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　元 年　 ６ 月 １４ 日現在

機関番号：３４３１５
研究種目：基盤研究(C)（一般）
研究期間：2016～2018
課題番号：１６Ｋ０６３２３

研究課題名（和文）半導体センサのばらつきを利用して捏造できない画像・映像を得る手法の研究

研究課題名（英文）Research to obtain pictures and videos that can not be forged using variations of semiconductor sensors

研究代表者

白畑　正芳（Shirahata, Masayoshi）

立命館大学・総合科学技術研究機構・准教授

研究者番号：７０７５５８５０

交付決定額（研究期間全体）：（直接経費）　　3,800,000円

研究成果の概要（和文）：　半導体センサのばらつきを利用して捏造できない画像・映像を得る手法の研究を行った。CMOSイメージセンサの画素毎に存在するソースフォロワートランジスタの特性ばらつきに注目し、ばらつき抽出する方法及び、偏りのない1/0列を生成する方法を提案した。実際の2M画素CMOSイメージ(CIS)センサからばらつき抽出、1/0生成を行いPUF(Physical Unclonable Function)としての評価を行い、PUFとして良好な出力が得られることを確認した。PUFの利用として、チャレンジ&レスポンス(C&R)認証のための空間拡大の検討、鍵利用を想定した鍵再生成の効率化の提案を行った。

研究成果の学術的意義や社会的意義
CMOSイメージセンサの特性ばらつきに注目し、これを利用して個々のセンサの固有の値を抽出することを可能にした。これまでのCMOSイメージセンサは画像を綺麗にするため、特性ばらつきをキャンセルして用いてきたが、回路動作の工夫で固有ばらつきを抽出し、再現性よく、かつ個体ごとにユニーク性のある固有値が抽出できた。
抽出された固有の値を用いてセンサ自体が本物かどうかの判定が容易に行える。またセンサごとの鍵を安定に生成することができ、これを用いて画像・映像を暗号化したり、改ざんが行われているかどうかの検出が可能となる。

研究成果の概要（英文）：　We researched the method to obtain pictures and videos which can not be forged using variations of semiconductor sensors. Focusing on the characteristic variations of the source follower transistors that exist for each pixel of the CMOS image sensor, we proposed a method of extracting the variations and a method of generating unbiased 1/0 data. From actual CMOS Image Sensors, variation extraction and 1/0 data generation were performed.It confirmed that a good output was obtained as PUF(Physical Unclonable Function).As the use of PUF, we examined space expansion for challenge and response (C & R) authentication, and proposed the efficiency improvement of the key regeneration that assumed the key use.

研究分野：半導体

キーワード：CMOSイメージセンサ　PUF　ばらつき　鍵再生成　軟判定　多ビット化

様　式　C－１９、F－１９－１、Z－１９、CK－１９（共通）

１．研究開始当初の背景

電子・情報機器の発達により監視カメラやカメラ機能搭載の携帯端末が普及し、様々な映像・画像がインターネット上に掲載され事実として捉えられる時代となった。また映像・画像が証拠として用いられる機会が増えている。一方、パソコンの高性能化・普及により、画像・映像の改ざんを精密に行うことも容易となり、送信されてきた画像・映像が本物かどうかを検証することが重要になっている。

２．研究の目的

本研究ではカメラの心臓部である半導体センサに注目し、センサの特性ばらつきを活用し、セキュリティ分野で用いられる PUF(Physical Unclonable Function)技術を応用して捏造できない画像・映像を得る手法を開発する。

３．研究の方法

半導体センサのばらつきを活用して鍵生成を行い、その鍵を用いて暗号技術による捏造できない画像・映像を得るようにする。キーとなる技術は如何にばらつきを取得するか、そしてそのばらつきから鍵の元となる素性のいいランダムデータが得られるかである。シミュレーションによる半導体センサの動作モード変更によるばらつきデータ取得可否の検討、及び実際の CMOS イメージセンサを用いた実データの取得と、そこからランダムデータが得られるかの検討を行う。

４．研究成果

(1)ばらつきデータ取得

①シミュレーション検討

CMOS イメージセンサ(以下、CIS と記述)では綺麗な画像を取得するために CDS(Correlated Double Sampling:相関二重サンプリング)によってノイズを除去している。CIS はアレイで構成された画素を持ち、画素ごとにフォトダイオードと次段に電圧を伝えるためのソースフォロワトランジスタ(以下 SF Tr.と記述)を搭載している。Tr.は製造加工によるばらつきや不純物ばらつきのため、必ず特性ばらつきを伴い画素ばらつきとなるが、CDS により除去されている。本研究ではこの画素ばらつきに注目した。シミュレーションを用いて CDS をしない場合、出力に画素ばらつきが反映されるか計算した。計算結果を図１に示す。左が CDS 有、右が CDS 無の結果を示している。計算結果より CDS 無だと SF Tr.の特性ばらつきが画素ばらつきとして出力に現れることを原理的に確認できた。

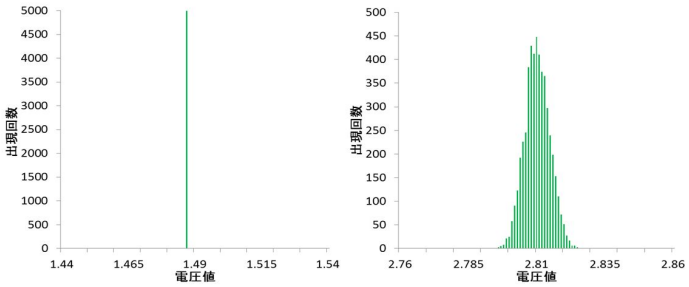


図１ シミュレーションによる出力分布

②実測結果

シミュレーション結果を受け、実物の CIS を用いて CDS なしの出力データを取得した。類似研究があるが(引用文献①)規模の小さい画素数までで、実用レベルの多画素で評価したのは我々が最初になる。実物の CIS チップ及び CDS なしのシーケンス設定には協力関係にある CIS 設計・製造会社の協力をいただいた。ばらつき取得のためのシーケンスを説明する。通常の CDS では同一 SF Tr.からの出力データを二度取り込む。一度目はリセットされた状態、二度目は光で発生した電荷により電位変動した状態。この二度取り込んだ出力の差分を取ることにより、ノイズと SF Tr.自身の特性ばらつきがキャンセルされる。特性ばらつき取得のための変更は一度目に基準となる電位を取り込み、二度目に SF Tr.の出力データを取り込む。この差分により SF Tr.自身の特性ばらつきが残ることになる。光による信号の影響を排除するためにリセットスイッチを常時 ON にした状態で信号を取り込む。これにより、光の有り/無しにかかわらず SF Tr.の特性ばらつきのみが出力され再現性向上が期待できる。出力結果は AD コンバーターによりデジタル出力で得られる。出力結果を図 2 に示す。赤が CDS 有、青が CDS 無のデータを示している。CDS 無でばらつきが出力されていることがわかる。

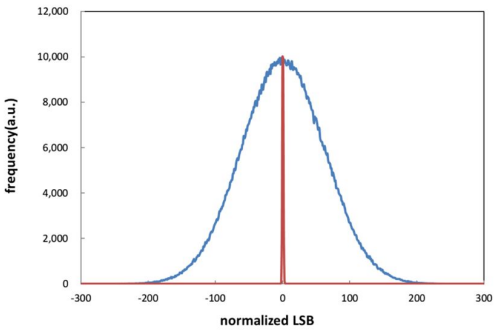
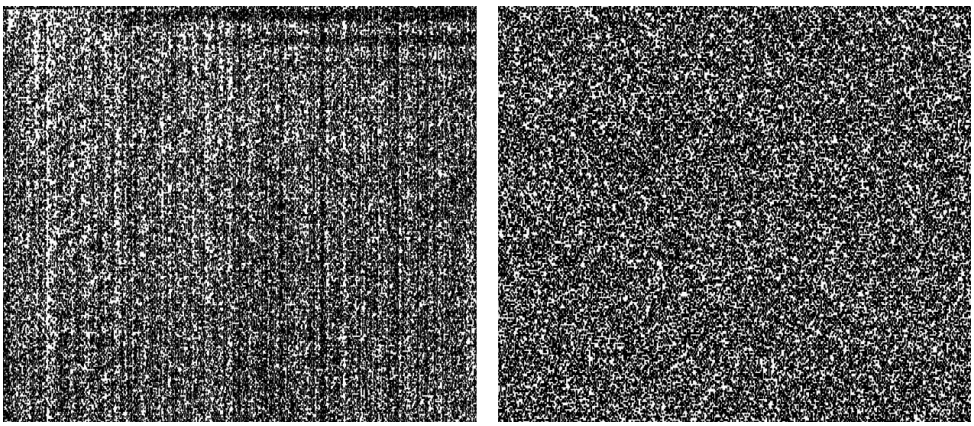


図２ 実測による出力分布

(2)ランダムデータ生成手法検討

評価した CIS の AD コンバーターは 12bit を用いており、4,096 階調のデジタル値で主力が

得られる。このデジタル出力値からランダム性の良い 1/0 データを生成する手法を考案した。単純には全データの中央値との大小関係で 1/0 を割り振ることが考えられる。しかしこの場合、列ごとに存在する AD コンバーターの特性偏り(縦筋と言われる)や、SF Tr.のグローバルばらつきが反映されてしまう。そのため隣接する上下の出力の大小関係より 1/0 を割り振る方法を考案した。これにより縦筋やグローバルばらつきがキャンセルされ偏りのない 1/0 データが生成できる。その様子を図 3 に示す。1/0 を黒/白ドットとした模様を示す。(a)は中央値からの大小比較で 1/0 を付与したもの。(b)は隣接上下の大小比較で 1/0 を付与したもの。(a)では明らかに縦筋が見られ、右上にも模様があり 1/0 に偏りがあることがわかる。(b)は(a)に比べランダムに分布しているのがわかる。ランダム性評価のため一般的に用いられている NIST 検定も行い良好な結果を得た。



(a) 中央値からの大小比較　　(b) 隣接上下での大小比較

図 3　生成方法違いによる 1/0 分布の様子

(3)PUF としての基本性能評価

CIS のばらつきデータ取得及び 1/0 データ生成ができたので、次に PUF としての性能評価を行った。理想の PUF は個体ごとに相関のない固有のデータを出力する。これの評価指標としてユニーク性、再現性が広く用いられている。

①ユニーク性、再現性

評価した CIS は 2 画素共有型フル HD 仕様のため 1M 個の SF Tr.ばらつきデータが得られ、今回の手法では 0.5Mbit の 1/0 データが生成される。これを 128bit ずつに区切り、18 個の CIS チップ、1 チップあたり 100 回の PUF 出力値を取得してユニーク性、再現性を評価した。その結果を図 4 に示す。ユニーク性に関しては無相関の理想値に近い値を示している。再現性に関しては反転ビット率に直すと 0.86%で、これまで提案されている他の半導体 PUF の再現性(反転ビット率 ～30%)と比べると優秀な値であると言える。

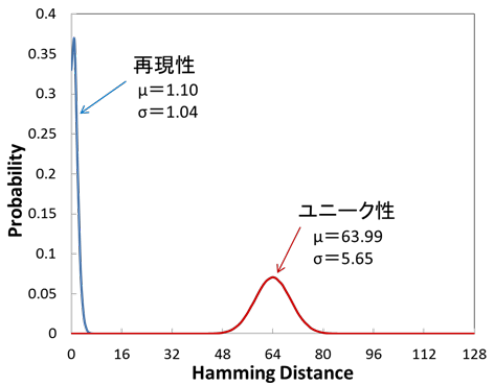


図 4 再現性、ユニーク性(128bit)

②温度・電圧依存性

再現性に関して温度変動、電圧変動を考慮したデータも評価した。電圧は中心から±0.2V、温度は 0℃と 60℃で測定した。評価結果を図 5 に示す。平均ハミングディスタンスは中心条件 1.1 ビットから 2.1 ビット(反転ビット率は 1.62%)まで上がるが性能を大きく落とすことはなく実用に耐えうる範囲と言える。

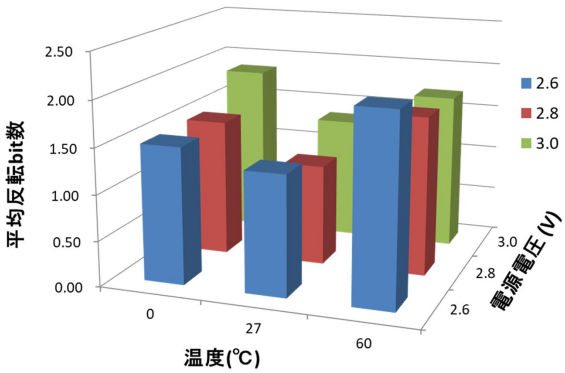


図 5 再現性の温度・電圧依存性

(4)CIS の PUF 機能を用いたセキュリティ

CIS を用いた PUF としての性能評価が良好であることを踏まえ、これを用いたセキュリティへの応用研究を行った。センサの真贋性、データの真正性保証を前提にセキュリティで一般的に用いられる手法を用いる場合、本研

究の CIS を用いた PUF の特徴を生かす研究を行った。

①真贋性(C&R 認証と LG 法による多ビット化)

画像を送信してくるセンサ自身が本物であるかの真贋性を保証する手段として C&R(Challenge & Response)認証が用いられる。これはセンサから出力される PUF データを事前に認証相手に登録しておき、認証のたびにデータの一部を抜き出し照合するもので、データは使い捨てとなるので認証回数を確保するためには PUF データ数(C&R 空間)が多いほどよい。一方で CIS を用いた PUF は SRAM PUF などと同様に搭載素子数により C&R 空間が制限され、これを広げる工夫が必要となる。CIS を用いた PUF ではばらつき出力が 1 か 0 ではなく値(階調)をもっているため、その値の順位づけにより情報量を増やすことができる。これは Lehmer 符号と呼ばれる。Lehmer 符号を用いた情報量を増やす手法はリングオシレーターPUF で検討されており、同様の手法を CIS PUF にも用いた。順位付けするために束ねる出力数を N とすると N=2 がこれまでの上下比較で 1/0 を付与する方法に相当し、N を増やすと順位付けできる場合の数が増えるため扱える情報量が log2 (N!) ビットと増える。

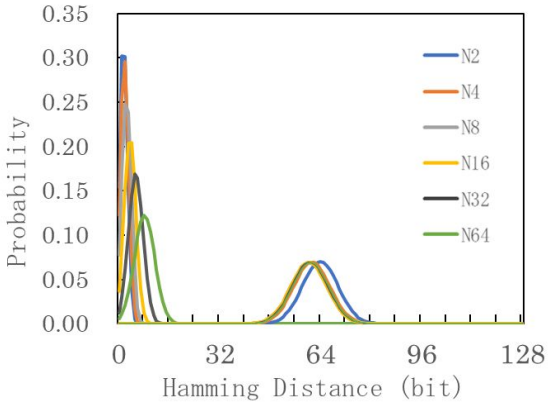


図 6 多ビット化でのユニーク性、再現性

N を増やした場合のユニーク性と再現性を図 6 に示す。扱えるビット数は増えるが、割り付けで出現しないコードが存在するためユニーク性が N=2 より落ちる。また複数の出力値に対する大小比較の順位付けのためにノイズの影響を受けやすくなり再現性の低下も見られる。次にビット数の増加に対し、ユニーク性、再現性の低下のトレードオフで正味の効果があるかどうかを見るために、ユニーク性、再現性を積分することにより、FPR(False Positive Rate:偽物を本物と認識する確率)、FNR(False Negative Rate:本物を偽物と認識する確率)を求めた。そのグラフを図 7 に示す。これによると例えば誤認識の確率を 0.001ppm 以下にする場合、FPR と FNR が交わらない N=32 まで使用可能となる。この時のビットの増加は 8 倍となり多ビット化に効果のあることがわかる。

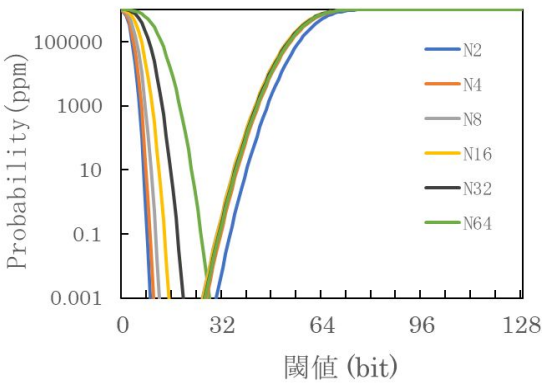


図 7 多ビット化での FPR, FNR

②真正性(MAC 生成による鍵再生成の効率化)

データが改ざんされていないことを保証する手段として MAC(Message Authentication Code)認証が用いられる。事前に共有する秘密鍵をお互いに持った上で、データと秘密鍵で認証コードを生成してデータとセットで相手に送るものである。受け取った側は送られたデータと共有している秘密鍵で認証コードを別途生成し、相手から送られてきた認証コードと比較し、一致すれば改ざんされていないことが保証される。今回の場合、秘密鍵に PUF を利用するが鍵再生成の時にエラー訂正が必要になる。このエラー訂正は誤り訂正符号を用いることにより実現される。誤り訂正の原理は誤りの含まれる符号から一番ハミング距離の近い正規の符号に寄せるものである。エラービットが多い場合、正規の符号に寄せても正しい符号ではない場合が生じ、訂正能力にも限界がある。正規符号間の最小ハミングディスタンスでエラー訂正能力が変わる。そのため冗長度の多い符号を用いると訂正能力が上がるが扱う情報ビットを多く用いなければならないデメリットがある。これを改善するために符号の各ビットに反転の起こし難さの信頼度を付与する軟判定という手法が

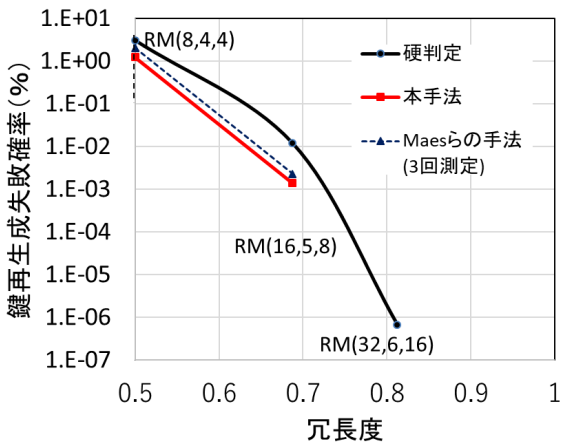


図 8 各判定方法による鍵再生成の比較

提案されている。通常の PUF では軟判定を行うために PUF の同じ出力を複数回取得してビットエラーの起こしやすさを各ビットに付与して訂正能力を向上させる手法が Maes 等(引用文献②)により提案されている。これに対し CIS を用いた PUF では bit 生成時に用いる二つの出力の差からビットエラーの起こしやすさを統計的に推定できる。これを活かして複数回の PUF 出力取得の手間を省いて軟判定によるエラー訂正能力の向上が期待できる。

誤り訂正符号としてリード・マラー符号 RM(n,k,d)(n:符号長、k:情報ビット長、d:最小ハミングディスタンス)を用い、軟判定でない従来法(硬判定)、従来の軟判定(繰り返し測定数 3 回)、CIS PUF の軟判定での鍵再生失敗確率を計算した。RM(8,4,4)、 RM(16,5,8)、RM(32,6,16)と冗長度を増やした場合に鍵生成に失敗する確率を計算している。結果を図 8 に示す。横軸の冗長度は k/n を示している。軟判定で RM(32,6,16)を用いると今回評価した範囲では全て鍵生成に成功したため失敗確率を求められていない。図より明らかなように硬判定より鍵再生成の失敗確率が下がり、CIS PUF の場合は 1 回の PUF 測定に関わらず 3 回測定の従来の軟判定と同等以上の性能がある。

(5)まとめと今後の展望

以下、研究成果をまとめる。

・CMOS イメージセンサ(CIS)の画素ばらつきに注目し、それを取り出す方法を提案した。
・取得した画素ばらつきからランダム性の高い 1/0 データ生成方法を提案した。
・実際の CIS を用いて 1/0 データを生成しランダム性が高いことを確認した。また PUF の基本性能としてユニーク性、再現性を評価し、従来の半導体 PUF に劣らぬ性能を確認した。
・Challenge & Response 認証を想定した多ビット化や、MAC 認証を想定した鍵再生成の高効率化について CIS PUF の特徴を生かした提案を行い、効果のあることを確認した。

今後の展望としては CIS の PUF 機能を用いて暗号化することによりセキュリティの高い画像・映像となることが期待される。さらなる実用・普及に向けて進めるためには CIS の画像生成シーケンスに沿した効率のよい暗号化手法の研究が必要と考えられる。

＜引用文献＞

①Y.Cao et al.,“CMOS image sensor based physical unclonable function for coherent sensor-level authentication,“IEEE Trans. Circuits Syst. I, vol.62, No.11, Nov. 2015
②R.Maes, P.Tuyls, and I.Verbauwhede,“Low-Overhead Implementation of a Soft Decision Helper Data Algorithm for SRAM PUFs,” CHES 2009, pp.332-347, 2009

５．主な発表論文等

〔学会発表〕（計　15 件）

① 一色良太、白畑正芳、大倉俊介、汐崎充、藤野毅　他、CMOS イメージセンサの画素ばらつきを活用した PUF(CIS-PUF)の誤り訂正手法の検討、電子情報通信学会　ハードウェアセキュリティ研究会(HWS)、2019
② S.Okura, R.Ishiki, M.Shirahata, M.Shiozaki, T.Fujino et.al.、A Dynamic Soft Decistion Fuzzy Extractor for a CMOS Image Sensor PUF、2018 International Symposium on Intelligent Signal Processing and Communication Systems、2018
③ M.Shirahata, S.Okura, M.Shiozaki and T.Fujino et.al.、A Proposal of Efficient Error Recovery Method Utilizing Output Characteristics of CMOS Image Sensor PUF、Conference on Cryptographic Hardware and Embedded Systems、2018
④ 井上栞、白畑正芳、大倉俊介、汐崎充、藤野毅　他、CMOS イメージセンサの特性ばらつきを利用した PUF(CIS-PUF)の Challenge & Response 認証の検討、暗号と情報セキュリティシンポジウム、2018
⑤ 白畑正芳、大倉俊介、汐崎充、藤野毅　他、複製不可能デバイスを活用した IoT ハードウェアセキュリティ基盤の研究開発、平成 29 年電気関係学会関西連合大会(招待講演)、2017
⑥ S.Okura, M.Shirahata, M.Shiozaki, T.Fujino et.al.、A Proposal of PUF Utilizing Pixel Variations in the CMOS Image Sensor、Image Sensor Workshop 2017、2017
⑦ 大倉俊介、名倉優輝、白畑正芳、汐崎充、藤野毅　他、CMOS イメージセンサの画素ばらつきを活用した PUF(CIS-PUF)の提案(1)　―基本コンセプトとシミュレーション検討―、暗号と情報セキュリティシンポジウム、2017
⑧ 名倉優輝、大倉俊介、白畑正芳、汐崎充、藤野毅　他、CMOS イメージセンサの画素ばらつきを活用した PUF(CIS-PUF)の提案(1)　―実データによる PUF 性能評価―、暗号と情報セキュリティシンポジウム、2017

〔産業財産権〕

○出願状況（計　5 件）

名称：個体撮像装置、個体撮像装置の駆動方法、および電子機器
発明者：大倉俊介、白畑正芳、汐崎充、藤野毅　他
権利者：ブリルニクスジャパン(株)、学校法人立命館

種類：特許
番号：特願 2019-039240
出願年：2019 年
国内外の別： 国内

名称カメラシステム及びカメラシステムの駆動方法
発明者：大倉俊介、白畑正芳、汐崎充、藤野毅　他
権利者：ブリルニクスジャパン(株)、学校法人立命館
種類：特許
番号：特願 2018-212194
出願年：2018 年
国内外の別： 国内

６．研究組織
(1)研究協力者
研究協力者氏名：藤野　毅
ローマ字氏名：(FUJINO, takeshi)

研究協力者氏名：汐崎　充
ローマ字氏名：(SHIOZAKI, mitsuru)

研究協力者氏名：大倉　俊介
ローマ字氏名：(OKURA, shunsuke)