SCIS 2022 2022 Symposium on
Cryptography and Information Security
Osaka, Japan & Online, Jan. 18 – 21, 2022
The Institute of Electronics,
Information and Communication Engineers

レーザー振動計を用いた MLCC からの音響サイドチャネルリークの測定
Measuring Acoustic Side-Channel Leakag from MLCC using Laser Vibrometer

土井 康平 * 菅原 健 *
Kohei Doi Takeshi Sugawara

キーワード サイドチャネル攻撃, 積層セラミックコンデンサ, 音響ノイズ

あらまし

多くのコンピュータは, マザーボード上の電子素子の振動によって, 動作中に高周波数帯域に及ぶ音響ノイズを出すことがある. この音響ノイズはコンピュータが計算している情報などセキュリティに関する情報を含んでいることがあり, その音響ノイズから情報が漏洩することを音響リークという. こういった音響ノイズを利用して暗号鍵などを盗聴する音響サイドチャネル攻撃 [1] が知られている.

このような音響ノイズの主要因は, 積層セラミックコンデンサ (MLCC) の逆圧電効果による振動だと考えられている. 従来の音響サイドチャネル攻撃はマイクを用いて音響ノイズを計測していたが, これはマイクが高周波数帯域の情報を取得できないことや, 音響ノイズが障害物に遮られてしまうことが攻撃における欠点であった.

以上の背景の元，マイクの代わりにレーザー振動計を用いた音響サイドチャネル攻撃がより強力になる可能性があると考えて研究を行ってきた [2]．レーザーはガラスなどの障害物を貫通して攻撃できるとともに，より高い周波数帯域まで計測できる能力があるためである．先行研究では，レーザー振動計で MLCC を計測することで，音響周波数を遥かに超える MHz 帯域まで振動を計測できることが分かった [2]．しかし，先行研究で行った基礎実験は MLCC の評価に留まっており，PC などのシステムにおける評価は行っていなかった.

本研究は，上記のギャップを埋めることを目的に，ノートパソコンのマザーボードに搭載された MLCC をレーザー振動計で計測する．より具体的には，次のことを行った.

ノートパソコンに搭載された MLCC の計測 実験対象のノートパソコンで, CPU 使用率が 100%近くになるプログラムを, 実行と停止を繰り返した．その間，ノートパソコンの基板上の MLCC にレーザーを当て, 振動を測定した．これにより，2 MHz の範囲まで振動が測定できた．これはすなわち, プログラムを動かしているときとそうでないとき, つまり CPU 使用率が 100%近い時とそうでないときで, MLCC からの音響リークに MHz 帯域まで差が出るということを意味している.

振動を生じる MLCC の特定 上記の実験を，計測対象の MLCC を変化させながら繰り返すことで，MLCC の個体によるリークの違いを調査する．攻撃者がどこにレーザーを当てるべきかを知ることができる．測定する MLCC はチップ電圧レギュレータ周辺にあるものをを候補にした．これにより, レギュレータ周辺の MLCC が音響リークすること, 音響リークを起こす MLCC が複数の場所に点在していることが分かった．これはつまり, 攻撃者の視点に立ったときに, 攻撃する MLCC の選択肢が複数あることを意味しており, この選択肢が多いほど攻撃の危険性が増す.

参考文献

[1] D. Genkin, A. Shamir, and E. Tromer ”Acoustic Cryptanalysis,” J. Cryptol., 30(2), pp. 392–443, 2017.

[2] 土井康平, 菅原健 ”レーザー振動計を用いた音響サイドチャネル攻撃の基礎実験” 電子情報通信学会ソサイエティ大会 , pp.120, 2021.

* 電気通信大学, The University of Electro-Communications,