

低電力 IoT デバイスを対象とするノイズに強く 測定の長さが制約されない小型電力解析装置の設計

北山 遼育¹ 竹中 崇² 柳澤 政生¹ 戸川 望¹

概要: IoT デバイスの低電力化やセキュリティ対策のため、IoT デバイスの電力解析が強く求められる。我々は IoT デバイスの汎用ポートを用いて同期加算平均法によるノイズ低減機能を実装した小型電力解析装置を提案した。本稿では、既存の小型電力解析装置へ (a) 2 段増幅回路による電流の値の大きさに応じた自動的な測定レンジ切り替え機能、(b) 制御マイクロコントローラのタイマモジュールによる正確な分割開始点の固定で実現する分割測定機能を導入した、低ノイズ小型電力解析装置を提案する。提案する低ノイズ小型電力解析装置は (a) によって既存の電力解析装置の 5.77 倍の大きさまで電流の値を読み取ることが可能となった。さらに、(b) によって高いサンプリング周波数のまま処理時間の長い測定対象を電力解析可能となった。提案する低ノイズ小型電力解析装置を用いて、IoT 向けのデバイスである Arduino に実装された AES 暗号の暗号化処理を電力解析した。低ノイズ小型電力解析装置と高性能な測定機器による電力解析結果の差は高々 1.3% に抑えられており、1.3% の差は既存の小型電力解析装置と高性能な測定機器による電力解析結果の差より小さな値であった。

Scalable and Small Power Analyzer Design with Noise Redcuton for Low-Power IoT Devices

RYOSUKE KITAYAMA¹ TAKASHI TAKENAKA² MASAO YANAGISAWA¹ NOZOMU TOGAWA¹

Abstract: Power analysis for IoT devices is strongly required to reduce power consumption and realize secure communications. In this paper, we propose a scalable and small power analyzer with noise reduction for low-power IoT devices. Our proposed power analyzer has the following advantages: (a) Our proposed power analyzer has a two-level amplifier and amplifies current signals adaptively depending on their magnitude. Thus minimum readable current can become small enough even if the small magnitude of current signal is given. (b) If long-time analysis is required, it can be partitioned into several analysis segments. Our proposed power analyzer can measure currents and voltages of each analysis segment by using a small amount of data memories. After that, by combining these analysis segments using a timer module, we can obtain long-time analysis results. We have analyzed power and energy consumption of encryption processes of AES block cipher on Arduino which is a typical IoT device for prototyping. The results demonstrate that our proposed power analyzer has only 1.3% measurement error compared with a high-precision oscilloscope.

1. はじめに

近年、社会で IoT が注目されている [8]。IoT はネットワーク技術で幅広い種類の膨大な数のデバイスを管理運

用する仕組みであり、ホームネットワークからインフラストラクチャまでの幅広い分野への応用が期待されている。IoT の普及にはセキュリティ対策とデバイスの省電力化が強く求められ、これらの課題解決には IoT デバイスに対する電力解析が有効である [2], [3]。

IoT デバイスに対する電力解析はデバイスの消費電力の小ささや設置場所の多様性から幅広い周波数成分を持つノイズの影響を強く受ける。従って、IoT デバイスに対する

¹ 早稲田大学大学院基幹理工学研究科情報理工・情報通信専攻
Dept. of Computer Science and Communications Engineering, Waseda University

² 日本電気株式会社グリーンプラットフォーム研究所
Green Platform Laboratories, NEC Corporation

電力解析装置は (1) 幅広い周波数成分のノイズに対するノイズ低減機能が求められる。加えて, IoT デバイスは限られたスペースに設置されるものが多いため, (2) 電力解析装置の小型化も求められる。

低電力デバイスに対する電力解析装置には, Bucci らや Jiang らのもの, SASEBO が知られている [5], [10], [14]. しかし, これらの電力解析装置の中で, (1) と (2) の要求を同時に満たすものは存在しない。そこで, 我々は IoT デバイスの汎用ポートを用いた同期処理で同期加算平均法によるノイズ低減機能を実現した小型電力解析装置を提案した。しかし, 小型電力解析装置には 2 つの問題が存在する。(問題 1) 小型電力解析装置 [11] は測定可能な電流の値の最大値が小さく, 消費電力の大きな IoT デバイスへの電力解析に対応できない。さらに, (問題 2) 測定データの一時的な保存に必要なメモリの大きさが小さく, 高いサンプリング周波数のまま処理時間が長い測定対象処理全体を電力解析することが難しい。

本稿では, (a) 2 段増幅回路による電流の値の大きさに応じた自動的な測定レンジ切り替え機能と (b) タイマによる正確な分割開始点の固定で実現する分割測定機能によって既存の小型電力解析装置と同等の解析精度を持ちつつ, (問題 1) と (問題 2) を解決した低ノイズ小型電力解析装置を提案する。低ノイズ小型電力解析装置では, (a) の導入によって解析可能な電流の値の最大値が既存の小型電力解析の 5.77 倍である 330mA まで拡大し, (b) によってサンプリング周波数を落とすことなく制御マイクロコントローラが小さなサイズのメモリしか持たない場合でも, 処理時間の長い測定対象処理の電力解析が可能となった。

低ノイズ小型電力解析装置を用いて IoT 向けのデバイスである Arduino 上に実装された AES 暗号の暗号化処理を電力解析した。低ノイズ小型電力解析装置による電力解析結果と高精度な測定機器で得られた電力解析結果との差は 1.3% であった。この値は既存の小型電力解析装置による電力解析結果と高性能な測定機器による電力解析結果との差に比べて小さく, 低ノイズ小型電力解析装置の解析精度は既存の小型電力解析装置と同等以上であるといえる。

本稿は以下で構成される。2 章で IoT デバイスに対する電力解析の必要性和既存手法の問題点を説明する。3 章で提案する低ノイズ小型電力解析装置の構造と測定動作を紹介し, 4 章で低ノイズ小型電力解析装置の性能を評価する。さらに, IoT 向けデバイスの Arduino 上に実装された AES 暗号の電力解析結果を示す。

2. IoT デバイスに対する電力解析

IoT デバイスに対する電力解析はセキュリティ対策とデバイスの省電力化に有効である。電力解析によって得られるデバイスの詳細な電力消費のデータから, サイドチャネル攻撃に対するデバイスの耐性や脆弱性を評価する指標

や, デバイスの省電力化に役立つ指標を手に入れることが可能である。さらに, 実装する処理がデバイスの求める電力の制約を満足するか検証することも可能である。

2.1 IoT デバイスモデル

多くの IoT デバイスはセンサ, 制御装置, 通信機能を持つ。センサにはデバイスの目的に応じたものが用いられる。例えば, スマートグリッドに利用される電力管理デバイスであれば, 電圧・電流センサが利用される。制御装置には低コストでプログラムの書き換えが容易なマイクロコントローラの利用が考えられる。通信機能には Ethernet, USB, RS-232C, wifi, zigbee, bluetooth などの通信モジュールが利用される。本稿では, 制御装置にマイクロコントローラを用い, 通信機能とセンサを持つデバイスを一般的な IoT デバイスであると考え, IoT デバイスモデルと定義する。

2.2 電力解析装置に求められる機能

IoT デバイスへの電力解析ではノイズが問題となる。IoT デバイスの電力はノイズに対して十分な大きさを持たないため, ノイズの影響を強く受ける。IoT デバイスの設置場所は多様であるため, ノイズには幅広い周波数の信号が含まれる可能性が高い。従って, 電力解析装置には (1) 幅広い周波数のノイズに対応可能なノイズ低減機能が求められる。IoT デバイスへの電力解析装置は解析装置の設置場所が限られるため, 機器は小型でなければならない。小型な機器に実装できる回路やプログラムには制限があり, 複雑な回路やプログラムは実装できない。そのため, (2) ノイズ低減機能を簡単な回路とソフトウェアのみで実装する必要がある。

2.3 既存手法

低電力デバイスに対する電力解析装置として, Bucci らと Jiang らの電力解析装置や SASEBO が知られている [5], [10], [14]. Bucci らの電力解析装置は強力なノイズ低減機能を持ち, 超低電力なデバイスに対して精度の高い電力解析が可能である。しかし, Bucci らの電力解析装置は複雑な回路やプログラムが必要となるため, 要求 (2) を満たさない。Jiang らの電力解析装置は低電力なセンサデバイス向けの電力解析装置であり, IoT デバイスとの親和性が高い。しかし, Jiang らの電力解析装置のノイズ低減機能は RC ローパスフィルタによるものであるため, 要求 (1) を満たさない。SASEBO は低電力なデバイスに対する電力解析攻撃の評価ボードである。しかし, SASEBO は電圧と電流の測定を容易にする回路を持つのみであり, 電力解析には別の測定装置を要する。従って, IoT デバイスへの電力解析装置としては不十分である。

そこで以前, 同期加算平均法によるノイズ低減機能を実

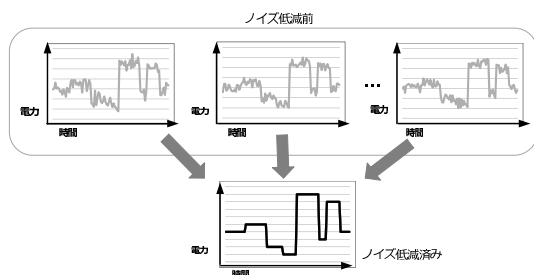


図 1 同期加算平均法。

装した小型電力解析装置を提案した [11]。同期加算平均法は複雑な回路やプログラムなしに幅広い周波数のノイズを低減できる。同期加算平均法によるノイズ低減処理を電力解析装置に実装する鍵は、いかに測定対象処理と電力解析装置の測定との同期を実現するかである。既存の小型電力解析装置では、IoT デバイスの汎用ポートを用いた同期信号線で同期を実現した。汎用ポートは IoT デバイスモデルで定義される IoT デバイスの制御装置が持つ基本的な機能であるため、既存の小型電力解析装置は幅広い IoT デバイスへの電力解析に利用できる。汎用ポートを用いた同期信号線による同期処理は複雑な回路やプログラムなしに実装でき、既存の小型電力解析装置は小型ながら (1) と (2) の要求を同時に満たす。

既存の小型電力解析装置は電力測定基板と電力解析ソフトウェアから構成される。電力測定基板は測定対象デバイスの電圧と電流の値を取得し、電力解析ソフトウェアへ送信する。電力解析ソフトウェアは電力測定基板から受け取ったデータを処理し、電力解析結果を保存する。同期加算平均法によるノイズ低減処理は電力解析ソフトウェア上で実行される。

図 1 に同期加算平均法によるノイズ低減の様子を示す。測定結果には図 1 中に黒線で示される測定対象処理による信号変化と図 1 中に灰色線で示されるノイズによる信号変化が含まれる。測定対象処理による信号変化は測定対象処理と測定が同期的に実行される場合、すべての測定結果で同様の信号変化となる。一方、ノイズによる信号変化は同様ではない。この性質を利用し、複数の測定結果を足し合わせて平均化することでノイズを低減する手法が同期加算平均法である [4], [9]。

2.4 既存の小型電力解析装置の問題点

既存の小型電力解析装置は、(問題 1) 測定可能な電流の値の最大値が小さく、大きな消費電力のデバイスを電力解析できない。低電力デバイス向けの無線通信モジュールとして [6], [7], 汎用マイクロコントローラとして [1] が存在する。[1], [6], [7] はすべて一般的なモジュール、マイクロコントローラである。IoT デバイスの消費電力は無線通信モジュール、マイクロコントローラ、センサそれぞれの消費電力の合計から得られる。センサの消費電力は小さいた

め今回は考慮しない。[1], [7] を用いて IoT デバイスを作成した場合、デバイスには最大 320mA の電流が流れる可能性がある。一方、既存の小型電力解析装置で取得可能な電流の値の最大値は 57.2mA である。従って、57.2mA までの電流の値しか取得できない既存の小型電力解析装置の性能は不十分である。

さらに、(問題 2) 既存の小型電力解析装置は測定データの一時的な保存に利用できるメモリの大きさが小さく、処理時間が長い測定対象処理全体の電力解析が難しい。電力測定基板から電力解析ソフトウェアへのデータ転送の速度は、A/D 変換の速度と比べ遅く、電力測定基板の制御マイクロコントローラは A/D 変換で取得した測定値を一時的に自身のメモリへ保存する必要がある。そのため、測定可能な時間はメモリへ測定値を保存できる長さ以下に制限され、処理時間が長い測定対象処理を電力解析するには、測定のサンプリング周波数を下げる必要が生じる。従って、高いサンプリング周波数のまま処理時間が長い測定対象処理全体を電力解析することが難しい。

3. 低ノイズ小型電力解析装置

(問題 1) の解決には電流の信号を増幅する増幅回路の増幅率を下げる必要がある。しかし、単純に増幅器の増幅率を下げると分解能も低下し、既存の小型電力解析装置と同等の解析精度を維持できない。そこで、(a) 2 段増幅回路による入力される電流の信号の大きさに応じた自動的な測定レンジ切り替え機能の導入を考える。(a) を用いる場合、小さな電流の信号に対する増幅率は既存の小型電力解析装置と同じ大きさに設定できるため、既存の小型電力解析装置と同等の解析精度を維持できる。(a) は既存の小型電力解析装置へ増幅回路を追加し、制御マイクロコントローラへ自動的な測定レンジの切り替え処理を実装することで実現できる。増幅回路に利用されるオペアンプ IC の多くは複数の増幅器が 1 つの IC に実装されているため、回路規模を大幅に大きくすることなく (a) の実装が可能である。加えて、自動的な測定レンジの切り替え処理も比較演算のみで実現できるため実装が容易である。

(問題 2) は測定可能な時間の制限を無くすことで解決できる。そこで、(b) 制御マイクロコントローラのタイマモジュールによる正確な分割開始点の固定で実現する分割測定機能の導入を考える。(b) は既存の小型電力解析装置が持つ IoT デバイスの汎用ポートを用いた同期信号線とマイクロコントローラが標準的に持つタイマ機能を利用することで実現できる。

以上より、(a), (b) を用いることで既存の小型電力解析装置の問題点を改善した小型電力解析装置が構成できるといえる。本稿では既存の小型電力解析装置に対し、(a), (b) を導入し、既存の小型電力解析装置と同等以上の解析精度を有する低ノイズ小型電力解析装置を提案する。

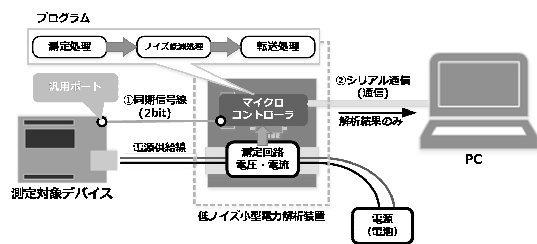


図2 低ノイズ小型電力解析装置.

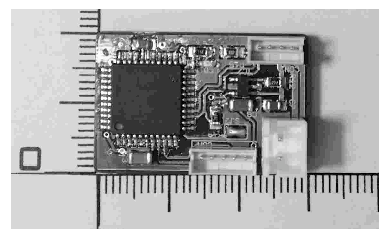


図3 低ノイズ小型電力解析装置の基板.

3.1 低ノイズ小型電力解析装置の構成

低ノイズ小型電力解析装置を図2に示す。低ノイズ小型電力解析装置は電圧変換回路、電流変換回路、制御マイクロコントローラから構成される。測定対象デバイスの電源は低ノイズ小型電力解析装置を介して供給される。測定対象デバイスに供給される電源の電圧と電流の信号は電圧変換回路もしくは電流変換回路を経由し、制御マイクロコントローラのA/D変換モジュールへ入力される。電力解析に必要な電圧と電流の値は入力信号のA/D変換によって取得される。制御マイクロコントローラのA/D変換モジュールは0Vから3.3Vまでの信号を10bitの幅で取得できる。

測定対象デバイスと低ノイズ小型電力解析装置は図2中①で示される2ビットの同期信号線によって接続される。2ビットのうち1ビットが低ノイズ小型電力解析装置から測定対象デバイスへ測定の開始を知らせる信号を送信し、残りが測定対象デバイスから低ノイズ小型電力解析装置へ測定対象処理の終了を知らせる信号を送信する。低ノイズ小型電力解析装置は外部のPCへ図2中②で示されるシリアル通信で接続される。同期加算平均法によるノイズ低減処理は低ノイズ小型電力解析装置の制御マイクロコントローラ上で実行されるため、ノイズ低減処理後の電力解析結果のみが外部のPCへ転送される。

図3に低ノイズ小型電力解析装置の基板を示す。図3の通り、低ノイズ小型電力解析装置は2cm×3cmの基板上に実現されている。これはBucciらの電力解析装置[5]やJiangらの電力解析装置[10]と比べ、小型である。

3.2 電圧変換回路

電圧変換回路は5.1K Ω の抵抗器2本による抵抗分圧回路から構成され、入力信号の電圧を半分にする。制御マイクロコントローラのA/D変換モジュールで読み取り可能な入力信号の電圧の値の幅が0Vから3.3Vであるため、低ノイズ小型電力解析装置は0Vから6.6Vまでの電圧の値を読み取れる。

3.3 電流変換回路

電流変換回路はシャント抵抗とオペアンプによる2段増幅回路によって構成される。シャント抵抗は小さな抵抗値

を持った抵抗器で測定対象デバイスと電源のGNDの間に挿入される。測定対象デバイスに流れる電流はすべてシャント抵抗を経由してGNDへ流れる。シャント抵抗は自身を通過する電流の大きさに応じて両端に電位差を生じる。この電位差を2段増幅回路によって増幅し、A/D変換モジュールによって読み込むことで電流の値を取得する。2段増幅回路の1段目は増幅率10倍の差動増幅回路、2段目は増幅率5.1倍の非反転増幅回路から構成され、2段目の増幅回路の出力は元の信号の51倍となる。各段の出力は制御マイクロコントローラのA/D変換モジュールの入力ピンへそれぞれ別々に接続される。制御マイクロコントローラは測定対象デバイスに流れる電流の大きさに応じて自動的に使用するA/D変換モジュールの入力ピンを切り替える。この機能によって(a)が実現される。シャント抵抗の抵抗値は1 Ω であるため、1段目と2段目、両方の増幅回路を用いる場合は64.7mAまで6.32 μ A単位で、1段目の増幅回路のみを用いる場合は330mAまで322 μ A単位で電流の値を取得できる。

3.4 制御マイクロコントローラ

制御マイクロコントローラは低ノイズ小型電力解析装置の測定動作を制御する。制御マイクロコントローラにはPIC24FJ64GA002を用いた。

制御マイクロコントローラ上のソフトウェアには、測定処理、同期加算平均法によるノイズ低減処理、通信処理が実装される。測定処理は同期信号を制御し、A/D変換モジュールを用いて測定対象デバイスに供給される電源の電圧と電流の値を取得する。自動的な測定レンジの切り替え処理は測定対象処理に含まれ、測定動作の開始時点で入力される電流の信号の大きさに応じて使用する電流変換回路からA/D変換への入力ピンを切り替える。同期加算平均法によるノイズ低減処理は測定処理で得られた測定値を同期加算平均法により処理し、ノイズが低減された電力解析結果を取得する。通信処理は得られた電力解析結果を外部のPCへ転送する。ソフトウェアはC言語で記述され、コンパイラはMicrochip社のXC16 v1.11を用いた[13]。

3.5 測定動作の流れ

図4に分割測定機能を利用した電力解析動作の流れを示す。図4は測定を3分割する場合の例である。分割測定機

能を用いる場合、測定対象処理に対する測定は複数の区間へ均等に分割される。1回の測定動作で取得される測定結果は分割された1区間分であり、測定動作ごとに外部PCへ電力解析結果が転送される。測定対象処理全体の電力解析結果は外部PC上で全分割区間の電力解析結果を統合し、作成される。

変換周期 t 、1回の測定動作で取得する測定結果の数 m 、繰り返し回数 n は外部PCから測定動作の開始前に低ノイズ小型電力解析装置へコマンドを入力し、設定する。分割測定機能の有効化も外部PCからコマンドで実行する。測定動作の流れは以下の通りである。

- (1) 測定開始を示す同期信号の出力 : 低ノイズ小型電力解析装置の制御マイクロコントローラが測定対象デバイスに対し、測定開始を示す同期信号を出力する。
- (2) 測定対象処理の開始 : 測定対象デバイスは測定開始を示す同期信号の入力と同時に、測定対象処理を開始する。
- (3) 測定開始 : 電力解析装置の制御マイクロコントローラは分割測定の開始時点まで待機し、待機後に A/D 変換を開始する。分割測定機能による最初の分割測定の場合か分割測定機能を利用しない場合は待機なしに A/D 変換を開始する。A/D 変換は $t[\mu\text{s}]$ の周期で、 m 組取得される。(1) から (3) までの処理の繰り返し回数が n 回に達するまで (1) に戻り処理を繰り返す。
- (4) 測定結果の変換と同期加算処理 : 電力解析装置の制御マイクロコントローラは得られたすべての A/D 変換結果を電圧と電流の値に変換する。変換後に同期加算平均法によるノイズ低減処理を実施し、電力解析結果を得る。
- (5) 電力解析結果の転送 : 電力解析装置の制御マイクロコントローラは得られた電力解析結果をシリアル通信モジュールを用いて外部PCへ転送する。分割測定機能による最後の分割測定が終了するまで (1) に戻り処理を繰り返す。分割測定機能を利用しない場合はここで測定動作を終了する。

4. 低ノイズ小型電力解析装置の性能評価

既存の小型電力解析装置と低ノイズ小型電力解析装置で取得可能な最大の電流の値と測定可能な時間の最大値を比較する。さらに、既存の小型電力解析装置と低ノイズ小型電力解析装置による電力解析結果を比較し、低ノイズ小型電力解析装置の解析精度が既存の小型電力解析装置と同等以上であるか検証する。

表1に既存の小型電力解析装置と低ノイズ小型電力解析装置の性能比較を示す。表1中の最大測定可能時間はA/D変換の速度を最高の500ksps、制御マイクロコントローラのデータメモリのサイズを8Kバイト、1組の測定結果の大きさを4バイトとした場合の値である。IoTデバイスモ

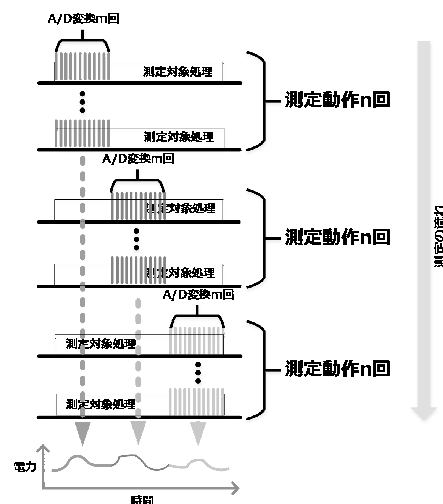


図4 分割測定機能。

表1 小型電力解析装置との性能評価。

	[11]	低ノイズ電力測定装置
最大取得可能電流値 [mA]	57.2	330
最大測定可能時間 [ms]	8	∞

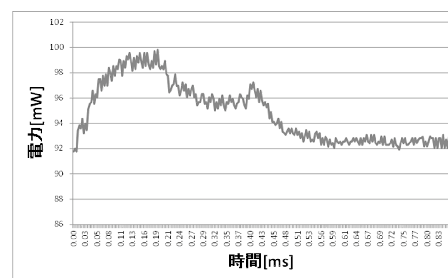


図5 低ノイズ小型電力解析装置による AES 暗号の電力波形。

デルで定義される一般的な IoT デバイスを電力解析する場合、測定可能な電流の値の最大値 330mA は 2.4 節から十分な大きさであると考えられる。以上より、表1から低ノイズ小型電力解析装置は (問題1) と (問題2) の問題を解決できているといえる。

4.1 電力解析

低ノイズ小型電力解析装置とオシロスコープで測定対象デバイス上で動作する AES 暗号の暗号化処理を電力解析し、電力解析結果を比較した。オシロスコープは Aglient 社製 MSO-X 3104A、電流プローブは Aglient 社製 1147A を利用した。AES 暗号のプログラムは AESLib を利用し、鍵長は 128 ビット、暗号化を施す平文の長さは 16 バイトとした [12]。測定対象デバイスには Arduino Pro Mini 328 5V 16MHz を用い、 $t = 0.83\mu\text{s}$ 、 $m = 1024$ 回の条件で A/D 変換を実行した。測定対象デバイスへ供給する電源の電圧は 5V とした。

4.2 解析結果

図5に低ノイズ小型電力解析装置で、図6にオシロス

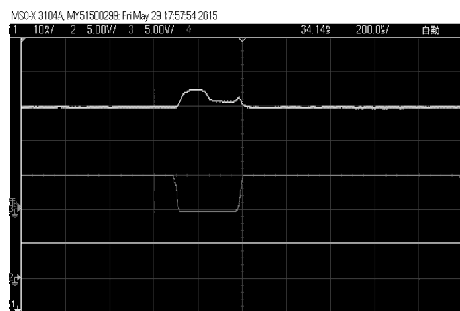


図 6 オシロスコープによる AES 暗号の解析結果.

コープで測定対象デバイス上で動作する AES 暗号の暗号化処理を電力解析した結果を示す. 図 6 中, 一番上が電流, 上から 2 番目が同期信号, 上から 3 番目が電圧の波形である. 測定対象デバイス上の AES 暗号が暗号化処理に要する平均電力とエネルギーは AES 暗号の暗号化処理実行時間を $450\mu\text{s}$ とする場合, 低ノイズ小型電力測定装置で平均電力 93.03mW , エネルギー $43.21\mu\text{J}$, オシロスコープで平均電力 97.34mW , エネルギー $43.80\mu\text{J}$ であった. この結果から低ノイズ小型電力解析装置による解析結果はオシロスコープによる解析結果に対し, 1.3% の差を持つといえる. 既存の小型電力解析装置とオシロスコープとの電力解析結果の差は 5% であったため, 低ノイズ小型電力解析装置は既存の小型電力解析装置と同等以上の解析精度を有しているといえる.

5. おわりに

本稿では既存の小型電力解析装置に対して 2 段増幅回路による電流の値の大きさに応じた自動的な測定レンジ切り替え機能, と制御マイクロコントローラのタイマモジュールによる正確な分割開始点の固定で実現する分割測定機能を導入した, 低ノイズ小型電力解析装置を提案した. 低ノイズ小型電力解析装置は既存の小型電力解析装置と比較して 5.77 倍の大きさの電流の値を取得可能となり, より幅広い IoT デバイスへの電力解析が可能となった. さらに, 高いサンプリング周波数のまま処理時間の長い測定対象全体を電力解析可能となった. 低ノイズ小型電力解析装置を用いて IoT 向けデバイスである Arduino 上の ASE 暗号の暗号化処理を電力解析した. 得られた電力解析結果は高性能な測定機器と比較し, 1.3% と既存の小型電力解析装置と高性能な測定機器との電力解析結果の差と比べ, 小さな値であった. 従って, 低ノイズ小型電力解析装置は既存の小型電力解析装置と比較し, 同等以上の解析精度を有しているといえる.

今後は高速な同期加算平均法によるノイズ低減処理の実装を目指す.

謝辞

本研究の実施にあたり NEC グリーンプラットフォーム

研究所のみなさまに感謝いたします. また本研究の一部は総務省 SCOPE の支援による.

参考文献

- [1] Atmel Corporation, “ATmega48A/PA/88A/PA/168A/PA/328/P Atmel 8-bit microcontroller with 4/8/16/32Kbytes in-system programmable flash,” <http://www.atmel.com/ja/jp/Atmel-8271-8-bit-AVR-Microcontroller-ATmega48A-48PA-88A-88PA-168A-168PA-328-328P-datasheet-Complete.pdf>, 2014.
- [2] S. Babar, A. Stango, N. Prasad, J. Sen, and R. Prasad, “Proposed embedded security framework for internet of things (IoT),” in *Proc. 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace and Electronic Systems Technology (Wireless VITAE)*, pp. 1–5, 2011.
- [3] D. Bandyopadhyay and J. Sen, “Internet of things: applications and challenges in technology and stanfordization,” in *Proc. Wireless Personal Communications*, vol. 58, no. 1, pp. 49–69, 2011.
- [4] C. L. Birkett, C. A. Ray, E. A. Anderson, and R. F. Rea, “A signal-averaging technique for the analysis of human muscle sympathetic nerve activity,” *Journal of Applied Physiology*, vol. 73, no. 1, pp. 376–381, 1992.
- [5] G. Bucci, E. Fiorucci, F. Ciancetta, and M. Luiso, “Measuring system for microelectric power,” *IEEE Trans. on Instrumentation and Measurement*, vol. 63, no. 2, pp. 410–421, 2014.
- [6] Digi International Inc, “XBee and XBee-PRO ZigBee ZigBee RF Modules for OEMs,” http://www.digi.com/pdf/ds_xbee_zigbee.pdf, 2015.
- [7] Digi International Inc, “XBee Wi-Fi Embedded Wi-fi Module for OEMs,” http://www.digi.com/pdf/ds_xbeewifis6b.pdf, 2015.
- [8] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things(IoT):a vision, architectural elements, and future directions,” *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.
- [9] M. E. Cain, J. W. Mason, J. L. Anderson, M. M. Scheinman, M. F. Arnsdorf, and A. L. Waldo, “Signal-averaged electrocardiography,” *Journal of the American College of Cardiology*, vol. 27, no. 1, pp. 238–248, 1996.
- [10] X. Jiang, P. Dutta, D. Culler, and I. Stoica, “Micro power meter for energy monitoring of wireless sensor networks at scale,” in *Proc. 6th International Conference on Information Processing in Sensor Networks*, pp. 186–195, 2007.
- [11] 北山遼育, 竹中崇, 柳澤政生, 戸川望, “低電力 IoT デバイスを対象としたノイズ低減機能を持つ小型電力解析装置の設計,” 第 28 回路とシステムワークショップ, 2015.
- [12] D. Landman, “AESLib,” <https://github.com/DavyLandman/AESLib>, 2015.
- [13] Microchip Technology Inc, “MPLAB XC16 C Compiler User’s Guide,” <http://ww1.microchip.com/downloads/en/DeviceDoc/50002071E.pdf>, 2014.
- [14] 独立行政法人産業技術総合研究所情報セキュリティ研究センター, “SASEBO の電力解析攻撃実験 Power Analysis Attacks on SASEBO,” 森田テック株式会社, http://satoh.cs.uec.ac.jp/SASEBO/pdf/SASEBO_PA_Report_Japanese.pdf, 2010.