USB 接続による暗号化デバイスの高速化

Improvement in speed of coding device by USB interface

055091　高橋 健弘

（指導教員　木村 誠聡 教授）

1. まえがき

2004 年以降，大容量な外部記憶装置として USB フラッシュメモリが多く用いられるようになってきた[1]．この USB フラッシュメモリは小型で軽く持ち運びが容易であるということが特徴である．しかしその特徴から置き忘れなどの紛失が多く発生し，個人情報が流出する場合が多々ある[2]．流出を防ぐためには紛失をしないことが一番であるが，人為的なミスを完全に防ぐことは不可能である．そこで転ばぬ先の杖として USB フラッシュメモリに入れるデータを暗号化させることが望まれる．暗号化の種類としては大きく分けて 3 種類あり，ソフトウェアを用いてファイルを暗号化する方法．USB フラッシュメモリに認証機能を付加させる方法．USB 接続による暗号化デバイスを用いる方法[3]が挙げられる．しかしそれぞれ問題点があり，ソフトウェアを用いた暗号化は，用いるソフトウェアが OS に依存するという問題，認証付加は認証装置付加の USB フラッシュメモリ自体に依存し，それ以外の USB フラッシュメモリには用いることができない．USB 接続による暗号化デバイスは，提案されているデバイス構成上低速にならざるを得ないという問題がある．しかし，ソフトウェアと認証付加は導入の際に問題が出るが，USB 接続に折る暗号化デバイスは導入に問題は発生しないため，3 種類の中では有用性が高いとし，問題を解決する価値があるため，この問題を解決するものとする．

2. 従来の暗号化デバイス．

文献 3)によって提案された暗号化装置は，PC―USB フラッシュメモリ間の通信過程で暗号化するように開発されており，PC のホストと暗号化装置のデバイス，暗号化装置のホストと USB フラッシュメモリが接続され，ファイル転送時に暗号化，複合化を行うようにしてある．しかしデータフロー自体は問題ないが，提案されたハードウェア構造に問題がある．図1に問題となっているハードウェア構造を示す．

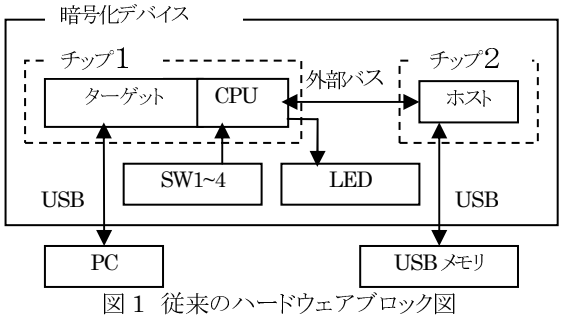

図 1　従来のハードウェアブロック図

3. 提案する暗号化装置

図 1 のハードウェアブロック図でデバイスを開発する場合，ターゲット用のチップとホスト用のチップの間に外部バスが存在する速度が低速になる．外部バスは CPU 制限上 8bit の通信しか出来ないことが理由となる．そこで本稿では用いるハードウェアブロック図を改良することにより高速化が可能となる．図 2 に本稿で提案するハードウェア構成図を示す．このハードウェア構成図ではターゲット機能とホスト機能の両方を持つチップを用いることを提案することで外部バスを用いないようにし，高速化するものである．

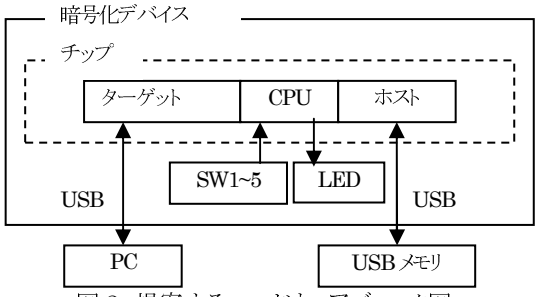

図 2　提案するハードウェアブロック図

4. 実験結果

試作機の開発に時間を要し，最後まで開発することは不可能だったが，一部のデータ通信の結果を見る限りでは高速化には成功している．そのため，全体を開発すれば高速で機能することが可能であると考えられる．とったデータ転送速度の比較表を表1に示す．

表1　速度比較表

システム	速度（KByte/Sec）
文献[3]のシステム	1
提案するシステム	30

5. まとめ

本稿では大筋として文献 3)の手法を用いている．そのため速度の問題を解決することには成功したと考えられるが，開発した試作機は USB1.1 の理想数値には未だ遠いため、未だ高速化の余地はある．また文献 3)に記載されている暗号化の強度の問題は未着である．今後の課題としては更なる高速化と暗号化の強度に関する問題の解決であるといえる．

参考文献

[1]トランジスタ技術　2007 年 2 月号　PP.107―109　CQ 出版社　2007 年 2 月 1 日発行
[2]毎日新聞“個人情報：生徒らの情報入りメモリー紛失　松戸・古ケ崎中2教諭”　2008 年 7 月 13 日発行
[3]平成 19 年度　情報工学科卒業論文要旨集“USB 接続による暗号化デバイスの開発”　PP.85　八木橋　和宏著　2008 年 3 月 21 日発行