

ISO/IEC 14443タイプB準拠  
セキュアメモリ

MAX66040

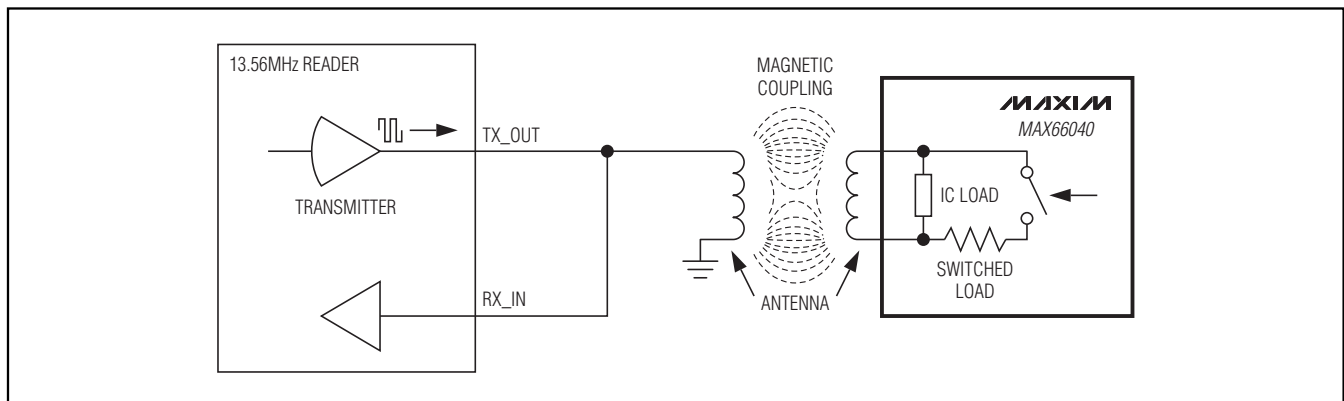
## 概要

MAX66040は、1024ビットのユーザーEEPROMと、セキュアハッシュアルゴリズム (SHA-1) チャレンジ&レスポンス認証 (ISO/IEC 10118-3 SHA-1)、64ビットの固有ID (UID)、1つの64ビットのシークレット、および13.56MHz RFインタフェース (ISO/IEC 14443 タイプB、パート2~4) をシングルチップに組み合わせています。メモリは、8バイトx 16ブロックに加えて3ブロック (シークレット用1ブロックとデータおよび制御レジスタ用2ブロック) で構成されています。シークレット以外の各ブロックは、ユーザーによる読取りが可能な書き込みサイクルカウンタを備えています。隣接する4つのユーザーEEPROMブロックが1つのメモリページを形成します (ページ0~3)。内蔵のSHA-1エンジンは、デバイスのEEPROMのデータと64ビットのシークレットを使用して、デバイスに対する読取りと書き込みの両方についてセキュアな対称形の認証を保証するためのメッセージ認証コード (MAC) を提供します。メモリ保護機能として書き込み保護とEPROMエミュレーションがあり、個々のメモリページについてユーザーが設定可能です。また、ページ3は読取り保護も可能であり、認証の強度を高めることができます。メモリアクセスは、ブロック送信プロトコル (ISO/IEC 14443-4) を介して行われ、デバイスがACTIVE状態になると要求および応答がブロックを介して交換されます。データレートは最大847.5kbpsが可能です。リーダは、26バイトのフレームサイズをサポートする必要があります。このデバイスは、アプリケーションファミリ識別子 (AFI) とカード識別子 (CID) をサポートしています。サポートされていないISO/IEC 14443機能は、チェイニング、フレーム待ち時間延長、および電力表示です。

## アプリケーション

ドライバID (車両アプリケーション)  
アクセス制御  
E-Cash (電子マネー)  
資産トラッキング

## 標準動作回路



## 特長

- ◆ ISO/IEC 14443 (パート2~4) タイプBインタフェースに完全準拠
- ◆ キャリア周波数: 13.56MHz  $\pm$ 7kHz
- ◆ ブロックロック機能、書き込みサイクルカウンタ、およびオプションでEPROMエミュレーションモードを備えた1024ビットのセキュアユーザーEEPROM
- ◆ 64ビットUID
- ◆ 160ビットのMACの計算とシークレットの生成を行う512ビットSHA-1エンジン
- ◆ 相互認証: 64ビットのシークレットを知っているホストがデバイスから読み取ったデータを検証および認証
- ◆ 読取りおよび書き込み (64ビットブロック)
- ◆ AFIおよびCID機能をサポート
- ◆ プログラミング時間: 10ms (max)
- ◆ 書き込み: 10% ASK変調 (105.9kbps、211.9kbps、423.75kbps、または847.5kbps時)
- ◆ 読取り: BPSK変調サブキャリアを使用する負荷変調 (105.9kbps、211.9kbps、423.75kbps、または847.5kbps時)
- ◆ 書き込み/消去サイクル: 20万回 (最小)
- ◆ データ保持期間: 40年 (最低)

## 型番

| PART             | TEMP RANGE     | PIN-PACKAGE |
|------------------|----------------|-------------|
| MAX66040E-000AA+ | -25°C to +50°C | ISO Card    |
| MAX66040K-000AA+ | -25°C to +50°C | Key Fob     |

+は鉛 (Pb) フリー/RoHS準拠パッケージを示します。

機械設計図はデータシートの最後に記載されています。

# ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

## ABSOLUTE MAXIMUM RATINGS

Maximum Incident Magnetic Field Strength .....141.5dBμA/m  
Operating Temperature Range .....-25°C to +50°C

Relative Humidity .....(Water Resistant)  
Storage Temperature Range .....-25°C to +50°C

*Stresses beyond those listed under "Absolute Maximum Ratings" may cause permanent damage to the device. These are stress ratings only, and functional operation of the device at these or any other conditions beyond those indicated in the operational sections of the specifications is not implied. Exposure to absolute maximum rating conditions for extended periods may affect device reliability.*

## ELECTRICAL CHARACTERISTICS

(T<sub>A</sub> = -25°C to +50°C.) (Note 1)

| PARAMETER                                     | SYMBOL | CONDITIONS          | MIN                           | TYP    | MAX    | UNITS  |
|-----------------------------------------------|--------|---------------------|-------------------------------|--------|--------|--------|
| SHA-1 ENGINE                                  |        |                     |                               |        |        |        |
| SHA-1 Computation Time                        | tCSHA  |                     | Refer to the full data sheet. |        |        | ms     |
| EEPROM                                        |        |                     |                               |        |        |        |
| Programming Time                              | tPROG  |                     | 9                             |        | 10     | ms     |
| Endurance                                     | NCYCLE | At +25°C            | 200,000                       |        |        | cycles |
| Data Retention                                | tRET   |                     | 40                            |        |        | years  |
| RF INTERFACE                                  |        |                     |                               |        |        |        |
| Carrier Frequency                             | fC     | (Note 1)            | 13.553                        | 13.560 | 13.567 | MHz    |
| Operating Magnetic Field Strength<br>(Note 1) | H      | At +25°C, MAX66040E | 110.0                         |        |        | dBµA/m |
|                                               |        | At +25°C, MAX66040K | 123.5                         |        |        |        |
| Power-Up Time                                 | tPOR   | (Note 2)            | 1.0                           |        |        | ms     |

**Note 1:** System requirement.

**Note 2:** Measured from the time at which the incident field is present with strength greater than or equal to H<sub>(MIN)</sub> to the time at which the MAX66040's internal power-on reset signal is deasserted and the device is ready to receive a command frame.  
Not characterized or production tested; guaranteed by simulation only.

# ISO/IEC 14443タイプB準拠 セキュアメモリ

## 詳細

MAX66040は、1024ビットのユーザーEEPROM、128ビットのユーザーおよび制御レジスタ、64ビットのUID、1つの64ビットのシークレット、512ビットSHA-1エンジン、および13.56MHz RFインタフェース(ISO/IEC 14443タイプB、パート2~4)をシングルチップに組み合わせています。メモリは、各8バイトx 19ブロックで構成されています。シークレット以外の各ブロックは、ユーザーによる読取りが可能な書込みサイクルカウンタを備えています。隣接する4つのユーザーEEPROMブロックが1つのメモリページを形成します(ページ0~3)。メモリ保護機能として書込み保護とEPROMエミュレーションを備えており、個々のメモリページについてユーザーが設定可能です。また、ページ3は読取り保護も可能であり、認証の強度を高めることができます。MAX66040へのアクセスは、ISO/IEC 14443-4ブロック送信プロトコルを介して行われ、デバイスがACTIVE状態になると要求および応答が1ブロックを介して交換されます。リーダは、少なくとも26バイトのフレームサイズをサポートする必要があります。データレートは最大847.5kbpsが可能です。MAX66040はAFIおよびCIDをサポートしています。サポートされていない機能は、チェイニング、フレーム待ち時間延長、および電力表示です。MAX66040のアプリケーションには、ドライバID(車両アプリケーション)、アクセス制御、電子マネー(e-Cash)、および資産トラッキングが含まれます。

## 概要

図1に、MAX66040の主な制御およびメモリセクション間の関係を示します。このデバイスは、64ビットの

UID、64ビットの読取り/書き込みバッファ、256ビットx 4ページのユーザーEEPROM、8バイトx 2ブロックのユーザー/制御レジスタ、64ビットのシークレットのメモリ、および512ビットSHA-1エンジンという、6つの主要データ要素で構成されています。図2に、ISO/IEC 14443タイプB準拠アクセスプロトコルの階層構造を示します。メモリおよび制御機能にアクセス可能になるためには、最初にマスターがネットワーク機能コマンドを適用してMAX66040をACTIVE状態にする必要があります。これらのネットワーク機能コマンドに必要なプロトコルについては、「ネットワーク機能コマンド」の項で説明します。MAX66040がACTIVE状態になると、マスターは利用可能なメモリおよび制御機能コマンドの中から任意の1つを発行することができます。そのコマンドが完了した時点でMAX66040はACTIVE状態に戻り、マスターは次のメモリおよび制御コマンドを発行するか、またはデバイスの選択を解除してHALT状態に戻すことができます。これらのメモリおよび制御機能コマンドのプロトコルについては、「メモリおよび制御機能コマンド」の項で説明します。すべてのデータは、最下位バイト(LSB)の最下位ビット(LSb)から順に読み書きが行われます。

## 寄生電力

MAX66040はワイヤレスデバイスであるため、どのような電源にも接続されません。動作のためのエネルギーを周囲のRFフィールドから取得します。周囲のRFフィールドは、「Electrical Characteristics (電気的特性)」の表に記載された最小強度を備えている必要があります。

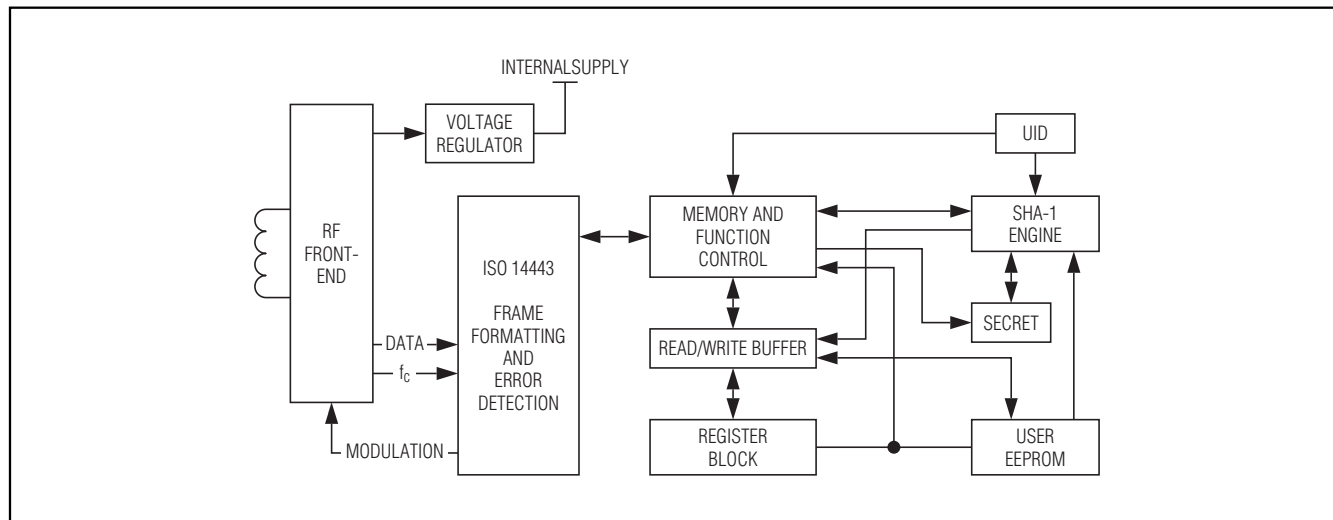


図1. ブロック図

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

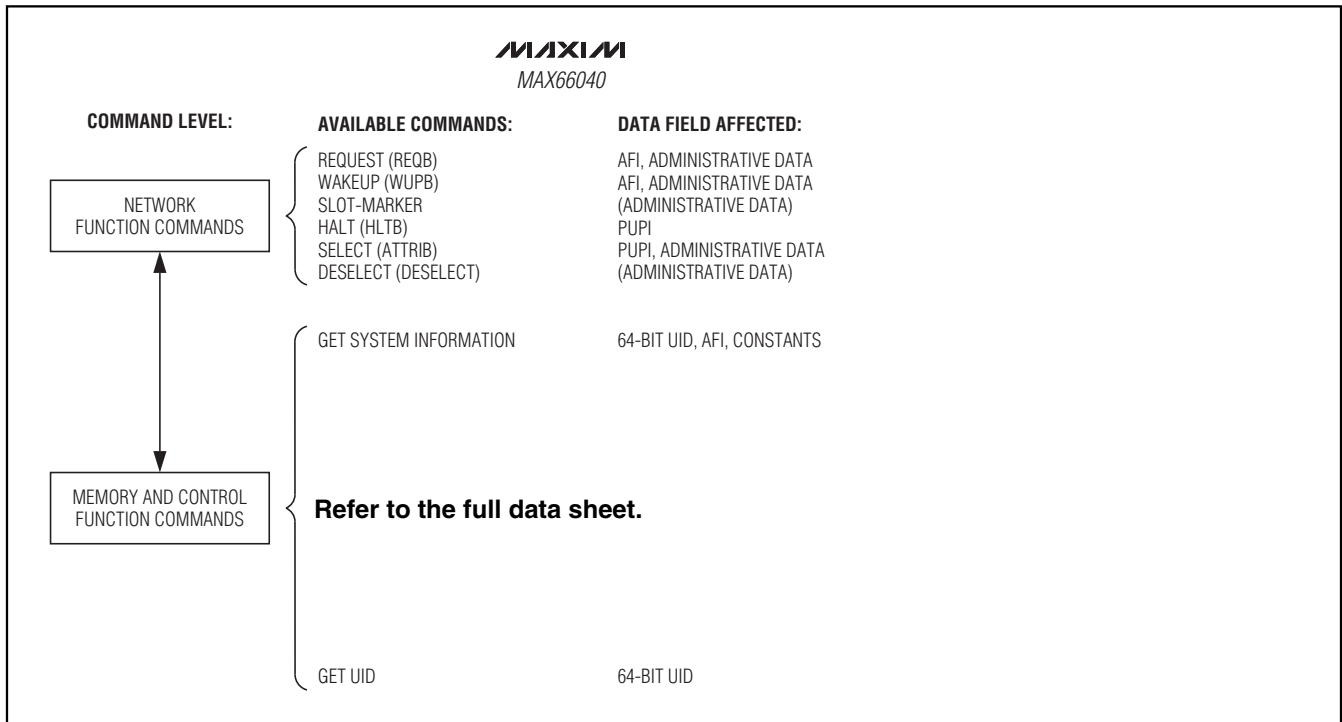


図2. ISO/IEC 14443タイプBプロトコルの階層構造

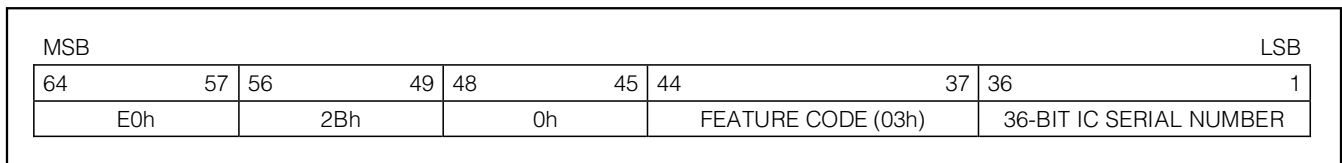


図3. 64ビットUID

### 固有ID番号(UID)

個々のMAX66040には、出荷時にプログラムされロックされる64ビット長のID番号が格納されています(図3)。下位36ビットは、チップのシリアル番号です。次の8ビットには、デバイスの機能コードである03hが格納されます。ビット45~48は0hです。ビット位置49~56のコードは、ISO/IEC 7816-6/AM1に従ってチップメーカーを特定します。Maximの場合、このコードは2Bhです。最上位8ビットのコードはE0hです。UIDは、Get UID コマンドおよびGet System Informationコマンドを介して読取りアクセスが可能です。UIDの下位32ビットは、REQB、WUPB、またはSLOT-MARKERコマンドに対するATQB応答のPUPIフィールドで送信されます。デフォルトでは、UIDの上位32ビットは出荷時にアプリケーションデータフィールドに書き込まれ、ATQB応答の一部として送信されます。こうして、マスターはスレーブ

からの最初の応答で完全なUIDを受信します。詳細については、「ネットワーク機能コマンド」の項を参照してください。

### メモリの詳細

この情報についてはフルデータシートをご参照ください。

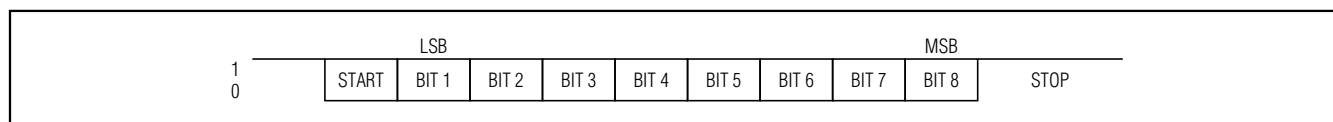


図5. ISO/IEC 14443のデータキャラクタ形式

### ISO/IEC 14443タイプBの通信の概念

マスターとMAX66040 (スレーブ)の間の通信は、データパケットの交換に基づいています。マスターが各トランザクションを開始し、どの時点においても一方の側(マスターまたはスレーブ)のみが情報を送信します。データパケットを構成する各キャラクタは、常にSTARTビットで始まり、通常は1つ以上のSTOPビットで終了します(図5)。最下位データビットが最初に送信されます。データキャラクタは8ビットです。各データパケットは、スタートオブフレーム(SOF)キャラクタで始まり、エンドオブフレーム(EOF)キャラクタで終了します。EOF/SOFキャラクタは9つのすべて0のデータビットで構成されます(図6)。SOFには2つのSTOPビットがあり、そのあとにデータ

キャラクタが送信されます。SOFとEOFの間に少なくとも3バイトが存在するデータパケットは、フレームと呼ばれます(図7)。ISO/IEC 14443タイプBフレームの最後の2データキャラクタは、CRC-16-CCITTの多項式に従って生成した先行するデータキャラクタの16ビットCRCを反転したものです。このCRCは、LSBから順に送信されます。CRC-16-CCITTの詳細については、ISO/IEC 14443-3のAnnex Bを参照してください。ネットワーク機能コマンドの場合、コマンドコード、パラメータ、および応答がSOFとCRCの間に埋め込まれます。メモリ機能コマンドの場合、コマンドコード、およびパラメータが1ブロック(「ブロックタイプ」の項を参照)の情報フィールドに配置され、さらにその1ブロックがSOFとEOFの間に埋め込まれます。

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

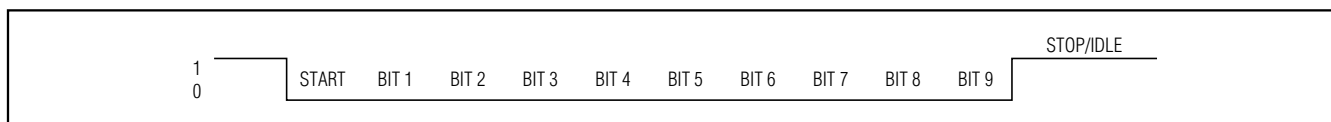


図6. ISO/IEC 14443 SOF/EOFのキャラクタ形式

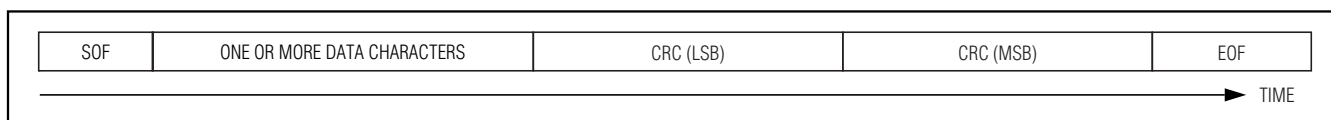


図7. ISO/IEC 14443のフレーム形式

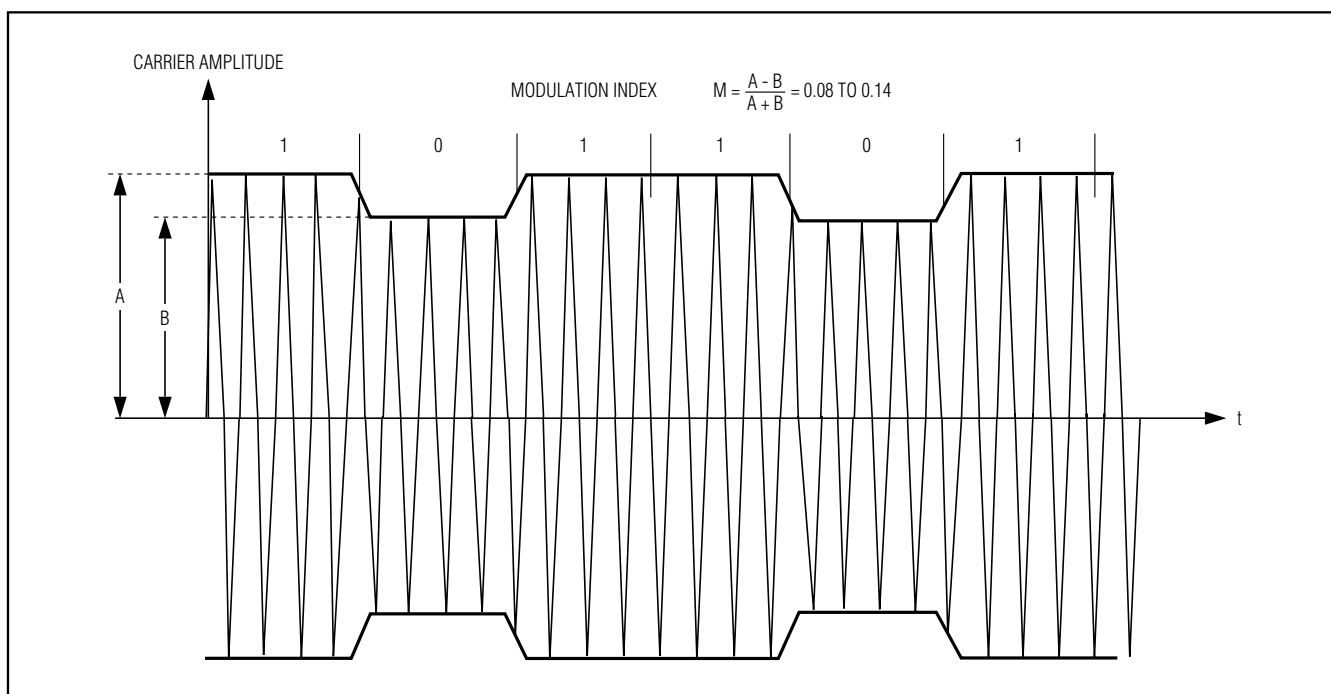


図8. ダウンリンク：8%～14%の振幅変調

送信に際して、フレームの情報はキャリア周波数 (ISO/IEC 14443の場合は13.56MHz)で変調されます。以下の各段落では、必要な変調および符号化について簡潔に説明します。SOF/EOFおよびサブキャリアのオン/オフタイミングを含む完全な詳細については、ISO/IEC 14443-3のセクション7.1および7.2を参照してください。

マスターからスレーブの経路では、変調指数8%～14%の振幅変調を使用します(図8)。この方向では、STARTビットおよびロジック0のビットが変調されたキャリアに対応し、STOPビットおよびロジック1のビットが変調されていないキャリアに対応します。EOFはSTOPビットの代わりに変調されていないキャリアで終了します。

## ISO/IEC 14443タイプB準拠 セキュアメモリ

スレーブからマスターの経路では、847.5kHzのサブキャリアを使用して、二位相偏移(BPSK)変調を使用し、データレートによって、1ビットの伝送に8、4、2、または1サブキャリアサイクルがかかります。スレーブは必要なときにのみサブキャリアを生成します。すなわち、SOFの直前に始まり、EOFの直後に終了します。規格では、SOFより前のサブキャリア

の位相を0°の基準と定義しており、これがロジック1に相当します。送信するキャラクタのビット値が遷移するたびに、サブキャリアの位相が180°変化します(図9)。最初の位相遷移はロジック1からロジック0への変化を表し、SOFの開始に一致します。BPSK変調されたサブキャリアは、デバイスのアンテナの負荷を変調させるために使用されます(図10)。

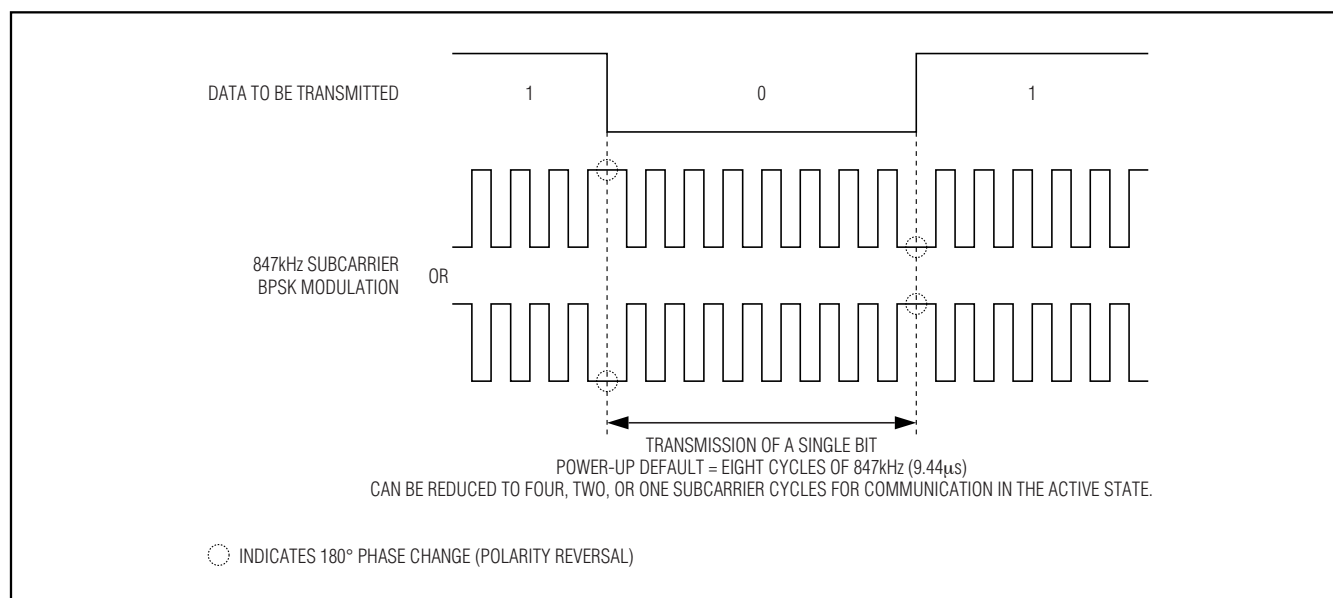


図9. アップリンク：847.5kHzのサブキャリアのBPSK変調

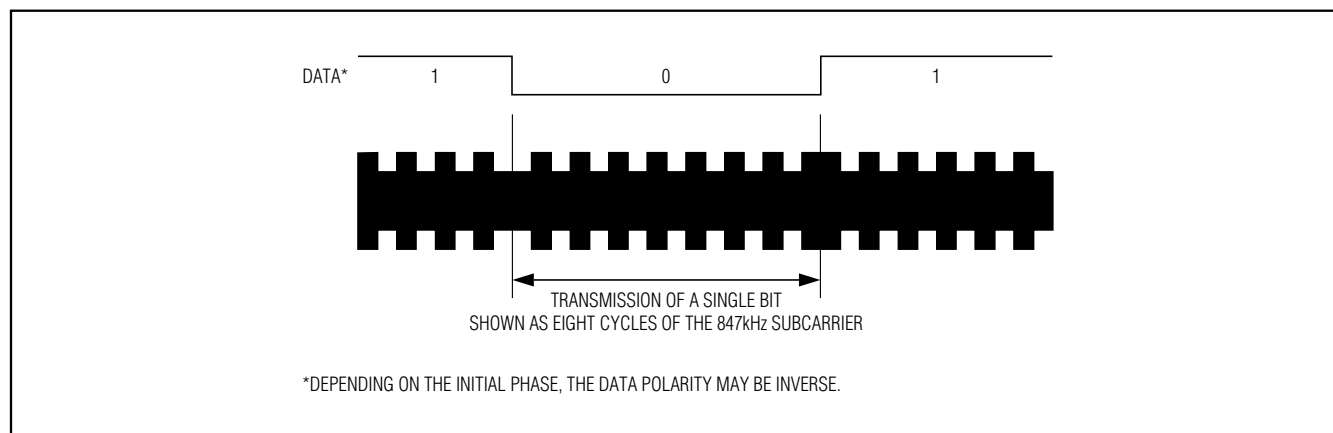


図10. アップリンク：BPSK変調されたサブキャリアによるRFフィールドの負荷変調

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

| PROLOGUE FIELD |        |        | INFORMATION FIELD | EPILOGUE FIELD |           |
|----------------|--------|--------|-------------------|----------------|-----------|
| PCB            | CID    | NAD    | (DATA)            | CRC (LSB)      | CRC (MSB) |
| 1 BYTE         | 1 BYTE | 1 BYTE | 0 OR MORE BYTES   | 1 BYTE         | 1 BYTE    |

図11. ISO/IEC 14443-4タイプBのブロック形式

|       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|
| MSB   |       |       |       | LSB   |       |       |       |
| BIT 8 | BIT 7 | BIT 6 | BIT 5 | BIT 4 | BIT 3 | BIT 2 | BIT 1 |
| 0     | 0     | 0     | CH    | CID   | NAD   | 1     | #     |

図12. IブロックのPCBのビット割当て

|       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|
| MSB   |       |       |       | LSB   |       |       |       |
| BIT 8 | BIT 7 | BIT 6 | BIT 5 | BIT 4 | BIT 3 | BIT 2 | BIT 1 |
| 1     | 0     | 1     | AN    | CID   | 0     | 1     | #     |

図13. RブロックのPCBのビット割当て

### ISO/IEC 14443のブロック 送信プロトコル

マスターがメモリアクセス用のデータパケットを送信するためには、MAX66040がACTIVE状態になっている必要があります。MAX66040をACTIVE状態にするためのプロトコルについては、「ネットワーク機能コマンド」の項で説明します。ACTIVE状態のとき、マスターとMAX66040の間の通信はISO/IEC 14443-4のセクション7で規定されたブロック送信プロトコルに従って行われます。そのためのブロック(図11)は、プロローグフィールド、情報フィールド、およびエピローグフィールドの3つの部分で構成されます。プロローグには、プロトコル制御バイト(PCB)、カード識別子(CID)、およびノードアドレス(NAD)と呼ばれる最大3バイトを格納可能です。エピローグは、EOFの前の16ビットCRCの別名です。情報フィールドは、データ用の汎用の領域です。

#### ブロックタイプ

規格では、Iブロック、Rブロック、およびSブロックという3種類のブロックを定義しています。図12、13、および14に、適切なPCBのビット割当てを示します。

Iブロックは、メモリへのアクセスおよびSHA-1エンジンの実行のための主要な手段です。Iブロックの場合、ビット2は1である必要があります。ビット6、ビット7、およびビット8は0である必要があります。ビット5 (CHと表記)はチェイニングを示すために使用されますが、この機能はMAX66040では使用もサポートもされていません。そのため、ビット5は常に0である必要があります。ビット4 (CIDと表記)は、プロローグフィールドがCID

バイトを含んでいるかどうかを示すためにマスターによって使用されます。MAX66040はCIDを含むブロックと含まないブロックを規格で定義されているように処理します。ビット4が1の場合、マスターはCIDバイトを含める必要があります。ビット3 (NADと表記)は、プロローグフィールドにNADバイトが含まれているかどうかを示すために使用されますが、MAX66040はこの機能をサポートしていません。そのため、ビット3は常に0である必要があります。ビット1 (#と表記)は、ブロック番号フィールドです。ブロック番号は、受信した応答が送信した要求に関するものであることを保証するために使用されます。この機能は、ISO/IEC 14443-4のAnnex Bで説明されているエラー処理で重要になります。ブロックの配番および処理についてのルールは、ISO/IEC 14443-4のセクション7.5.3および7.5.4に記載されています。MAX66040は、ビット5またはビット3に1がセットされているIブロックを無視します。

Rブロックの場合、ビット2、ビット3、ビット6、ビット7、およびビット8の状態は固定で、図13に示すように送信する必要があります。ビット1 (ブロック番号)およびビット4 (CIDインジケータ)の機能は、Iブロックの場合と同様です。ビット5 (ANと表記)は、特定のエラー状態からの復帰のために、最後のフレームに対する受信のアクノリッジ(0が送信された場合)または非アクノリッジ(1が送信された場合)に使用されます。MAX66040は規格で定義されたRブロックの機能を完全にサポートしています。詳細および適用可能なルールについては、ISO/IEC 14443-4のセクション7.5.3と7.5.4およびAnnex Bを参照してください。



## ISO/IEC 14443タイプB準拠 セキュアメモリ

| MSB   |       |       |       | LSB   |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|
| BIT 8 | BIT 7 | BIT 6 | BIT 5 | BIT 4 | BIT 3 | BIT 2 | BIT 1 |
| 1     | 1     |       |       | CID   | 0     | 1     | 0     |

図14. SブロックのPCBのビット割当て

| MSB           |       |         |       | LSB                   |       |       |       |
|---------------|-------|---------|-------|-----------------------|-------|-------|-------|
| BIT 8         | BIT 7 | BIT 6   | BIT 5 | BIT 4                 | BIT 3 | BIT 2 | BIT 1 |
| 0             | 0     | 0       | 0     |                       |       |       |       |
| (POWER LEVEL) |       | (FIXED) |       | CARD IDENTIFIER VALUE |       |       |       |

図15. IブロックのCIDバイトのビット割当て

|     |     |     |                   |           |           |     |
|-----|-----|-----|-------------------|-----------|-----------|-----|
| SOF | PCB | CID | INFORMATION FIELD | CRC (LSB) | CRC (MSB) | EOF |
|-----|-----|-----|-------------------|-----------|-----------|-----|

図16. ブロック送信プロトコルのフレーム形式

Sブロックの場合、ビット1、ビット2、ビット3、ビット7、およびビット8の状態は固定で、図14に示すように送信する必要があります。ビット4 (CIDインジケータ)の機能は、Iブロックの場合と同様です。ビット5およびビット6が00bの場合は、SブロックがDESELECTコマンドを表すことを示します。ビット5およびビット6が11bの場合、Sブロックはフレーム待ち時間延長(WTX)要求を表します。これは、応答にかかる時間がフレーム待ち時間(FWT) (「ATQB応答」の項を参照)の指定より長くなることをマスターに伝える機能です。しかし、MAX66040ではこの機能を使用していないため、Sブロックの唯一の用途は、DESELECTコマンドを使用してデバイスをACTIVE状態からHALT状態に遷移させることです(「ネットワーク機能コマンド」の項を参照)。

### カード識別子

図15に、カード識別子バイト内のビット割当てを示します。ビット1~4の目的は、マスターがACTIVE状態に昇格させた複数のスレーブデバイスの1つを選択することです。CIDは、ATTRIBコマンドのParam 4を介してスレーブに割り当てられます(「ネットワーク機能コマンド」の項を参照)。ACTIVE状態のとき、規格に準拠したスレーブは一致するCIDを含んだブロックのみを処理

し、割り当てられたCIDがすべて0の場合はCIDのないブロックを処理します。マスターがCIDを含めた場合は、スレーブの応答にもCIDバイトが含まれます。一致しないCIDを含んだブロックは無視されます。

規格によれば、スレーブはビット8および7を使用して、電力レベル指示をサポートしているかどうか、サポートしている場合は、完全に機能するために十分な電力が利用可能かどうかをマスターに伝えることができます。MAX66040は電力レベル指示をサポートしていないため、電力レベルビットは常に00bです。マスターがCIDバイトを送信するときは、電力レベルビットを00bにする必要があります。

### 情報フィールド

MAX66040はWTX要求を生成しないため、情報フィールド(図11)はIブロックにのみ存在します。情報フィールドの長さは、ブロック全体のバイト数からプロローグおよびエピローグフィールドの長さを引いたものを数えることによって計算されます。ISO/IEC 14443規格は、情報フィールドの内容に関するルールを何も定義していません。MAX66040は、情報フィールドの中で最初に受信したバイトがコマンドコードで、後に0個以上のコマンド固有のパラメータが続くことを想定しています。Iブロックに応答する場合、情報フィールドの最初のバイトは成功(コード00h)を示してその後にコマンド固有のデータが続くか、または失敗(コード01h)を示してその後に1つのエラーコードが続きます。

### メモリおよび制御機能コマンド

この項で説明するコマンドは、ブロック送信プロトコルを使用して送信されます。図16に示すように、ブロックのデータ(プロローグからエピローグまで)はSOFとEOFの間に埋め込まれます。CIDフィールド(網掛け)はオプションです。要求にCIDが含まれている場合、応答にもCIDが含まれます。

この項のコマンドの説明では、要求と応答の送信に使用されるIブロックの情報フィールドのみを示します。MAX66040はチェイニングをサポートせずWTX要求も生成しないため、Iブロックを受信した場合、MAX66040はIブロックで応答します。Iブロック応答のブロック番号は、Iブロック要求のものと同一です。

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

### エラー通知

機能の複雑性に応じて、さまざまなエラー条件が発生する可能性があります。エラーが発生した場合、要求に対する応答は01hのバイトで始まり、その後に1つのエラーコードが続きます。

表5に、コマンドと発生する可能性のあるエラーとの対照表を示します。エラーが発生しなかった場合、応答の情報フィールドは00hで始まり、その後にコマンドの詳細で示すコマンド固有のデータが続きます。

MAX66040がコマンドを認識することができない場合は、応答を生成しません。

表5. エラーコードの対照表

この情報についてはフルデータシートをご参照ください。

# 要約版

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

### Get System Informationコマンドの応答の情報フィールド(エラーなしの場合)

| INDICATOR | INFO<br>FLAGS | UID       | U1       | AFI      | NUMBER OF<br>BLOCKS | MEMORY BLOCK<br>SIZE | IC REFERENCE |
|-----------|---------------|-----------|----------|----------|---------------------|----------------------|--------------|
| 00h       | 0Fh           | (8 Bytes) | (1 Byte) | (1 Byte) | 13h                 | 07h                  | (1 Byte)     |

### コマンドの詳細

#### Get System Information

このコマンドによって、マスターはMAX66040についての技術的情報を取得することができます。応答では、最下位のUIDバイトが最初に送信されます。応答は、ISO 15693-3のセクション10を元としています。IC REFERENCEのコードは、A1h、A2h、B1hなどの16進形式でダイのリビジョンを示します。システム情報を取得するには、情報フィールドにコマンドコード2Bhを含んだ要求を発行してください。

その他コマンドの詳細についてはフルデータシートをご参照ください。

### Get UID

このコマンドによって、マスターはデバイスの固有ID番号(UID)を取得することができます。応答では、最下位のUIDバイトが最初に送信されます。UIDを読み取るには、情報フィールドにコマンドコード30hを含んだ要求を発行してください。

#### Get UIDコマンドの応答の情報フィールド(エラーなしの場合)

| INDICATOR | UID       |
|-----------|-----------|
| 00h       | (8 Bytes) |

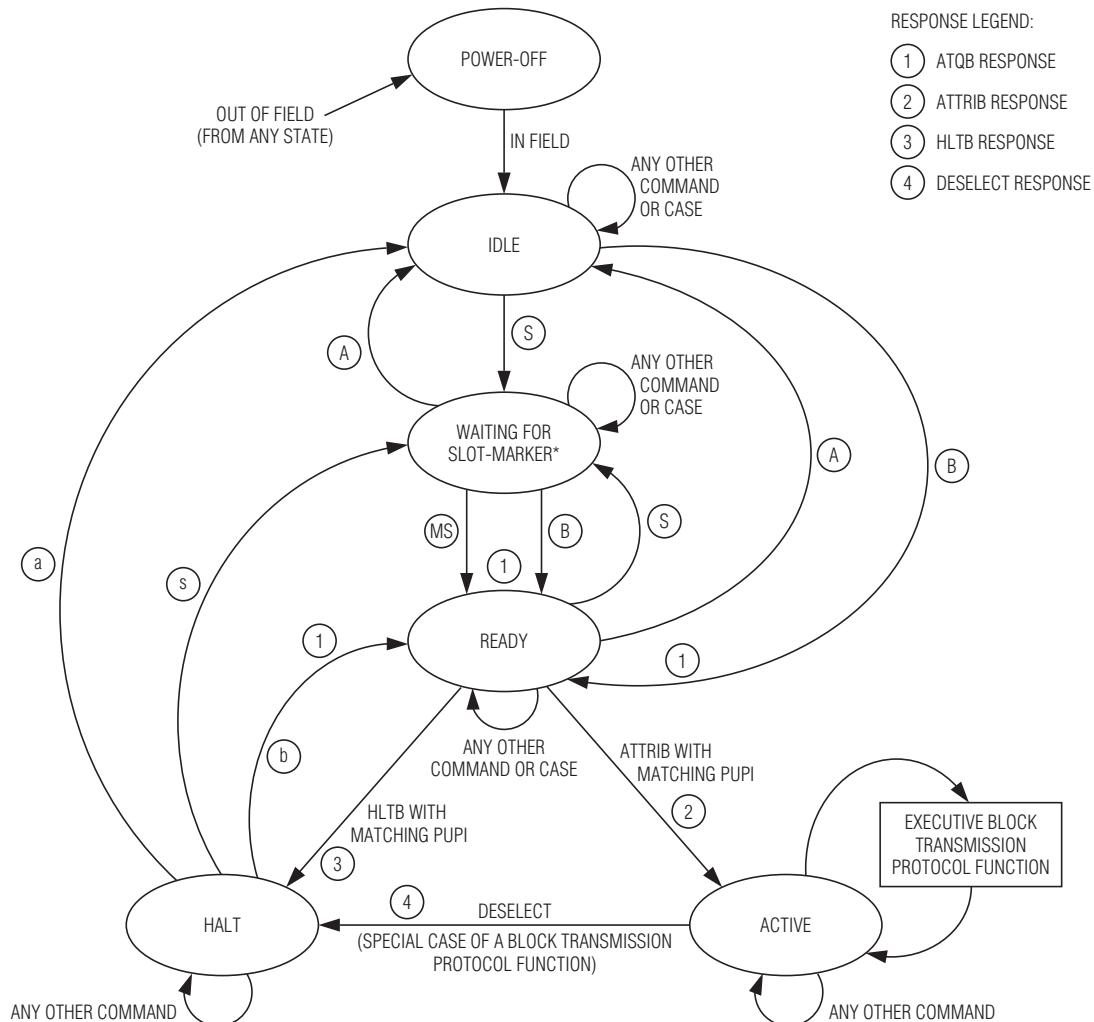
## ISO/IEC 14443タイプB準拠 セキュアメモリ

---

MAX66040

### ISO/IEC 14443-3タイプBの初期化および アンチコリジョンプロトコル

ISO/IEC 14443準拠のRFデバイスのメモリへのアクセスが可能となるためには、その前にマスターとRFデバイス間の通信経路を確立する必要があります。最初は、マスターのアンテナの電界内にRFデバイスが存在するかどうか不明です。既知の規格に準拠したRFデバイスが電界内に1つ以上存在するかどうかを判断するために、マスターは規格ごとに固有の初期化およびアンチコリジョンプロトコルを使用します。ISO/IEC 14443タイプBプロトコルは、POWER-OFF、IDLE、WAITING FOR SLOT-MARKER、READY、HALT、およびACTIVEの6種類の状態を定義しています。図17に、これらの状態およびスレーブが状態間を遷移する条件を示します。ほとんどの場合、小さな丸で囲まれた文字は遷移が発生する条件を示します。それぞれの条件については、図17の凡例で説明しています。表14は、アンチコリジョンプロトコルおよびネットワーク機能コマンドの説明で使用される用語についての説明です。



\*WHEN ENTERING "WAITING FOR SLOT-MARKER," EACH TAG SELECTS A RANDOM NUMBER R IN THE RANGE OF 1 TO "NUMBER OF SLOTS."

**CONDITIONS LEGEND:**

| NAME               | DESCRIPTION                                                        | RESULT                                        |
|--------------------|--------------------------------------------------------------------|-----------------------------------------------|
| A (AFI MISMATCH)   | REQB/WUPB WITH NONMATCHING AFI                                     | RETURN TO IDLE                                |
| a                  | WUPB WITH NONMATCHING AFI                                          |                                               |
| B (BYPASS SM)      | REQB/WUPB WITH MATCHING AFI <b>AND</b> [(N = 1) <b>OR</b> (R = 1)] | TRANSITION DIRECTLY TO READY                  |
| b                  | WUPB WITH MATCHING AFI <b>AND</b> [(N = 1) <b>OR</b> (R = 1)]      |                                               |
| S (SLOT-MARKER)    | REQB/WUPB WITH MATCHING AFI <b>AND</b> (N ≠ 1) <b>AND</b> (R ≠ 1)  | WAIT FOR MATCHING SLOT NUMBER                 |
| s                  | WUPB WITH MATCHING AFI <b>AND</b> (N ≠ 1) <b>AND</b> (R ≠ 1)       |                                               |
| MS (MATCHING SLOT) | SLOT-MARKER COMMAND WITH SLOT NUMBER = R                           | TRANSITION TO READY WITH MATCHING SLOT-MARKER |

図17. ISO/IEC 14443タイプBの状態遷移図

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

表14. ISO/IEC 14443タイプBの技術用語

| TERM                    | DESCRIPTION                                                                                                                                                                                                       |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ACTIVE                  | One of the slave's six states. In this state, the memory and control function commands and deselect apply.                                                                                                        |
| ADC                     | Application Data Coding. 2-Bit field of the 3rd protocol info byte of the ATQB response.                                                                                                                          |
| AFI                     | Application Family Identifier. 1-Byte field used in the REQB/WUPB request to preselect slaves.                                                                                                                    |
| ATQB                    | Answer to Request, Type B. Response to REQB, WUPB, and SLOT-MARKER command.                                                                                                                                       |
| ATTRIB                  | Slave Selection Command, Type B. Used to transition a slave from READY to the ACTIVE state.                                                                                                                       |
| BPSK                    | Binary Phase-Shift Keying Modulation                                                                                                                                                                              |
| CID                     | Card Identifier. 4-Bit temporary identification number assigned to a slave through the ATTRIB command, used in conjunction with the block transmission protocol.                                                  |
| EOF                     | End of Frame                                                                                                                                                                                                      |
| DESELECT                | Slave Deselection Command. Transitions the slave from the ACTIVE state to the HALT state.                                                                                                                         |
| fc                      | Carrier Frequency = 13.56MHz                                                                                                                                                                                      |
| FO                      | Frame Option. 2-Bit field of the 3rd protocol info byte of the ATQB response.                                                                                                                                     |
| fs                      | Subcarrier Frequency = $f_c/16 = 847.5\text{kHz}$                                                                                                                                                                 |
| FWI                     | Frame-Waiting Time Integer. 4-bit field of the 3rd protocol info byte of the ATQB response.                                                                                                                       |
| FWT                     | Frame-Waiting Time. Calculated from FWI.                                                                                                                                                                          |
| HALT                    | One of the slave's six states. The master puts a slave in this state to park it.                                                                                                                                  |
| HLTB                    | Halt Command, Type B                                                                                                                                                                                              |
| IDLE                    | One of the slave's six states. In this state, the slave has power and is waiting for action.                                                                                                                      |
| INF                     | Information Field for Higher Layer Protocol (per ISO/IEC 14443-4)                                                                                                                                                 |
| MBLI                    | Maximum Buffer Length Index of Slave (per ISO/IEC 14443-4). 4-Bit field of the first protocol info byte of the ATQB response.                                                                                     |
| N                       | Number of Anticollision Slots (or response probability per slot)                                                                                                                                                  |
| NAD                     | Node Address (per ISO/IEC 14443-4)                                                                                                                                                                                |
| POWER-OFF               | One of the slave's six states. In this state, the slave has no power and consequently cannot do anything.                                                                                                         |
| PUPI                    | Pseudo Unique Identifier. 4-Byte field of the ATQB response.                                                                                                                                                      |
| R                       | 4-Bit Random Number Chosen by a Slave When Processing the REQB or WUPB Command                                                                                                                                    |
| READY                   | One of the slave's six states; official name is READY-DECLARED SUBSTATE. In this state, the slave has identified itself and is waiting for transition to ACTIVE (memory and control functions) or HALT (parking). |
| REQB                    | Request Command, Type B. Used to probe the RF field for the presence of slave devices.                                                                                                                            |
| RF                      | Radio Frequency                                                                                                                                                                                                   |
| S                       | Slot Number. 4-Bit field sent to slave with SLOT-MARKER command.                                                                                                                                                  |
| SLOT-MARKER             | Command used in the time-slot approach to identify slaves in the RF field                                                                                                                                         |
| SOF                     | Start of Frame                                                                                                                                                                                                    |
| TR0                     | Guard Time per ISO/IEC 14443-2                                                                                                                                                                                    |
| TR1                     | Synchronization Time per ISO/IEC 14443-2                                                                                                                                                                          |
| WAITING FOR SLOT-MARKER | One of the slave's six states; official name is READY-REQUESTED SUBSTATE. In this state, the slave is waiting to be called by its random number R to transition to READY.                                         |
| WUPB                    | Wake-Up Command, Type B. Similar to REQB, required to wake up slaves in the HALT state.                                                                                                                           |

# ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

## ISO/IEC 14443タイプBの状態および遷移

### POWER-OFF状態

この状態は、スレーブがマスターのRFフィールドの範囲外にいる場合に該当します。スレーブは、電力を供給するRFフィールドから離れたときPOWER-OFF状態に遷移します。RFフィールドに入ったとき、スレーブは自動的にIDLE状態に遷移します。

### IDLE状態

IDLE状態の目的は、スレーブ群をアンチコリジョンプロトコルに参加可能な状態にすることです。IDLE状態に遷移するとき、スレーブは何も応答を生成しません。この状態を維持するためには、スレーブはPOWER-OFF状態への遷移を防ぐのに十分な電力をマスターのRFフィールドから連続的に受信する必要があります。IDLE状態の間、スレーブはマスターが送信するコマンドを監視しますが、REQBおよびWUPBコマンドにのみ反応します(一致するAFI値が含まれていることが条件です)。また、マスターが一致しないAFIバイトを含むコマンドを送信した場合は(条件Aおよびa)、HALT状態、READY状態、およびWAITING FOR SLOT-MARKER状態からIDLEへの遷移も可能です。IDLEから、スレーブはより上位の状態であるREADY (条件B)またはWAITING FOR SLOT-MARKER (条件S)に遷移することができます。詳細については、「ネットワーク機能コマンド」の項のREQB/WUPBコマンドの説明を参照してください。

### WAITING FOR SLOT-MARKER状態 (READY REQUESTED SUBSTATE)

WAITING FOR SLOT-MARKER状態は、タイムスロット方式のアンチコリジョンに使用されます。スレーブは、一致するAFIを含んだREQBまたはWUPBコマンドを受信した時点で、REQB/WUPBコマンドで指定されたスロット数およびスレーブが選択した乱数がともに1でないことを条件として、IDLE、HALT、またはREADY状態からWAITING FOR SLOT-MARKERに遷移することができます(条件Sおよびs)。この状態を維持するためには、スレーブはPOWER-OFF状態への遷移を防ぐのに十分な電力をマスターのRFフィールドから連続的に受信する必要があります。WAITING FOR SLOT-MARKER状態のスレーブはマスターが送信するコマンドを監視しますが、REQB、WUPB、およびSLOT-MARKERコマンドにのみ反応します。WAITING FOR SLOT-MARKERから、条件B (SLOT-MARKERのバイパス)、またはMS (スロット一致、SLOT-MARKERコマンドのスロット番号が乱数Rに一致)によって、スレーブはより上位の状態であるREADYに遷移します。条件A (AFI不一致)によって、スレーブはIDLE状態に戻ります。

### READY状態(READY DECLARED SUBSTATE)

READY状態は、アンチコリジョンプロトコルにおいてATQB応答を送信する基準に適合したスレーブに適用されます。スレーブは、IDLEまたはHALTから(条件Bおよびb)、あるいはWAITING FOR SLOT-MARKERから(条件BおよびMS) READYに遷移することができます。READY状態に遷移するとき、スレーブはATQB応答を送信します。この状態を維持するためには、スレーブはPOWER-OFF状態への遷移を防ぐのに十分な電力をマスターのRFフィールドから連続的に受信する必要があります。READY状態のスレーブはマスターが送信するコマンドを監視しますが、REQB、WUPB、ATTRIB、およびHLTBコマンドにのみ反応します。READYから、スレーブはACTIVE (一致するPUPIを含んだATTRIBコマンド)、HALT (一致するPUPIを含んだHLTBコマンド)、またはIDLE (条件A)に遷移することができます。

### HALT状態

HALT状態は、識別が終って以後はアンチコリジョンプロトコルに参加しないスレーブを沈黙させるために使用します。また、この状態はACTIVE状態での通信が完了した後にスレーブを休止させるためにも使用します。スレーブは、READY (一致するPUPIを含んだHLTBコマンド)またはACTIVE (一致するCIDを含んだDESELECTコマンド)からHALT状態に遷移します。HALT状態に遷移するとき、スレーブは遷移を確認する応答を送信します。この状態を維持するためには、スレーブはPOWER-OFF状態への遷移を防ぐのに十分な電力をマスターのRFフィールドから連続的に受信する必要があります。HALT状態を抜ける通常の方法は、WUPBコマンドによるものです。HALTから、スレーブはIDLE (条件a)、READY (条件b)、またはWAITING FOR SLOT-MARKER (条件s)に遷移することができます。

### ACTIVE状態

ACTIVE状態は、ブロック送信プロトコルを介して送信されたコマンドに対するスレーブの処理を可能にします。ACTIVE状態に遷移するとき、スレーブは応答によって遷移を確認します。スレーブがACTIVE状態に遷移する唯一の方法は、READY状態からの遷移です(一致するPUPIを含んだATTRIBコマンド)。ATTRIBコマンドの中で、マスターは4ビットのCIDを割り当てて、すべてACTIVE状態になる可能性のある複数のスレーブから1つをアドレス指定するために使用します。この状態を維持するためには、スレーブはPOWER-OFF状態への遷移を防ぐのに十分な電力をマスターのRFフィールドから連続的に受信する必要があります。ACTIVE状態を抜ける通常の方法は、DESELECTコマンドによるもので、それによってスレーブはHALT状態に遷移します。



## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

### ネットワーク機能コマンド

スレーブデバイスに状態間の遷移を行わせるために、ISO/IEC 14443タイプB規格は、REQB、WUPB、SLOT-MARKER、HLTB、ATTRIB、およびDESELECTと呼ばれる6つのネットワーク機能コマンドを定義しています。マスターは要求フレームの形でコマンドを発行し、スレーブは応答フレームの送信によって応答します。ネットワーク機能コマンドの場合、コマンドコード、パラメータ、および応答がSOFとCRCの間に埋め込まれます。この項では、応答および要求フレームの形式とフレーム内のデータフィールドの符号化について、MAX66040の動作に必要な範囲で説明します。規格で定義されているすべてのフィールドおよびすべての場合がMAX66040に関係するわけではありません。それらのフィールドの完全な説明については、ISO/IEC 14443-3のセクション7を参照してください。

### REQB/WUPBコマンド

REQUESTコマンド、タイプB (REQB)およびWAKEUPコマンド、タイプB (WUPB)は、マスターがRFフィールドを探索してスレーブデバイスの存在を調べ、アクションを行う前にアプリケーションファミリー識別子(AFI)の値に基づいて事前にそれらを選択するための一般的な手段です。ISO/IEC 14443タイプBに準拠したスレーブは、IDLE状態、WAITING FOR SLOT-MARKER状態、およびREADY状態のときにこれらのコマンドを待ち受けます。HALT状態では、スレーブはWUPBコマンドを

受信した場合にのみ反応します。図18に示すように、REQBまたはWUPBコマンドは1つのフレームとして送信されます。要求には、コマンドコード以外にAFIとPARAMの2つのパラメータが含まれます。REQB/WUPBへの応答はATQBと呼ばれます。詳細については、「ATQB応答」の項を参照してください。

ISO/IEC 14443規格は、AFIコードの割当ておよびREQB/WUPB要求受信時のスレーブの振る舞いに関するルールを定義しています。要求で指定されたAFIが00hの場合、スレーブは実際のAFIの値に関係なくそのコマンドを処理する必要があります。要求に含まれるAFIの下位ニブルが0000bの場合、マスターが送信したAFIの上位ニブルがスレーブのAFIの上位ニブルと一致する場合のみスレーブはそのコマンドを処理する必要があります。その他のすべてのAFI値については、要求に含まれるAFIとスレーブのAFIが一致する場合のみ、スレーブはそのコマンドを処理します。AFIのコードは、ユーザーによる書込みおよびロックが可能です。詳細については、「メモリおよび制御機能コマンド」の項を参照してください。

PARAMバイトのビット割当てを図19に示します。ビット5～8は予備であり、0にして送信する必要があります。ビット4が0の場合、要求がREQBコマンドであることを示します。ビット4が1の場合、WUPBコマンドを定義します。ビット1、2、および3は、アンチコリジョンプロトコルで使用するスロット数(N)を指定します。表15に、そのコードを示します。N = 1の場合、SLOT-MARK-

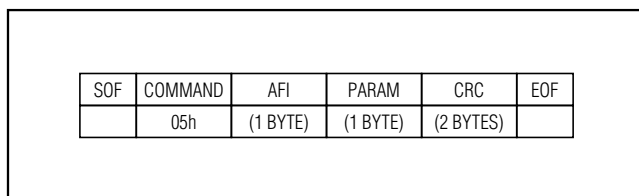


図18. REQB/WUPB要求フレーム

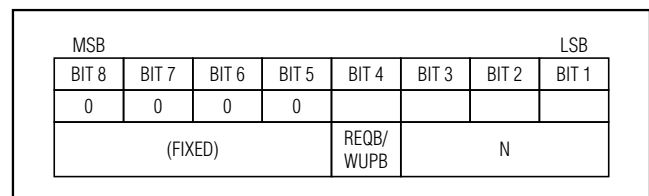


図19. PARAMバイトのビット割当て

表15. スロット数のコード

| BIT 3 | BIT 2 | BIT 1 | N          |
|-------|-------|-------|------------|
| 0     | 0     | 0     | 1          |
| 0     | 0     | 1     | 2          |
| 0     | 1     | 0     | 4          |
| 0     | 1     | 1     | 8          |
| 1     | 0     | 0     | 16         |
| 1     | 0     | 1     | (RESERVED) |
| 1     | 1     | X     | (RESERVED) |

# ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

ERコマンドは適用されず、AFIが一致するすべてのスレーブがREADY状態に遷移します。電界内に複数のスレーブが存在する場合、応答フレームが同時に送信されるため、これによってデータの衝突が発生します。Nが1より大きい場合、電界内の個々のスレーブが1～Nの範囲で自分用の4ビットの乱数(R)を選択します。たまたまR = 1を選択したスレーブが、REQB/WUPB要求に応答します。Nが大きいほど応答フレームの衝突の可能性が低くなりますが、Nが16で電界内のスレーブが1つのみの場合、応答を取得するために最大15のSLOT-MARKERコマンドが必要になります。乱数RとREQB/WUPBコマンドのみに依存して電界内のすべてのスレーブを識別する手法は、「確率論的アプローチ」と呼ばれます。アンチコリジョンプロトコルの詳細については、「アンチコリジョンの例」の項を参照してください。

## SLOT-MARKERコマンド

参加するスレーブがREQB/WUPBコマンドごとに新しい乱数を選択するという事実に依存する代わりに、「タイムスロット方式」ではマスターがSLOT-MARKERコマンドを使用してスレーブをそれぞれの乱数Rで呼びます。これが可能になるためには、その前にマスターが1より大きいスロット数(N)の値でREQB/WUPBコマンドを発行する必要があります。マスターは最大(N - 1)のSLOT-MARKERコマンドを送信することができます。図20に、SLOT-MARKER要求フレームの形式を示します。スレーブはすでに先行するREQB/WUPB要求によって事前に選択されているため、AFIフィールドは不要です。SLOT-MARKERコマンドへの応答はATQBと呼ばれます。詳細については、「ATQB応答」の項を参照してください。

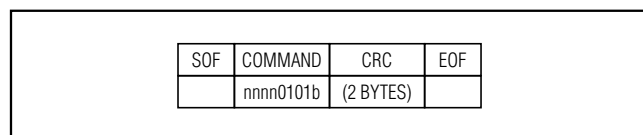


図20. SLOT-MARKER要求フレーム

「nnnn」と表記されているビットは、表16の定義に従ってスロット番号を示します。許容範囲のスロット番号の任意のシーケンスが使用可能です。

## ATQB応答

REQB/WUPBおよびSLOT-MARKERコマンドのどちらに対する応答もATQBと呼ばれ、「answer to request, Type B (要求への回答、タイプB)」を表します。図21に、ATQB応答の形式を示します。PUPIフィールド(疑似固有識別子)は、マスターがスレーブをアドレス指定してACTIVEまたはHALT状態に遷移させるために使用します。PUPIとして通知されるデータは、64ビットUIDの下位4バイトです。アプリケーションデータフィールドは、それ以外の点では同等なRFフィールド内のスレーブの区別に関連したユーザー定義のデータを通知します。アプリケーションデータは、メモリブロック10hの最初の4バイトです。デフォルトでは、アプリケーションデータフィールドは64ビットUIDの上位4バイトを反映するように出荷時に設定されています。これによって、マスターはスレーブからの最初の応答で完全な64ビットUIDを取得することができます。しかし、このフィールドは出荷時にロックされていないため、任意の値を書き込むことが可能です。

プロトコル情報フィールドは、データレート、フレームサイズ、ISO/IEC 14443-4への準拠、フレーム待ち時間、およびISO/IEC 14443-4ブロック送信プロトコルでスレーブがCIDとNADをサポートしているかどうかなどの、システム管理用の情報をマスターに提供します。図22に、プロトコル情報フィールド内でのこの情報の位置および値を示します。

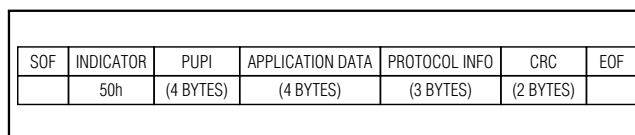


図21. ATQB応答フレーム

表16. スロットの配番

| BIT 8 | BIT 7 | BIT 6 | BIT 5 | SLOT NUMBER |
|-------|-------|-------|-------|-------------|
| 0     | 0     | 0     | 1     | 2           |
| 0     | 0     | 1     | 0     | 3           |
| 0     | 0     | 1     | 1     | 4           |
| ...   | ...   | ...   | ...   | ...         |
| 1     | 1     | 1     | 0     | 15          |
| 1     | 1     | 1     | 1     | 16          |

# ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

| 1ST BYTE          | 2ND BYTE                          | 3RD BYTE,<br>UPPER NIBBLE | 3RD BYTE,<br>BIT 4, BIT 3 | 3RD BYTE,<br>BIT 2, BIT 1 |
|-------------------|-----------------------------------|---------------------------|---------------------------|---------------------------|
| BIT RATE CABILITY | MAXIMUM FRAME SIZE, PROTOCOL TYPE | FWI                       | ADC                       | FO                        |
| 77h               | 21h                               | 0111b                     | 00b                       | 01b                       |

図22. プロトコル情報フィールドの詳細

|     |         |           |           |     |
|-----|---------|-----------|-----------|-----|
| SOF | COMMAND | PUPI      | CRC       | EOF |
|     | 50h     | (4 BYTES) | (2 BYTES) |     |

図23. HLTB要求フレーム

|     |           |           |     |
|-----|-----------|-----------|-----|
| SOF | INDICATOR | CRC       | EOF |
|     | 00h       | (2 BYTES) |     |

図24. HLTB応答フレーム

MAX66040のビットレート性能は、双方向(要求および応答)とも105.9kbps～847.5kbpsの範囲で、要求と応答のビットレートが同一である必要はありません。どの要求/応答でも、最大フレームサイズ(第2のバイトの上位ニブル)には32バイトが指定されます。MAX66040で発生する最大のフレームサイズは26バイトです(Copy Bufferの要求、Compute Page MACの応答)。プロトコルタイプ(第2のバイトの下位ニブル)は、MAX66040がISO/IEC 14443-4ブロック送信プロトコルをサポートしていることを示しています。FWIのコード0111bは、フレーム待ち時間が38.7msであることを示し、これは計算されたシーケットの生成に十分な長さです。スレーブは最大フレーム待ち時間が経過するずっと前に応答する可能性があることに注意してください。ADCのコード00bは、MAX66040がアプリケーションデータフィールドに独自の符号化を使用することを示しています。FOのコード01bは、MAX66040がCIDをサポートし、しかしISO/IEC 14443-4ブロック送信プロトコルのNADフィールドをサポートしていないことを示します。

## HLTBコマンド

HLTBコマンドは、HALT状態で休止させることによってスレーブを沈黙させることができる唯一のネットワーク機能コマンドです。ATQB応答に基づいてマスターがそれ以上そのスレーブとの通信を希望しない場合、マスターはHLTBコマンドを発行します。図23および24に、HLTB要求フレームとそれに対応する応答フレームの形式を示します。PUPIフィールドで使用するデータは、

スレーブがATQB応答で送信したPUPI情報と一致している必要があります。HALT状態の間、スレーブはWUPB要求にのみ応答します。

## ATTRIBコマンド

ATTRIBコマンドは、スレーブを1つ選択して、ISO/IEC 14443ブロック送信プロトコルに従って送信されるコマンドを処理させるための唯一の方法です。ATQB応答に基づいてマスターがそのスレーブとの通信を希望する場合、マスターはスレーブ選択コマンドATTRIBを使用してそのスレーブをACTIVE状態にする必要があります。マスターがスレーブをACTIVE状態から抜けさせる通常の方法は、Sブロックを使用してネットワーク機能コマンドを伝達するDESELECTコマンドの送信によるものです。

図25に、ATTRIB要求フレームの形式を示します。PUPIフィールドで使用するデータは、スレーブがATQB応答で送信したPUPI情報と一致している必要があります。Param 1は、マスターが送信から受信に切り替わるために必要な時間(TR0)、マスターがスレーブのサブキャリアに同期するために必要な時間(TR1)、およびマスターがSOFおよび/またはEOFのない応答フレームを受信することができるかどうかをスレーブに伝えます。

MAX66040は、Param 1のデータを無視します。ISO/IEC 14443タイプBリーダの要件を簡易化するため、MAX66040はTR0およびTR1を128/fs (151μs、fsは847.5kHzのサブキャリア周波数)の固定とし、応答の開始と終了を常にそれぞれSOFおよびEOFとしています。

|     |         |           |          |          |         |          |             |           |     |
|-----|---------|-----------|----------|----------|---------|----------|-------------|-----------|-----|
| SOF | COMMAND | PUPI      | PARAM 1  | PARAM 2  | PARAM 3 | PARAM 4  | HLINF       | CRC       | EOF |
|     | 10h     | (4 BYTES) | (1 BYTE) | (1 BYTE) | 01h     | (1 BYTE) | (≥ 0 BYTES) | (2 BYTES) |     |

図25. ATTRIB要求フレーム

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

| MSB                         |       |                               |       | LSB                            |       |       |       |
|-----------------------------|-------|-------------------------------|-------|--------------------------------|-------|-------|-------|
| BIT 8                       | BIT 7 | BIT 6                         | BIT 5 | BIT 4                          | BIT 3 | BIT 2 | BIT 1 |
|                             |       |                               |       | X                              | X     | X     | X     |
| RESPONSE DATA RATE (UPLINK) |       | RESPONSE DATA RATE (DOWNLINK) |       | RECEIVER FRAME SIZE CAPABILITY |       |       |       |

図26. Param 2バイトのビット割当て

| MSB     |       |       |       | LSB                         |       |       |       |
|---------|-------|-------|-------|-----------------------------|-------|-------|-------|
| BIT 8   | BIT 7 | BIT 6 | BIT 5 | BIT 4                       | BIT 3 | BIT 2 | BIT 1 |
| 0       | 0     | 0     | 0     |                             |       |       |       |
| (FIXED) |       |       |       | CARD IDENTIFIER VALUE (CID) |       |       |       |

図27. Param 4バイトのビット割当て

| SOF | INDICATOR | HL RESPONSE | CRC       | EOF |
|-----|-----------|-------------|-----------|-----|
|     | MBLI, CID | (≥ 0 BYTES) | (2 BYTES) |     |

図28. ATTRIB応答フレーム

| FRAME WITHOUT CID |         |           |           |     |
|-------------------|---------|-----------|-----------|-----|
| SOF               | COMMAND | CRC       | EOF       |     |
|                   | C2h     | (2 BYTES) |           |     |
| FRAME WITH CID    |         |           |           |     |
| SOF               | COMMAND | CID       | CRC       | EOF |
|                   | CAh     | (1 BYTE)  | (2 BYTES) |     |

図29. DESELECT要求および応答フレーム

Param 2は、ACTIVE状態での通信に使用するデータレートおよびマスターが受信可能な最大フレームサイズについてスレーブに通知します。図26に、Param 2バイトのビット割当てを示します。MAX66040は、105.9kbps (コード00b)、211.9kbps (コード01b)、423.75kbps (コード10b)、および847.5kbps (コード11b)のデータレートをサポートしています。マスターは、要求と応答に異なるデータレートを選択することができます。チェイニングをサポートしていないため、MAX66040はフレームサイズ性能を無視して、ATQB応答で指定された大きさのフレームをマスターが受信可能であると想定します。

Param 3の下位ニブルは、ATQBの Protokol 情報の第2バイトの下位ニブルで指定された Protokol タイプの確認に使用されます。ISO/IEC 14443-3ではParam 3の上位ニブルを0000bに設定しているため、MAX66040の場合にATTRIB要求で使用するParam 3の値は01hになります。

Param 4は、ACTIVE状態の複数のスレーブの1つをアドレス指定するためにブロック送信 Protokol で使用されるCID番号をスレーブに割り当てます。図27に、Param 4のビット割当てを示します。MAX66040はCIDフィールドをサポートしているため、マスターは0～14の範囲の任意の番号を割り当てることができます。ISO/IEC 14443-3によれば、コード15は予備となっています。

ATTRIB要求フレームは、上位層情報(HLINF)と呼ばれる1つのオプションのフィールドを含んでいます。このフィールドは、ISO/IEC 14443タイプBブロック送信 Protokol の情報フィールド(図11を参照)と同様のデータを含めるために使用することができます。このデータが存在し、かつスレーブがHLINFフィールドをサポートしている場合、スレーブはHLINFのデータを処理して、ATTRIB要求に対する応答で結果を返します。通常は、ATTRIB要求はHLINFフィールドなしで送信されます。MAX66040が受付けて処理する唯一のHLINFデータは、Get UIDコマンド(コード30h)です。

ATTRIB要求に一致するPUPUおよび正常なCRCが含まれていた場合、スレーブは図28に示すATTRIB応答フレームを送信します。インジケータの上位ニブルはMBLIとも呼ばれ、0000bの値によって、スレーブが内部入力バッファサイズについて何も情報を提供しないことを示します。下位ニブルは、マスターがそのスレーブに割り当てたカード識別子の値を返します。

HL応答フィールドはオプションです。次の3種類の場合に区別されます。

- ATTRIB要求にHLINFフィールドがなかった場合、応答にHL応答フィールドは存在しません。
- ATTRIB要求のHLINFフィールドにGet UIDコマンドコード(30h)が存在した場合、HL応答フィールドはGet UIDの応答の情報フィールドと同じ(すなわち、00hの後に8バイトのUID)になります。
- ATTRIB要求のHLINFフィールドのコードが30h以外だった場合、応答フレームにHL応答フィールドは含まれません。

### DESELECTコマンド

DESELECTコマンドは、マスターがスレーブとの通信を完了した後で、そのスレーブをACTIVE状態からHALT状態に遷移させるために使用します。DESELECT要求フレームには、CIDを含むものとCIDを含まないものの2つのバージョンが存在します。図29に、両方のバージョンを示します。図27に、CIDの形式を示します。

論理上、DESELECTコマンドはISO/IEC 14443規格のパート4で定義されたブロック送信 Protokol のSブロックの特別な場合です。MAX66040は、要求のCIDと

# ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

デバイスのCIDが一致した場合に、DESELECTコマンドに応答します。DESELECT要求がCIDを含んでいない場合、MAX66040は自分のCIDが0000bの場合のみその要求に応答します。

DESELECTコマンドへの応答フレームは、要求フレームと同一です。スレーブは、受信したものと同じデータを返すことによって、要求でアドレス指定されたスレーブがHALT状態に遷移したことを確認します。

## アンチコリジョンの例

### 確率論的アンチコリジョン

マスターは、REQBまたはWUPBコマンドの発行によってアンチコリジョンプロセスを開始します。WUPBコマンドは、AFIコードが一致する電界内のすべてのスレーブに影響を与えます。REQBコマンドもこれと同じ機能を実行しますが、HALT状態のスレーブはこれを無視します。どちらのコマンドもパラメータNを含んでおり、表15に従ってATQB応答の確率を $1/N$ に設定するために使用されます。

$N = 1$ の場合、参加しているすべてのスレーブがATQB応答で応答します。 $N$ が1より大きい場合、個々のスレーブが1～ $N$ の範囲で乱数Rを選択します。たまたま $R = 1$ を選んだ場合、スレーブはATQBで応答します。 $R$ が1より大きい場合、スレーブは次のREQBまたはWUPBコマンドを待ち、そのコマンドによって参加しているスレーブが新しい乱数Rを選択します。

ATQB応答はPUP1というフィールドを含んでおり、アンチコリジョンプロセス中に特定のスレーブに対してコマンドを発行するために使用されます。ATQB応答を受け取った場合、マスターは一致するHLTBコマンドを発行してスレーブを停止させるか、または一致するATTRIB

コマンドを発行してCIDを割当て、スレーブをACTIVE状態にしてください。これが行われない場合、各スレーブはアンチコリジョンプロセスに参加し続けます。ACTIVE状態のスレーブは、すべてのREQB、WUPB、SLOT-MARKER、ATTRIB、およびHLTBコマンドを無視しますが、DESELECTコマンドには応答します。

受信したATQB応答にCRCエラーがある場合、2つ以上のスレーブが同時に応答したために衝突が発生したことを示します。確率論的アンチコリジョンでは、マスターが再びREQBコマンドを発行して、HALTまたはACTIVE状態でない電界内のスレーブに新しい乱数Rを選択させる必要があります。スレーブの1つが $R = 1$ を選択した場合、そのスレーブはATQBで応答します。REQBに対してATQB応答がない場合でも、電界内のすべてのスレーブが識別されたという保証はありません。

図30に、電界内にIDLE状態の4つのスレーブが存在すると仮定した場合の、確率論的アンチコリジョンの例を示します。プロセスは、マスターが $N = 1$ のREQB要求を送信することによって開始され、それによってすべてのスレーブがATQBで応答するため、衝突が発生します。スレーブが存在することを知ったマスターは、次に $N = 8$ のREQBを送信します。これによって、すべてのスレーブが1～8の範囲で乱数を選択することになります。 $R = 1$ を選択したスレーブのみが応答し、この例ではそれがスレーブCです。電界内にさらに多くのスレーブが存在することを知って、マスターはREQBコマンドの発行を続け、この例では、それによって最終的にすべてのスレーブが識別されています。その統計学的な性質から、確率論的アンチコリジョンはタイムスロット式アンチコリジョンよりも電界内のすべてのスレーブが見つかる可能性が低くなります。

|         | TESTING FOR SLAVES  |      | ATTEMPT 1           | ATTEMPT 2           | ATTEMPT 3           | ATTEMPT 4           | ATTEMPT 5           | ATTEMPT 6           |
|---------|---------------------|------|---------------------|---------------------|---------------------|---------------------|---------------------|---------------------|
| MASTER  | REQB<br>( $N = 1$ ) |      | REQB<br>( $N = 8$ ) | REQB<br>( $N = 8$ ) | REQB<br>( $N = 8$ ) | REQB<br>( $N = 8$ ) | REQB<br>( $N = 8$ ) | REQB<br>( $N = 8$ ) |
| SLAVE A |                     | ATQB | ( $R = 3$ )         | ( $R = 7$ )         | ( $R = 1$ ) ATQB    | ( $R = 3$ )         | ( $R = 6$ )         | ( $R = 8$ )         |
| SLAVE B |                     | ATQB | ( $R = 6$ )         | ( $R = 4$ )         | ( $R = 8$ )         | ( $R = 8$ )         | ( $R = 5$ )         | ( $R = 1$ ) ATQB    |
| SLAVE C |                     | ATQB | ( $R = 1$ ) ATQB    | ( $R = 8$ )         | ( $R = 2$ )         | ( $R = 4$ )         | ( $R = 3$ )         | ( $R = 4$ )         |
| SLAVE D |                     | ATQB | ( $R = 2$ )         | ( $R = 1$ ) ATQB    | ( $R = 5$ )         | ( $R = 8$ )         | ( $R = 4$ )         | ( $R = 2$ )         |

図30. 確率論的アンチコリジョンの例

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

|         | TESTING FOR SLAVES |      | SLOT 1          | SLOT 2 | SLOT 3 | SLOT 4 | SLOT 5 | SLOT 6 | SLOT 7 | SLOT 8 |
|---------|--------------------|------|-----------------|--------|--------|--------|--------|--------|--------|--------|
| MASTER  | REQB<br>(N = 1)    |      | REQB<br>(N = 8) | SM2    | SM3    | SM4    | SM5    | SM6    | SM7    | SM8    |
| SLAVE A |                    | ATQB | (R = 3)         |        | ATQB   |        |        |        |        |        |
| SLAVE B |                    | ATQB | (R = 6)         |        |        |        |        | ATQB   |        |        |
| SLAVE C |                    | ATQB | (R = 1)         | ATQB   |        |        |        |        |        |        |
| SLAVE D |                    | ATQB | (R = 2)         | ATQB   |        |        |        |        |        |        |

図31. タイムスロット式アンチコリジョンの例

### タイムスロット式アンチコリジョン

マスターは、REQBまたはWUPBコマンドの発行によってアンチコリジョンプロセスを開始します。WUPBコマンドは、AFIコードが一致する電界内のすべてのスレーブに影響を与えます。REQBコマンドもこれと同じ機能を実行しますが、HALT状態のスレーブはこれを無視します。どちらのコマンドもパラメータNを含んでおり、表15に従ってアンチコリジョンプロトコルに使用するスロット数を指定します。

N = 1の場合、参加しているすべてのスレーブがATQB応答で応答します。Nが1より大きい場合、個々のスレーブが1～Nの範囲で乱数Rを選択します。たまたまR = 1を選んだ場合、スレーブはATQBで応答します。Rが1より大きい場合、スレーブはスロット番号がRに等しいSLOT-MARKERコマンドを待った後、ATQBで応答します。スレーブの漏れがないことを保証するために、マスターは2～Nのすべてのスロット番号を試行する必要があります。

ATQB応答はPUPIというフィールドを含んでおり、アンチコリジョンプロセス中に特定のスレーブに対してコマンドを発行するために使用されます。ATQB応答を受け取った場合、マスターは一致するHLTBコマンドを発行してスレーブを停止させるか、または一致するATTRIBコマンドを発行してCIDを割当て、スレーブをACTIVE状態にしてください。ACTIVE状態のスレーブは、すべてのREQB、WUPB、SLOT-MARKER、ATTRIB、およびHLTBコマンドを無視しますが、DESELECTコマンドには応答します。

受信したATQB応答にCRCエラーがある場合、2つ以上のスレーブが同時に応答したために衝突が発生したことを

示します。通常、マスターは1以外の乱数RのスレーブをテストするためにSLOT-MARKERコマンドの発行を続けます。さらなる衝突に遭遇した場合、マスターは新しいREQBコマンドを発行し、それによってHALTまたはACTIVE状態でない電界内の各スレーブに新しい乱数Rを選択させる必要があります。その後、電界内のすべてのスレーブが識別されてHALTまたはACTIVE状態になるまで、この方法でアンチコリジョンプロセスが継続されます。

図31に、電界内にIDLE状態の4つのスレーブが存在すると仮定した場合の、タイムスロット式アンチコリジョンの例を示します。プロセスは、マスターがN = 1のREQB要求を送信することによって開始され、それによってすべてのスレーブがATQBで応答するため、衝突が発生します。スレーブが存在することを知ったマスターは、次にN = 8のREQBを送信します。これによって、すべてのスレーブが1～8の範囲で乱数を選択することになります。これで2つのスレーブがRに同じ値を選ぶことを防ぐことはできませんが、Nが大きいほどその発生確率は低くなります。この例では、スレーブCがR = 1を選択して、REQBの直後に応答しています。マスターは次にスロット番号2 (SM2)のSLOT-MARKERコマンドを送信し、それによってスレーブDが応答します。マスターはすべてのスロットについてテストを続行し、Rが一致するスレーブが存在した場合、ATQBを受信します。マスターが1つのスロットで衝突を検出した場合、残りのスロットで識別されたスレーブを先にHALTまたはACTIVE状態にしてから、次のアンチコリジョンプロセスを開始する必要があります。マスターは、この例のように番号順にスロットのテストを行う必要はないことに注意してください。

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

### CRC生成

MAX66040は2種類のCRCを使用します。一方のCRCは8ビットのタイプです。このCRCの等価多項式関数は、 $X^8 + X^5 + X^4 + 1$ です。

もう一方のCRCは16ビットのタイプであり、CRC-16-CCITTの多項式関数である $X^{16} + X^{12} + X^5 + 1$ に従って生成されます(図33)。このCRCは、要求および応答データパケットの誤り検出に使用され、常に反転形式で伝送されます。すべてのデータバイトをCRCジェネレータにシフトインした後、16個のフリップフロップの状態がシフトレジスタに並列コピーされ、送信のためにLSbから順にシフトアウトされます。このCRCの詳細については、ISO/IEC 14443-3, Annex B、CRC\_B encodingを参照してください。

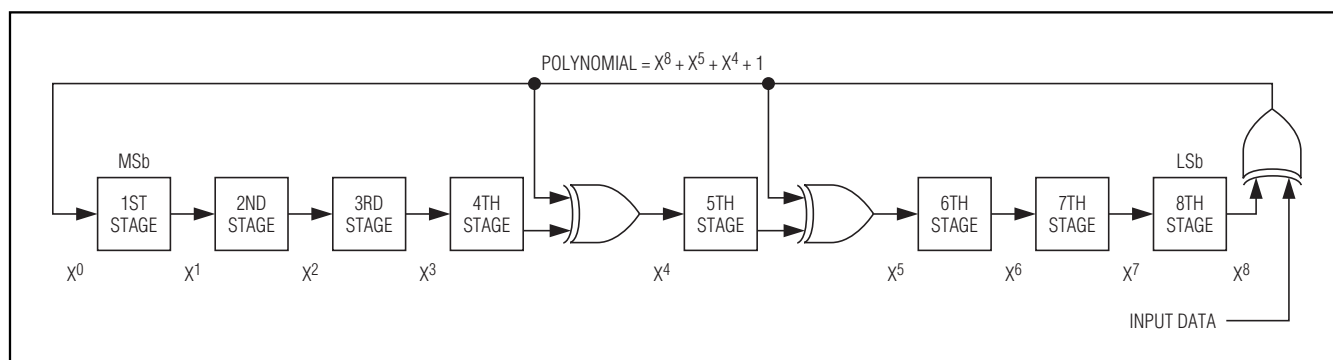


図32. 8ビットCRCジェネレータ

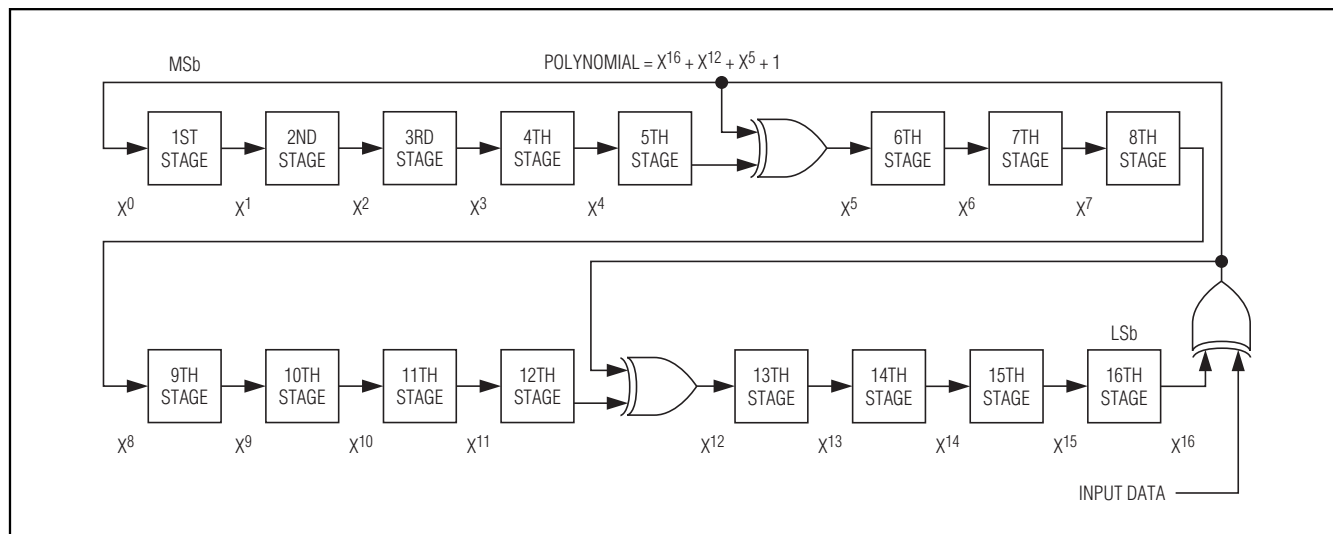


図33. CRC-16-CCITTジェネレータ

# 要約版

## ISO/IEC 14443タイプB準拠 セキュアメモリ

### 機械設計図

MAX66040

TOP VIEW

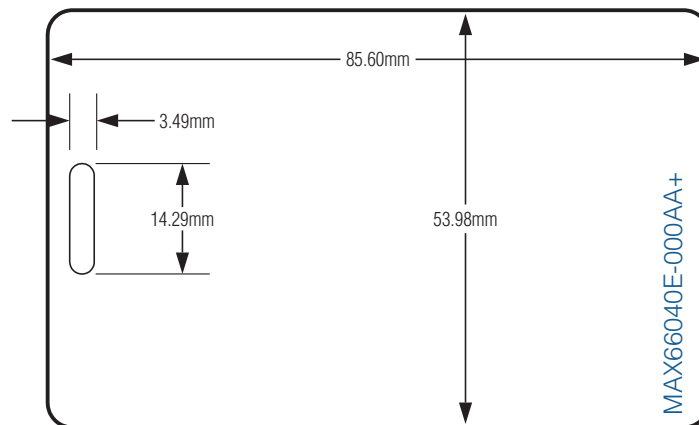


SIDE VIEW



KEY FOB

TOP VIEW



SIDE VIEW



ISO CARD



# 要約版

## ISO/IEC 14443タイプB準拠 セキュアメモリ

MAX66040

### 改訂履歴

| 版数 | 改訂日  | 説明 | 改訂ページ |
|----|------|----|-------|
| 0  | 1/11 | 初版 | —     |

マキシム・ジャパン株式会社 〒141-0032 東京都品川区大崎1-6-4 大崎ニューシティ 4号館 20F TEL: 03-6893-6600

Maximは完全にMaxim製品に組込まれた回路以外の回路の使用について一切責任を負いかねます。回路特許ライセンスは明言されていません。Maximは随時予告なく回路及び仕様を変更する権利を留保します。

38 **Maxim Integrated Products, 120 San Gabriel Drive, Sunnyvale, CA 94086 408-737-7600**

© 2011 Maxim Integrated Products

MaximはMaxim Integrated Products, Inc.の登録商標です。