユニーク性等，システム動作中の PUF の性能を定量的に評価し，PUF-KEY 回路の実用性・有効性を実証する．

本研究では，回路面積当たりのスループットが最も高いPUF-KEY回路が実現できると想定される．また，世界で初めて，実システム中で動作検証されたPUF-KEY回路の学術報告が行われることになる． PUF-KEY は，様々な組込み機器・情報機器の高いセキュリティ要件を満たす重要な回路となる．また，先進的攻撃の下で FPGA 回路を安全に構築する手法が確立すれば，FPGA の採用機会の増えている産業界にとっても大変有意義である．さらに，動的再構成システムのセキュリティの懸念を払拭することで，専用回路を柔軟に切り替える高性能かつ多機能なシステムの開発が促進されると考えられる．

３．研究の方法

本研究では，動的再構成のアプリケーションとして，マルチ暗号プロセッサを採用する．上図は，本研究で開発する，PUF-KEY ベースのセキュアなマルチ暗号プロセッサのブロック図である．マルチ暗号プロセッサは，6 種類の共通鍵ブロック暗号（AES, Camellia, SEED, MISTY1, TDES, CAST128）を再構成モジュールとし，その回路構成情報をダウンロードしながら動的に構築する．

○平成 25 年度

２５年度は，(I) PUF-KEY 回路の開発と性能評価，(II) マルチ暗号プロセッサの開発と性能評価，を行う．本研究では PUF-KEY のみでなくマルチ暗号プロセッサも同時に実装する必要があるため，実装環境として 28-nm プロセスの大規模 FPGA を実装した SASEBO-GIII を使用する．デバイスのばらつきによってチップごとに異なる暗号カギを生成できることを確認するため，4 枚の SASEBO-GIII に PUF-KEY を実装し，ユニーク性等の性能を評価する．当該年度の成果として，PUF-KEY 回路の開発と評価に関して国際会議に論文１本を投稿できることを見込んでいる．

具体的には，以下のように作業を進める．

I) PUF-KEY 回路の開発と性能評価

(i) PL-PUF 単体の制御回路や通信プログラムを開発する．
(ii) PL-PUF 単体の安定性やユニーク性等の性能を評価する．これは，後に PUF-KEY における誤り訂正符号のパラメータ（符号長，情報ビット長，誤り訂正能力）を決定するためである．性能評価には申請者が過去に行ってきた手法が適用でき，また，PUF の研究を共同で進めている組織内の研究者にも意見を求めてゆく．
(iii) 誤り訂正部・鍵生成部を開発し，PL-PUF と統合して PUF-KEY 回路を構築する．誤り訂正符号として BCH 符号の使用を考えているが，LDPC 符号等についても検討したい．PL-PUF 単体の性能に応じ，誤り訂正符号のパラメータを調整する．誤り訂正・鍵生成については，符号理論の研究者と既に議論を行っており，高効率な鍵生成ができる目処が立っている．必要に応じ，当該研究者と議論を行いながら開発を進める．
(iv) 回路規模やスループット等の性能を評価する．

(II) マルチ暗号プロセッサの開発と性能評価

(i) 通信制御回路，動的再構成制御回路，通信プログラムを開発する．再構成モジュールであるブロック暗号回路は，既存資産を使用する．申請者は，過去に同様のシステムを開発した経験があり，本研究では実装対象（SASEBO-GIII）に合わせた改良を行う．
(ii) マルチ暗号プロセッサの回路規模とスループットを評価する．

○平成 26 年度

26 年度は，(III) 安全な回路構築プロトコルを開発し，それに基づいて (IV) PUF-KEY とマルチ暗号プロセッサを統合した動的再構成システムを構築するとともに，(V) システム中の PUF-KEY の性能評価を行う．当該年度の成果として，システム全体の評価に関して国際会議に１本，学術雑誌に１本の論文投稿を見込んでいる．また，開発されるシステムは新規性・実用性が高いと考えられるため，可能であれば積極的に特許を申請したい．

(III) 安全な回路構築プロトコルの開発

PUF-KEY 回路そのものの安全性を検証した後，PUF-KEY 回路をトラスト・ポイント（信頼できるセキュリティの根源）とする安全な回路構築プロトコルを開発する．

(IV) PUF-KEY とマルチ暗号プロセッサを統合した動的再構成システムの構築

(i) 上記(III)で開発したプロトコルに基づき，PUF-KEY，マルチ暗号プロセッサおよびそれらの制御回路や通信回路を開発し，統合する．
(ii) システム全体の回路規模およびスループットを評価する．

(V) システム中の PUF-KEY の性能評価

(i) 通信回路や動的再構成の制御回路等が動作している最中に PUF-KEY で鍵を生成し，その安定性，ユニーク性等の性能を評価する．

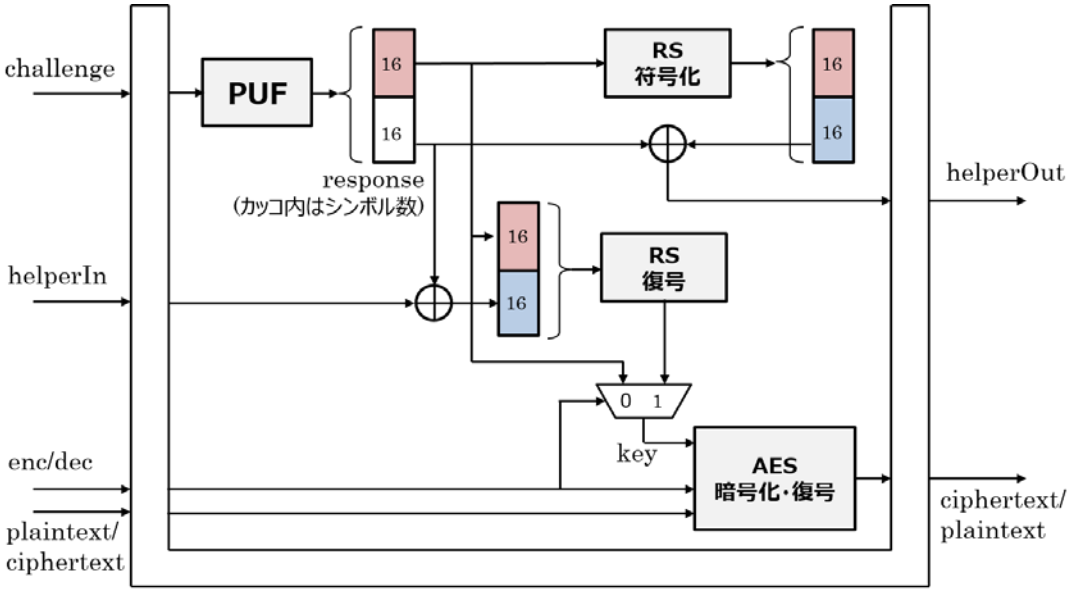

図 1　Fuzzy Extractor を用いた安全な動的部分再構成回路の概観

(ii) 性能評価の結果に応じ，必要があれば誤り訂正符号のパラメータを再調整する．
(iii) パラメータの再調整を行った場合は，新たに誤り訂正部を開発し，再度 PUF-KEY の性能評価を行う．

なお，システム動作中の PUF-KEY の性能が予想以上に悪く，動的再構成システムへの応用が困難となる等の問題が考えられる．その場合，動的再構成のアプリケーションとして，よりノイズの少ないもの（加算・減算等の演算器の切り替えなど）に変更する．

それでも動作しない場合は，PUF-KEY 回路単体を様々なデバイスに実装して比較評価するような研究に変更する．SASEBO-GIII には 28-nm という最先端のプロセスを利用した FPGA が搭載されているが，本提案書の申請時には 28-nm FPGA を用いた PUF の研究報告はなく，本研究期間にもそれほど多くの研究報告は出ないと考えられる．申請者は，45-nm や 65-nm 等の FPGA を搭載するボードも有しており，半導体プロセスの違いによる PUF-KEY 回路の性能比較ができる．このような比較実験も非常に学術的価値の高い研究である．

４．研究成果

（１）SASEBO-GIII 上の Kintex-７FPGA 上に Arbiter PUF，Fuzzy Extractor，AES から成る PUF-KEY 回路を実装した．Arbiter PUF は過去に開発したものを，AES は東北大学の暗号ハードウェアプロジェクトで公開されているものを利用した．Fuzzy Extractor は，本研究の中で Matlab HDL Coder を主に利用して開発した．これら要素回路を含むシステムとして PUF-KEY を動作させることに成功した．以下で詳細について述べる．

（２）今回実装した．Fuzzy Extractor の誤り訂正符号には Reed-Solomon 符号を使用し，1 シンボルを 8 ビット，符号語を 255 シンボル，情報長を 239 シンボルとした．ただし，RS 符号化を適用するのは 128 ビット（=16 シンボル）の暗号鍵であるので，実際には (32,16)短縮 RS 符号となる.図 1 に PUF-KEY 回路のブロック図を示す.

Fuzzy Extractor の主要構成要素である Reed-Solomon(RS)符号化器および復号器の回路開発は，Matlab/Simulink HDL Coder を用いた高位合成により行った．回路の論理合成，配置配線および回路構成情報の生成には，Xilinx ISE14.7 を使用した．実装対象 FPGA は，SASEBO-G3 に搭載されている Xilinx Kintex-7 XC7K160T FBG676 である．

表 1 に，PUF-KEY 回路全体と，各構成要素である RS 符号化器，RS 復号器，AES 回路のハードウェア使用量（使用 Slice 数，ルックアップテーブル(LUT)数，フリップフロップ(FF)数）および動作周波数を示す．また，各構成要素回路は処理に要するクロック数も示した．

（３）SASEBO-G3 を 3 枚使用し，それぞれに実装された PUF から異なる鍵が生成されることを確認した．また，PUF のチャレンジ・レスポンス・ペア(CPR)を大量に収集し，再現性やユニーク性を評価するとともに，回路規模についても評価を行った．実験では，FPGA 上の Arbiter PUF のユニーク性が低い場合に，ある PUF によって生成された鍵を他の PUF が復元できることも示された．以下で実験方法とその結果について説明する．

PUF-KEY を用いたシステムでは，予め PUF のチャレンジ・レスポンスのデータセットおよび鍵を復元するための補助データを収集する「Enrollment」のフェーズと，PUF と補

表 1　PUF-KEY 回路のハードウェアリソース使用量

	Slice	LUT	FF	Block RAM	動作周波数 [MHz]	所要クロック数
Arbiter PUF	34	134	2	0	-	(1bit あたり) 8
RS 符号化	95	196	258	0	554.5	33
RS 復号	1,371	4,795	2,151	1	93.8	560
AES 暗号化・復号	2,435	4,795	796	0	203.2	15(暗号化) / 26(復号)
全体	3,240	5,109	10,319	3	91.9	-

助データから鍵を復元する「Verification」のフェーズがある．以下に，PUF-KEY における鍵生成と復元の手順を示す．

[Enrollment]

1. 特定のチャレンジセットを用いて PUF をアクセスし 256 ビットのレスポンスを入手する．使用したチャレンジはデータベース（DB）に格納する．
2. レスポンスの上位 128 ビット（=16 シンボル）を秘密鍵とする．秘密鍵を誤り訂正符号により符号化する．
3. 符号化により得られた 16 シンボルのシンドロームをレスポンスの下位 128 ビットでマスクし，これを鍵復元のための「補助データ（helper data)」として DB に格納する．

[Verification]

4. DB からチャレンジセットを取り出し，これを用いて PUF をアクセスし 256 ビットのレスポンスを得る．
5. DB から helper data を取り出し，レスポンスの下位 128 ビットによって補助データのマスクを外し，シンドロームを復元する．
6. レスポンスの上位 128 ビットとシンドロームを結合して 32 シンボルを得る．これに誤り訂正符号の復号処理を行い，鍵を復元する．

以下では，3 枚の SASEBO-G3 上の PUF をそれぞれ PUF1，PUF2，PUF3 とする．

まず Enrollment では，上記の手順に従い PUF1～PUF3 に同一のチャレンジを与えて暗号鍵を生成し，それぞれ暗号文 1～3 と補助データ 1～3 を得る．この時得られた鍵，暗号文，補助データは，それぞれの PUF で異なることが確認された．

次に Verification では，再度 PUF1～3 を用いてレスポンスを生成し，対応する補助データ 1～3 を用いてそれぞれ鍵を復元する．この鍵を用いて，それぞれの暗号文が元の平文に戻ることが確認された．また，例えば PUF1 によって復元された鍵では暗号文 2 や 3 は復号できないことが確認された．

ただし，PUF1 のレスポンスに，補助データ 2 を組み合わせたところ，PUF1 によって暗号文 2 が復号できることが確認された．これは，Arbiter PUF のユニーク性が低いため，誤り訂正によって同一の鍵が生成されてしまったためである．ゆえに本システムのセキュリティを確保するためには，補助データを隠蔽する必要がある．

以上より，PUF と Fuzzy Extractor を用いた PUF-KEY 回路は FPGA 上に実装され，正しく動作していることが確認された．ただし，ユニーク性の低い Arbiter PUF を用いたことで，セキュリティが低下することとなった．これは，FPGA 上でもユニーク性が高いことが確認されている Pseudo Linear Feedback Register PUF (PL-PUF)を用いることによって解決されると考えられる．

本研究では動的再構成システムの構築には至らなかった．これは，RS 符号化・復号回路の開発に想定以上の期間を要したためである．しかし，PUF-KEY が回路化されて複数の FPGA ボード上で動作確認できたことから，あとわずかな作業で動的再構成システムとして完成できる見込みである．今後，FPGA 上の PUF のユニーク性向上方法や Fuzzy Extractor の効率の用意構成方法について検討するとともに，動的再構成システムの完成を目指す．

５．主な発表論文等

〔学会発表〕（計 1 件）

堀洋平，片下敏宏：“PUF と Fuzzy Extractor を用いた暗号鍵生成回路の SASEBO-G3 への実装”，電子情報通信学会 RECONF 研究会，2015 年 6 月 20 日，京都大学百周年時計台記念館（京都府・京都市）．

６．研究組織

(1)研究代表者

堀　洋平（HORI, Yohei）
独立行政法人産業技術総合研究所・セキュアシステム研究部門・主任研究員
研究者番号：60530368