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 １２ 日現在

機関番号：５２６０１
研究種目：基盤研究(C)（一般）
研究期間：2019～2021
課題番号：１９Ｋ１１９７７

研究課題名（和文）アナログ部品に対する物理的クローン不可関数の発見

研究課題名（英文）Physical Unclonable Functions Using Analog Circuit

研究代表者
姜　玄浩（Kang, Hyunho）

東京工業高等専門学校・電子工学科・准教授

研究者番号：４０５０９２０４

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：ハードウェアの指紋のような，物理的クローン不可関数を発見する研究として，1番目の成果は，アナログ部品から物理的クローン不可関数が発見できたことである．２番目の成果は，高校・高専・大学などの電子回路実験でよく使用されるアナログ部品から最先端技術と認識される物理的クローン不可関数が発見できる実験ができたことである．今回のアプローチは，ブレッドボード上に組んだもの全体を一つの物理的クローン不可関数として扱って実験可能なので，学校の実験授業でも教えやすい作りになっていることで，革新的な実験テーマになることを確信している．

研究成果の学術的意義や社会的意義
現在までに研究された電子的特性を利用した物理的クローン不可関数(Physical Unclonable Function，以下PUF)の多くはSRAM PUFと呼ばれるメモリを利用したものやFPGA（Field-Programmable Gate Array）の内部の細かい特性によるデジタル的な変化を特徴として利用しているものが主であった．そこでPUF製造が目的ではなかったアナログ部品から固有の信号を取り出すことで，固有のトークン製造コストを極端に低くすることが可能であり，このような研究アプローチは学術的・社会的に非常に価値があると考える．

研究成果の概要（英文）：As a study to discover physical unclonable functions (PUFs) such as hardware fingerprints, the first result was the discovery of physical unclonable functions in analog components. The second achievement is that students were able to experience state-of-the-art research experiments in electronic circuit experiments conducted in high schools, KOSEN and universities.
In other words, this study proposes a PUF that uses analog devices. Because many IoT devices contain many analog elements, we assume it is possible to create a PUF for each device individually. Our research on analog PUFs proposes four types of circuits, one is to use a resistor matrix circuit and it is also suggested to use a Hartley oscillator circuit, a wien bridge oscillator circuit and an astable multivibrator circuit.

研究分野：情報セキュリティ，機械学習

キーワード：物理的クローン不可関数　アナログ部品　PUF

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９（共通）

１．研究開始当初の背景

物理的クローン不可関数の技術に関する研究は，個々人で異なる人間の指紋を利用するバイオメトリクス認証と同様に，個々の物理的特性を指紋のように利用して暗号・認証機能を実現しようという目的として発展してきた．

この概念が世の中に初めて認識されたのは 2001 年マサチューセッツ工科大学(以下，MIT)の博士論文と 2002 年 Science 誌発表からである．概念としてレーザー光をプラスチックのようなトークンに角度ごとに投影することで物理的クローン不可のパターンが生成されることを示し，強力な暗号・認証機能が実現できる可能性を開いた．その後，より実用的な物理的クローン不可関数の特徴をシリコンチップの特徴から抽出する研究が 2004 年 MIT 修士論文で発表された．つまり，IC チップの製造工程にて発生する，シリコンの結晶パターンなどによる個体差を，デジタル情報に変換し，IC チップを識別する技術である．同じ回路を持つ半導体でも，信号の遅延は少しずつ異なるので，同じウエハーから取れるチップであっても，不純物の状態は少しずつ異なるため，個体ごとに異なる値になることを示した．実際にこの MIT グループは遅延の特許を持ち，Verayo 社を創設し，商品化にも成功している．

２．研究の目的

本研究では，ハードウェアの指紋のような，物理的クローン不可関数(Physical Unclonable Function，以下 PUF という)を発見する研究として，これまでに例のないアナログ回路の各部品からのアプローチを目的としている．一般的にこの技術は，模造や複製ができないので，偽造防止のために製品を明確に特定する用途に使用できる．

本研究は以下のような特徴を有する．

①現在はマイクロチップに内蔵されて利用することが主流となっているが，固有のトークン製造が目的ではなかったアナログ部品から固有の信号を取り出すことで，固有のトークン製造コストを極端に低くすることが可能である．

②高校・高専・大学などの電子回路実験でよく使用されるアナログ部品から最先端技術と認識される物理的クローン不可関数が発見できることは極めて魅力的な教育実験であると言える．

３．研究の方法

１番目の目的を達成するため，対象となるアナログ部品が再現性とユニーク性を持つような仕組みを考案し，理論的・実験的観点から明らかにする．最初の一歩はチャレンジ・レスポンスシステムで実現できる．PUF（アナログ部品）に与えられたチャレンジ信号に対してレスポンスを出力することで，他の PUF では表せないばらつき信号（ノイズのような信号）を抽出することが考えられる．抽出された信号に対しては，基本的にバイオメトリクスで評価する尺度で PUF としての可能性は判断できる．つまり，再現性とユニーク性がどこまで理想的な結果に近づいているかを解析する．特に，本研究では一般的なデータの特徴解析の手法に加えて機械学習と深層学習を用い解析した場合においても検証を行った．

２番目の目的を達成するため，高校・高専・大学などの電子回路実験でよく使用されるアナログ部品から最先端技術と認識される物理的クローン不可関数が発見できるようにブレッドボード上に回路を複数個作成し，授業中に PUF の特性解析ができるようにした．本研究代表者は例

のないアナログ回路の各部品から PUF の特徴を発見する仕組みを学校の実験で実現することを提案した．例えば，Hartley 発振器を用いた PUF の実験例を簡単に説明すると下記となる．

① ブレッドボード上に該当回路を作成したものを 5 個用意する．なお素子値はすべて同じ素子値を用いてそれぞれの回路を構成する．

② 印加電圧としてオペアンプの電源は±5V, Hartley 発振回路の電源は 1V とする．

③ オペアンプの出力信号について Picoscope から PC に接続し Python により自動的にデータを取得する．データは各 PUF につき 1000 回ごと測定を行い，1 回の測定は 10000plot(サンプリングレート:16μs, 分解能:16bit)とする．またアナログ素子は温度によって特性が変化してしまうため周囲温度を 28℃一定にして測定を行う．

④ 測定データの処理方法としては細かい事前処理を行い固有識別コード(32000bit)を生成する．処理を行ったデータについて HD(Hamming Distance)を計算することで評価を行う．

⑤ 他の評価方法として，出力信号について機械学習・深層学習を用いて識別を行うことも検証の手法として導入する．結果として，非常に高い精度で識別可能であることが確認できた．

４．研究成果

本研究の重要な研究成果は PUF の発見において未発展なアナログ素子に注目し，PUF の特徴が発見できたことである．大きく四つに分けて説明する．

(1) 最初の一歩は抵抗に電圧を印加し，その抵抗の電圧降下を測定することによって個体を識別するアプローチであった．抵抗値の誤差を用いた測定手法を検証するため，6x2 の直並列接続してある抵抗計 12 本について同時に電圧降下を測定した．その得られた値から固有識別コードを作成しそれぞれの PUF 同士で HD を計算し，認証する手法を考えた．なお固有識別コードは，測定されたデータ内の最小値を 0 とした値に変換し，印加電圧に応じて数値の割り振り幅を変化させた．バイナリーコード化及びグレーコード化し，12 個の値を一つに結合し，一つの識別コードを作成した．

(2) 次は Hartley 発振器を用いた PUF の発見として，Hartley 発振器とオペアンプの反転増幅回路の組み合わせ回路についての検証を行った．これは Hartley 発振器の信号を増幅度 1 に設定したオペアンプにより増幅する回路を 1 つの PUF とする． なお回路によって出力される信号から固有識別コードを作成することによりそれぞれの PUF 同士で HD を計算し，個体識別を行うといった手法である．
もう一度整理して，Hartley 発振器を用いた PUF の検証ではデジタル値を用い識別を行う手法を検証した． その結果， 使用するデータを選択した場合について PUF としての利用ができる結果を得ることができた． この結果からアナログ回路から出力される周期信号を基にする個体識別コードはこの手法にて解析が可能である可能性を示したことになる．しかし， 周囲環境の変化やチャレンジの概念を導入していない点を検証できなかったため再度実験を行い解析する必要があるといえる．

(3) 現在までに研究されたアナログ PUF は， 各レスポンス同士で HD をとることによって PUF を検証されてきた．次の提案として，無安定 multivibrator の出力信号であるレスポンスを変形したのち HD をとる手法および回路から出力されたレスポンスであるアナログ信号についてその特徴量を機械学習にて識別する手法について比較し検証を行った． 機械学習にて解析する手法のメリットとして， デジタル値ではなくアナログ値を扱えるというメリットがある． これは， アナログ値からデジタル値に変更する過程で生じるデータの損失が PUF の特徴を損失してしまっている可能性があるからである．特に機械学習と深層学習にて解析する手法については無安定 multivibrator と Wien bridge 発振回路を対象に検証を行った．
もう一度整理して，無安定 multivibrator を用いた PUF の検証では，デジタル値およびアナログ値から得た特徴量から PUF を検証する手法を試みた． デジタル値を用いる手法では 2 パターンの処理をバイナリーコードとグレーコードで検証を行った． 両手法とも個体識別ができる結果にはならなかったもののグレーコードにて解析を行った結果についてのほうが PUF としての性能が高かったことからアナログ回路から個体識別を行う際はグレーコード化するべきであることが分かった． PUF としての性能は完璧ではないもののどこかに閾値を与えることによって個体の認識ができるといえる．
デジタル値を用いる手法では特徴量と生データの両方を用いたデータにおいて機械学習にて 99.7%， 深層学習にて 98.9%という識別精度を達成することができた．機械学習を用いた手法は個体識別できる精度であるといえることから PUF としての性能を満たしていることが分かった． さらに深層学習を用いた手法では PUF としての性能は機械学習を

用いた手法には劣るが，高い精度を示した．機械学習を用いた手法に劣った理由としては測定時に生じる測定誤差が原因でエラーを起こしていると考えられる．また，深層学習による解析はモデルの影響を強く受けるためモデルを改善することによって100%を達成できるのではないかと考えられる．

(4) 次の提案である Wien bridge 発振回路を用いた手法では，回路から出力されたアナログ値から特徴量を計算し機械学習，深層学習にて解析を行った．機械学習を用いた手法，深層学習を用いた手法ともに100%の識別精度を達成することができた．これは，無安定multivibrator のような非安定な発振回路ではなく，Wien bridge 発振回路のような安定した発振回路であれば特徴量のみで識別可能であることを示した．このことから，ほかの安定な発振回路ではこの手法により非常に簡単に PUF としての性能を見出せると考えられる．また回路の数や経年劣化，周囲温度の与える影響を再度実験する必要があるといえる．チャレンジの概念を導入する前段階の実験としては非常に貢献できた検証であったといえる．今後検証回路内のスイッチを ON/OFF した場合の 256 通りの検証を行うことで初めてアナログ PUF の分野においてチャレンジの概念を導入することができると考えられる．

研究論文は投稿中の論文誌を含め，下記のようになる．特に最初の一歩として考えたカーボン抵抗を用いた PUF については，IEEE の国際学会で発表し，Excellent Poster Paper Award Gold Prize を受賞され，大変注目を集めた．

(1) Ryota Soga, Hyunho Kang, “PUFs Analysis for Unstable Signals Using Analog Circuit,” Research Briefs on Information & Communication Technology Evolution (ReBICTE) 【投稿中】
(2) 植田優貴，姜玄浩，“画像認識を用いた森林火災検知に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2022 年 3 月．
(3) 曽我 諒太，姜玄浩，“Wien bridge 発振器を用いた物理的クローン不可関数に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2022 年 3 月．
(4) 小林 佐介，姜玄浩，“フェイク動画の検出に有効な顔領域の検討,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2022 年 3 月．
(5) Ryota Soga, Hyunho Kang, “Physical Unclonable Function Using Hartley Oscillator,” 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE2021), Kyoto, IEEE Xplore, pp. 426-429, Oct. 12-15, 2021.
(6) 曽我諒太，姜玄浩，“ハートレー発振器を用いた物理的クローン不可関数に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2021 年 3 月．
(7) Ryota Soga, Hyunho Kang, “Physical Unclonable Function Using Carbon Resistor,” 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE2020), IEEE Xplore, pp. 828-830, Oct. 2020. (GCCE 2020 Excellent Poster Paper Award Gold Prize)
(8) 大村秀，姜玄浩，“画像処理を用いた自律走行システムに向けた GAN 応用の検討,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2020 年 3 月．
(9) 工藤玲央，姜玄浩，“頬を用いた 3D マスクの顔認証なりすまし防止に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2020 年 3 月．
(10) 田島リオ，姜玄浩，“機械学習を用いた危険物検出に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2020 年 3 月．
(11) 曽我諒太，姜玄浩，“カーボン抵抗を用いた物理的クローン不可関数に関する研究,” 電子情報通信学会 マルチメディア情報ハイディング・エンリッチメント研究会（EMM），2020 年 3 月．

５．主な発表論文等

〔雑誌論文〕　計0件

〔学会発表〕　計10件（うち招待講演　0件／うち国際学会　2件）

１．発表者名 Ryota Soga, Hyunho Kang
２．発表標題 Physical Unclonable Function Using Carbon Resistor
３．学会等名 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE2020), (国際学会)
４．発表年 2020年

１．発表者名 曽我諒太, 姜玄浩
２．発表標題 ハートレー発振器を用いた物理的クローン不可関数に関する研究
３．学会等名 電子情報通信学会　マルチメディア情報ハイディング・エンリッチメント研究会（EMM）
４．発表年 2021年

１．発表者名 曽我諒太, 姜玄浩
２．発表標題 カーボン抵抗を用いた物理的クローン不可関数に関する研究
３．学会等名 電子情報通信学会　マルチメディア情報ハイディング・エンリッチメント研究会（EMM）
４．発表年 2020年

１．発表者名 Ryota Soga, Hyunho Kang
２．発表標題 Physical Unclonable Function Using Hartley Oscillator
３．学会等名 2021 IEEE 10th Global Conference on Consumer Electronics (GCCE2021) (国際学会)
４．発表年 2021年

１．発表者名 曽我諒太，姜玄浩
２．発表標題 Wien bridge 発振器を用いた物理的クローン不可関数に関する研究
３．学会等名 電子情報通信学会　マルチメディア情報ハイディング・エンリッチメント研究会（EMM）
４．発表年 2022年

〔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

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