# ＰＩＣ１６Ｆ８４を応用した鍵・錠システム

金野茂男

## １．はじめに

盗難防止、プライバシーの保護のために様々な鍵システムが実用化されている。が、殆どの鍵システムではその道のプロの手に掛かると訳もなく開錠されてしまい、防護及び安全対策が追いついていない状況である。

このことを考え、非常に簡単な回路でかつ安価であるが、その秘匿性、即ち他人による開錠は極めて困難な鍵システムとして、ワンチップマイコンを応用し、論理信号パルス列をキーとして用いた鍵システムを構築した。正当な鍵を用いれば、数秒以内で開錠することができる。不正な方法で開錠を試みようとしても開錠することはできる。が、短時間での開錠は不可能である。時間の設定は任意であるが、現時点の設定では、開錠のために数ヶ月以上は必ずかかる鍵・錠システムである。

そのからくりは単純である。鍵を錠に差し込む。鍵側から１０進数６桁の論理信号パルスを、数秒間の時間幅で錠側に送信する。錠側は登録している１０進数６桁の暗号番号と、入力してきた１０進数６桁の開錠番号を比較し、一致すれば、開錠信号を出す。数秒間で１０進数６桁の数値を送受信する。従って、同じ形式の合い鍵を作り、開錠を試みることができるが、１０進数６桁の数値を全て網羅しなければならない。１つの開錠番号で数秒間の時間が必要なので、暗号番号と一致させるためには、数秒×１００００００＝数百万秒　かかることになる。

現時点ではこの鍵・錠システムは試作品である。錠が開いたことをＬＥＤを点灯させることで認識している。実用とするならば、ＬＥＤの点灯信号で同時にリレー、モーター等を駆動することで簡単に実際の錠に適用できるはずである。

## ２．設計及び製作

システムの原理は次の通りである。

鍵側には錠の数に対応させて何種類かの１０進数６桁の暗号番号を登録する。錠側には、特定の一つの暗証番号を登録しておく。開錠したければ、鍵を錠に差し込み鍵側から暗証番号を送信し、それを錠側で受信し、暗証番号が一致すれば、開錠する。

システムの素子数はできるだけ少なくすることを心がけ、図１，２の回路図を作成した。図１は鍵側の回路図、図２は錠側の回路図である。両方の回路図とも極めて単純である。鍵と錠の両方にワンチップマイコンＰＩＣ１５Ｆ８４を使用している。この素子にはＥＥＰＲＯＭが内蔵されており、電源が切れてもデータが保存できる機能が備わっている。暗証番号を記録させておくにはとっておきの機能であるからこの素子を使用することにした。

キー番号及び、暗証番号を１０進数で入力するため、ＢＣＤ４段回転スイッチを用いている。４ビットのＢＣＤコードの各論理電圧値をＲＡ０～ＲＡ３端子に入力し、プログラ

ム内で１０進数に復元する。暗証番号の登録時には、スタートスイッチと選択スイッチを同時に使用する。暗証番号の送信はスタートスイッチだけで行う。１０進数６桁の暗証番号は各桁の数値の回数だけのパルスとして出力ポートＲＢ７から６桁分が順次出力される。そのフローチャートは図３に示している。

ＰＩＣ１６Ｆ８４のＥＥＰＲＯＭは６４バイトである。一つのキー番号に６桁の数値を使用し、各桁の数値に１バイトを割り当てている。従って、１つの暗号番号に６バイト使用しているので、登録できる暗証番号は１０種である。

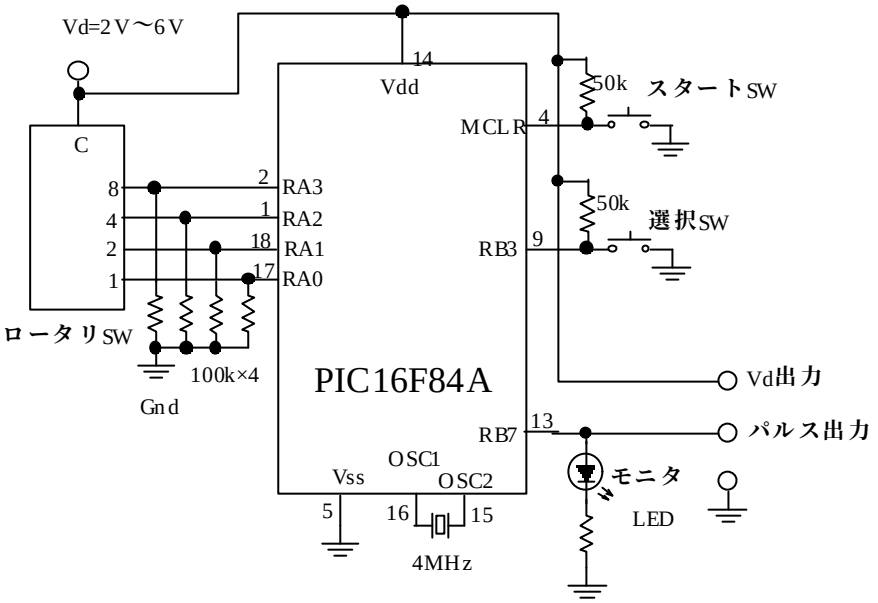



**図１　キー側の回路図**

錠側には電池は用いない。鍵を錠に差し込んだときに、電源は鍵側から供給される。ＰＩＣの正常な動作の開始を保証するため、ＭＣＬＲ端子にＲＣ回路を付加している。コンデンサに並列に付いている抵抗は電源オフ時のチャージの放電用抵抗である。ＭＣＬＲ端子を単純に、Ｈレベルに設定しておき、ピンジャックが結合した時の電源供給開始でプログラムをスタートさせると、時折動作不良を起こしてしまう。鍵からのパルス電圧はＲＡ０端子に入力する。この錠の動作には、暗号番号を登録する場合と、通常の暗号番号を受け付ける場合とがある。スライドスイッチでその動作を切り替える。暗号番号を登録する場合にはスイッチを「暗号登録」側とする。登録が終了したら、「スタンバイ」側としておく。

回路に電源が供給された時点で、プログラムにリセットがかかり、スタートする。選択スイッチが「暗号登録」側であれば、プログラム中の暗号登録の箇所が実行される。「スタンバイ」側であれば、暗号番号を受信し、比較して、一致すれば、黄緑ＬＥＤを点灯する。不一致ならば赤ＬＥＤを点灯する。

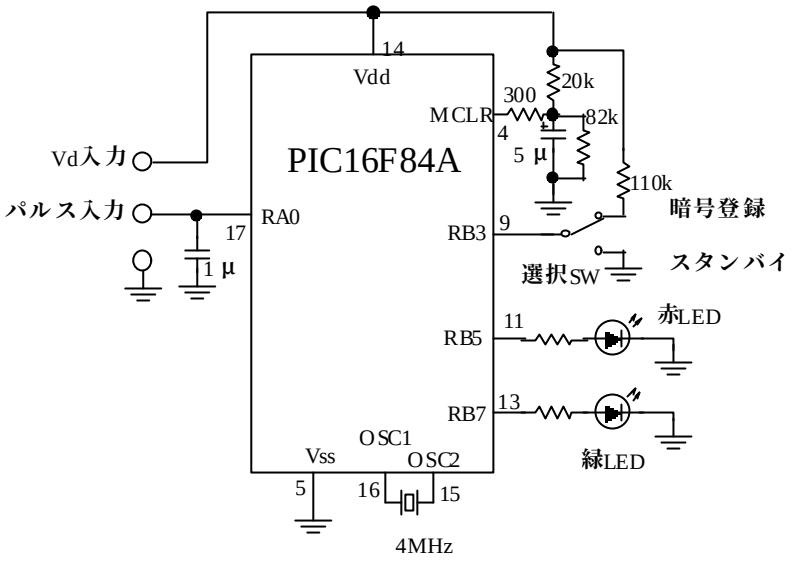
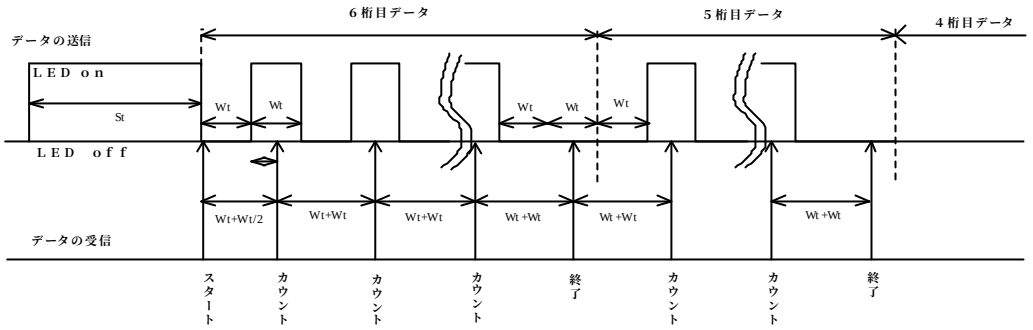



**図２　錠側の回路図**

**図３に鍵側から出力されるパルスのタイミングチャートとそれを受信する錠側のタイミングチャートを示している。錠側で鍵側からのスタートパルスを受信すると、一定時間間隔で入力してくるパルスを計数する。トリガ信号は鍵側から最初に送信されてくるスタートパルスだけである。錠側でこのスタートパルスを認識すると、プログラムは入力パルスの計数を始める。この計数のタイミングは、鍵側と錠側で一致するように前もってプログラム中で設定されている。錠側で、入力してくるＨレベルを認識する毎に計数を行ってはいないことに留意して欲しい。この方法がこのシステムの高度な秘匿性を与えれいるのである。従って、開錠時間を短縮するために、錠側でパルス列を圧縮して送信しても、錠側ではそれに正常に応答しない。このことは、偽の合い鍵を防止する最大の特徴を持っているのである。錠側のタイミングに完全に一致したパルス列でなければならないからである。偽鍵を作り、タイミングも一致させることに成功しても、６桁の数値を全て網羅しなければならないので、開錠には時間がかかることになる。**

**現時点では送受信に必要な最長時間は、暗証番号が９９９９９９の時で約３秒程度に設定している。任意に変更可能である。**




（１）Ｗｔは送信側と受信側とで同じとする。＝timewidshort
調整時には大きな値としておけば、調整し易い。
（２）Ｓｔはデータの送受信開始前のＬＥＤ点灯時間幅である。
適当な長さに設定して良い。＝timewid long
（３）その桁の数値の数だけＬＥＤを点滅させる。桁の終了はＬＥＤ
不点灯で認識させる。これを６桁分繰り返す。

**図３　パルスのタイミングチャート**

## ３．使用方法

錠側には電池はない。錠側の電源は、開錠のため鍵（ピンジャックのオス）を差し込むと鍵側から供給される。鍵側には電源スイッチはない。電池を接続すると電源が入る

鍵側は安定動作にはいると、スリープの省電力モードにはいるので、電池を外す必要はない。電池を外しても、暗号番号はＥＥＰＲＯＭに書き込まれているので消えることはない。

（イ）鍵側に暗号番号を登録する方法

初期状態では、１０個のキー番号には、データが入っていないので、希望するキー番号に予定の暗号番号を設定する操作を行うことになる。

（１）スタートスイッチと選択スイッチを同時に押し、スタートスイッチを離してから、選択キーを離す。ＬＥＤが連続点灯となる。

（２）ダイアルを回し、希望するキー番号を設定し、選択スイッチを１度押す。ＬＥＤ少しの間点滅し、すぐ連続点灯となる。（キー番号が登録された）

（３）１０進数６桁の暗号番号の最初の数値をダイアルで設定し、選択スイッチを１度押す。ＬＥＤが少しの間点滅し、すぐ連続点灯となる。（暗号番号の１つが登録された）

（４）（３）と同じ操作を６回繰り返す。最後の数値を設定し、選択スイッチを押すと、ＬＥＤは消灯する。

（５）これで、希望するキー番号に予定の暗号番号を登録したことになる。

（６）他のキー番号で暗号番号を登録したければ、（１）から繰り返す。

（７）既に登録したキー番号の暗号番号を変更したいときには、（１）からくり返せばよい。暗号番号が上書きされる。

（ロ）錠側に暗号番号を登録する方法

（１）錠側のスライドスイッチをトウロク側としてから、鍵を錠（ピンジャックのメス）に差し込む。

（２）鍵側のダイヤルを、この錠に割り当てたいキー番号に設定し、スタートスイッチを押す。

（３）数秒間以内で、錠側にも暗号番号の登録が完了する。

（４）錠側のスライドスイッチをスタンバイ側とし、鍵を抜き取り、これで登録完了。

（ハ）鍵側及び錠側に暗号番号が登録されている場合。

通常の使用方法である。

（１）錠のピンジャック・メスに鍵のピンジャック・オスを差し込む。

（２）鍵側のダイアルを錠のキー番号に設定する。

（３）ジャックを差し込んでから、１秒以上待って（用は焦らないで）から、錠のスタートスイッチを押す。早過ぎると、プログラムが正常に動作しない場合が時折起こる。

（４）両方の暗号番号が一致すれば、開錠の印として黄緑ＬＥＤが数秒間点灯する。不一致ならば、不成功の印として赤ＬＥＤが数秒間点灯する。

（５）途中で失敗した場合、或いは赤ＬＥＤが点灯した場合には、ジャックを抜いて、再度（１）からやり直す。が、その場合にはジャックは外してから１秒以上立って差し込むこと。焦って早過ぎると、正常に動作しない場合がある。

（ロ）暗号番号を変更したい場合

（イ）の（７）の項で説明している。

４．アセンブラプログラム（ここで添付は省略。プログラムをダウンロードして下さい）

巻末に２つのアセンブラプログラムを添付している。前者は鍵側のＰＩＣ１６Ｆ８４に、後者は錠側のＰＩＣ１６Ｆ８４に書き込んでいる。注釈をできるだけ書き込むようにしているので、理解し易いであろう。

若干理解しがたい所として、ＥＥＰＲＯＭへの書き込み箇所がある。サブルーチン eepromwrite 中の movlw　55h、 movlw　0aah　等である。おまじないのようなステップである。これはＰＩＣ１６Ｆ８４のテクニカルノートに紹介されている手順をそのまま踏襲したものである。テクニカルノートにもその理由については明瞭な説明はしていない。ただ、書き込みには１０m秒程度の長い時間がかかることが記されている。多分何度も書き込みを行い、確実にＥＥＰＲＯＭへのデータの書き込みを保証する方法なのであろう。

１０進数６桁の暗号番号を桁毎に、 keycode6, keycode5, keycode4, keycode3, keycode2, keycode1 の変数に代入している。これを通常のプログラムのように keycode(6) の配列としてやる方法もある。工夫すれば、ＭＰＡＳＭでも配列変数らしきものを取り扱うこともできる。が、それをすると少しプログラムがわかりにくくなること。従って、バグチェックに困難を伴うこと。次数が６なのでそれほどの大きな配列ではないこと。等から、配列

の方法を適用しないこととした。

## ５．終わりに

暗号番号の桁数をより大きくすれば、秘匿性をより高めることができる。開錠に要する時間も短縮することもできる。

このシステムの欠点はいろいろある。

（１）電気回路なので、湿気や水に弱い。
防湿、防水対策はそれほど困難ではない。

（２）ＩＣを用いているので静電気に弱い。
絶縁対策はそれほど困難ではない。

（３）秘匿性が高い故に、鍵を紛失或いは暗号番号を忘却したときの開錠が極めて困難である。
本文中で説明しているが、何ヶ月或いは何年かかけて開錠する方法はある。その他には、錠を破壊する以外に妙案の対策は今のところ無い。

（４）同じく錠側が故障し、開錠できなくなる場合があり得る。
これは錠を破壊する以外に方法がない。