AN1879
アプリケーションノート

M41ST87W のタンパー検出・RAM クリアの使用方法

はじめに

M41ST87W は、最新のオンチップセキュリティソリューションを提供するスーパバイザー製品です。このタンパー検出・RAM クリア回路は、機密上重要なデータを改竄から守るあらゆるシステムに使用可能です。このチップは、クレジットカード端末から POS 端末や電気式データメータなど様々な用途のセキュリティ保護に使用できます。M41ST87W は、システム改竄の検出とタイムスタンプ記録を行い、イベント発生時にはデバイスメモリを消去する機能を備えています。これにより、改竄事象の発生時には、デバイスメモリや外付け RAM を消去し、侵入者がメモリに格納されたデータにアクセスするのを阻止します。

コンテンツ

1 説明

1.1 動作内容

M41ST87W デバイスには、$TP1_{IN}$ と $TP2_{IN}$ の 2 本の独立したタンパー入力ピンがあり、異なる 2 つの信号の監視に使用できます。この 2 本のタンパー入力ピンは、1) スイッチ（ノーマルオープン）を閉じてグラウンドまたは V_{OUT} に接続するか、2) グラウンドまたは V_{OUT} に接続された閉じているスイッチ（ノーマルクローズ）を開くかのいずれかの方法により、タンパーイベントの発生を示すように設定できます。スイッチの開閉については、タンパーレジスタで設定するビットを用いて設定可能です。

M41ST87W デバイスには 128 バイトの内部 RAM が備わっており、タンパーレジスタの TEB ビットと CLR ビットの設定によりクリアすることも自由にできます。

1.2 タンパーレジスタを用いて外付けメモリをクリア

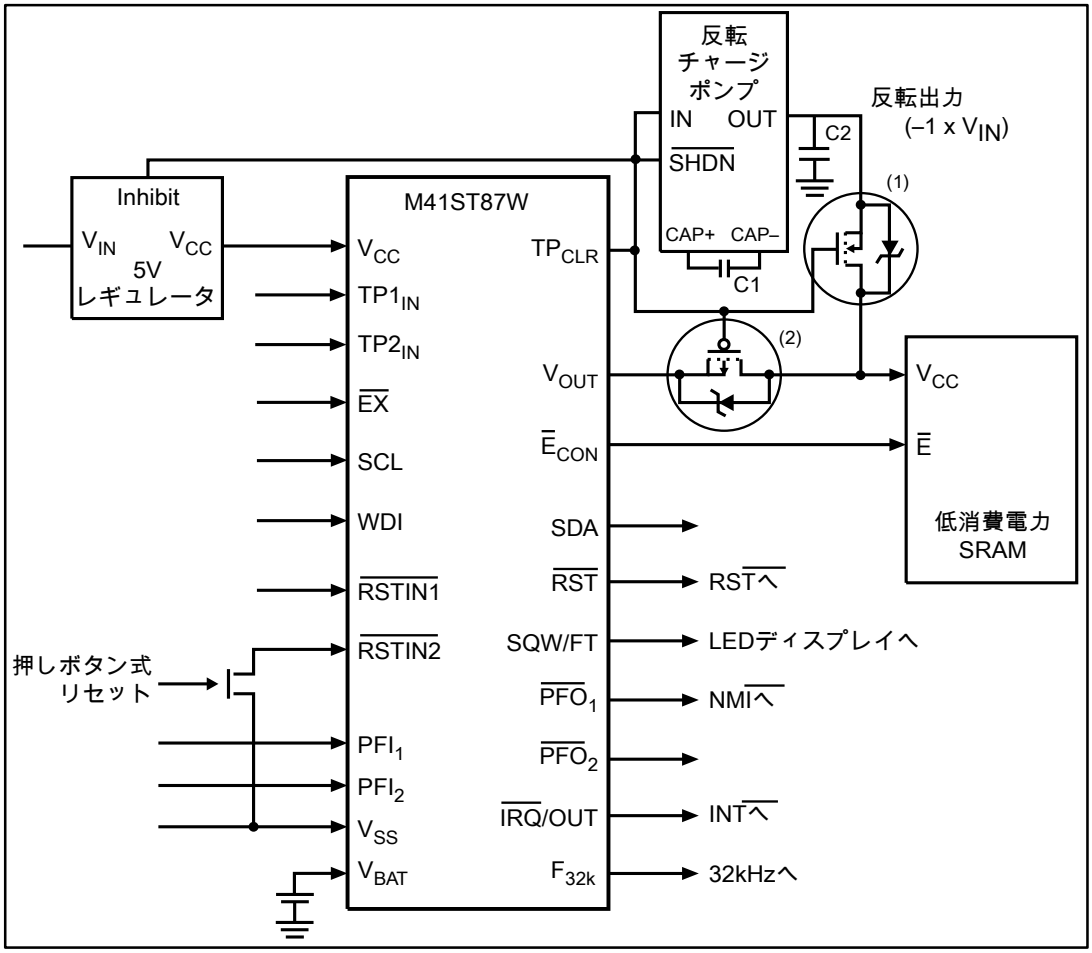
M41ST87W は、タンパーレジスタの TEB ビットと CLREXT ビットの設定により、バッテリーバックアップされたデバイスの外付け SRAM のクリアも可能です。外付けメモリをクリアまたは消去するには、SRAM の V_{CC} をグラウンドに接続する方法があります。ただし、ある特定の SRAM では、単純に V_{CC} を接地するとメモリが消去されるまでにかなりの時間が必要となります。妥当な時間以内にメモリを消去するためには、SRAM の V_{CC} を負の電圧とする方法もあります。V_{CC} を負の電圧とすることにより、入力保護ダイオードがターンオンしてメモリが消去される導通モードとなります。

1.3 外付けチャージポンプを用いて外付けメモリをクリア

タンパー状態の間、SRAM の V_{CC} を負電圧までドライブするためには、M41ST87W に外付けチャージポンプデバイスを使用する必要があります。 図 1 にこの回路の接続方法を示します。M41ST87W にチャージポンプデバイスを使用した場合、MOSFET を 2 個追加して、通常動作時にはチャージポンプの出力（OUT）から、タンパー状態では M41ST87W デバイスの V_{OUT} から、M41ST87W の V_{OUT} を分離する必要があります。通常動作時には、TP_{CLR} 信号は強制的に Low となり、チャージポンプが無効化されます。無効化されると、多くのチャージポンプの出力は強制的にグラウンドとなります。SRAM の正しい動作を可能とするには、MOSFET(1)はオフとし、チャージポンプの出力から SRAM の V_{CC} を分離する必要があります。同時に、P チャンネル MOSFET(2)はオンとなって SRAM に電源を供給します。

タンパー状態では、TP_{CLR} 信号が強制的に High となって DC レギュレータの inhibit ピンを制御します。これにより、t_{CLR} の間、レギュレータは STANDBY モードとなります。t_{CLR} はタンパークリアタイミングであり、レジスタの CLRPW1 ビットと CLRPW0 ビットの設定次第で 1、4、8 または 16 秒の間、レギュレータがオフとなります。TP_{CLR} 信号によってもチャージポンプは有効となります。チャージポンプが有効になると、OUT によって（設定可能な期間）SRAM の V_{CC} ピンに負の電圧が生じ、データが消去されます。M41ST87W の V_{OUT} 出力の寄生ダイオードが順バイアスされることによる M41ST87W のデータ消去を避けるため、M41ST87W は SRAM の V_{CC} から分離されている必要があります。この状態は、TP_{CLR} 信号を用いて N チャンネル MOSFET(1)をオン、P チャンネル MOSFET(2)をオフとすることで実現されます。

図 1: 回路接続

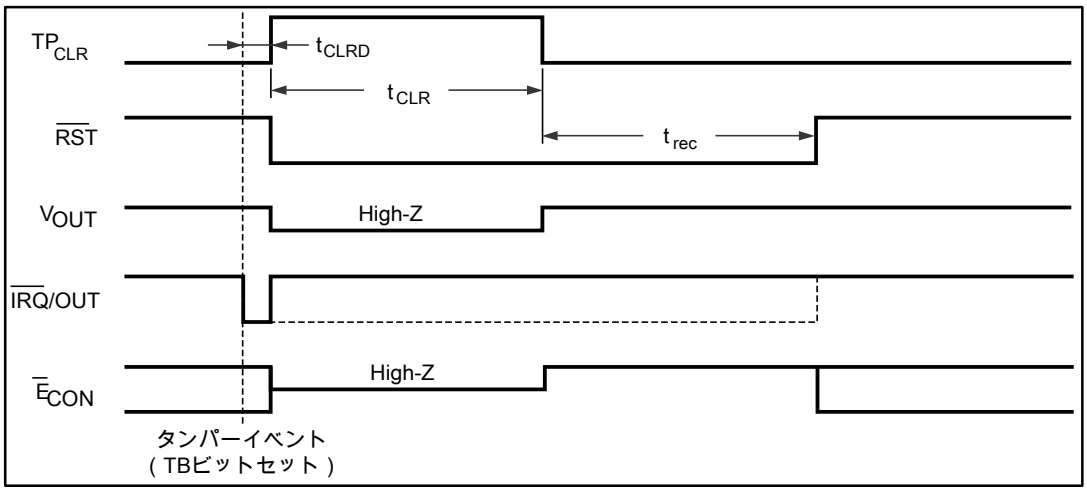


1. N チャンネル MOSFET
2. P チャンネル MOSFET

1.4 RAM クリアデータ

メモリをクリアするための時間は、外付け SRAM に用いられたプロセス技術に依存しますので、ばらつきを考慮した一定時間、VCC ピンを負の電位とする必要があります。M41ST87W デバイスでは、個々のアプリケーションに要求される時間を設定することが可能となっています。日データレジスタの中にあるコントロールビットの CLRPW0 と CLRPW1 により、タンパーイベント中の tCLR パルス幅の時間長が決まります（*図 2: "タンパー出力タイミング"*参照）。こうすることで、負パルスの電圧と時間長を制御して、さまざまな LPSRAM に対する回路を設定できます。

図 2: タンパー出力タイミング



注: タイミングの詳細については、M41ST87W データシートを参照してください。

1.5 タンパータイムスタンプ

デバイスが改竄された場合には、どの改竄が最初に起こったかにかかわらず、クロックレジスタの更新を停止するタイムスタンプが発生し、ユーザーは、改竄が行われた時間を知ることができます。直ちにタンパービット（フラグレジスタ内の TB1 と TB2）がセットされます。したがって、改竄が発生した場合には、まず時間レジスタを読み込んでタンパーイベントが発生した時刻を正確に割り出した後、フラグレジスタを読み込んでどのタンパー条件がトリガされたか確認することもできます。タンパーレジスタの TEB ビットをリセットすると、クロックは現在時刻まで更新されます。現在時刻を読み出すためには、該当する TEB ビットが常に 0 にリセットされている必要があります。タンパー検出機能は、V_{CC} 状態でもバッテリーバックアップ状態でも動作します。

2 まとめ

クレジットカード詐欺や個人情報の盗用が増加する中で、ST は、セキュアな RTC 新製品群により、この機密上重要なデータを保護する方法をリードしています。機密上重要なデータは、ATM 装置や POS 端末のような大半の機器の内部メモリや外付けメモリに格納されています。M41ST87W が提供するソリューションによって、これらの機器が改竄されたことを早期に検知し、侵入者がこのデータにアクセスする前に RAM をクリア可能です。

3 改版履歴

表 1: 表 1. 文書改版履歴

日	版	変更内容
2004 年 2 月 4 日	1	初版リリース
2004 年 4 月 12 日	2	文書フォーマットを変更。ベンダ SRAM 情報(表 1)を更新。
2004 年 6 月 3 日	3	図(*図 1: "回路接続"*)を修正。
2009 年 1 月 16 日	4	文書フォーマットを変更。カバーページ、*セクション 1.3: "外付けチャージポンプを用いて外付けメモリをクリア"*、*図 1: "回路接続"*、RAM クリアデータを更新。
2013 年 10 月 16 日	5	表 1(各種ベンダの RAM クリアデータ)を削除し更新。*セクション 1.4: "RAM クリアデータ"*

表 2: 表 2. 日本語版文書改版履歴

日	版	変更内容
2016 年 6 月 17 日	1	日本語版 初版リリース

重要なお知らせ (よくお読み下さい)

STMicroelectronics NV およびその子会社(以下、ST)は、ST 製品及び本書の内容をいつでも予告なく変更、修正、改善、改定及び改良する権利を留保します。購入される方は、発注前に ST 製品に関する最新の関連情報を必ず入手してください。ST 製品は、注文書発行時点で有効な ST の販売条件に従って販売されます。

ST 製品の選択並びに使用については購入される方が全ての責任を負うものとします。購入される方の製品上の操作や設計に関して ST はー切の責任を負いません。

明示又は黙示を問わず、ST は本書においていかなる知的財産権の実施権も許諾致しません。

本書で説明されている情報とは異なる条件で ST 製品が再販された場合、その製品について ST が与えたいかなる保証も無効となります。

ST および ST ロゴは STMicroelectronics の商標です。その他の製品またはサービスの名称は、それぞれの所有者に帰属します。

本書の情報は本書の以前のバージョンで提供された全ての情報に優先し、これに代わるものです。