セキュリティ確保に最適なSRAMを使ったマイクロコントローラ

ATM(現金自動預払機)やパスポート認証デバイス、個人認証デバイス、コンビニのPOS端末などは、パスワードやPIN(個人識別番号)、暗号キー、独自の暗号アルゴリズムなどがハッカーによって盗まれないよう保護する必要があります。金融機関では、二重三重の防衛策を講じ、ハードウェアとソフトウェアの両方を守っています。そのため、年間何千億円もの処理を行う金融業務用システム機器の開発には、さまざまな困難があります。

セキュアマイクロコントローラが持つ最も優れた安全機能は、タンパー活動を検出したら直ちにメモリ内容を消去することです。

信頼性を確保するためには、すべてにおいて安全な決済システムが必要です。中央銀行のサーバは、フェンスで囲まれ、関係者以外の立ち入りが禁じられているビルに置くことができますが、そのサーバとつながっている預払機は公共の場所に設置されており、ハッカーは簡単に侵入することができます。マイクロコントローラの周りに物理的保護と補助警報システムを取り付けることは可能ですが、高い技能を持つハッカーなら、電源を切って警報システムを無効にすることができます。このようにして物理的保護が破られてしまっても、保護ケースをマイクロコントローラのタンパー反応型暗号境界と連動させておけば、内部の情報は守ることができます。本当にセキュアな決済システムを実現するためには、高信頼コンピュータを搭載したチップを使うだけでなく、タンパー反応型技術も搭載しておく必要があります。このようにすれば、侵入が試みられた時、演算を行うチップによって秘密キーやプログラムメモリ、データメモリが直ちに消去され、暗号境界は保護されます[1]。セキュアマイクロコントローラが持つ最強の防御策は、タンパー活動が検出されたら一瞬でメモリ内容を消去してしまうことです。DS5250高速セキュアマイクロコントローラは、メモリ内容を消去できるだけでなく、プログラムやデータ保存にSRAMを使用する安価な組込システムの一例です。

物理メモリと信頼関係の構築

組込システムの多くは、柔軟性が高くデバッグが容易に行えるように、汎用コンピュータ上で開発されます。しかし、その結果セキュリティが低下してしまったのでは、利点ではなく大きな欠点になってしまいます[2]。ハッカーはマイクロコントローラの物理メモリを最初に狙うことが多いので、預払機では、適切なメモリ技術を採用することが非常に重要です。ヒューレットパッカード社のHP16500Bなどの市販ロジックアナライザを使えば、アドレスとデータバスの電気信号を物理的にモニタリングし、秘密キーなどメモリ上に記録されている内容や個人データを読み出すことが可能です。このような盗聴行為を防止するためには、メモリバスを暗号化し解読困難にすることと、メモリ内容を電源が落とされてもすばやく消去できるメモリ技術を採用することの2点が重要です。一部の組込システムでは、EPROMやフラッシュメモリなどのフローティングゲートメモリを内蔵したマイクロコントローラの採用によってセキュリティを確保しようとしています。しかし、望ましいのは、記録内容が漏れるメモリ技術ではなく、内容を消去できるメモリ技術です。たしかに、紫外線によって消去できるEPROMなら電気がなくても消去可能ですが、何分にもわたって紫外線を照射しなければならないという弱点があります。フラッシュメモリやEEPROMは、プロセッサが正常に動作し、電源電圧が動作可能範囲に保たれていないと消去できません。このように、フローティングゲートメモリは、セキュアなアプリケーションには不向きです。電源が落ちたあともメモリの状態が保たれるため、ハッカーは、重要なデータを見つけだすために十分な時間をかけられるからです。より望ましいメモリは、電源が遮断されたりタンパー検知回路が起動されたりした時、以下のいずれかの動作を実現できるメモリ(SRAMなど)です。

ハッカーはマイクロコントローラの物理メモリを最初に狙うことが多いので、現金支払機では、適切なメモリ技術を採用することが非常に重要です。

- **電源が落とされると、メモリ内容が失われ、すべてゼロになる。**
- **タンパー検知回路によって、ナノ秒単位で内部メモリと暗号キーが消去できる。**
- **外部メモリは、アプリケーションソフトウェアによって、書込時間100ns以下で消去できる。**

フローティングゲートメモリとマイクロコントローラを同じチップ上に搭載すれば、フローティングゲートメモリの脆弱性をカバーできると思うかもしれません。たしかに、そのようにすれば、メモリへの不正アクセスを防止できます。例えば、内部ロックビットとして1ビットあるいは複数のビットを使用し、プログラミングの最後にロックビットを設定するようになっている構成もあります。ロックビットがセットされると、マイクロコントローラをプリント基板から取り外し、広く使われているユニバーサルエンジニアリングプログラマ、BP-1700(BP

Microsystems社製)などのデバイスプログラマに取り付けても、その内容を読むことができません。ロックビットを消去するためには、メモリ全体を消去するしか方法はありません。つまり、デバイスをプログラミングしなおすことは可能ですが、その途中でメモリ内容はすべて破壊されるわけです。セキュリティをさらに強化する方法として、内部メモリ暗号行列の採用が考えられます。これにより、デバイスプログラマがメモリ内容を検証あるいはダンプしようとすると、メモリ行列の内容が暗号化して出力されるようになります。この技術を採用している例に、インテル社のMCS® 51ファミリのプロセッサがあります。このプロセッサは64ビットのユーザプログラマブルな暗号行列を採用しており、メモリ内容の検証時には、その暗号行列とメモリ内容のXNORが出力されます。このため、暗号行列が分からない限り、検証によって得た情報は意味を持ちません。しかし、このようなロックビット手法にも弱点があります。技術ジャーナルやインターネットのニューズグループでは、EPROMやEEPROM、フラッシュメモリなどのフローティングゲートデバイスをハッキングし、セキュリティロックビットのみを選択的に消去する方法が簡単に見つけられます[3]。消去窓のないプラスチックパッケージに収めたOTP(One Time Programmable)デバイスとすれば、ある程度のロックビットハッキング対策になるというメーカもあります。しかし、「ある程度の対策」ということは、あくまで相対的な違いにすぎません。高温の酸を使えば、ダイを傷つけることなく封止したプラスチックだけを溶かすことができます。その後、Karl Suss PM 8マニュアルProbe Stationなどのシンプルで安価なツールを使ってダイレイアウトを検討すれば、セキュリティロックビットの位置を知ることができます。この方法は、紫外線でデータを消去するタイプのEPROMに対してよく適用されます。封止剤を取り除いたら、ダイに不透明な塗料を塗ったり絶縁テープを貼ったりした上で、ロックビットのところにピンホールをあけます。このような加工を施したデバイスに紫外線を照射すると、メインメモリはそのままでセキュリティロックビットだけが消去されます。その結果、ロックビットなど初めから存在しなかったかのように、ごく普通のプログラマでデータを読み出せるようになります(図1及び図2)。半導体企業では、故障診断を行う時にこのようなやり方をよくします。

フローティングゲートメモリは、セキュアアプリケーションには不向きです。電源が落ちたあともメモリの状態が保たれるため、ハッカーは、重要なデータを見つけだすために十分な時間をかけられるからです。SRAMのようなメモリの使用が望まれます。

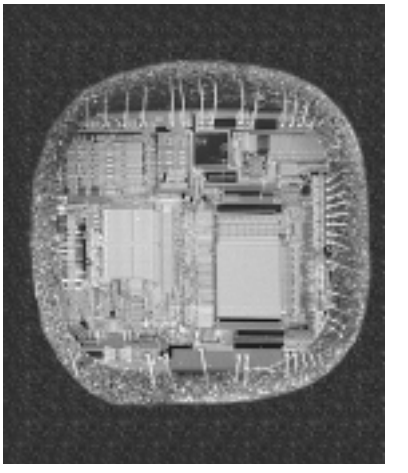

図1. 酸で封止剤を取り除くと、マイクロコントローラダイのEPROMを露出させることができます。

フローティングゲートメモリ技術が持つもう一つの問題は、メモリセルが本質的に不揮発性であり、マイクロコントローラの電源が遮断された後もメモリ内容を保持しているという点です。フローティングゲートデバイスでは、電源遮断後のデータの減衰時間は何百年という単位になります。これは、PKI(公開キー認証基盤)[4]を使用したシステムで秘密キーを長期的に保護しなければならない時、大きな問題になります。それは、デバイスが耐タンパー機能を実行する前に、ハッカーは十分な時間をかけてチップを守る物理的な保護策を破り、メモリにアクセスすることが可能になるからです。

SRAMとスピード

保護レベルの高いセキュアアプリケーションを実現するためには、メモリの読み書き速度が速くなければなりません。メモリの中でもっとも高速なのはSRAMです。SRAMなら、耐タンパー機能の一部として、瞬時に内容を「ゼロ化」して消去することができます。また、SRAMは広く普及しており価格も適度で、かつ、セキュアなデータ保存ができます。SRAMは揮発性メモリですが、バックアップ用リチウム電池を搭載すれば、V_{CC}の供給がない状態で10年以上データを保持させることも可能です。このリチウム電池によってリアルタイムクロックを動かせば、タイムスタンプや日付処理なども行えます。このような機能は、フローティングゲートメモリでは実現不可能です。

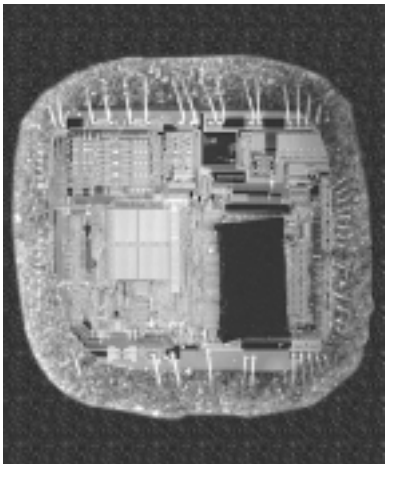

図2. 露出させたEPROMにカバーをかけることで、セキュリティロックビットのみを簡単に消去できます。

処理の認証

金融決済システムを支える信用をつかさどっているのは、預払機に搭載されているPINpadモジュールです。このモジュールは銀行業務の監督官庁やクレジットカード発行者が統制しており、搭載されているセキュアマイクロコントローラには、キーパッドや磁気テープリーダ、スマートカードリーダ、LCDディスプレイなどのデバイスドライバを含むソフトウェアが内蔵されています。また、汎用ホスト(PC、486、ARM)と高速シリアル通信を行う機能や、セキュアなエンドトゥエンド通信を行うためのPKI暗号ルーチンなども搭載されています。PINpadモジュールマイクロコントローラのメモリ搭載量は数百キロバイトに達し、シングルチップに搭載しようとすると高コストになってしまうため、外部メモリが使用されます。この時、すでに述べたように、マイクロコントローラと外部メモリ間で暗号強度の高い通信を行わないと、外部メモリの内容を簡単に盗まれてしまいます。そのような暗号スキームを実現するためには、以下のように、互いに依存し合う複数の条件が満足されなければなりません。

MCSは、Intel Corporationの登録商標です。

決済システム用EMV ICカードの仕様に関する関連情報は、www.emvco.comをご覧ください。

- 暗号化・復号化処理の速度は、命令実行速度と同等でなければなりません。暗号処理は、プログラムがデータを要求するごと、あるいは、DES(データ通信用暗号標準)のようなブロック暗号化を採用していれば何バイトかごとに行わなければなりません。暗号アルゴリズムは、強度が高く高速で、しかも、ハードウェアで構成されていなければなりません。優れたソリューションとして、現在、専用のオンチップ3DES (トリプルDES)ハードウェアを使う3DESがあります。この方が、シングルDES暗号コア1台で複数回の処理を行うよりもはるかに高速で処理できます。

- 暗号エンジンではデータを高速で読み書きするので、外部メモリにはSRAMを使う必要があります。SRAMはバッテリバックアップとし、耐タンパー機能によってすばやく内容を消去できるようにします。

- 暗号キーなど、暗号処理を左右するデータは、プロセッサ外から見えないようにしなければなりません。暗号キーの少なくとも一部は、プロセッサで生成し、安全に保管する必要があります。また、耐タンパー機能では、暗号キーを消去し、外部メモリを解読不能にできなければなりません。

SRAMはメモリの中で最も高速で、耐タンパー機能の一部として、瞬時に内容を「ゼロ化」して消去することができます。

- 初期ロード及びプログラムとデータの暗号処理は、マイクロプロセッサ内に搭載したブートローダで行います。こうすればアプリケーションコードを不正に見られなくなるとともに、暗号方式を隠すことにもなります。つまり、ブートローダがファイアウォールとしても機能するわけです。ブートローダは、すでにロードした情報へのアクセスを拒否するだけでなく、悪意のエージェントによって不正なソフトウェアがロードされないように防ぐ必要があります。不正なソフトウェアとしては、作動中のPINpadやATMに侵入し、正規ソフトウェアを消去して、ユーザに知られないようにPIN番号を集めるソフトウェアをロードするなどの例が考えられます。このように、悪意のエージェントによる傍受やデコードを防止するため、ブートローダ・ホストシステム間の通信を暗号化する必要があります。

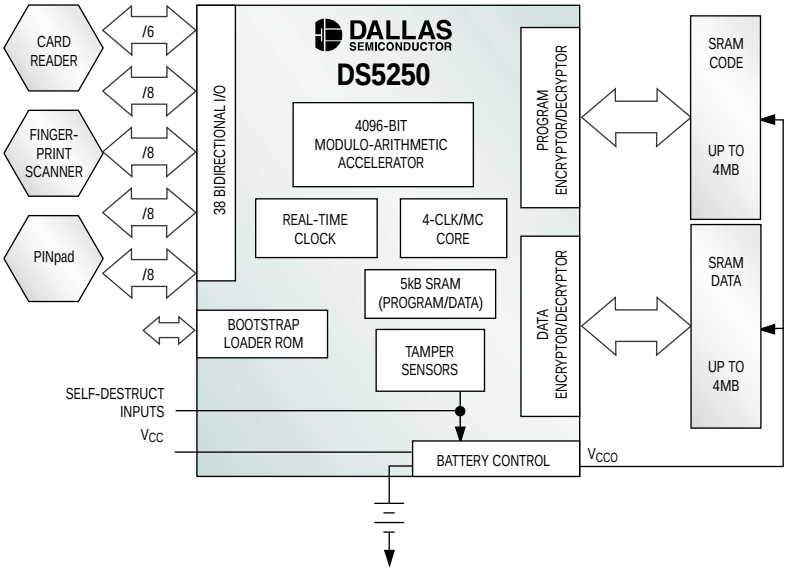

図3. DS5250はプログラムとデータ用に8MBの外部SRAMを持ち、6.25MIPSを実行することができます。

オールインワンのDS5250

SRAMにプログラムとデータを記憶し、暗号処理を行う組込システムを構築することは可能です。当社のセキュアマイクロコントローラ、DS5250も、まさにそういうシステムです(図3)。DS5250はプログラムとデータ用に8MBの外部SRAMを持ち、8051ベースの命令を1秒あたり625万も実行することができます。機密度の高い情報は、5kBの内部データメモリに格納します。SRAMデータの保持は、マイクロプロセッサに搭載されたバッテリスイッチング専用ハードウェアにより、V_{CC}かバッテリ電力を外部メモリに供給することによって行います。このシステムには、ISO-7816準拠のスマートカードリーダや指紋スキャナ、キーパッドなどの認証用周辺機器を接続することができます。

プログラムバスとデータバスに専用暗号復号エンジンを搭載し、外部バスのセキュリティを確保します。DS5250のプログラムメモリバスには8バイトのブロック暗号(シングルDESか3DES)が施されます。データメモリバスについても、専用ハードウェアによるリアルタイム暗号処理がオプションで用意されています。キーの生成に使用する真乱数発生器は、FIPS(米連邦情報処理規格)140-1(FIPS PUB 140-1)、「*暗号モジュールのセキュリティ要件*」のSection 4.11.1で規定された統計的乱数発生器テストに合格したものです。プログラムメモリの完全性検査機能も備えており、各ブロックのチェックサムを前回の計算値と比較することによってメモリセキュリティを高めています。記録されている前回値と新しいブロックチェックサムが異なっていると、ユーザプログラマブルの耐タンパー機能が起動され、改ざん攻撃を防止するのです。

DS5250は、NV SRAMのサポート以外にも、システムセキュリティを高めるさまざまな機能を備えています。高性能の4096ビットモジュロ演算アクセラレータ(MAA)を持ち、1024ビットのモジュロ累乗法によるRSA暗号演算を6ミリ秒以内で行えます。5kBの内部SRAMは、秘密キーの保管に使ったり、データメモリやプログラムメモリとして、また、MAAのスクラッチパッドメモリーとして使うことができます。アプリケーションソフトウェアは、二重キーの3DES暗号アルゴリズムを用いたブートローダチャレンジレスポンスプロトコルによってシリアルポート

から安全にロードすることができます。ブートローダソフトウェアについては、DS5250によってマイクロコントローラのセキュリティ機能を十分に活用し、個別のアプリケーションに合わせたものを開発することも可能です。

マイクロプロセッサのダイに対して物理的な攻撃が加えられると、内蔵タンパーセンサが耐タンパー機能を起動し、外部メモリの復号に使う暗号キーを消去します。自己破壊入力ピンにユーザ定義センサかスイッチをつないでおけば、暗号キー消去に加え、内蔵のプログラムデータ用RAMの内容も破壊することができます。また、自己破壊入力をオンにするとSRAMへの電源供給が遮断されるので、プログラムメモリとデータメモリもすべて消失されます。外部ピンに接続された自己破壊割込ソースがあるおかげで、各構成で必要とされる特殊な耐タンパー機能を柔軟に構築することが可能なのです。しかも、DS5250セキュアマイクロコントローラはタンパー反応型の暗号境界も内蔵しているため、外付け耐タンパー機能によるシステムコストの上昇が避けられます。図4A及び図4Bは、よく行われるセキュリティ確保の方法とDS5250を用いた方法を比較したものです。

安全で確実に

PINpadやPOS端末、ATMなどの金融用端末は、処理する秘密情報をRAMやROMに記録しています。そのため、メモリが金融業務のセキュリティを左右するのです。向上し続けるハッカーの能力に対応するため、秘密情報を保護するセキュリティも高度化していかなければなりません。保護方法はいろいろと考えられますが、組込メモリ内容の保護には暗号SRAMがベストです。

最も重要な点は、DS5250高速セキュアマイクロコントローラなら、金融業界で求められる重要情報の保護と信頼性の高い決済システムの構築が可能だということでしょう。危険な状況になれば、耐タンパー機能によって、秘密キーやプログラム、データがすべて消去され、データは安全かつ確実に保たれるのです。

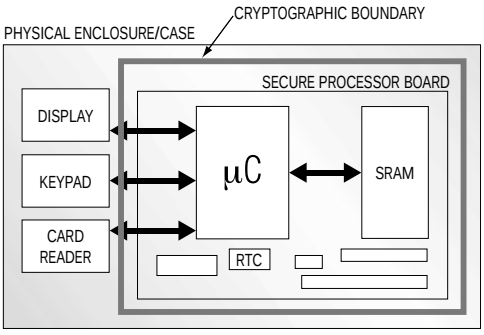

図4A. 汎用マイクロコントローラと周辺機器やメモリを組み合わせ、高価なタンパーセンサを複数用いてプリント基板全体を保護することで、セキュアなコンピュータを構築しようとすることがよくあります。

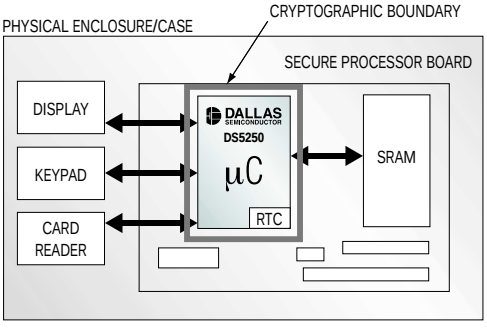

図4B. タンパー反応型の暗号境界も内蔵しているDS5250セキュアマイクロコントローラなら、外付けの耐タンパー機能は不要で、システムコストが削減されます。

参考文献

1. Smith, Sean; Palmer, Elaine; Weingart, Steve. *Using a High-Performance, Programmable Secure Coprocessor*. Proceedings of the Second International Conference on Financial Cryptography, Springer-Verlag Lecture Notes in Computer Science, 1998.

2. J. D. Tygar and B. S. Yee. *Dyad: A System for Using Physically Secure Coprocessors*. Proceedings of the joint Harvard-MIT Workshop on Technological Strategies for the Protection of Intellectual Property in the Network Multimedia Environment, April 1993.

3. A variety of sources discuss this subject, and can be found via a web search engine using the keywords “EPROM,” “plastic,” and “acid.”

4. RSA Laboratories. *PKCS #1 v2.1: RSA Cryptography Standard*, Bedford, Massachusetts, 2002.