SDカード等の外部ストレージへのアクセスをセキュアにする

学習駆動コース今岡ゼミ　　岩佐　知虎

1.暗号化USBメモリの内部的な問題

USBメモリを落とし、市の住民情報などの内部データが流出したというニュースを時折みかける*1 ）。

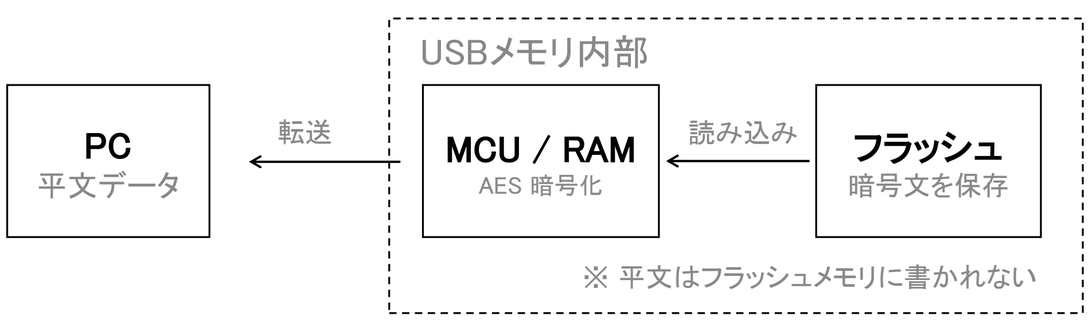
従来までの暗号化には次のような問題点がある
- ・データ全て暗号化する為、計算負荷が高い
- ・メモリを多く使う

そのため、次のような状況が生じる
- ・安価なコントローラーでは計算速度が遅い
- ・計算にかかる時間で**アクセス速度が低下する**。

自分ならどのような暗号化ができるか検証してみた。

2.暗号化USBメモリの仕組み

暗号化USBメモリでは、PCあるいはUSBメモリに内蔵されたマイクロコントローラが用いて、「データ」を暗号化する。暗号化にAESを用いる場合、大容量のRAMが必要かつ多くの乗算を要する。ゆえに暗号化に時間がかかる。

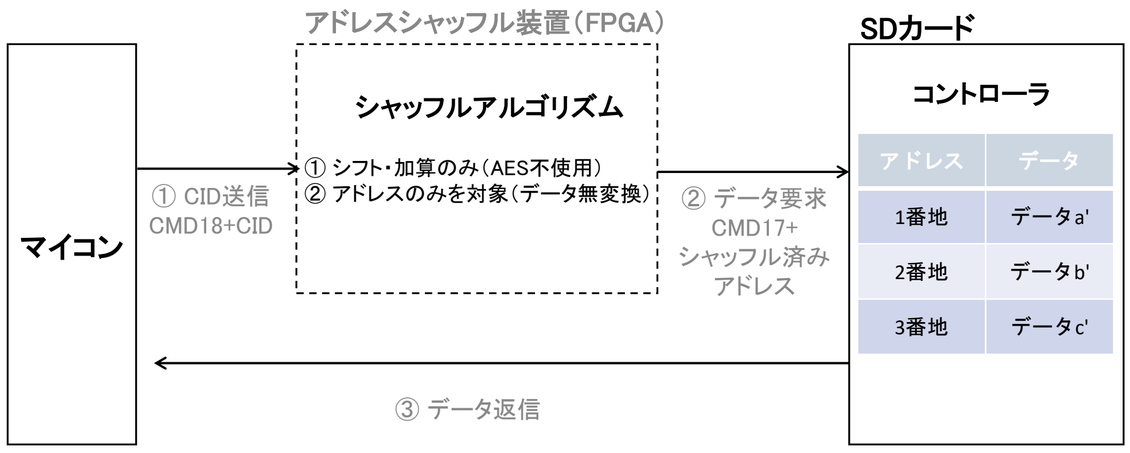


3.アドレスをシャッフルする

一般的にはデータを暗号化する手順が用いられているが、私はデータに関しては全く触らずにシャッフルするのはアドレスのみというような実装をした。
以下の方法により、既存の暗号化USBメモリよりも実装回路の負荷を軽くした。

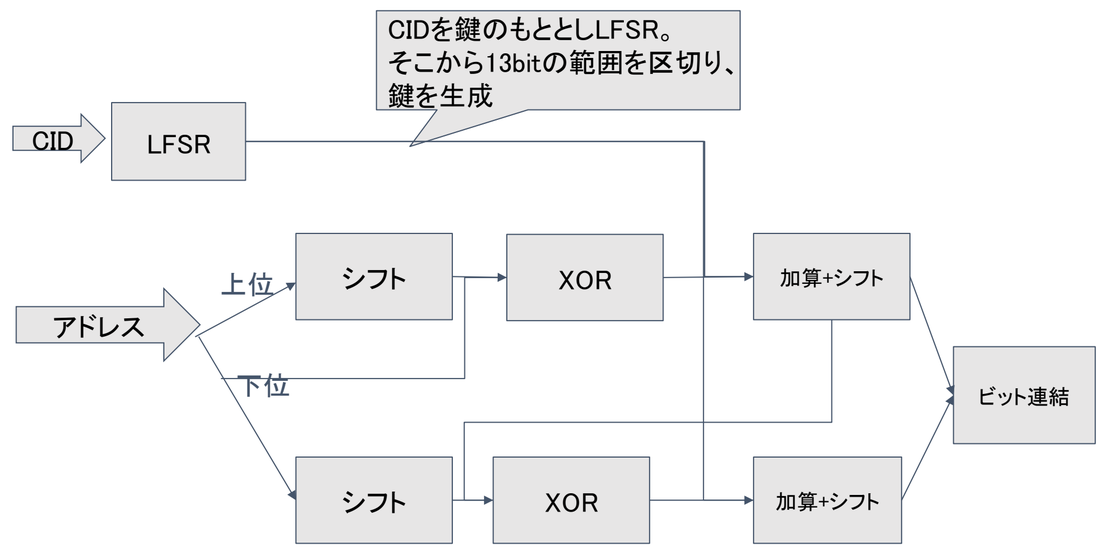
①AESのような大きな計算を行わず、シフトや加算のみを行う
②データではなくアドレスのみを対象とする

SDカードとマイコンの間に、『アドレスをシャッフルして暗号化する装置』を作成した。



4.シャッフル方法

アドレスのシャッフルには、シフト・XOR・加算のみを用いた軽量な処理を採用した。鍵はCIDを入力としたLFSRから生成し、アドレスを上位・下位に分割してそれぞれ変換した後、ビット連結で出力する。これらの演算は全単射が保証されている。



途中のシフト回数は略。上位と下位の組み合わせはあと3回行う

5.実装結果 LUT(FPGAの回路数)の使用量

Sipeed Tang Nano 9Kを用いて回路規模の比較を行った。
以上の手順で、極力少ない資源量での実装ができた。

LUT 450(417 LUT, 33ALU) / 8640
レジスタ 368/6693
BRAM 0 → ねらい通り貴重なBlockRAMの消費は0

AESよりも小規模
- ・AESはLUTを1117、BlockRAMを5つ使う（XILINX＊2）
  → 本機構の2倍の資源を消費
- ・本装置はSDカードのパケットを処理する周辺回路を含んでいるので単体で動作する。

その結果、安価なFPGAでも動作した。
下位モデルTang Nano 1K（1,430円）の半分の回路数で実装可能である。AES回路を実装しようとすると、2倍の回路規模が必要になるため、実装できない可能性が高い。

6.全体のまとめ

外部ストレージのアクセスを軽量にセキュアにする装置を作りました。そのために、私はRAMを使わないようにアドレスのみをシャッフルすることで、回路数は削減できました。しかし、アクセスがすべてランダムアクセスになるため、メモリアクセス自体に速度低下が生じる可能性があります。今後は、実測して、速度低下を軽くする方法の検討をする必要があります。

＊1：2025/11/6 ABCニュース『匿名の封書で生徒の成績データが届き発覚』
https://news.yahoo.co.jp/articles/15052e7f2f49fcc866067041cd1c3e79492cea62
＊2：AESの出典　ハードウェアAES暗号処理とIPsecへの適用
堤大祐　北海道工業試験場報告No.308
https://www.hro.or.jp/upload/27816/308_01.pdf