2D-04

USB3.0フラッシュメモリに対する個体識別のための特徴量抽出

蒲原智也
関西大学総合情報学部

1 はじめに

近年，製造時に偶然生じるばらつきを用いてチップ固有の値を生成する Physical Unclonable Function（PUF）を用いた認証が注目されている [1]．この PUF を用いた認証では，チップにあるデータを入力するとそれぞれのチップから固有の出力が得られる．この固有のデータをサーバに登録し，認証の際に参照することでチップ認証が可能となる．

本稿では USB3.0 フラッシュメモリ（以下，USB メモリ）においても，PUF と同様にディバイス固有の特徴量を抽出する．USB メモリの個体識別を行うための指標として，データの転送時の瞬時値や平均値を利用することを検討する．

通常 PUF による ID 生成は，データを入力したときのトランジスタ電流や SRAM のしきい値電圧のばらつきを用いるため特別な回路を必要とすることが多い．そこで本稿では USB メモリに作業をさせることで，その作業時間や複数回実行した場合の平均時間など特別な回路などを必要としない方法を提案する．

次に，同一型番のいくつかの USB メモリに対して実際に計測を行い，指標として実際に定量的評価を行う．

2 計測手法

2.1 対象とする USB3.0 フラッシュメモリ

ELECOM 社の MF-RDSU3 16G を 9 本用いる．また対象とする USB メモリの記憶領域は 16 GB のものとした．同一の型番であるため，USB メモリの外見による識別が困難なため，それぞれに No.1 から No.9 までのナンバリングを行っている．実験対象の USB メモリのファイルシステムは NTFS である．

2.2 サイズが大きいファイルに対する計測手段

これらの USB メモリに対して，転送速度を調べるため，Microsoft Windows 8.1 に付属しているパフォーマンス・モニタを用いた．このパフォーマンス・モニタでは，約 1 秒毎のデータ転送量などの情報などを取得することができる．

[転送方法] 0x00 のバイト・データで埋めた 0.5・1・2・4・8 GB のものを用意した．このファイルをメインメモリに保存したあと，メインメモリから USB メモリに転送する．またキャッシュを無効化するために，書込みと読み出しの間には，当該ボリュームをアンマウントし，再度マウントする処理を行った．

[計測回数] 5 つのファイルサイズの異なるデータに対して，読み書きの組み合わせを他のコンピュータでの作業による影響を小さくするため，小さいファイルから順に大きいファイルに変更していくのを 1 回として．これを 10 回繰り返した．また既に書き込まれているデータによる転送速度への影響を調べるため，0.5 GB のファイルを順に追加していき，計測を行った．

2.3 サイズが小さいファイルに対する計測手段

2.2 節と転送するファイル容量が違うのみで，他の項目については同じ方法で計測を行った．ファイルサイズは 32・64・128・256・512・1024 KB のファイルと 32・64・128・256 MB のファイルの 10 通りである．

3 実験結果

3.1 8 GB のファイルの転送速度

サイズが大きいファイルに対するデータの中から 8 GB のファイルデータを USB メモリに書込みを行った場合の結果を図 1 に示す．同図は 8 GB のファイル全てを書込めた場合のものだけを抽出している．また凡例の番号は，USB メモリにナンバリングされた番号である．そして各点が反比例しているように見えるのは，転送速度と経過時間の積が 8 GB になるためである．

図 1 を見てわかる通り各 USB メモリ毎に点が密集していることがわかる．大きく分けて二つのグループになっているが，それぞれのグループ内を詳細に確認しても個体ごとの差異が確認できる．

次にすでに書込まれている容量による転送速度への影響をしらべるために No.9 の USB メモリの計測結果

Feature Extraction Of USB3.0 Flash Memory For Individual Recognition
Tomoya KAMBARA
Faculity of Informatics, Kansai University
569-1095, Osaka, Japan

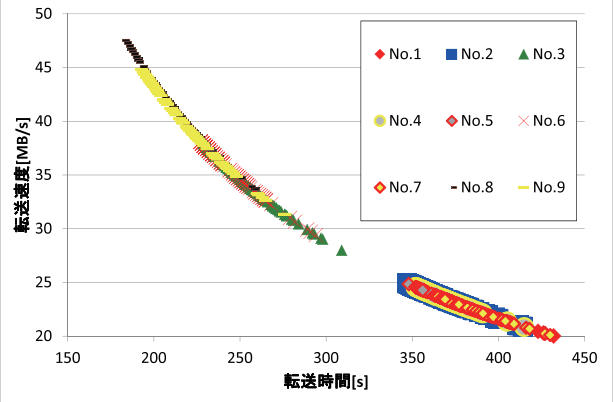

図 1: 8 GB のファイルを書込みした場合

を図 2 に示す．0.5 GB ごとの測定結果が得られているが，同図は，簡略化のため 1 GB 単位で記載している．

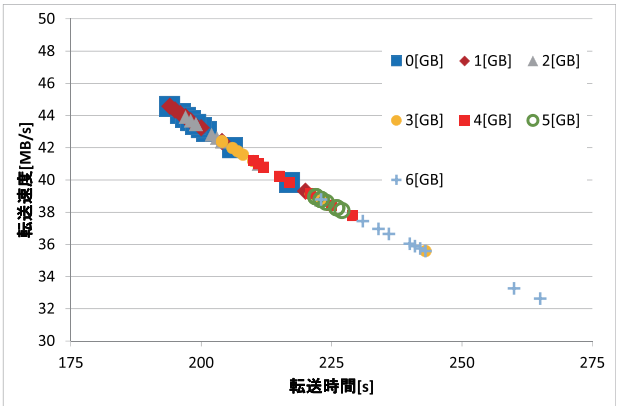

図 2: 図 1 の No.9 を抽出

図 2 を見ると既に書き込まれている容量が少ないほど高速で，多くなるにつれ遅くなっていることがわかる．この USB メモリでは，最も高速に書込めた場合と遅かった場合を比較すると，約 80 秒の差があることがわかった．他の USB メモリでも同等の差が存在するため，既に書き込まれている容量を判定することによって，点の集合のどのあたりにこの USB メモリが現在存在するか想定することが可能だと考えられる．

3.2 1024 KB のファイルの転送速度

サイズが小さなファイルに対する計測データの中から 1024 KB のファイルデータを USB メモリに書込みを行った場合の転送量と転送時間の関係を図 3 に示す．同図は，図 1 と異なり，1024 KB のファイルを書き込んだ場合の全計測 290 回の平均値である．これはパフォーマンス・モニタでは 1 秒単位の転送量と転送時間を記録しているため，図 1 と同様にプロットした場合，USB メモリ間の差がごく小さく点が密集しすぎて判別できないことによる．

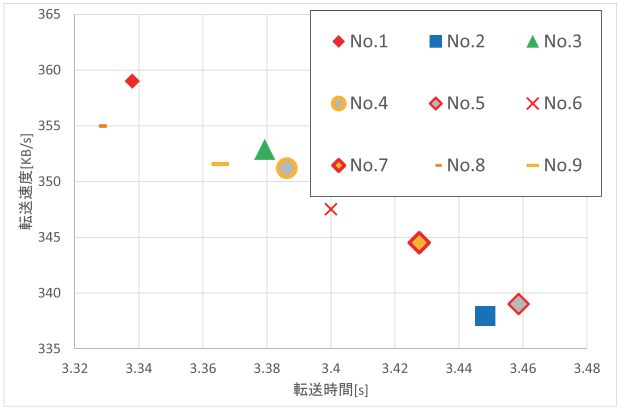

図 3: 1024 KB のファイルを書込みした場合の平均

図 3 を見ると大ファイルに対するデータと同様な優劣のグラフとなっている．しかし転送速度の上限に至る前に，ファイル転送が終了しているとみられることからサイズが小さいファイルの転送速度を USB メモリの特徴量として利用することは難しい．

4 おわりに

本稿では，同一メーカ同一型番同一記憶容量の USB メモリであっても 8 GB のファイルの転送速度を個体識別のための特徴量として利用できることを示した．また，同一の USB メモリでも，既に書込まれているデータ量によって，転送速度が異なることを示した．このデータを元に機械学習を行うことや他メーカの USB3.0 フラッシュメモリを含めた実験や他のフォーマット形式に対する実験は，今後の課題である．

謝辞 本研究は，平成 27 年度関西大学研究拠点形成支援経費において，研究課題「Device Fingerprint による識別技術の深化」として研究費を受け，その成果を公表するものである．

参考文献

[1] 奥村俊介, 吉本秀輔, 川口博, 吉本雅彦: ”SRAM セルを用いた Low 書込みによるチップ ID 生成手法”, 電子情報通信学会技術研究報告 ICD, 集積回路 112(15), 97-102, 2012