注意：この日本語版文書は参考資料としてご利用ください。
最新情報は必ずオリジナルの英語版をご参照願います。

ATSHA204A

Microchip 社製 ATSHA204A CryptoAuthentication データシート

特長

- ハードウェア ベースの鍵ストレージを備えた暗号エレメント デバイス
- セキュアな非対称認証デバイスによるホスト/クライアント動作
- 高性能 SHA-256 ハッシュ アルゴリズムと MAC (Message Authentication Code)および HMAC (Hash-Based Message Authentication Code)オプション
- クラス最高水準の 256 ビット鍵(最大 16 個の鍵を保存可能)
- 一意性が保証された 72 ビットシリアル番号
- 高品質の乱数生成器(RNG)を内蔵
- 4.5 kb EEPROM メモリ(鍵とデータを保存)
- 固定情報を保存する 512 ビットの OTP (One Time Programmable)メモリ
- 各種 I/O オプション:
  - UART 互換高速単線式インターフェイス
  - 1 MHz I^2C インターフェイス
- 電源電圧レンジ: 2.0～5.5 V
- 通信電圧レンジ: 2.7～5.5 V
- スリープ電流: <150 nA
- セキュアなダウンロードとブート
  - エコシステム制御
  - メッセージ セキュリティ
  - 複製防止
- 8 ピン SOIC、 8 ピン TSSOP (2)、3 ピン SOT23、8 ピン UDFN、3 ピン CONTACT パッケージ

応用例

- セキュアなダウンロードとブート
- エコシステム制御
- 複製防止
- メッセージ セキュリティ

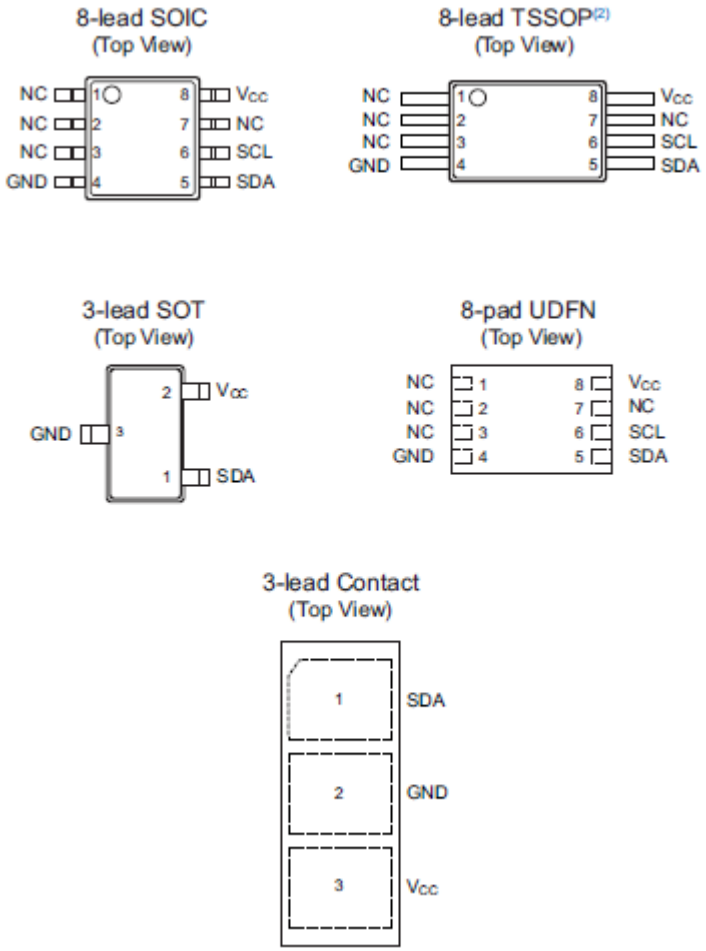
© 2019 Microchip Technology Inc.

パッケージタイプ

表 1. ピン配置

ピン名	機能
NC	未接続
GND	グランド
SDA	シリアルデータ
SCL	シリアルクロック入力
VCC	電源

図 1. ピン配置(1)



Note:

1. 図面の縮尺は不定です。
2. 新規設計には非推奨です。

© 2019 Microchip Technology Inc.

目次

© 2019 Microchip Technology Inc.

© 2019 Microchip Technology Inc.

1. はじめに

以下では、Microchip ATSHA204A 暗号エレメント デバイスの特長と機能を紹介します。

1.1 応用例

ATSHA204A は、Microchip 社の CryptoAuthentication™ 高セキュリティ ハードウェア認証デバイスファミリに属します。本デバイスは柔軟なコマンドセットを備え、以下を含む各種のアプリケーションで使えます。

- **偽造防止**
  脱着型、交換型、消耗型クライアントが信頼できるかどうか検証します。これらのクライアントにはプリンタのインクタンク、電子ドータカード、医療機器の消耗品、スペアパーツ等が含まれます。本デバイスは、ソフトウェア/ファームウェア モジュールまたはメモリストレージ エレメントの検証(認証)用にも使えます。
- **ファームウェアまたはメディアの保護**
  ブート時のフラッシュメモリ内のコードの検証(改ざんの防止: セキュアブートとも呼ばれる)、ダウンロードしたメディアファイルの暗号化、単一システムだけで使える一意コードイメージの暗号化を行います。
- **セッション鍵の交換**
  機密通信チャンネルや暗号化されたダウンロードデータ等を管理するため、システム マイクロプロセッサ内の暗号化/復号エンジンによって使われるストリーム暗号鍵を安全かつ容易に交換します。
- **データのセキュアな保存**
  標準的なマイクロプロセッサ内の暗号処理アクセラレータによって使われる秘密鍵を保存します。少量の機密データ(設定値、校正値、ePurse 値、使用/消費量データ等)の保存用にも使えます。暗号化/認証された読み書きによる保護設定が可能です。
- **ユーザパスワードの検証**
  正しい値を知られる事なくユーザが入力したパスワードを検証します。単純なパスワードを複雑なパスワードにマッピングします。パスワード値をリモートシステムとの間でセキュアに交換します。

1.2 デバイス機能

ATSHA204A は鍵、各種読み書き可能データ、読み出し専用データ、機密データ、使用/ 消費量ログ、セキュリティ設定等の保存用に使える EEPROM (Electrically Erasable Programmable Read-Only Memory) アレイを備えています。メモリ内の各種セクションへのアクセスを各種の方法で制限でき、コンフィグレーションが変更されないようロックできます。詳細は**「EEPROM の構成」**を参照してください。

ATSHA204A は、デバイス自体への物理的攻撃またはデバイスとシステムの間の転送データに対する論理的攻撃に対抗するよう専用に設計された防御機能を豊富に備えています。詳細は**「セキュリティ機能」**を参照してください。鍵の使用または生成方法に対するハードウェア制約により、特定形態の攻撃に対する防御が強化されます。

デバイスへのアクセスには標準 I^2C インターフェイス(最大速度 1 Mb/s)を使います。詳細は**「I^2C インターフェイス」**を参照してください。このインターフェイスは I^2C インターフェイス仕様と互換です。
本デバイスは単線式インターフェイス(SWI)もサポートします。SWI を使うと、システム プロセッサに要求される GPIO の数とコネクタピンの数を節減できます。詳細は**「単線式インターフェイス」**を参照してください。

© 2019 Microchip Technology Inc.

複数のクライアント(例: 色の異なる複数のインクタンクや複数のスペアパーツ等)を持つシステムでは、単線式インターフェイス使って複数の ATSHA204A デバイスが同じバスを共有する事により、プロセッサ GPIO の使用数を節約できます。詳細な実装方法は**「インターフェイスの共有」**と**「Pause コマンド」**を参照してください。

各 ATSHA204A は、一意性が保証された 9 バイト(72 ビット)のシリアル番号付きで出荷されます。ホストシステムまたはリモートサーバは、本デバイスがサポートする暗号プロトコルを使ってシリアル番号が信頼できる(複製ではない)事を確認できます。多くの場合、シリアル番号は標準的なシリアル EEPROM に保存されますが、それらは容易に複製され、そのシリアル番号が信頼できる(クローンではない)事をホストが確認する方法はありません。一意性を保証するには、シリアル番号の全ての桁を使う必要があります。

ATSHA204A は高品質の乱数を生成でき、それらは本デバイスの暗号プロトコルの一部として使える他、各種の目的で使う事ができます。各 32 バイト(256 ビット) 乱数は、そのデバイスまたは他のデバイスで過去に生成された番号とは無関係に生成されます。このため、これらの番号をプロトコル計算に含める事で、リプレイ攻撃(例: 以前に成功したトランザクションの再送信)を防ぐ事ができます。**「乱数生成器 (RNG)」**と**「Random コマンド」**を参照してください。

幅広い電圧レンジ(2.0～5.5 V)と超低スリープ電流(<150 nA)により、本デバイスは容易にシステムに統合できます。全ての DC パラメータは**「電気的特性」**に記載しています。これらの特性は超小型 UDFN パッケージ(2.0x3.0 mm)を含む各種パッケージ オプションに適用されます。各パッケージの詳細と注文コードは**「パッケージ図面」**を参照してください。

Microchip 社の ATSHA204 との互換性については**「互換性」**を参照してください。

1.3 暗号演算

ATSHA204A は、プログラムを簡素化するために、標準的なチャレンジ-レスポンス プロトコルもサポートします。その最も基本的な実装では、ホストシステムがチャレンジ(番号等)をクライアント内のデバイスへ送信します。チャレンジを受け取ったデバイスは、ホストシステムからの MAC (Message Authentication Code)コマンド(**「MAC コマンド」**参照)を使って、そのチャレンジと秘密鍵の組み合わせから生成したレスポンスをホストシステムへ返します。本デバイスは、暗号ハッシュアルゴリズムを使って、その組み合わせ(ダイジェストと呼ぶ)を生成します。ハッシュ アルゴリズムを使う事で、バス上の観察者が秘密鍵の値を引き出す事を防ぎます。
受信者は、ホストシステムと同じ計算方法を使って、保存されている秘密鍵の複製とチャレンジの組み合わせからダイジェストを生成します。

ATSHA204A の柔軟なコマンドセットにより、この基本動作は各種の方法で拡張できます。GenDig コマンド(**「GenDig コマンド」**参照)を使うと、他のスロット内の値をレスポンス ダイジェストに含める事ができます。これにより、データが本当にそのデバイスから読み出されたのか(それとも中間者攻撃によって挿入されたのか)を効果的に検証できます。このコマンドを使うと、2 つの鍵をチャレンジと組み合わせる事もできます。これは複数層の認証を実行する場合に便利です。

DeriveKey コマンド(**「DeriveKey コマンド」**参照)は鍵のローリング(差し替え)処理を実装します。コマンドモード パラメータを設定する事で、例えばリモート制御式ガレージ扉と同様の動作を実装できます。鍵が使われるたびに、鍵の現在の値とシステムに固有の値が暗号的に組み合わされて次の暗号演算用の鍵が生成されます。攻撃者が 1 つの鍵の値を入手しても、その鍵は二度と使えません。

DeriveKey を使うと、限られた条件(特定のホスト ID、特定の期間等)に対してのみ有効となる新しいランダム鍵を生成する事もできます。新しく生成される鍵は、過去に生成されどのデバイスのどの鍵とも異なります。

© 2019 Microchip Technology Inc.

現場でこの方法を使ってホスト-クライアント ペアを「アクティベート」する事により、そのクライアントのクローンは他のどのホストに対しても動作できなくなります。

ホスト-クライアント構成においてホスト(例: 携帯電話)がクライアント(例: OEM バッテリ)を検証する必要がある場合、クライアントからのレスポンスを検証するために、秘密鍵をホストに保存する必要があります。CheckMac コマンド(**「CheckMac コマンド」**参照)を使うと、ホストデバイスはクライアントの秘密鍵を安全に保存し、 正しいレスポンス値を PIN から隠す事ができます(システムに対して yes/no だけを返します)。

ユーザからのパスワード入力が必要な場合、CheckMac コマンドを使う事で、パスワードを通信バス上に暴露する事なく検証できると共に、パスワードをデバイスに保存されているよりエントロピの高い値に割り当てる事ができます。詳細は**「パスワードの検証」**を参照してください。

最後に、チャレンジと秘密鍵のハッシュの組み合わせ (例: ダイジェスト)をデバイスで保持できます。このダイジェストとスロットの内容の XOR を取る事で暗号化された読み出し(**「Read コマンド」**参照)を実装でき、このダイジェストと暗号化された入力データの XOR を取る事で暗号化された書き込み(**「Write コマンド」**参照)を実装できます。

これらの各動作は、計算にランダムノンス(**「Nonce コマンド」**参照)を含める事により、リプレイ攻撃から保護できます。

全てのセキュリティ機能は、業界標準の SHA-256 セキュア ハッシュ アルゴリズムを使って実装されます。このアルゴリズムは、関連機関と暗号の専門家によって推奨される一連の最新高セキュリティ暗号アルゴリズムの 1 つです。**「SHA-256」**には、このアルゴリズムの詳細情報へのリンクを記載しています。
必要に応じ、SHA-256 アルゴリズムを HMAC シーケンス(**「HMAC コマンド」**参照)に含める事もできます。 ATSHA204A は、フルサイズ(256 ビット)の秘密鍵を採用する事で、全ての種類の全数攻撃を防ぎます。

© 2019 Microchip Technology Inc.

2. デバイスの構成

本デバイスは以下のメモリブロックを含みます。

- EEPROM
- SRAM

2.1 EEPROM の構成

EEPROM は全部で 664 バイト(5312 ビット)の容量を持ち、以下のゾーンに分割されます。

表 2-1. ATSHA204A のゾーン

ゾーン	概要	命名法
Data	512 バイト(4.0 kb) のゾーンが 16 個の読み出し専用または読み書き可能汎用メモリスロット(1 スロットは 32 バイト = 256 ビット) に分割されます。 各スロットには鍵、校正データ、モデル番号等の情報(一般的に ATSHA204A が接続される先のデバイスに関連する情報)を保存できます。各データスロットのアクセス条件は、対応するコンフィグレーション値に書き込まれた値によって決まります。この条件を有効にするには、LockValue バイトを設定する必要があります。	Slot<YY> = Data ゾーンのスロット YY に保存されている全内容
Configuration	EEPROM 内の 88 バイト(704 ビット) のゾーンは、ID 情報(シリアル番号等)と、データメモリの各スロットに対するアクセス許可情報を格納します。Configuration ゾーンに書き込まれた値によって各データスロットのアクセス条件(各スロットがどのように応答するか)が決まります。 Configuration ゾーンは、ロックされる(LockConfig != 0x55 に設定される)まで変更可能です。アクセス条件を有効にするには、LockValue バイトを設定する必要があります(上記参照)。	SN<a:b> = Configuration ゾーンのフィールド内のバイトのレンジ
One Time Programmable (OTP)	64 バイト(512 ビット)の OTP ビットを格納します。これらのビットは、OTP ゾーンがロックされる前に、標準 `Write` コマンドを使って自由に書き込めます。 OTP ゾーンは、読み出し専用データまたは単方向ヒューズタイプの使用/消費ログ情報を保存するために使えます。	OTP<bb> = OTP ゾーン内の 1 バイト OTP<aa:bb> = バイトのレンジ

本書内で使う用語の意味を下表に示します。

表 2-2. 本書内の用語の意味

用語	意味
ブロック	1 ブロックは、特定メモリゾーンの 256 ビット(32 バイト)領域です。業界標準 SHA-256 文書では、「ブロック」はメッセージ入力の 512 ビット セクションを意味します。加えて、本書の I/O 関連の説明では、「ブロック」はシステムと本デバイスの間で転送される可変長集合体エレメントを意味します。
スロット	Data ゾーンの場合、「ブロック」と「スロット」は同義です。OTP および Configuration ゾーンには 32 バイトのブロックが複数個存在します。
param<b>	パラメータまたはバイトフィールドの 1 ビットを表します。
SRAM	入力および出力バッファと、状態保存領域を格納します。 **「スタティック RAM (SRAM)」**を参照してください。

© 2019 Microchip Technology Inc.

Microchip 社からの出荷時に、EEPROM に工場検査データが書き込まれます。このデータは、固定値による基板検査用に使えます。このデータは、デバイスの Configuration および/または Data セクションをロックする前に、必要な内容で上書きする必要があります。出荷時の値を記載した文書はこちらからご覧になれます。

2.1.1 EEPROM の Data ゾーン

Data ゾーンは EEPROM アレイ内の 512 バイト(4 kb) 領域であり、セキュアストレージ向けに使えます。

Lock(Config)を使って Configuration セクションをロックするまで Data ゾーンにはアクセスできません(読み出しも書き込みもできません)。Configuration ゾーンをロックした後は、Write コマンドを使って Data ゾーン全体に書き込めます。必要に応じ、書き込みデータを暗号化できます。

下表の「バイトアドレス」は、Data ゾーン内の各スロットの先頭バイトのアドレスです。ATSHA204A の全ての Read および Write 命令は、ワード(4 バイト = 32 ビット)単位で実行されます。Read および Write コマンドに渡すアドレス パラメータには、下表内のワードアドレスを使う必要があります。

表 2-3. Data ゾーンのスロット

Slot	バイトアドレス(HEX)	ワードアドレス(HEX)	Slot	バイトアドレス(HEX)	ワードアドレス(HEX)
0	0x0000	0x0000	8	0x0100	0x0040
1	0x0020	0x0008	9	0x0120	0x0048
2	0x0040	0x0010	10	0x0140	0x0050
3	0x0060	0x0018	11	0x0160	0x0058
4	0x0080	0x0020	12	0x0180	0x0060
5	0x00A0	0x0028	13	0x01A0	0x0068
6	0x00C0	0x0030	14	0x01C0	0x0070
7	0x00E0	0x0038	15	0x01E0	0x0078

2.1.2 Configuration ゾーン

Configuration ゾーン内の 88 バイト(704 ビット)は、製造 ID データ、一般的デバイスおよびシステム コンフィグレーション、Data ゾーン内のスロットに対するアクセス制限設定を格納します。Configuration ゾーン内のバイトの値は、いつでも Read コマンドを使って読み出せます。このゾーンのバイトの配列を下表に示します。

表 2-4. Configuration ゾーン

Word	バイト 0	バイト 1	バイト 2	バイト 3	既定値	書き込みアクセス	読み出しアクセス
0x00	SN<0:3>				01 23 xx xx	常時禁止	常時可能
0x01	RevNum				xx xx xx xx	常時禁止	常時可能
0x02	SN<4:7>				xx xx xx xx	常時禁止	常時可能
0x03	SN<8>	予約済み	I2C_Enable	予約済み	EE 55 xx 00	常時禁止	常時可能
0x04	I2C_Address	CheckMacConfig	OTP モード	セレクタモード	C8 00 55 00	Configuration ゾーンがアンロックの場合に可能	常時可能

Word	バイト 0	バイト 1	バイト 2	バイト 3	既定値	書き込みアクセス	読み出しアクセス
0x05	SlotConfig 0		SlotConfig 1		8F 80 80 A1	Configuration ゾーンがアンロックの場合に可能	常時可能
0x06	SlotConfig 2		SlotConfig 3		82 E0 A3 60	Configuration ゾーンがアンロックの場合に可能	常時可能
0x07	SlotConfig 4		SlotConfig 5		94 40 A0 85	Configuration ゾーンがアンロックの場合に可能	常時可能
0x08	SlotConfig 6		SlotConfig 7		86 40 87 07	Configuration ゾーンがアンロックの場合に可能	常時可能
0x09	SlotConfig 8		SlotConfig 9		0F 00 89 F2	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0A	SlotConfig 10		SlotConfig 11		8A 7A 0B 8B	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0B	SlotConfig 12		SlotConfig 13		0C 4C DD 4D	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0C	SlotConfig 14		SlotConfig 15		C2 42 AF 8F	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0D	UseFlag 0	UpdateCount 0	UseFlag 1	UpdateCount 1	FF 00 FF 00	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0E	UseFlag 2	UpdateCount 2	UseFlag 3	UpdateCount 3	FF 00 FF 00	Configuration ゾーンがアンロックの場合に可能	常時可能
0x0F	UseFlag 4	UpdateCount 4	UseFlag 5	UpdateCount 5	FF 00 FF 00	Configuration ゾーンがアンロックの場合に可能	常時可能
0x10	UseFlag 6	UpdateCount 6	UseFlag 7	UpdateCount 7	FF 00 FF 00	Configuration ゾーンがアンロックの場合に可能	常時可能
0x11	LastKeyUse 0	LastKeyUse 1	LastKeyUse 2	LastKeyUse 3	FF FF FF FF	Configuration ゾーンがアンロックの場合に可能	常時可能
0x12	LastKeyUse 4	LastKeyUse 5	LastKeyUse 6	LastKeyUse 7	FF FF FF FF	Configuration ゾーンがアンロックの場合に可能	常時可能
0x13	LastKeyUse 8	LastKeyUse 9	LastKeyUse 10	LastKeyUse 11	FF FF FF FF	Configuration ゾーンがアンロックの場合に可能	常時可能
0x14	LastKeyUse 12	LastKeyUse 13	LastKeyUse 14	LastKeyUse 15	FF FF FF FF	Configuration ゾーンがアンロックの場合に可能	常時可能
0x15	UserExtra	Selector	LockValue[1]	LockConfig	00 00 55 55	UpdateExtra コマンドによってのみ可能	常時可能

Note:

1. LockValue は、以前は LockData と呼びました。

2.1.2.1 I2C_Enable

Bit 7–1: これらのビットは無視されます(Microchip 社が設定)。

Bit 0: 0 = 単線式インターフェイス モード
1 = I²C インターフェイス モード

2.1.2.2 I2C_Address

I²C モード(I2C_Enable<0> = 1)の場合

Bit 7–1: I²C デバイスアドレス

Bit 3: TTL イネーブル
このビットは I²C アドレスの一部として使われるか、以下の通りにしきい値レベルを設定します。
0 = 入力レベルは固定された参照電圧を使う
1 = 入力レベルは V_{CC} を参照電圧として使う

Bit 0: 無視

単線式モード(I2C_Enable<0> = 0)の場合

Bit 7–4: 無視
Bit 3: TTL イネーブル
0 = 入力レベルは固定された参照電圧を使う
1 = 入力レベルは V_{CC} を参照電圧として使う

Bit 2-0: 無視

2.1.2.3 CheckMacConfig

このバイトは CheckMac、Read、Write コマンドにのみ適用されます。

- **Read および Write コマンドの場合:** CheckMacConfig<n>はスロット n および n+1 を制御します(n = 0、1、2、...)。TempKey.SourceFlag の値がこのバイト内の対応するバイトと一致しない場合、 暗号化された Read または Write コマンドの実行は失敗します。このバイトは平文の読み書きでは無視されます。
- **CheckMac コマンドの場合:** CheckMacConfig<n>はスロット nx2+1 を制御します(n = 0、1、2、...)。複製機能は、ターゲット スロットに対応する CheckMacSource 値が CheckMac コマンドの Mode の bit 2 の値と一致する場合にのみ有効にできます。Mode の bit 2 が TempKey.SourceFlag に一致しない場合、コマンドの実行は失敗します。すなわち、このバイト内の対応するビットは TempKey.SourceFlag と一致する必要があります。

2.1.2.4 OTP モード

0xAA (Read-only モード): OTP ゾーンがロックされている場合、書き込みは禁止されますが、全てのワードの読み出しは許可されます。

0x55 (Consumption モード) = OTP ゾーンがロックされている場合、書き込みによって現在「1」のビットを「0」に書き換える事だけが可能です。全てのワードの読み出しは許可されます。

0x00 (Legacy モード) = OTP ゾーンがロックされている場合、書き込みは禁止され、ワード 0 および 1 の読み出しと 32 バイト読み出しも禁止されます。

その他のモードは全て予約済みです。

© 2019 Microchip Technology Inc.

2.1.2.5 セレクタモード

0x00 の場合、セレクタは UpdateExtra により更新されます。

その他の値では、セレクタの値が 0 の場合にのみセレクタの更新が可能です。

2.1.2.6 SlotConfig

表 2-5. SlotConfig ビット(スロットごと)を参照してください。

2.1.2.7 UseFlag

スロット 0～7 の使用回数を制限します。「1」のビットの数がスロット 0～7 の使用可能回数(スロットが無効になるまでの残回数)を表します。

2.1.2.8 UpdateCount

DeriveKey によってスロット 0～7 が更新された回数(0～7)を示します。

2.1.2.9 LastKeyUse

スロット 15 の使用回数を制限します。「1」のビットの数がスロット 15 の使用可能回数(スロットが無効になるまでの残回数)を表します。SlotConfig<5> LimitedUse がセットされている場合にのみ適用されます。

2.1.2.10 UserExtra

一般的なシステム用途向けに、Configuration ゾーン内の UserExtra バイトは UpdateExtra コマンドを使って変更できます。

2.1.2.11 Selector

Pause コマンドの実行後にアクティブモードを維持するデバイスを選択します。

2.1.2.12 LockValue

Data および OTP ゾーンのロックを制御します。この値は自由に書き込めますが、読み出す事はできません。

0x55 = Data および OTP ゾーンをロックしない(書き込みが可能)

0x00 = Data および OTP ゾーンをロックし、Configuration ゾーンで定義されているアクセス条件を適用する(Data ゾーン内のスロットは、対応する WriteConfig フィールドに基づいて変更する事しかできません。OTP ゾーンは、OTP モードに基づいて変更する事しかできません。)

2.1.2.13 LockConfig

Configuration ゾーンへのアクセスを制御します。

0x55 = Configuration ゾーンへの書き込みアクセスを許可する(アンロック)

0x00 = Configuration ゾーンへの書き込みアクセスを禁止する(ロック)

2.1.2.14 SlotConfig (バイト 20–51)

16 個の SlotConfig エレメントにより、ATSHA204A 内の 16 個のスロットのアクセス保護をスロットごとに設定します。各 SlotConfig エレメントは 16 ビットで構成され、対応するスロットまたは鍵に対する使用またはアクセスを制御します。Data ゾーンがロックされている時、SlotConfig フィールドは表 2-5 に従って解釈されます。Data ゾーンがロックされていない場合、これらの制約は適用されず、全てのスロットは自由に書き込めますが、読み出しはできません。

表 2-5. SlotConfig ビット(スロットごと)

Bit	名称	概要
15-12	WriteConfig	表 2-6 参照
11-8	WriteKey	暗号化された書き込みの検証用に使う鍵のスロット

© 2019 Microchip Technology Inc.

Bit	名称	概要
7	IsSecret	0 = このスロットは秘密ではない (平文読み出し、平文書き込み、MAC チェックなし、Derivekey コマンドなしを許容) 1 = このスロットは秘密 (暗号化された読み書きが必要)
6	EncryptRead	0 = 平文読み出しを許容する 1 = スロットは秘密である事が必要であり、アクセスするには暗号化された読み出しが必要
5	LimitedUse(1)	0 = 鍵の使用回数を制限しない 1 = スロットに対応する UseFlag (または LastKeyUse)に基づいて鍵の使用回数を制限する
4	CheckOnly	0 = このスロットは全ての暗号コマンド向けに使える 1 = このスロットは CheckMac コマンドおよび CheckMac の前の GenDig コマンド向けにのみ使える
3-0	ReadKey	暗号化された読み出し用に使う鍵のスロット この値が 0x0 の場合、このスロットは CheckMac/Copy コマンド向けのソーススロットとして使えます。

Note:

1. LimitedUse ビットは、以前は SingleUse と呼んでいました。

表 2-6. 書き込みコンフィグレーション ビット — Derivekey コマンド

Bit 15	Bit 14	Bit 13	Bit 12	ソース鍵(1)	概要
0	X	1	0	ターゲット	DeriveKey コマンドは MAC を認証せずに実行できます (鍵のローリング)。
1	X	1	0	ターゲット	DeriveKey コマンドを実行するには MAC を認証する必要があります(鍵のローリング)。
0	X	1	1	ペアレント	DeriveKey コマンドは MAC を認証せずに実行できます(鍵の生成)。
1	X	1	1	ペアレント	DeriveKey コマンドを実行するには MAC を認証する必要があります(鍵の生成)。
X	X	0	X	—	WriteConfig フィールドがこの値である場合、そのスロットは DeriveKey コマンドのターゲットとして使えません。

Note:

1. DeriveKey コマンドによって実行する計算のソース鍵には、Param2 (ターゲット)で直接指定された鍵または SlotConfig<Param2>. WriteKey (ペアレント)で指定された鍵が使えます。
   詳細は**「鍵の値」**を参照してください。

© 2019 Microchip Technology Inc.

表 2-7. 書き込みコンフィグレーション ビット — Write コマンド

Bit 15	Bit 14	Bit 13	モード名	概要
0	0	0	Always	このスロットでは、平文書き込みが常に可能です。「Always」に設定したスロットを鍵ストレージとして使ってはいけません。このスロットには 4 バイト書き込みと 32 バイト書き込みが可能です。
X	0	1	Never	Write コマンドを使ってこのスロットに書き込む事はできません。「Never」に設定したスロットは鍵ストレージとして使えます。
1	0	X	Never	Write コマンドを使ってこのスロットに書き込む事はできません。「Never」に設定したスロットは鍵ストレージとして使えます。
X	1	X	Encrypt	このスロットに書き込むには正しく計算された MAC が必要であり、システムは WriteKey を使って入力データを暗号化する必要があります。これには 8.5.18 「Write コマンド」に記載した暗号アルゴリズムを使います。 このスロットへの 4 バイト書き込みは禁止されます。

Write コマンドは 4 ビットの WriteConfig フィールドを**表 2-7. 書き込みコンフィグレーション ビット - Write コマンド**の通りに解釈します(表内の「X」は「ドントケア」を意味します)。

表 2-6 と表 2-7 はコマンドごとに独立して適用されます。例えばコードが「0b0110」の場合、スロットは Write コマンドを使って暗号化された形態で書き込めると共に、そのスロットは未認証の DeriveKey コマンドのターゲットになる事ができます(ターゲットをソースとして使用)。

IsSecret ビットは、読み出しまたは書き込み(もしくはその両方)を暗号化する必要のあるスロットまたは読み書きが完全に禁止されているスロットのセキュリティに必要な内部回路を制御します。このビットは、鍵として使われる全てのスロット(DeriveKey によって生成または変更されるスロットを含む)向けにセットする必要もあります。デバイスを適正に動作させるには、WriteConfig が「Always」でない限り、このビットをセットする必要があります。このビットがセットされている場合、そのスロットに対する 4 バイト読み書きアクセスは禁止されます。

鍵値を保存するスロットでは、セキュリティを最大限に高めるため、IsSecret ビットを「1」に設定し、EncryptRead ビットを「0」(読み出し禁止)に設定する必要があります。固定された鍵値を使う場合、WriteConfig ビットは「Never」に設定します。このように設定した場合、Data ゾーンがロックされた後の鍵の読み書きは全て禁止されます。この鍵は暗号演算用にのみ使われます。

セキュリティ条件によっては、秘密鍵を時々更新する必要があります。ATSHA204A は、以下の方法によりこれをサポートします。

- 特定スロットの WriteConfig を「Encrypt」に設定し、SlotConfig.WriteKey で同じスロットを指定します(WriteKey をそのスロットの ID に設定します)。次に、標準 Write コマンドを使って、 新しい値をこのスロットに書き込む事ができます(ただし、認証 MAC は古い(現在の)鍵値を使って計算されます)。

2.1.2.15 Configuration ゾーン内の特殊メモリ値(バイト 0–12)

ATSHA204A には各種の固定された情報が書き込まれています。いかなる場合もそれらの情報に書き込む事はできませんが、ロックビットの状態に関係なくいつでも読み出す事ができます。

- **SerialNum**
  SN<0:8>は 9 バイトの一意値を形成します。この値は、CryptoAuthentication ファミリの全てのデバイスで異なります。このシリアル番号は以下の 2 つに分割されます。

  1.1. **SN<0:1>と SN<8>**

  ATSHA204A のほとんどのバージョンでは、これらのビットの値は製造時に固定されています。既定値は(0x01 0x23 0xEE)です。これらの 24 ビットは、ATSHA204A が実行する SHA-256 計算に常に含まれます。

© 2019 Microchip Technology Inc.

1.2. **SN<2:7>**
これらのビットの値はダイごとに異なり、製造工程中に Microchip 社によって書き込まれます。これらの 6 バイト(48 ビット)は、必要に応じて ATSHA204A が実行する SHA-256 計算に含まれます。

- **RevNum**
この 4 バイトの情報は、製造リビジョン情報として Microchip 社が使います。これらのバイトは RevNum<0:3>としていつでも読み出せますが、シリコン リビジョンに応じて変更される可能性があるため、この値をシステム ソフトウェアで使ってはいけません。

2.1.3 One Time Programmable (OTP)ゾーン

OTP ゾーンは EEPROM アレイ内の 64 バイト(512 ビット) 領域であり、読み出し専用ストレージとして使えます。

Lock (LockConfig)を使って Configuration セクションをロックするまで OTP ゾーンにはアクセスできません(読み出しも書き込みもできません)。Configuration ゾーンをロックした後は、Lock(LockValue)を使って OTP ゾーンをロックするまで、Write コマンドを使って OTP ゾーン全体に書き込む事ができます。必要に応じ、書き込みデータを暗号化できます。アンロック時に OPT ゾーンから読み出す事はできません。

OTP ゾーンをロックすると、Configuration ゾーン内の OTP モードバイトは OTP ゾーンへのアクセスを以下の通りに制御します。

- **Read-only モード**
データを書き換える事はできません。このモードは、各種の変更不可データ(モデル番号、校正情報、製造履歴等)を保存するために使います。Write コマンドは常にエラーを返し、メモリの内容は変更されません。OTP セクション内の 64 バイトは、全て 4 バイトまたは 32 バイト読み出しを使っていつでも読み出せます。
- **Consumption モード**
このビットは片方向ヒューズとして機能し、ATSHA204A の接続先アイテムの使用/消費量または使用回数を追跡するために使えます。例えば、バッテリの充電サイクルまたは使用時間、プリンタ インク カートリッジの消費量、医療機器の使用回数が制限されるアイテムの使用状況等を監視できます。
このモードでは、Write コマンドは「1」のビットを「0」に書き換える事しかできません。すなわち、入力パラメータリスト内のデータ値とワード内の現在の値の間で論理積(AND)が取られ、その結果がメモリに書き戻されます。例えば、値「0xFF」を書き込んでもメモリ内のバイトの値は全く変更されず、値「0x00」を書き込むと以前の値に関係なくバイトの値は 0 になります。一度「0」に変更されたビットを「1」に戻す事は絶対にできません。
- **Legacy モード**
OTP ゾーンの動作は、Microchip 社(以前は Atmel 社)の ATSA102S 上のヒューズアレイと同じです。ワード 0 とワード 1 の読み出しは常に禁止され、残りの 14 ワードだけが常に読み出し可能です。4 バイト(32 ビット)読み出しだけが許容され、32 バイト(256 ビット)読み出しを試みるとエラーコードが返されます。OTP ゾーンに対する全ての書き込みは禁止されます。Microchip 社製 ATSA102S との互換性については 9. 「互換性」を参照してください。

OTP ゾーン内の全てのビットは、Micorhip 社工場からの出荷時に「1」に設定されています。

表 2-8. OTP ゾーン

ワード(HEX)	アドレス(HEX)	既定値
0x00	0x00	0xFFFFFFFF
0x01	0x04	0xFFFFFFFF
0x02	0x08	0xFFFFFFFF

© 2019 Microchip Technology Inc.

ワード(HEX)	アドレス(HEX)	既定値
0x03	0x0C	0xFFFFFFFF
0x04	0x10	0xFFFFFFFF
0x05	0x14	0xFFFFFFFF
0x06	0x18	0xFFFFFFFF
0x07	0x1C	0xFFFFFFFF
0x08	0x20	0xFFFFFFFF
0x09	0x24	0xFFFFFFFF
0x0A	0x28	0xFFFFFFFF
0x0B	0x2C	0xFFFFFFFF
0x0C	0x30	0xFFFFFFFF
0x0D	0x34	0xFFFFFFFF
0x0E	0x38	0xFFFFFFFF
0x0F	0x3C	0xFFFFFFFF

2.1.4 デバイスのロック

本デバイスには 2 つの異なるロックバイトがあります。

- 1 つは Configuration ゾーンをロックします(LockConfig (バイト 87)により制御)。
- もう 1 つは Data ゾーンと OTP ゾーンをロックします(LockValue (バイト 86)により制御)。これは、各 Data ゾーンスロットに対するアクセス条件をスロット コンフィグレーションに基づいて有効にします。

これらのロックは、Configuration ゾーン内の別々のバイトに保存されており、Lock コマンドによってのみ変更可能です。メモリゾーンがロックされた後にロックを解除する方法はありません。Data/OTP ゾーンがロックされた後でも、スロット コンフィグレーションによって定義されたアクセス条件に基づいてスロットを変更する事ができます。

システム製造者は、必要なコンフィグレーション情報でデバイスをパーソナライズした後に、Configuration ゾーンをロックする必要があります。このロックが完了した後は、EEPROM に対する公開および非公開情報の全ての書き込みは、暗号化する必要があります。Data および OTP ゾーンに対する書き込みを完了した後に、LockValue バイトに書き込む必要があります。

極めて重要な事として、本デバイスを使ったシステムをフィールドへリリースする前に、LockValue バイトを設定してロックする事により Data および OTP ゾーン内のデータを保護する必要があります。これらのゾーンをロックしないと、秘密鍵の変更を許してしまい、セキュリティの問題が生じる可能性があります。

Configuration ゾーンをロックする前に Data または OTP ゾーンの読み書きを試みると、デバイスはエラーを返します。

オプションのセキュア パーソナライゼーション サービスについては Microchip 社にお問い合わせください。

2.1.4.1 Configuration ゾーンのロック

Configuration ゾーン内の特定バイトは、LockConfig の状態に関係なく、変更できません。このゾーン内のその他のバイトへのアクセスは、Configuration ゾーン内の LockConfig バイトにより、表 2-9 の通りに制御されます。本書では、LockConfig が 0x55 である状態をアンロックと呼び、その他の状態をロックと呼びます。

© 2019 Microchip Technology Inc.

表 2-9. Configuration ゾーンのロック

ロック状態	読み出しアクセス	書き込みアクセス
LockConfig == 0x55 (アンロック)	許可	許可
LockConfig != 0x55 (ロック)	許可	禁止

2.1.4.2 Data および OTP ゾーンのロック

本書では、LockValue が 0x55 である状態をアンロックと呼び、その他の状態をロックと呼びます。

Configuration ゾーンがロックされる前に Data および OTP ゾーンに対して読み書きする事はできません。

表 2-10. Data および OTP ゾーンのアクセス制限

ロック状態	読み出しアクセス	書き込みアクセス
LockValue == 0x55 (アンロック)	禁止	許可
LockValue != 0x55 (ロック)	許可(1)	許可(1)

Note:

1. そのスロットのスロット コンフィグレーションに基づきます。

2.1.4.3 OTP ゾーンのロック

OTP ゾーンに対する読み書きは、LockConfig および LockValue の状態と Configuration ゾーン内の OTP モードバイトに基づきます。

2.2 スタティック RAM (SRAM)

本デバイスは SRAM アレイを備えています。これは入力コマンドまたは出力結果、中間計算結果値、一時鍵を保存するために使います。
このメモリ全体の内容は、デバイスがスリープモードに移行するか電源が遮断されると無効になります。一時鍵は TempKey と呼び、MAC、HMAC、CheckMac、GenDig、DeriveKey コマンドへの入力として使えます。この鍵は、Read および Write コマンドによってデータ保護(暗号化または復号)鍵としても使われます。「TempKey」を参照してください。

2.2.1 TempKey

TempKey は SRAM アレイ内のストレージ レジスタであり Nonce、GenDig、CheckMac、SHA コマンドからの一時結果値を保存するために使えます。このレジスタの内容をデバイスから読み出す事はできません(デバイス自体は内部でこの内容を読み出して使用できます)。

このレジスタは、表 2-11 に示すエレメントを格納します。

表 2-11. TempKey ストレージ レジスタ

名称	ビット長	概要
TempKey	256 (32 バイト)	ノンス (Nonce コマンドから)またはダイジェスト(GenDig コマンドから)
SlotID	4	GenDig によって TempKey が生成された場合(GenData および CheckFlag ビット参照)、これらのビットはその計算にどの鍵が使われたのかを示します。この 4 ビットは、Data ゾーン内のスロットの 1 つを表します。

© 2019 Microchip Technology Inc.

名称	ビット長	概要
SourceFlag	1	TempKey における乱数化のソース: 0 = 内部生成した乱数(Rand) 1 = 入力シードのみ(内部で乱数を生成しない) (Input)
GenData	1	0 = TempKey.SlotID は意味を持たず無視される 1 = TempKey の内容は Data ゾーン内のスロットの 1 つを使って GenDig により生成された(TempKey.SlotID は意味を持つ)
CheckFlag	1	0 = TempKey の内容は、CheckMac 鍵制限なしで Nonce、SHA、GenDig のいずれかを使って生成された 1 = TempKey の内容は GenDig コマンドによって生成され、その生成に使われた鍵の少なくとも 1 つは CheckMac コマンドに対して制限される (SlotConfig.CheckOnly = 1)
Valid	1	0 = TempKey 内の情報は無効 1 = TempKey 内の情報は有効

本書では、「TempKey」という呼び名は 32 バイト(256 ビット) の「データレジスタ」を指す意味で使います。残りのビットフィールドは TempKey.SourceFlag、TempKey.GenData 等と呼びます。

TempKey.Valid ビットは、以下の条件のいずれかが発生した時に「0」にクリアされます。

- 電源投入、スリープ、ブラウンアウト、ウォッチドック例外、改ざん検出

  デバイスがアイドルモードに移行しても TempKey の内容は保持されます。
- Nonce または GenDig 以外のコマンドが実行された後(実行に成功したかどうかには無関係)

  複製が正常に実行されないと、このビットは CheckMac コマンドによってクリアされる可能性があります。通信に問題があってもこのビットはクリアされませんが、巡回冗長検査(CRC)エラーにより、問題が生じた事は分かります。
- パーシング中または GenDig および/または Nonce コマンド実行中のエラー
- GenDig の実行は、Nonce コマンドの以前の出力を GenDig コマンドの出力で置き換えます。Nonce コマンドの実行も、同様に GenDig コマンドの以前の出力を置き換えます。

© 2019 Microchip Technology Inc.

3. セキュリティ機能

3.1 物理セキュリティ

ATSHA204A は、EEPROM の内容が不正に暴露される事を防ぐための各種物理セキュリティ機能を備えています。これには以下が含まれます。

- デバイスのアクティブ シールド
- 内部メモリの暗号化
- セキュア テストモード
- グリッチ保護
- 電圧タンパ検出
- 温度タンパ検出

ATSHA204A に保存されたプログラミング済みトランスポート鍵は、外部からの解析によって値を盗み取る事が非常に困難となるよう暗号化されています。

ロジック用のクロックと電源電圧の両方を内部で生成する事により、これら 2 つの信号に対するデバイスピンを使った直接攻撃を防ぎます。

3.2 乱数生成器(RNG)

ATSHA204A は、32 バイトの乱数をシステムに返す高品質の乱数生成器(RNG)を備えています。本デバイスは、生成された乱数を個別の入力番号と組み合わせる事でノンスを形成し、後続のコマンドが使えるようデバイス内部の TempKey に保存します。

システムはこの RNG を任意の目的で使えます。例えば、別の CryptoAuthentication デバイス上で MAC コマンドに対する入力チャレンジとして使えます。本デバイスは、そのような用途向けに特別な乱数コマンドを提供します。これは、内部に保存されたノンスに影響を与えません。

システムのテストをシンプルにするため、Configuration ゾーンがロックされる前は、RNG は常に以下の 32 バイト値を返します。

```
0xFF FF 00 00 FF FF 00 00 …
```

0xFF はデバイスから読み出される最初のバイトであり、SHA メッセージ用に使われます。

ATSHA204A に入出力される暗号化されたデータをリプレイ攻撃から保護するため、本デバイスは、データの読み書きを防ぐために使う暗号化シーケンスの一部として新しく内部で生成されたノンスが含まれる事を要求します。この要求を満たすため、GenDig によって生成され Read または Write コマンドによって使われるデータ保護鍵は、ノンスの生成時に内部 RNG を使う必要があります。

乱数は、ハードウェア RNG の出力と内部シード値(外部からのアクセスは不可能)の組み合わせから生成されます。内部シード値は EEPROM に保存され、通常は電源投入またはスリープ/復帰サイクルが発生するたびに更新されます。更新後に、このシード値はデバイス内の SRAM レジスタで保持されます。これらのレジスタは、デバイスがスリープモードに移行するか電源が遮断されると無効になります。

© 2019 Microchip Technology Inc.

4. 一般的 I/O 情報

ATSHA204A との通信には、I²C または単線式のどちらかのプロトコルが使えます(デバイスの注文時に指定)。

- **単線式インターフェイス**
  システム マイクロプロセッサ上の GPIO を 1 つだけ使って本デバイスの SDA ピンに接続します。これにより、脱着式または交換式アクセサリを最小限のコネクタピン数で接続できます。最大ビットレートは 25.6 kb/s であり、標準 UART 信号と互換です。
- **I²C インターフェイス**
  このモードは、Microchip 社の AT24C16 シリアル EEPROM インターフェイスと互換です。シリアルデータ(SDA)とシリアルクロック(SCL)の接続用に 2 本のピンが必要です。本 I²C インターフェイスは最大 1 Mb/s のビットレートをサポートします。

I/O プロトコルの最下層については**「単線式インターフェイス」**と**「I²C インターフェイス」**で説明します。I/O プロトコルの最上層では、**「セキュリティ コマンド」**に記載した暗号コマンドとエラーコードを実装するために、どちらのインターフェイスも全く同じバイトを本デバイスとシステムの間で転送します。

本デバイスは、フェイルセーフのためのウォッチドッグ タイマを内蔵しています。このタイマは、現在のアクティビティに関係なく、特定の時間が経過した後にデバイスを低消費電力動作モードに移行させます。システム プログラミングでは、この事を考慮に入れる必要があります。詳細は**「ウォッチドッグ フェイルセーフ」**を参照してください。

4.1 バイトおよびビット順

CryptoAuthentication デバイスは共通のバイト順を採用し、以下の方法で番号と配列を扱います。

- 全てのマルチバイト集合エレメントはバイトの配列として扱われ、インデックス#0 を先頭として送受信された順番に処理されます。
- 2 バイト(16 ビット)整数(一般的に Param2)は LSB 先頭でバス上に現れます。

ビット順は、以下の通りに、使用する I/O チャンネルによって異なります。

- 単線式インターフェイスの場合、バス上のデータは LSb 先頭で ATSHA204A に対して双方向に転送されます。
- I²C インターフェイスの場合、バス上のデータは MSb 先頭で ATSHA204A に対して双方向に転送されます。

4.1.1 出力の例

Configuration ゾーン(入力アドレス: `0x0000`) の 32 ビット読み出しにより、以下のバイトが上記の順番でバスに返されます。

SN<0>, SN<1>, SN<2>, SN<3>, RevNum<0>, RevNum<1>, RevNum<2>, RevNum<3>, SN<4>, SN<5>, SN<6>, SN<7>, SN<8>, reserved, I2C_Enable, reserved, I2C_Address, OTPmode, SelectorMode, SlotConfig<0>.Read, SlotConfig<0>.Write, SlotConfig<1>.Read, SlotConfig<1>.Write, SlotConfig<2>.Read, SlotConfig<2>.Write, SlotConfig<3>.Read, SlotConfig<3>.Write, SlotConfig<4>.Read, SlotConfig<4>.Write, SlotConfig<5>.Read, SlotConfig<5>.Write

© 2019 Microchip Technology Inc.

4.1.2 MAC メッセージの例

MAC コマンド(Mode 値 = 0x71、SlotID = スロット x)に対して以下のバイトが SHA エンジンに渡されます。下の例では、K<x>は Data ゾーン内のスロット x の SlotID を示し、K<0>はそのスロットに対する読み書きによってバス上で転送される最初のバイトです。OTP<0>は、OTP ゾーン(アドレス 0)の読み出しによってバス上で転送される最初のバイトを示します。

K<0>, K<1>, K<2>, K<3> … K<31>, TempKey<0>, TempKey<1>, TempKey<2>, TempKey<3> … TempKey<31>, Opcode (=0x08), Mode (=0x71), Param2(LSB = 0xYY), Param2(MSB = 0x00), OTP<0>, OTP<1>, OTP<2>, OTP<3>, OTP<4>, OTP<5>, OTP<6>, OTP<7>, OTP<8>, OTP<9>, OTP<10>, SN<8>, SN<4>, SN<5>, SN<6>, SN<7>, SN<0>, SN<1>, SN<2>, SN<3>

MAC メッセージの詳細は**「MAC コマンド」**を参照してください。

© 2019 Microchip Technology Inc.

5. 単線式インターフェイス

単線式インターフェイス モードでは、ATSHA204A に対する双方向通信は SDA ピンのみを介して行われ、非同期タイミング ラインと SCL ピンは無視されます。

スリープ電流の仕様値は、SCL ピンを Low に保持するか未接続のままにした場合にのみ保証されます。

全体の通信構造は階層化されています。表 5-1 に、標準 RS-232 ポートによる単線式インターフェイスで使われるトークンを示します。ホスト UART ポートは 7 ビット データワード/230.4 k baud レートに設定する必要があります。

表 5-1. Wake および I/O トークン

トークンのタイプ	トークンの値	Start (1)	Wake トークンの LSb: MSb							Stop (1)
			b0	b1	b2	b3	b4	b5	b6	
Wake (2)	0x00	0	0	0	0	0	0	0	0	1
Logic 0 (3)	0x7D	0	1	0	1	1	1	1	1	1
Logic 1 (3)	0X7F	0	1	1	1	1	1	1	1	1

Note:

1. データキャプチャを同期させるため、全てのトークンの前に Low Start パルスが必要であり、全てのトークンは High Stop 値によって終了します。
2. Wake トークンは、デバイスを復帰させるために十分な長さの Low パルスを生成します。
3. Logic 0 および Logic 1 I/O トークンは、データの 1 つのビットを表します。1 バイトのデータを生成するには 8 個の I/O トークンが必要です。

I/O フラグ - このフラグは 8 個のトークン (ビット)で構成され、次に送信するビットのグループが存在すれば、その方向と意味を示します。フラグは常に LSb 先頭で送信されます。

ブロック - コマンドと送信フラグに続くデータのブロックです。これらのブロックは、正しくデータを転送するために、バイト数情報とチェックサムの両方を含みます。

パケット - ブロックのコアを形成するバイトのパケットです(バイト数と CRC を含まず)。パケットは、CryptoAuthentication コマンドの入出力パラメータまたは ATSHA204A からのステータス情報のどちらかです。

5.1 I/O トークン

単線式インターフェイスを介して以下の I/O トークンを伝送できます。

- **入力** (ATSHA204A への伝送)
  - Wake: スリープまたはアイドル状態からデバイスを復帰させます。
  - Zero: システムからデバイスへ値が「0」の 1 個のビットを送信します。
  - One: システムからデバイスへ値が「1」の 1 個のビットを送信します。
- **出力** (ATSHA204A からの伝送)
  - ZeroOut: デバイスからシステムへ値が「0」の 1 個のビットを送信します。
  - OneOut: デバイスからシステムへ値が「1」の 1 個のビットを送信します。

どちらの伝送方向でも波形は同じです。しかしタイミングは伝送方向によって少し異なります。ホストは非常に高精度で安定したクロックを備えるのに対し、ATSHA204A の内部クロック ジェネレータからのクロックは製造ばらつきと環境条件によって大きく変動します。

© 2019 Microchip Technology Inc.

ビットタイミングは、230.4 k baud レートの標準 UART 動作でトークンを効率的に送受信できるよう設定されています。UART により送受信される各バイトは、デバイスによって送受信される単一ビットに対応します。UART は 7 ビットデータ (0x7F が論理「1」、0x7D が論理「0」に対応) 向けに設定する必要があります。

Wake トークンには、SDA ピン上で特別に長い Low パルス(長さは t_{WLO})が必要です(**表 7-2. AC パラメータ – 全 I/O インターフェイス**を参照)。これにより、データトークン(Zero、One、ZeroOut、OneOut)中に発生する短い Low パルスから区別されます。アイドルまたはスリープ状態中のデバイスは、正しい Wake トークンを受信するまで全てのデータトークンを無視します。復帰済みのデバイスに対して Wake トークンを送信してはいけません。送信すると、波形から「0」も「1」も正しく認識できなくなるため、同期が失われます。同期を回復するための手順は**「同期手順」**を参照してください。

5.2 I/O フラグ

システムが常にバスマスタとなります。従って、全ての I/O トランザクションを開始する前にシステムから本デバイスへ 8 ビットフラグを送信する事で、この後に I/O 動作が続く事をデバイスに知らせる必要があります(表 5-2 参照)。

表 5-2. I/O フラグ

名称	値	意味
Sleep (low-power)	0xCC	ATSHA204A は低消費電力スリープモードに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。デバイスの揮発性ステートは全てリセットされます。
Idle	0xBB	ATSHA204A はアイドルステートに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。TempKey および RNG シードレジスタの内容は保持されます。
Command	0x77	後続のバイトを入力コマンドバッファ内の連続したアドレスに書き込みます。
予約済み	その他の値	これらの値のフラグをデバイスへ送信してはいけません。
Transmit	0x88	バス ターンアラウンド時間を待機した後に直前に送信されたコマンドブロックに対する応答の送信を開始するようデバイスに伝えます。出力バッファ内に有効データが存在する場合、Transmit フラグを繰り返しデバイスへ送信する事で、バッファの内容をシステムへ再送信させる事ができます。
Wake	インターフェイス参照	デバイスを低消費電力モードから復帰させ、ウォッチドッグ カウンタをリセットします。

5.2.1 Transmit フラグ

Transmit フラグは、ATSHA204A がデータをシステムへ返送できるよう、バスの伝送方向を変更します。デバイスからシステムへ返されるバイトは、デバイスの現在のステートに応じてステータス、エラーコード、コマンド結果のいずれかを含みます。

デバイスは、コマンドの実行中(ビジー状態の時)に SDA ピンとシステムから送信される全てのフラグを無視します。本デバイスにおける各コマンドタイプの実行遅延時間については、**「コマンド オペコードの概要と実行時間」**を参照してください。システムは、コマンドを送信した後にデバイスとの通信を試みる前に、これらの遅延要件を守る必要があります。

© 2019 Microchip Technology Inc.

5.3 同期

この通信プロトコルは半二重であるため、システムと ATSHA204A の間の同期が失われる可能性があります。速やかに同期を回復するため、本デバイスは特定の状況でスリープへの移行を強制するタイムアウトを実装しています。

5.3.1 I/O タイムアウト

ATSHA204A は、データトークンのリーディングエッジを受信した後、$t_{TIMEOUT}$ 以内にトークンの残りのビットを正しく受信する事を期待します。十分な数のビットが送信されなかった場合、または無効なトークンが送信された(Low パルスが t_{ZLO} を超えた)場合、$t_{TIMEOUT}$ 後にデバイスはスリープ状態に移行します。

コマンドブロックの送信中にも同じタイムアウトが適用されます。正しいコマンドフラグが送信された後、I/O タイムアウト回路は期待する最後のデータビットを受信するまで有効になります。

Note: タイムアウト カウンタは、正しいトークンが受信されるたびにリセットされます。コマンド送信の総時間は $t_{TIMEOUT}$ を超えても構いませんが、ビットとビットの間の時間は $t_{TIMEOUT}$ を超えない事が必要です。

I/O タイムアウト回路は、デバイスがコマンドの実行中(ビジー中)である時に無効になります。

5.3.2 同期手順

システムが送信フラグを送信した時にデバイスがビジーではなかった場合、デバイスは $t_{TURNAROUND}$ 以内に応答する必要があります。t_{EXEC} が過ぎるまでは、デバイスはビジーである可能性があり、システムは最大 t_{EXEC} が過ぎるまでポーリングまたは待機する必要があります。2 回目の Transmit フラグに対してもデバイスが $t_{TURNAROUND}$ 以内に応答しない場合、同期が失われている可能性があります。この場合、システムは以下の手順により通信を再確立できます。

1. $t_{TIMEOUT}$ を待機する。
2. 送信フラグを送信する。
3. デバイスが $t_{TURNAROUND}$ 以内に応答した場合、システムは後続のコマンドを送信できる。
4. Wake トークンを送信する。
5. t_{WHI} が過ぎるまで待機する。
6. Transmit フラグを送信する。
7. デバイスが $t_{TURNAROUND}$ 以内にステータス `0x11` で応答した場合、システムは後続のコマンドを送信できる。

I/O バッファ内の全てのコマンド結果は、システムとデバイスが同期を失った時に失われる可能性があります。

5.4 インターフェイスの共有

以下の手順により、複数の CryptoAuthentication デバイスで同じインターフェイスを共有できます。

1. システムは Wake トークンを発行する事で、全てのデバイスを復帰させます(**「ウォッチドッグ フェイルセーフ」**参照)。
2. システムは `Pause` コマンドを発行する事で、1 つを除く全てのデバイスをアイドルモードにします。1 つのデバイスだけが、システムから送信されるコマンドを受信します。システムは、1 つのアクティブ デバイスへの通信を完了した時に Idle フラグを送信します。既にアイドル中のデバイスはこれを無視し、アクティブであった 1 つのデバイスはアイドルモードに移行します。詳細は**「Pause コマンド」**を参照してください。

手順 1 と 2 を、接続されている各デバイスに対して繰り返します。最後のデバイスとの通信が完了した後は、消費電力を低減するために、システムは全てのデバイスを復帰させた後に全てのデバイスをスリープに移行させる必要があります。

© 2019 Microchip Technology Inc.

どのデバイスがアクティブ状態を維持するかは、Configuration ゾーン内の Selector バイトによって決まります。この Selector 値が Pause コマンドの入力パラメータと一致するデバイスだけがアクティブ状態を維持します。システムが複数デバイスによる共有モードを使う場合、後で容易に設定を変更できるようにするため、Selector バイト向けに以下の 3 通りの更新機能がサポートされます。

1. **無制限の更新**
   いつでも UpdateExtra コマンドを使って Configuration ゾーンの Selector フィールドに値を書き込む事ができます。このモードを有効にするには、Configuration ゾーン内の SelectorMode バイトを 0 に設定します。

2. **ワンタイム フィールド更新**
   Configuration ゾーンをロックする前に SelectorMode バイトを非 0 値に設定し、Selector バイトを 0 値に設定した場合、Configuration ゾーンのロック後に UpdateExtra コマンドを一度だけ使って Selector を非 0 値に設定できます。UpdateExtra コマンドは、LockValue バイトによる影響を受けません。

3. **固定セレクタ値**
   SelectorMode と Selector の両方を非 0 値に設定した場合、Configuration ゾーンのロック後は、Selector バイトを一切変更できなくなります。UpdateExtra コマンドは常にエラーコードを返します。

5.5 トランザクションの例

Wake (Single-Wire)		
Host		Device
Wake	→	
Transmit	→	
	←	Data

Example (Single-Wire)		
Host		Device
Wake	→	
Transmit	→	
	←	Data
Command	→	
Data	→	
Transmit	→	
	←	Data
Idle/Sleep	→	

表 5-3. 例 (単線式)

	Wake Token 0x00								Transmit 0x88								Count 0x04								Status 0x11							
Host									0	0	0	1	0	0	0	1																
Device																	0	0	1	0	0	0	0	0	1	0	0	0	1	0	0	0

	CRC-16 0x33								CRC-16 0x43								Command 0x77								Count							
Host																	1	1	1	0	1	1	1	0								
Device	1	1	0	0	1	1	0	0	1	1	0	0	0	0	1	0																
	Opcode								Param1								Param2								Param2							
Host																																
Device																																
	Data (0 – N)								Transmit 0x88								Count								Data (1 – N)							
Host									0	0	0	1	0	0	0	1																
Device																	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	CRC-16								CRC-16								Idle															
Host																	1	1	0	1	1	1	0	1								
Device	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X																

5.6 単線式インターフェイスの接続

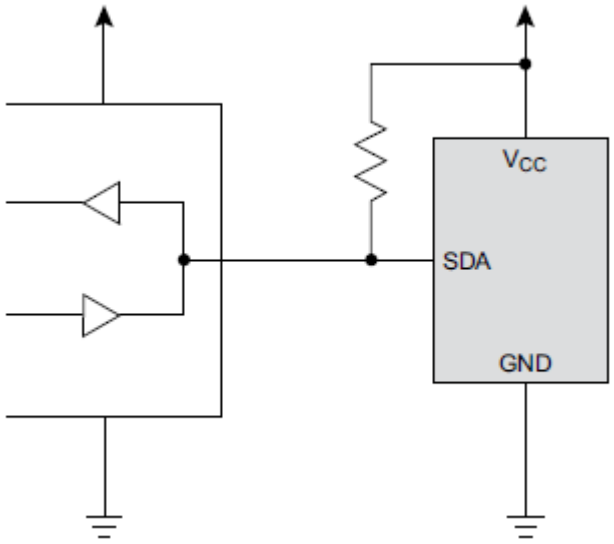
単線式インターフェイスを使うと、1 本の SDA ピンだけで ATSHA204A とホストの間の双方向データ転送ができます。このインターフェイスは SCL ピンを使いません。この方法で接続する場合、電源および電源に戻されるグランド信号のインピーダンスが低ければ、ATSHA204A はバイパス コンデンサを必要としません。しかし、Microchip 社は最高の安定性を得るためにバイパス コンデンサを常に使う事を推奨します。

内部ダイオードが順方向にバイアスされて電源プレーンからシステムに電流が引き込まれる事を防ぐため、SDA ピンのプルアップ抵抗を V_{CC} ピンに接続している同じ電源またはそれより電圧が低いレールに接続する必要があります。

SDA の信号レベルが V_{CC} 電圧とは異なる場合、本書内の仕様表を参照し、スリープモード時にリーク電流が最小限となる信号レベルである事を確認してください。このような状況は、ATSHA204A とバスマスタ デバイスの間の物理的距離が大きい場合、またはバスマスタの電源電圧が ATSHA204A の電源電圧と異なる場合に生じる可能性があります。

© 2019 Microchip Technology Inc.

図 5-1. 単線式インターフェイスの接続(3 線接続)



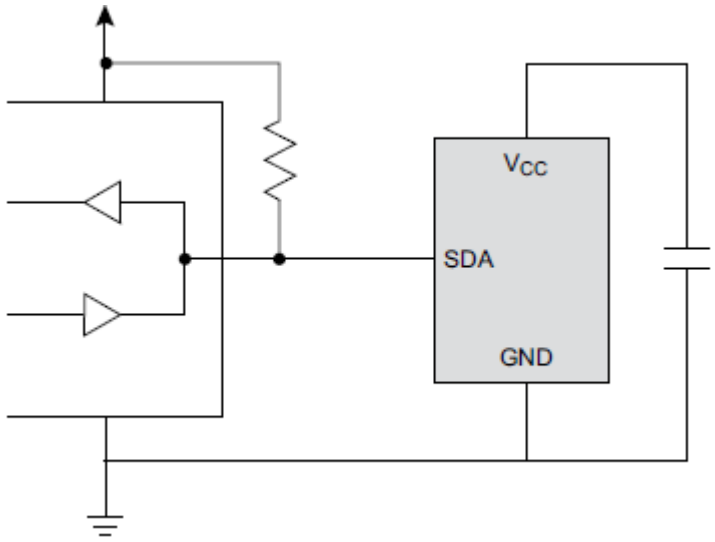
5.6.1 2 線接続

ATSHA204A は SDA ピンと V_{CC} ピンの間に内部ゲートスイッチを備えており、電力を SDA ピンから取り込んでバイパス コンデンサに蓄える事ができます。この場合、V_{CC} ピンをホストの電源に接続する必要はありません。この接続方法では、ATSHA204A とバイパス コンデンサ実装した基板を 2 本の配線(SDA と GND)だけでホストのマイクロプロセッサに接続できます。

システム電圧レベルが 3 V 以上である場合、1 kΩ 以下のプルアップ抵抗と 0.03 µF 以上のコンデンサを使います。デバイスは、V_{CC} を仕様電圧レベル(2 V)以上の適正レベルに保って動作します。接続方法に関するその他の情報は弊社にお問い合わせください。

2 線接続の場合、アクティブ ドライバを使って SDA ピンを High (V_{CC})レベルに駆動する必要があります。ドライバには、全てのコマンドの実行時間全体を通して I_{CC} を供給可能な能力が必要であり、データをデバイスへ送信するためにトーテムポール ドライバを使う必要があります。ATSHA204A からシステムへのデータ転送中は、SDA ラインはプルアップ抵抗によってのみ駆動されます。

図 5-2. 単線式インターフェイスの接続(2 線接続)



© 2019 Microchip Technology Inc.

6. I²C インターフェイス

I²C インターフェイスは、SDA ピンと SCL ピンを使って、各種の I/O 状態を ATSHA204A に対して示します。このインターフェイスは、1 MHz 以下で動作する他の I²C デバイスとプロトコルレベルで互換となるよう設計されています。

ATSHA204A の出力ピンはオープンドレイン ドライバしか備えないため、SDA ピンは外付けプルアップ抵抗を使って High に駆動する必要があります。バスマスタにはオープンドレインまたはトーテムポールが使えます。後者を使う場合、ATSHA204A がバス上で結果を駆動している時にバスマスタはトライステートになる必要があります。SCL ピンは入力であり、常に外部デバイスまたは外付けプルアップ抵抗によって High および Low に駆動される必要があります。

6.1 I/O 条件

ATSHA204A は、以下の**「スリープ中のデバイス」**および**「アクティブ中のデバイス」**に記載した I/O 条件に応答します。

6.1.1 スリープ中のデバイス

スリープ中のデバイスは Wake 条件を除く全ての条件を無視します。

- **Wake**: SDA が t_{WLO} よりも長く LOW に保持されるとデバイスは低消費電力モードを終了し、遅延時間 t_{WHI} 後に I²C コマンドの受信が可能になります。アイドルまたはスリープ中のデバイスは、t_{WLO} が過ぎるまで SCL ピン上の全てのレベルまたは状態遷移を無視します。t_{WHI} 中のある時点で SCL ピンが有効になり、デバイスは**「アクティブ中のデバイス」**に記載した条件に応答します。

Wake 条件が成立するには、SDA ピンがシステム プロセッサによって手動で t_{WLO} の間 Low に駆動されるか、0x00 のデータバイトが十分に遅い(すなわち SDA の Low 期間が t_{WLO} より長くなる)クロックレートで転送される必要があります。デバイスがアクティブである場合、デバイスの通信(デバイスを低消費電力モード(スリープ等)に戻すための I/O シーケンスまで含む)には通常のプロセッサ I²C ハードウェアおよび/またはソフトウェアが使えます。

バス上に複数の ATSHA204A が存在する場合、I²C インターフェイスが 133 kHz 以下の低速で動作すると、特定データパターン(例: 0x00)の送信によってバス上の全ての ATSHA204A が復帰します。しかし、その後に続けてバス上で送信されるデバイスアドレスは必要なデバイスとのみ一致し、不必要なデバイスは非アクティブのままとなるため、バスの競合は発生しません。

I²C モードでは、既に復帰済みのデバイスは Wake シーケンスを無視します。

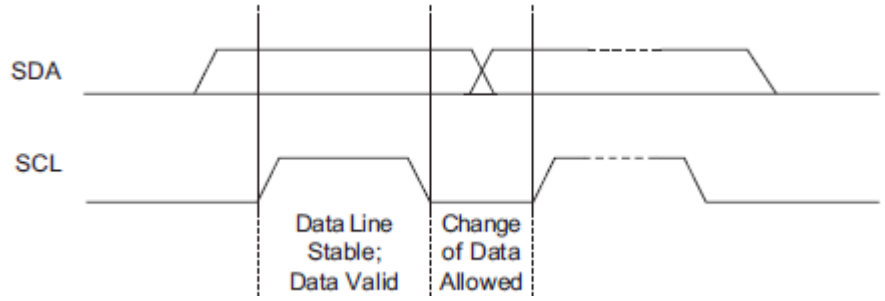
6.1.2 アクティブ中のデバイス

アクティブ中のデバイスは以下の条件に応答します。

- **「0」データ**: SCL が Low→High→Low と遷移する間 SDA が Low を保持した場合、「0」のビットがバス上で転送されます。SDA は SCL が Low の時に遷移できます。
- **「1」データ**: SCL が Low→High→Low と遷移する間 SDA が High を保持した場合、「1」のビットがバス上で転送されます。SDA は SCL が Low の時に遷移できます。

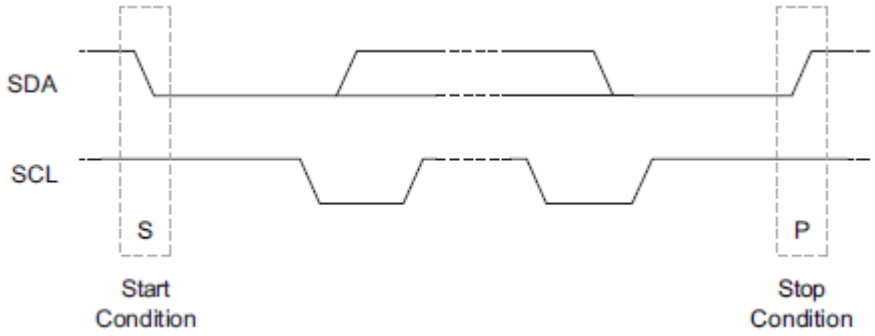
© 2019 Microchip Technology Inc.

図 6-1. I²C インターフェイスにおけるデータビットの転送



- **Start 条件**: SCL が High の時に SDA が High→Low に遷移すると Start 条件が発生します。全てのコマンドの前に Start 条件が必要です。
- **Stop 条件**: SCL が High の時に SDA が Low→High に遷移すると Stop 条件が発生します。デバイスは、Stop 条件を受信した後に現在の I/O トランザクションを終了します。デバイスは入力でコマンドの実行に必要な全てのバイトを受信すると、ビジー状態に移行してコマンドの実行を開始します。デバイスへパケットを送信するたびに Stop 条件を(たとえそれが必要ない場合であっても)送信する事を推奨します。デバイスは、適正な数のバイトを受信した時点でコマンドの実行を開始します。バスでエラーが発生した場合、デバイスはウォッチドッグ タイマによりリセットします。

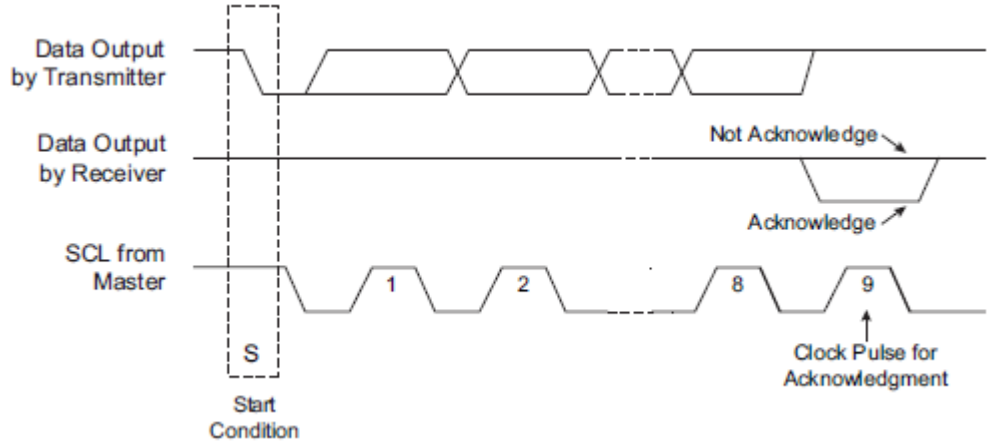
図 6-2. I²C インターフェイスの Start および Stop 条件



- **肯定応答(ACK)**: 各アドレスバイトまたはデータバイトが転送された後の 9 番目のクロックサイクルで、レシーバは SDA ピンを Low にする事によって、そのバイトを正常に受信した事を知らせます。
- **否定応答(NACK)**: 各アドレスバイトまたはデータバイトが転送された後の 9 番目のクロックサイクルで、レシーバは SDA ピンを High のままにする事によって、そのバイトの受信に問題があった事またはそのバイトでブロック転送が完了する事を知らせます。

© 2019 Microchip Technology Inc.

図 6-3. I²C インターフェイスの NACK および ACK 条件



互いに異なる I2C_Address を持つ複数の ATSHA204A は同じ I²C インターフェイスを共有できます。デバイスアドレスの 6 ビットは設定可能であるため、ATSHA204A はシリアル EEPROM を含む標準 I²C デバイスとの間で I²C インターフェイスを共有する事もできます。Bit 3 (TTL イネーブル)は、必要な入力しきい値に応じて設定する必要があります。これは特定のアプリケーションにおいて設定します。

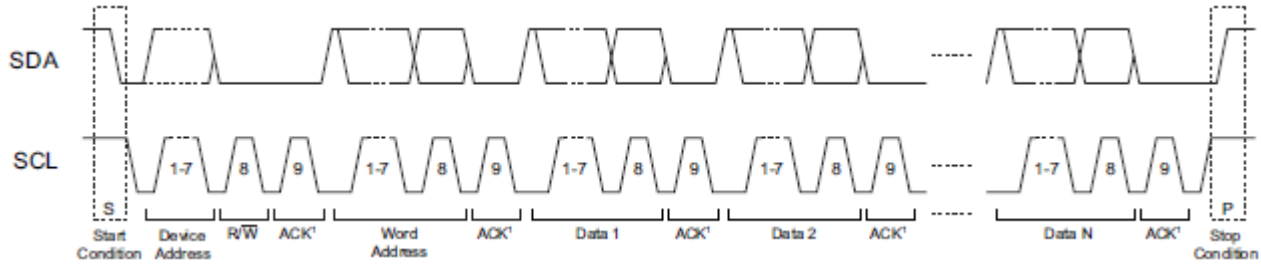
6.2 ATSHA204A への I²C 送信

システムから ATSHA204A へのデータ送信の概要は以下の通りです。

送信の順序:

1. Start 条件
2. デバイスアドレス バイト
3. ワードアドレス バイト
4. データバイト(1～N) (必要に応じて)
5. Stop 条件

図 6-4. ATSHA204A への標準 I²C 送信



Note: ACK 期間中に SDA は ATSHA204A によって Low に駆動されます。

表 6-1 に、I/O トランザクションの各バイトを示します。「I²C 名」列は、AT24C16 のデータシートに記載されているバイト名です。

表 6-1. ATSHA204A への I²C 送信

ATSHA204A	I²C 名	方向	概要
Device Address	Device Address	マスタ→スレーブ	このバイトは、I²C インターフェイス上で特定デバイスを選択します。このバイトの bit 1～7 が Configuration ゾーン内の I2C_Address の bit 1～7 に一致する場合、その ATSHA204A が選択されます。

ATSHA204A	I2C 名	方向	概要
			このバイトの bit 0 は標準 I²C の R/W ビットであり、書き込み動作(デバイスアドレス バイトに続くバイトをマスタからスレーブへ転送する)を示す「0」である事が必要です。
Data	Data1,N	マスタ→スレーブ	入力ブロック

本デバイスはコマンド入力バッファを FIFO として扱うため、入力ブロックは 1 つまたは複数の I²C コマンドブロックに格納してデバイスへ送信できます。デバイスへ最初に送信されるバイトはカウント(この後にデバイスが受信するバイトの数)です。デバイスは、実行が終了するまでこの数を超える後続の受信バイトを無視します。

システムは、最後のコマンドバイトの後に Stop 条件を送信する必要があります。これにより、ATSHA204A はコマンドの処理を開始します。Stop 条件の送信に失敗した場合、同期が失われる可能性があります(同期の回復手順は**「I²C の同期」**参照)。

6.2.1 ワードアドレス値

I²C 書き込みパケットでは、ATSHA204A は 2 番目のバイトをワードアドレスとして解釈します。ワードアドレス値は、表 6-2 の通りにパケットの機能を示します。

表 6-2. ワードアドレス値

名称	値	概要
リセット	0x00	アドレスカウンタをリセットします。次の読み出しまたは書き込みトランザクションは、I/O バッファの先頭位置で始まります。
スリープ (低消費電力)	0x01	ATSHA204A は低消費電力スリープモードに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。デバイスの揮発性ステートは全てリセットされます。
アイドル	0x02	ATSHA204A はアイドルステートに移行し、次の Wake フラグまで後続の I/O トランザクションを全て無視します。TempKey および RNG シードレジスタの内容は保持されます。
コマンド	0x03	後続のバイトを入力コマンドバッファ(前回の書き込み位置の次のアドレス)に書き込みます。これは標準の動作です。
予約済み	0x04 - 0xFF	これらワードアドレス値をデバイスへ送信してはいけません。

6.2.2 コマンド完了のポーリング

1 つの完全なコマンドが送信されると、ATSHA204A はそのコマンドの処理を完了するまでビジー状態になります。システムは、以下の 2 通りの方法でデバイスによるコマンド処理の完了を待機できます。

- **ポーリング**
  システムは t_{EXEC} (typ.)が過ぎるまで待機した後に、読み出しシーケンス(**「ATSHA204A からの I²C 送信」**参照)を送信します。デバイスがデバイスアドレスに対して NACK を返した場合、そのデバイスはまだビジー状態です。システムはしばらく待機してから(あるいは直ちに)次の読み出しシーケンスを送信できます。デバイスがビジー中である間は、NACK が繰り返し返されます。総遅延 t_{EXEC} (max.) の後に、デバイスは処理を完了して結果を返す事ができます。
- **遅延の待機**
  システムは t_{EXEC} (max)が過ぎるまで待機します。その間にデバイスは実行を完了します。その後、システムは標準読み出しシーケンスを使ってデバイスから結果を読み出す事ができます。

© 2019 Microchip Technology Inc.

6.3 ATSHA204A からの I²C 送信

ATSHA204A がアクティブであり、かつビジー状態ではない場合、バスマスタは I²C 読み出しを使ってデバイスから現在のバッファの内容を読み出せます。有効なコマンド結果が得られた場合、デバイスから返されるブロックのサイズは実行されたコマンドによって決まります(**「セキュリティ コマンド」**参照)。有効な結果が得られなかった場合、ブロックのサイズ(最初に返されるバイトの値)は常に 4 です(1x カウントバイト、1x ステータス/エラー バイト、2x CRC バイトの計 4 バイト)。バスのタイミングは**図 7-3. I²C 同期データタイミング**を参照してください。

表 6-3. ATSHA204A からの I²C 送信

名称	I²C 名	方向	概要
Device Address	Device Address	マスタ→スレーブ	このバイトは I²C インターフェイス上の特定デバイスを選択します。このバイトの bit 1～7 が Configuration ゾーン内の I2C_Address バイトの bit 1～7 に一致すると、その ATSHA204A が選択されます。 このバイトの bit 0 は標準 I²C の R/W ビットであり、読み出し動作(デバイス アドレス バイトに続くバイトをスレーブからマスタへ転送する)を示す「1」である事が必要です。
Data	Data1,N	スレーブ→マスタ	出力ブロックはカウントバイト + ステータス/エラーバイトまたは出力パケット + 2 バイトの CRC で構成されます。

マスタはステータス、エラー、コマンド出力を繰り返し読み出せます。Read コマンドが I²C インターフェイスを介して ATSHA204A へ送信されるたびに、デバイスは出力バッファ内の次のバイトを送信します。本デバイスによるアドレスカウンタの扱い方は、この後で説明します。
ATSHA204A がビジー、アイドル、スリープ状態のいずれかである場合、デバイスは読み出しシーケンス中のデバイスアドレスに対して NACK を返します。デバイスへコマンドの一部だけが送信された場合、デバイスはデバイスアドレスに対して NACK を返しますが、データ期間中にバスをフロート状態にします。

6.4 アドレスカウンタ

I²C インターフェイス介する ATSHA204A の I/O バッファに対する読み書きは、デバイスが FIFO であるかのように扱われます。I²C バイトまたはブロック読み/書きプロトコルが使えます。各ブロックシーケンスで転送されるバイトの数は、デバイスの動作に影響を与えません。

デバイスへ送信された最初のバイトは常にカウントバイトとして扱われます。この数を超えるバイトの送信が試みられた場合、または I/O バッファのサイズ(84 バイト)を超える書き込みが試みられた場合、ATSHA204A はそれらのバイトに対して NACK を返します。

ホストが 1 つのコマンドバイトを入力バッファに書き込んだ後は、デバイスがそのコマンドの実行を完了するまで、ホストからのデバイス Read コマンドは禁止されます。

最後のコマンドバイトが送信される前にデバイスからの読み出しが試みられた場合、デバイスアドレスに対して ACK は返されますが、バス上のビットは全て「1」(0xFF)になります。コマンドを実行中のデバイスに対してマスタがバイト読み出しを送信した場合、デバイスはデバイスアドレスに対して NACK を返します。

デバイスからのデータの読み出しは、以下の 3 通りの条件で可能です。

- 電源投入時に、4 バイトブロック内で 1 バイト(0x11)が読み出せます(**「コマンド オペコードの概要と実行時間」**参照)。
- デバイスが完全なブロックを受信したものの、コマンドの構文解析または実行でエラーが発生した場合、4 バイトブロック内で 1 バイトのエラーコードが読み出せます。
- コマンドの実行が完了した場合、1～32 バイトのコマンド結果が 4～35 バイトのブロック内で読み出せます。

© 2019 Microchip Technology Inc.

出力バッファの終端を超えて読み出しが試みられた場合、0xFF がシステムへ返されます。アドレスカウンタはバッファの先頭へロールオーバーしません。

システムから出力バッファを再度読み出す必要が生じる場合があります(例: CRC チェックでエラーが生じた場合)。この場合、2 バイト(デバイスアドレス + 0x00 のワードアドレス)のシーケンス (表 6-2 内の「リセット」参照) の後に Stop 条件を送信する必要があります。これによりアドレスカウンタは 0 にリセットされ、デバイスへの再書き込みまたはデバイスからの再読み出しが可能になります。このアドレスリセット シーケンスの実行前に I/O バッファ内に読み出し可能なデータが存在していた場合、アドレスリセット シーケンス後の読み出し動作は禁止されません。

コマンドの実行結果を読み出すための 1 回または複数回の読み出し動作の後は、最初の書き込み動作によってアドレスカウンタは I/O バッファの先頭へリセットされます。

6.5 I²C の同期

システムリセットや I/O ノイズ等によってシステムと ATSHA204A 上の I/O ポートの間の同期が失われる可能性があります。このような場合、ATSHA204A は期待通りに応答できなくなります(スリープ状態になるか、システムがデータを送信しようとしているタイミングでデータを送信してしまう等)。I/O バッファ内の全てのコマンド結果は、システムとデバイスが同期を喪失した時に失われる可能性があります。再同期するには、以下の手順が必要です。

1. I/O チャンネルを確実にリセットするため、システムは以下の通りに標準 I²C ソフトウェア リセット シーケンスを送信する必要があります。
   - Start 条件
   - 9 SCL サイクルの間 SDA を High に保持
   - 再度 Start 条件
   - Stop 条件

   以上の手順によって同期が正しく確立されると、読み出しシーケンスの送信が可能になり、ATSHA204A はデバイスアドレスに対して ACK を返します。データ期間中に、デバイスはデータを返すかバスをフロート状態(システムによって値が 0xFF のデータとして解釈される)にします。

   デバイスがデバイスアドレスに対して ACK を返した場合、システムは内部アドレスカウンタをリセットする必要があります。これにより、ATSHA204A はそれまでに送信された不完全な入力コマンドを無視します。アドレスカウンタは、ワードアドレス 0x00 (リセット)への書き込みシーケンスを送信した後に Stop 条件を生成する事によりリセットできます。
2. デバイスがデバイスアドレスに対して ACK で応答しない場合、デバイスはスリープ中である可能性があります。この場合、システムは完全な Wake トークンを送信し、立ち上がりエッジ後に t_{WHI} が過ぎるまで待機する必要があります。その後、システムは読み出しシーケンスを再度送信できます。同期が確立されていれば、デバイスはデバイスアドレスに対して ACK を返します。
3. それでもデバイスがデバイスアドレスに対して ACK で応答しない場合、デバイスはビジー状態(コマンドの実行中)である可能性があります。システムは最長の t_{EXEC} (max)が過ぎるまで待機してから読み出しシーケンスを送信する事で、デバイスから ACK が返されます。

© 2019 Microchip Technology Inc.

6.6 トランザクションの例

表 6-4. Wake (I^2C)

Wake (I^2C)		
Host		Device
Start	→	
Wake	→	
Stop	→	
Start	→	
Slave Address / R	→	
	←	Data
Stop	→	

表 6-5. トランザクションの例

Example (I^2C)		
Host	→	Device
Start	→	
Wake	→	
Stop	→	
Start	→	
Slave Address / R	→	
	←	Data
Stop	→	
Start	→	
Slave Address / W	→	
Command	→	
Data	→	
Stop	→	
Start	→	
Slave Address / R	→	
	←	Data
Stop	→	
Start	→	
Slave Address / W	→	
Idle / Sleep	→	
Stop	→	

© 2019 Microchip Technology Inc.

7. 電気的特性

7.1 絶対最大定格

動作温度	-40～+85 ℃
保管温度	-65～150 ℃
最大動作電圧	6.0 V
DC 出力電流	5.0 mA
全ピンの電圧	0.5 V～ (V_{CC} + 0.5 V)
ESD 耐圧:	
HBM:	> 4 kV
CDM:	> 1kV

Note: ここに記載した「絶対最大定格」を超える条件は、デバイスに恒久的な損傷を生じさせる可能性があります。これはストレス定格です。本書の動作表に示す条件外でのデバイスの運用は想定していません。絶対最大定格条件を超えて長期間曝露させるとデバイスの信頼性に影響が及ぶ可能性があります。

7.2 信頼性

ATSHA204A は Microchip 社の高信頼性 CMOS EEPROM 製造技術を採用しています。

表 7-1. EEPROM の信頼性

パラメータ	Min.	Typ.	Max.	単位
書き換え耐性(各バイト @25 ℃)	100,000			書き込みサイクル数
データ保持寿命(@55 ℃)	10			年
データ保持寿命(@35 ℃)	30	50		年
読み出し耐性	制限なし			読み出しサイクル数

7.3 AC パラメータ (全 I/O インターフェイス)

図 7-1. AC タイミング — 全 I/O インターフェイス

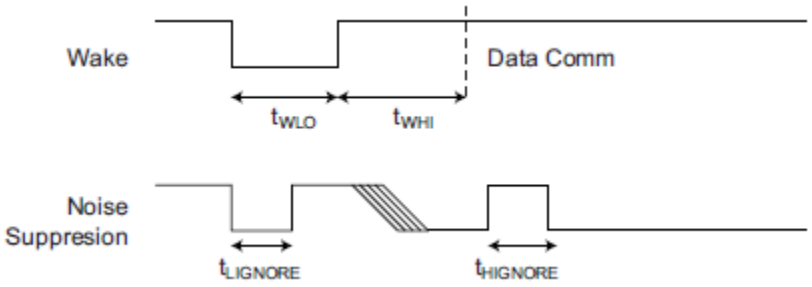


表 7-2. AC パラメータ — 全 I/O インターフェイス

パラメータ	記号	方向	Min.	Typ	Max.	単位	注釈
Wake Low 時間	t_{WLO}	To Crypto Authentication	60		—	µs	延長されたスリープ期間中に SDA は High または Low レベルで安定できます。
電源投入遅延	t_{PU}	To Crypto Authentication	100[1]			µs	V_{CC} > V_{CC} min から t_{WLO} の計測を開始するまでの時間
Wake High からデータ通信開始までの遅延時間	t_{WHI}	To Crypto Authentication	2.5			ms	この期間中は SDA が安定して High である事が必要です。
アクティブ時 High レベルグリッチフィルタ	$t_{HIGNORE\_A}$	To Crypto Authentication	45			ns	アクティブ時に、デバイスはそのステートに関係なくこの時間より短いパルスを無視します。
アクティブ時 Low レベルグリッチフィルタ	$t_{LIGNORE\_A}$	To Crypto Authentication	45			ns	アクティブ時に、デバイスはそのステートに関係なくこの時間より短いパルスを無視します。
スリープ時 High レベルグリッチフィルタ	$t_{HIGNORE\_S}$	To Crypto Authentication	15			µs	スリープ時に、デバイスはこの時間より短いパルスを無視します。
スリープ時 Low レベルグリッチフィルタ	$t_{LIGNORE\_S}$	To Crypto Authentication	15			µs	スリープ時に、デバイスはこの時間より短いパルスを無視します。
ウォッチドッグリセット	$t_{WATCHDOG}$	To Crypto Authentication	0.7[1]	1.3	1.7	s	復帰してからデバイスがスリープモードへ移行させられるまでの最大時間(**「ウォッチドッグ フェイルセーフ」**参照)

Note:

1. これらのパラメータは特性データであり、製造時の検査は実施していません。

© 2019 Microchip Technology Inc.

7.3.1 AC パラメータ — 単線式インターフェイス

図 7-2. AC タイミング — 単線式インターフェイス

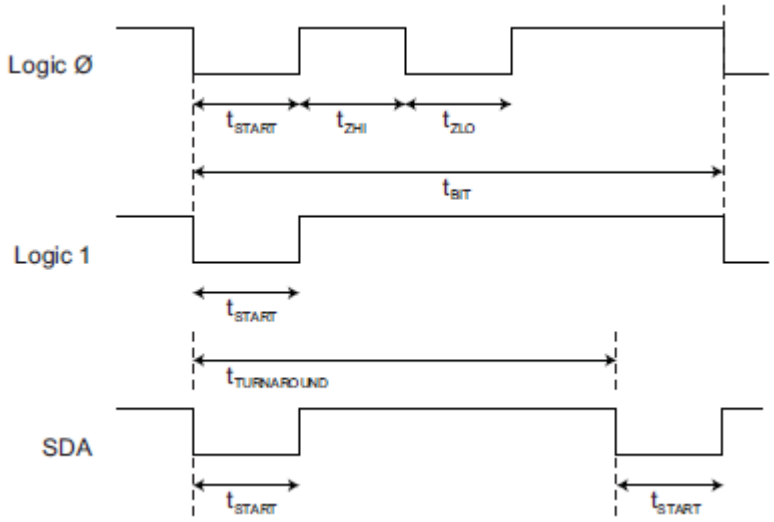


表 7-3. AC パラメータ — 単線式インターフェイス

特に明記しない限り、T_A = -40～+85 ℃、V_{CC} = +2.0～+5.5 V、C_L =100 pF の条件に適用

パラメータ	記号	方向	Min.	Typ.	Max.	単位	注釈
Start パルス期間(1)	tSTART	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6.00	8.60	µs	
0 送信 High パルス(1)	tZHI	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6.00	8.60	µs	
0 送信 Low パルス(1)	tZLO	To Crypto Authentication	4.10	4.34	4.56	µs	
		From Crypto Authentication	4.60	6.00	8.60	µs	
ビット時間(1)	tBIT	To Crypto Authentication	37	39	—	µs	ビット時間が $t_{TIMEOUT}$ を超えると、ATSHA204A はスリープ状態へ移行できます。 詳細は**「I/O タイムアウト」**を参照してください。
		From Crypto Authentication	41	54	78	µs	
ターンアラウンド遅延	tTURNAROUND	From Crypto Authentication	64	80	131	µs	送信フラグの最終ビット(t_{BIT})の開始後にこの時間が過ぎると、ATSHA204A は最初の Low への遷移を開始します。

パラメータ	記号	方向	Min.	Typ.	Max.	単位	注釈
		To Crypto Authentication	93			µs	ATSHA204A がブロックの最終ビットを送信した後、システムはフラグの最初のビットを送信する前に、この時間が過ぎるまで待機する必要があります。
I/O タイムアウト	$t_{TIMEOUT}$	To Crypto Authentication	45	65	85	ms	バスの非アクティブ状態がこの時間よりも長く続くと、ATSHA204A はスリープ状態へ移行できます。詳細は**「I/O タイムアウト」**を参照してください。

Note:

1. t_{START}、t_{ZLO}、t_{ZHI}、t_{BIT} は送信と受信の両方で標準 UART (230.4 kBaud で動作)と互換性を持つよう設定されています。UART は 7x データビット/パリティなし/1x ストップビットに設定する必要があります。

7.3.2 AC パラメータ — I²C インターフェイス

図 7-3. I²C 同期データ タイミング

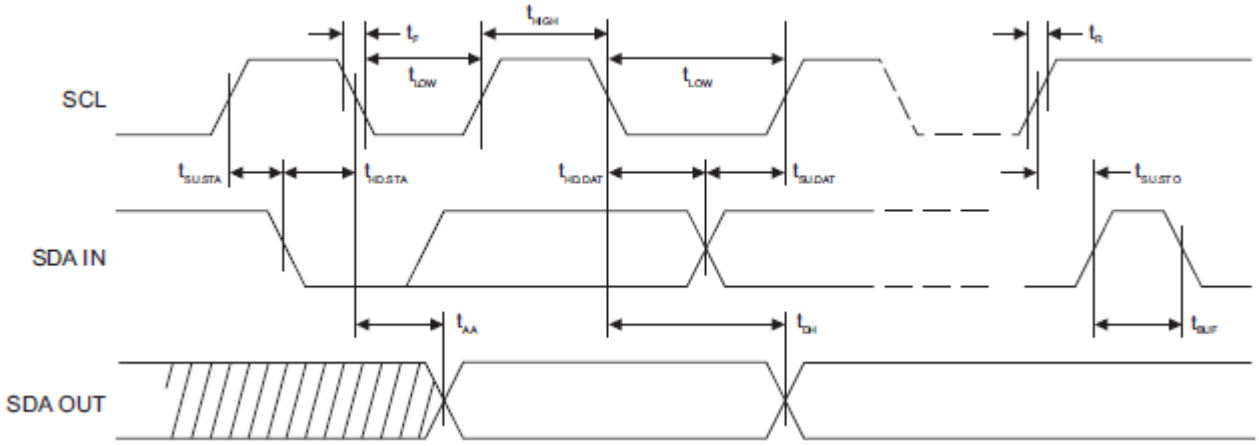


表 7-4. I²C インターフェイスの AC 特性

特に明記しない限り、T_A - -40～+ 85 ℃、V_{CC} = +2.0～+5.5 V、C_L = 1 TTL ゲート+100 pF の推奨動作レンジに適用

記号	パラメータ	Min	Max.	単位
f_{SCK}	SCK クロック周波数		1000	kHz
	SCK クロック デューティサイクル	30	70	%
t_{HIGH}	SCK High 時間	400		ns
t_{LOW}	SCK Low 時間	400		ns
$t_{SU.STA}$	Start セットアップ時間	250		ns
$t_{HD.STA}$	Start ホールド時間	250		ns
$t_{SU.STO}$	Stop セットアップ時間	250		ns

© 2019 Microchip Technology Inc.

記号	パラメータ	Min	Max.	単位
$t_{SU.DAT}$	データ入力セットアップ時間	100		ns
$t_{HD.DAT}$	データ入力ホールド時間	0		ns
t_R	入力立ち上がり時間(1)		300	ns
t_F	入力立ち下がり時間(1)		100	ns
t_{AA}	クロック Low からデータ出力確定までの時間	50	550	ns
t_{DH}	データ出力ホールド時間	50		ns
t_{BUF}	次の伝送が開始可能になるまでに必要なバスフリー時間(1)	500		ns

Note:

1. これらのパラメータは特性データであり、製造時の検査は実施していません。
   AC 計測条件:
   - RL (SDA と V_{CC} の間を接続): 1.2 kΩ (V_{CC} = +2.0～+5.0 V)
   - 入力パルス電圧: 0.3～0.7 V_{CC}
   - 入力立ち上がり/立ち下がり時間: ≤ 50 ns
   - 入出力タイミング参照電圧: 0.5V_{CC}

7.4 DC パラメータ(全 I/O インターフェイス)

表 7-5. 全 I/O インターフェイスの DC パラメータ

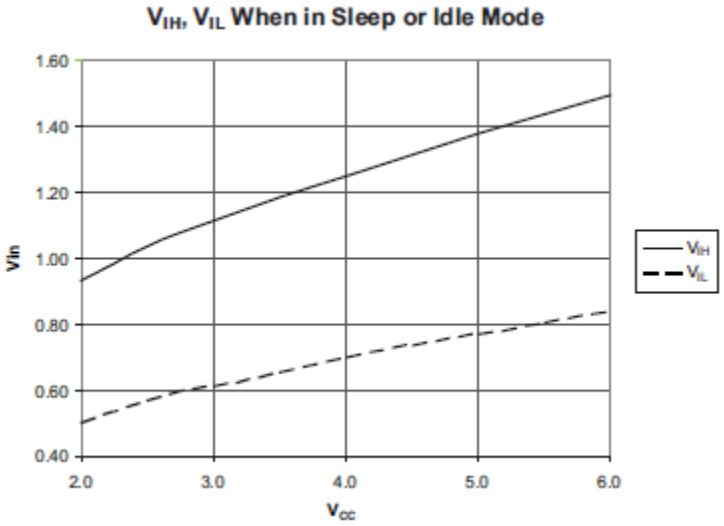
パラメータ	記号	Min.	Typ	Max.	単位	注釈
動作時周囲温度	T_A	-40		85	℃	
電源電圧	V_{CC}	2.0		5.5	V	
アクティブ時消費電流	I_{CC}		500		µA	0 ℃ → +70 ℃、V_{CC} = 3.3 V
			—	2	mA	-40 ℃ → +85 ℃、V_{CC} = 5.5 V
アイドル時消費電流	I_{IDLE}		200		µA	アイドルモード時(V_{CC} = 3.3 V、V_{SDA} および V_{SCL} < 0.3 V または > V_{CC} - 0.3 V)
スリープ電流	I_{SLEEP}		30	150	nA	スリープモード時(V_{CC} = 3.6 V、V_{SDA} および V_{SCL} < 0.3 V または > V_{CC} - 0.3 V、T_A ≤ 55 ℃)
				2	µA	スリープモード時(全動作条件において)
出力 Low 電圧	V_{OL}			0.4	V	アクティブモード時(V_{CC} = 2.5～5.5 V)
出力 Low 電流	I_{OL}			4	mA	アクティブモード時(V_{CC} = 2.5～5.5 V) V_{OL} = 0.4 V

© 2019 Microchip Technology Inc.

7.4.1 V_{IH} と V_{IL} の仕様

スリープまたはアイドルモード中の入力電圧しきい値(V_{IH} と V_{IL})は、図 7-4 に示す通り、V_{CC} レベルに応じて変化します。

図 7-4. スリープおよびアイドルモード中の V_{IH} と V_{IL}



デバイスがアクティブの時(スリープモードでもアイドルモードでもない場合)、入力電圧しきい値は、TTLenable (EEPROM の Configuration ゾーンに保存されている I2C_Address バイトの bit 3)の状態によって決まります。ATSHA204A の V_{CC} ピンと入力プルアップ抵抗に共通の電圧を使う場合、TTLenable ビットを「1」に設定する必要があります。これにより、入力しきい値は電源電圧に応じて**図 7-5** の通りに変化します。

ATSHA204A の V_{CC} ピンに供給される電圧がシステム電圧(入力プルアップ抵抗の接続先)とは異なる場合、TTLenable は「0」に設定できます。これにより、固定された入力しきい値が有効になります。入力信号は**表 7-6** に示すしきい値レベルを満足する必要があります。

図 7-5. TTLenable = 「1」の場合の全 I/O インターフェイスの V_{IH} と V_{IL}

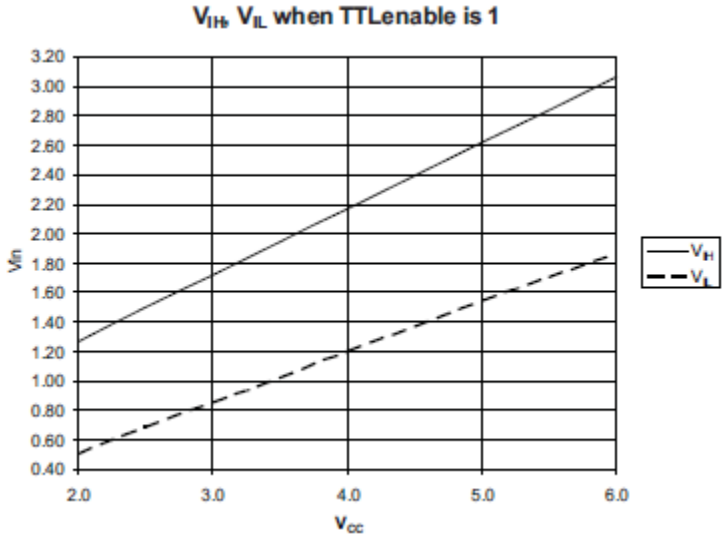


表 7-6. TTLenable = 「0」の場合の全 I/O インターフェイスの V_{IH} と V_{IL}

パラメータ	記号	Min	Typ	Max.	単位	注釈
入力 Low 電圧	V_{IL}	GND - 0.5		0.5	V	デバイスがアクティブかつコンフィグレーション メモリ内の TTLenable ビットが「0」の場合 (これ以外の場合は上記参照)
入力 High 電圧	V_{IH}	1.5		V_{CC} + 0.5	V	デバイスがアクティブかつコンフィグレーション メモリ内の TTLenable ビットが「0」の場合 (これ以外の場合は上記参照)

© 2019 Microchip Technology Inc.

8. セキュリティ コマンド

8.1 I/O ブロック

使用する I/O プロトコル(単線式か I^2C か)に関係なく、1 つのブロック内でコマンドが本デバイスに向けて送信され、応答が本デバイスから返されます。ブロックは以下の通りに構成されます。

表 8-1. ブロック

バイト	名称	意味
0	Count	パケットサイズ (Count、Data、Checksum を含むサイズ)
1〜N-2	Data	デバイスへの入力の場合: コマンドとパラメータ デバイスからの出力の場合: 入力されたコマンドに対するデバイスからの応答
N-1〜N	Checksum	CRC-16 (CRC 多項式は 0x8005)

ATSHA204A は、入力ブロック内の Count 値がコマンド パラメータ内で指定されたサイズに一致する事を要求します。Count 値がパケット内のコマンド オペコードまたはパラメータに一致しない場合、ATSHA204A はコマンドに応じて異なる方法で応答します。応答にエラーの通知が含まれる場合もあれば、一部の入力バイトが黙って無視される場合もあります。

8.1.1 ステータス/エラーコード

本デバイスは専用のステータス レジスタを備えておらず、ステータス、エラー、コマンド結果は全て出力 FIFO に格納されます。デバイスからの全ての出力は、完全なブロックとしてシステムへ返されます。

デバイスが入力コマンドブロックの最初のバイトを受信した後は、システムから残りの全てのバイトがデバイスへ送信されるまで、システムはデバイスから何も読み出せません。

デバイスが復帰してコマンドを実行した後は、デバイスの出力レジスタにエラー、ステータス、結果バイトのいずれかが格納され、システムからその内容を読み出す事ができます。ブロックの長さが 4 バイトである場合に返されるコードの詳細を表 8-2 に示します。一部のコマンドでは、実行に成功した場合に 4 バイトより長いコードが返されます。デバイスから返されるパケットの説明は、8.5「コマンド シーケンス」に記載しています。

CRC エラーは常に他のどのエラーよりも前に返されます。それらは、何らかの I/O エラーが発生した事およびコマンドをデバイスへ再送信可能である事を示します。コマンドの構文エラーと実行エラーには優先順位が決められていません。あるコマンドが両方のエラーを含む場合、実行エラーが先に発生する場合もあれば、構文エラーが先に発生する場合もあります。

表 8-2. 4 バイトブロック内のステータ/エラーコード

状態	エラー/ステータス	概要
Successful Command Execution	0x00	コマンドは正常に実行された。
Checkmac Miscompare	0x01	CheckMac コマンドは正しくデバイスへ送信されたが、入力クライアントからの応答が期待した値に一致しなかった。
Parse Error	0x03	コマンドは正しく受信されたが、ATSHA204A の状態(揮発性および/または EEPROM コンフィグレーション)に関係なく長さ、コマンド オペコード、パラメータのいずれかが無効であった。

© 2019 Microchip Technology Inc.

状態	エラー/ステータス	概要
		コマンドが再試行される前に、コマンドビットの値を変更する必要があります。
Execution Error	0x0F	コマンドは正しく受信されたが、デバイスの現在の状態では実行できなかった。 コマンドが再試行される前に、デバイスの状態またはコマンドビットの値を変更する必要があります。
After Wake, Prior to First Command	0x11	ATSHA204A は正しい Wake トークンを受信した。
CRC or other Communications Error	0xFF	コマンドは ATSHA204A によって正しく受信されなかったため、システム内の I/O ドライバによってコマンドを再送信する必要がある。 コマンドの構文解析または実行は試みられなかった。

8.2 スリープ シーケンス

システムは、ATSHA204A の使用を終了した時点でスリープ シーケンスを発行してデバイスを低消費電力モードに移行させる必要があります。I²C インターフェイスを使うこのシーケンスは、先頭から順番にデバイスアドレス、スリープフラグ、Stop 条件で構成されます。低消費電力状態に移行すると、デバイスの内部コマンドエンジンと入出力バッファは完全にリセットされます。このシーケンスは、デバイスがアクティブかつ非ビジーの時にいつでもデバイスへ送信できます。

8.3 アイドル シーケンス

コマンドの総シーケンス時間が $t_{WATCHDOG}$ を超えた場合、デバイスは自動的にスリープに移行し、揮発性レジスタ内の情報は全て失われます。これを防ぐには、ウォッチドッグ期間が終了する前にデバイスをアイドル状態に移行させる必要があります。デバイスは、Wake トークンを受信した時にウォッチドック タイマを再始動し、実行を継続できます。

I²C インターフェイスを使うこのシーケンスは、先頭から順番にデバイスアドレス、値 0x02 (ワードアドレス)、Stop 条件で構成されます。このシーケンスは、デバイスがアクティブかつ非ビジーの時にいつでもデバイスへ送信できます。

CheckMac コマンドの複製モードの結果として TempKey が生成された場合、デバイスがアイドル状態に移行した時に TempKey は保持されません。

8.4 ウォッチドッグ フェイルセーフ

ATSHA204A が Wake トークンを受信すると、デバイス内部でウォッチドッグ カウンタが始動します。$t_{WATCHDOG}$ が過ぎると、I/O 伝送またはコマンド実行が進行中かどうかに関係なく、デバイスはスリープモードに移行します。カウンタをリセットするには、デバイスをスリープまたはアイドルモードに移行させた後に復帰させる以外に方法はありません。

ウォッチドッグ タイマは、問題(I/O 同期の問題等)がシステム側またはデバイス内部のどちらで発生したかに関係なく、デバイスを自動的に超低消費電力スリープモードに移行させるフェイルセーフ機構として実装されています。

デバイスはスリープ状態への移行時に SRAM および内部ステータス レジスタ内の値をリセットします。しかし、適切な I/O シーケンスによってデバイスをアイドルモードへ明示的に移行させた場合、2 つの SRAM レジスタの内容(例: TempKey、RNG シート)は保持されます。

© 2019 Microchip Technology Inc.

通常、SRAM レジスタに保存されている状態を必要とする全てのコマンド シーケンスは、$t_{WATCHDOG}$ 以内に完了する必要があります。システム ソフトウェアは、コマンドとコマンドの間でこのアイドルモードを使う事により、$t_{WATCHDOG}$ 以内に完了しない長いコマンド シーケンスを実装する事ができます。

8.5 コマンド シーケンス

8.5.1 コマンドパケット

コマンドパケットは表 8-3 の通りに構成されます。

表 8-3. コマンドパケット

バイト	名称	意味
0	Command	コマンドフラグ(I^2C モードは**「ワードアドレス値」**参照、単線式インターフェイス モードは**「I/O フラグ」**参照)。Count または CRC フィールドには含まれない。
1	Count	パケットサイズ: Count、Opcode、Param1、Param2、Data、Checksum を含むサイズ (Command フラグは含まず)
2	Opcode	呼び出す ATSHA204A 動作
3	Param1	第 1 パラメータ(常に 1 バイト)
4 – 5	Param2	第 2 パラメータ(常に 2 バイト)
	Data	任意のデータ(呼び出されるコマンドに基づく)
N-1～N	Checksum	CRC-16(CRC 多項式は 0x8005) Count、Opcode、Param1、Param2、Data を含む(Command フラグは含まず)

ATSHA204A はブロック内の全てのバイトを受信した後にビジー状態に移行し、コマンドの実行を開始します。デバイスがビジー中の場合、ステータスも結果もデバイスから読み出す事はできません。ビジー中のデバイスの I/O インターフェイスは(I^2C か単線式かに関係なく) 全ての SDA 遷移を無視します。コマンド実行遅延は**「Data ゾーン内の読み出し動作」**に記載しています。

単線式モードの場合、十分な数のバイトがデバイスへ送信されると、$t_{TIMEOUT}$ 後にデバイスは自動的に低消費電力スリープ状態に移行します。I^2C モードの場合、ウォッチドッグ タイマ期間($t_{WATCHDOG}$)が終了するか Start/Stop 条件を受信するまで、デバイスは残りのバイトを待機します。

表 8-8～表 8-41 内の各コマンドの説明では、「サイズ」列は各パラメータのバイト数を示します。コマンドの入力ブロックサイズが正しくない場合、デバイスはコマンドに応じて異なる方法で応答します。デバイスがエラー表示を返さない場合もあります(**「ステータス/エラーコード」**参照)。

8.5.2 コマンド オペコードの概要と実行時間

パラメータの構文解析中および正しく受信したコマンドの実行中にデバイスはビジー状態になり、ピンの状態遷移に対して応答できなくなります。ビジー状態の持続時間はコマンドとそのパラメータ値、デバイスの状態、環境条件等に応じて異なります(表 8-4 参照)。

© 2019 Microchip Technology Inc.

ほとんどの場合(全ての場合ではない)、不適切なコマンドに対しては、標準的な実行時間が過ぎる前に応答が返されます。

表 8-4. コマンド オペコードの概要と実行時間

コマンド	オペコード	概要	Typ. 実行時間 (1) ms	Max. 実行時間 (2) ms
DeriveKey	0x1C	ターゲットまたはペアレント鍵からターゲット鍵値を生成します。	14	62
DevRev	0x30	デバイスのリビジョン情報を返します。	0.4	2
GenDig	0x15	乱数または入力シードと鍵からデータ保護ダイジェストを生成します。	11	43
HMAC	0x11	HMAC/SHA-256 を使って鍵とその他の内部データからレスポンスを計算します。	27	69
CheckMac	0x28	他の Microchip 社製 CryptoAuthentication デバイスで計算された MAC を検証します。	12	38
ロック	0x17	デバイスの 1 つのゾーンに対する後続の変更を禁止します。	5	24
MAC	0x08	SHA-256 を使って鍵とその他の内部データからレスポンスを計算します。	12	35
Nonce	0x16	32 バイトの乱数と内部保存されるノンスを生成します。	22	60
Pause	0x01	バスを共有するデバイスの中から 1 つのデバイスを選択してアイドル状態に移行させます。	0.4	2
Random	0x1B	乱数を生成します。	11	50
Read	0x02	デバイスから 4 バイトを読み出します(平文または暗号化)。	0.4	4
SHA	0x47	システム向けに SHA256 ダイジェストを計算します。	11	22
UpdateExtra	0x20	Configuration ゾーンがロックされた後に、Configuration ゾーン内のバイト 84 または 85 を更新します。	8	12
Write	0x12	デバイスに 4 また 32 バイトを書き込みます(平文または暗号化)	4	42

Note:

1. 表に記載した実行時間(typ.)は、エラー条件なし/最速モード設定/オプション内部動作(鍵の使用制限等)なし/好ましい環境条件を想定したコマンドの代表的実行時間です。最善の性能を得るには、この時間が過ぎてからポーリングを開始して実際のコマンド完了を検出します。
2. 最大実行時間は、より幅広い統計的および環境条件の下で全てのモードと内部動作を考慮に入れた、正常なコマンド実行の最長時間を表します。極端な状況では、実行時間がこれらの値を超える可能性があります。

8.5.3 ゾーンの指定

Read コマンドと Write コマンドの Param1 の値は、コマンドのアクセス先ゾーンを指定します。各ゾーンのロック/アンロックの制御については**「Configuration ゾーンのロック」**を参照してください。表 8-5 に記載した以外のゾーン値(Param1)は全て予約済みであり、使用禁止です。

© 2019 Microchip Technology Inc.

表 8-5. ゾーンの指定(Param1)

ゾーン名	Param1 の値	サイズ	読み出し	Write
Config	0	704 ビット 88 バイト 3 スロット	常に可能	アンロック時は一部可能 ロック時は常に不可 暗号化せず
OTP	1	512 ビット 64 バイト 2 スロット	アンロック時は常に不可 ロック時は常に可能(レガシーモード中は除く) **「OTP(One Time Programmable)ゾーン」**参照	LockConfig がアンロック時は不可 LockConfig がロックかつ LockValue がアンロックの場合は全て書き込み可能 LockValue がロック時は OTPmode により制御 **「OTP(One Time Programmable)ゾーン」**参照
Data	2	4096 ビット 512 バイト 16 スロット	アンロック時は常に不可、 ロック時は IsSecret と EncryptRead により制御	LockConfig がアンロック時は不可 LockConfig がロックかつ LockValue がアンロックの場合は全て書き込み可能 LockValue がロック時は WriteConfig により制御 **「デバイスのロック」**参照

8.5.4 アドレスの指定

Param2 は、アクセス先のメモリを指定する 1 つのアドレスを含みます。全ての読み書きはワード(4 バイト)単位で実行されます。有効な ATSHA204A アドレスの最上位バイトは常に 0 です。未使用のアドレスビットは常に 0 に設定する必要があります。アドレスの最下位ビットは、ブロック/スロット内でアクセスされる最初のワードに対するオフセットを表し、上位ビットはスロット番号(表 8-6 参照)を表します。

表 8-6. アドレスの指定(Param2)

ゾーン	バイト 0 (バス上の最初のバイト)								バイト 1							
	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
Data	0	ブロック				オフセット			0	0	0	0	0	0	0	0
Config	0	0	0	ブロック		オフセット			0	0	0	0	0	0	0	0
OTP	0	0	0	0	ブロック	オフセット			0	0	0	0	0	0	0	0

表 8-7 に示す通り、各ゾーンには各種のアクセス制限があります。

表 8-7. 有効なブロック/スロット値

ゾーン	有効なブロック/スロット値(最小値-最大値)	注釈
Data	0 – 15	全てのスロット内の全てのオフセットが読み出しおよび書き込みの両方で利用できます。 4 バイトアクセスは、SlotConfig.IsSecret が「0」の場合にのみ特定スロットで許容されます。
Config	0 – 2	16 (ブロック 2、オフセット 6)を超える領域は常に読み出せません。

© 2019 Microchip Technology Inc.

ゾーン	有効なブロック/スロット値 (最小値-最大値)	注釈
		10 (ブロック 2、オフセット 0)を超える領域は、ワード(4 バイト)モードで読み書きする必要があります。 04 (ブロック 0、オフセット 4)未満の領域と 15 (ブロック 2、オフセット 5)を超える領域は常に書き込めません。
OTP	0 – 1	OTPmode が read-only である場合、両方のブロックの全てのオフセットは 4 バイトおよび 32 バイトモードで読み出せます。 OTPmode が Consumption である場合、全てのオフセットに書き込む事もできます。 OTPmode が Legacy の場合については**「OTP (One Time Programmable)ゾーン」**を参照してください。

8.5.5 CheckMac コマンド

CheckMac コマンドは、CryptoAuthentication デバイス上で生成された MAC レスポンスを計算し、その MAC レスポンスと入力値を比較します。このコマンドは、比較の結果を示す論理値を返します。

このコマンドを実行する前に、必要に応じて Nonce または GenDig コマンド(もしくはその両方)を実行する事で、鍵またはノンス値を生成して TempKey に書き込む事ができます。Mode パラメータは「鍵」のソース(SHA メッセージの最初の 32 バイト)と「チャレンジ/ノンス」(SHA メッセージの次の 32 バイト)を指定します。

TempKey が計算値に含まれる場合、Mode<2>はランダムノンスの要件を指定します。Mode<2> = 1 の場合、Nonce(Fixed)を使って TempKey を生成する必要があります。Mode<2> = 0 の場合、Nonce(Random)を使って TempKey を生成する必要があります。

Mode<2> = 1 に設定した場合、状況によってはリプレイ攻撃を許してしまう可能性があります。

比較が一致しなかった場合、ターゲットスロット値を TempKey へ複製できます。SlotID が偶数である場合のターゲットスロットは SlotD+1 であり、奇数である場合のターゲットスロットは SlotID です。複製が実行されるには、以下の条件が全て真である事が必要です。いずれかの条件が偽である場合、ATSHA204A は比較結果を返しますが、鍵値を複製しません。

1. CheckMac に対する Mode パラメータの値が 0x01 または 0x05 である。
2. ターゲット鍵の SlotConfig.ReadKey が 0 である。
3. 鍵スロットに対応する Config.CheckMacSource 内のビットの値が Mode<2>と一致する。

表 8-8. 入力パラメータ

	名称	サイズ	注釈
Opcode	CheckMac	1	0x28
Param1	Mode	1	**Bit 7-6:** 0 である事が必要 SHA メッセージの 8 バイト **Bit 5:** 0: 全ビットが「0」 1: OTP ゾーン **Bit 4-3:** 0 である事が必要 **Bit 2:** TempKey を使う場合、このビットは TempKey.SourceFlag の値と一致する必要がある **Bit 1:** SHA メッセージの最初の 32 バイトのソース

	名称	サイズ	注釈
			0: Slot<SlotID> 1: TempKey SHA メッセージの 2 番目の 32 バイトのソース **Bit 0:** 0: ClientChal パラメータ 1: TempKey
Param2	SlotID	2	レスポンスを生成するために使う内部スロット(bit 3-0 のみを使用)
Data1	ClientChal	32	クライアントへ送信するチャレンジ(入力ストリーム内に含まれる事が必要)
Data2	ClientResp	32	クライアントによって生成されるレスポンス
Data3	OtherData	13	レスポンスの計算に必要なその他の定数データ

表 8-9. 出力パラメータ

名称	サイズ	注釈
Result	1	ClientResp が内部計算されたダイジェストと一致した場合に「0」の 1 バイト値を返し、一致しなかった場合に「1」を返します。

SHA-256 アルゴリズムによりハッシュ化されるメッセージは以下の情報を含みます。

32 バイト	key<SlotID>または TempKey (モードによって決まる)
32 バイト	ClientChal または TempKey (モードによって決まる)
4 バイト	OtherData<0:3>
8 バイト	OTP<0:7>または全ビットが「0」 (モードによって決まる)
3 バイト	OtherData<4:6>
1 バイト	SN<8>
4 バイト	OtherData<7:10>
2 バイト	SN<0:1>
2 バイト	OtherData<11:12>

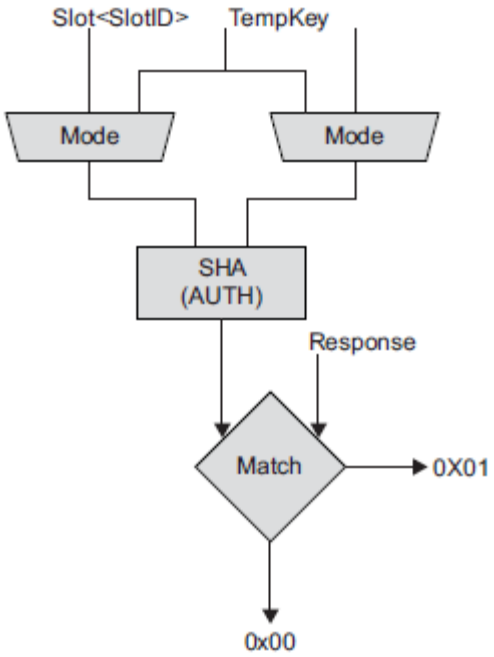
OtherData の目的は、ClientResp を生成するために使われた MAC メッセージと完全に一致する SHA-256 メッセージを構成する事です。MAC コマンドの SHA-256 向けに使われたメッセージを比較する事により、OtherData は表 8-10 の通りに解析されます。

表 8-10. OtherData

サイズ	CheckMac	MAC	注釈
1	OtherData<0>	OpCode	MAC OpCode = 0x08
1	OtherData<1>	Mode	MAC コマンドに使われたモード
2	OtherData<2:3>	SlotID	MAC コマンドに使われた SlotID
3	OtherData<4:6>	OTP<8:10>	MAC コマンドに使われた OTP<8:10> (Legacy モード向けに使用)
4	OtherData<7:10>	SN<4:7>	MAC コマンドに使われた SN<4:7> (クライアントごとに一意)
2	OtherData<11:12>	SN<2:3>	MAC コマンドに使われた SN<2:3> (クライアントごとに一意)

© 2019 Microchip Technology Inc.

図 8-1. CheckMac コマンドのデータフロー



8.5.6 Derivekey コマンド

本デバイスは、SHA-256 を使って、鍵の現在の値と TempKey に保存されているノンスを組み合わせ、その結果をターゲット鍵スロットに格納します。SlotConfig<TargetKey>.Bit13 はセットされている必要があります。クリアされている場合、DeriveKey はエラーを返します。

SlotConfig<TargetKey>.Bit12 がクリアされている場合、TempKey と組み合わされるソース鍵は、コマンドラインで指定されたターゲット鍵です(Roll-Key 動作)。 SlotConfig<TargetKey>.Bit12 がセットされている場合、ソース鍵はターゲット鍵のペアレント鍵であり、これは SlotConfig<TargetKey>.WriteKey 内にあります(Create Key 動作)。

DeriveKey コマンドの実行前に、Nonce コマンドを実行して TempKey 内で有効なノンスを生成しておく必要があります。このノンスの生成方法(内部 RNG による生成、または、固定)は、入力モードの bit 2 の状態によって決まります。

SlotConfig<TargetKey>.Bit15 がセットされている場合、以下の通りに計算された入力 MAC が必要です。

SHA-256 (ParentKey、Opcode、Param1、Param2、SN<8>、SN<0:1>)
ParentKey ID は常に SlotConfig<TargetKey>.WriteKey です。

SlotConfig<TargetKey>.Bit12 または SlotConfig<TargetKey>.Bit15 がセットされかつ SlotConfig<ParentKey>.LimitedUse もセットされている場合、UseFlag<ParentKey> = 0x00 であれば DeriveKey はエラーを返します。SlotConfig<TargetKey>.Bit12 と SlotConfig<TargetKey>.Bit15 の両方がクリアされている場合、DeriveKey はターゲット鍵の LimitedUse と UseFlag を無視します。

スロット 0～7 では、入力の構文解析とオプションの MAC チェックが成功すると、UseFlag<TargetKey>は 0xFF に設定され、UpdateCount<TargetKey>がインクリメントします。UpdateCount の現在の値が 0xFF である場合、UpdateCount は 0 にロールオーバーします。何らかの理由でコマンドの実行に失敗した場合、これらのバイトは更新できません。DeriveKey の実行中に停電した場合、UpdateCount の値は破損する可能性があります。

© 2019 Microchip Technology Inc.

Note: ソース鍵とターゲット鍵が同じである場合、書き込み動作中に停電すると鍵の値が恒久的に失われる危険があります。コンフィグレーション ビットによって許可されている場合、ペアレント鍵に基づく認証/暗号化された書き込みを使って鍵スロットを復元する事ができます。

表 8-11. 入力パラメータ

	名称	サイズ	注釈
Opcode	DeriveKey	1	0x1C
Param1	Random	1	**Bit 7-3:** 0 である事が必要 **Bit 2:** このビットの値は、TempKey.SourceFlag 内の値と一致する必要があります。一致しない場合、コマンドはエラーを返します。 **Bit 1-0:** 0 である事が必要
Param2	TargetKey	2	書き込み先の鍵スロット
Data	Mac	0 または 32	動作を検証するために使うオプションの MAC

表 8-12. 出力パラメータ

名称	サイズ	注釈
Success	1	正常に完了すると、ATSHA204A は値「0」を返します。

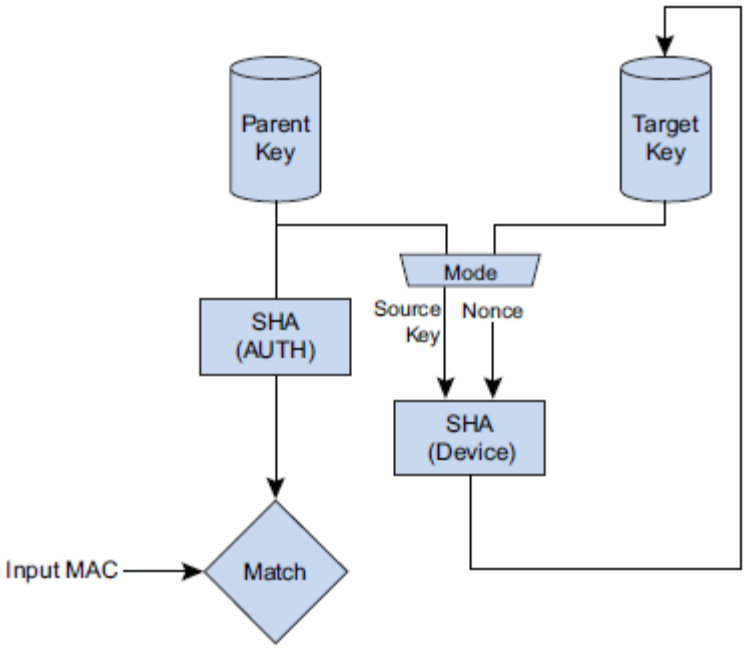
ターゲットスロットに書き込まれる鍵は、以下のメッセージの SHA-256 の結果です。

32 バイト	ターゲットまたはペアレント鍵(SlotConfig Bit12 によって決まる)
1 バイト	Opcode
1 バイト	Param1
2 バイト	Param2
1 1 バイト	SN<8>
2 バイト	SN<0:1>
25 バイト	全ビットが「0」
32 バイト	TempKey 値

このコマンドのデータフローを図 8-2 に示します。

© 2019 Microchip Technology Inc.

図 8-2. DeriveKey コマンドのデータフロー



8.5.7 DevRev コマンド

DevRev コマンドは、デバイスのリビジョン番号を表す 4 バイトワードを返します。この値は時に応じて変更される場合があるため、ソフトウェアでこの値を使わない事が必要です。

表 8-13. 入力パラメータ

	名称	サイズ	注釈
Opcode	DevRev	1	0x30
Param1	Mode	1	0 である事が必要
Param2	—	2	0 である事が必要
Data	—	0	—

表 8-14. 出力パラメータ

名称	サイズ	注釈
Success	4	現在のデバイス リビジョン番号

8.5.8 GenDig コマンド

GenDig コマンドは、SHA-256 を使って、保存されている値と TempKey の内容を組み合わせます。このコマンドを実行する前に、この値が有効である事が必要です。保存値には、OTP ページまたは Configuration ゾーンの最初の 2 ページに含まれるデータスロットの 1 つからの値を使うか、ハードウェア トランスポート鍵配列からの値が使えます。結果として得られるダイジェストは TempKye で保持され、以下の 3 通りの方法で使えます。

1. MAC、CheckMac、HMAC コマンドで使う事により、ダイジェストをメッセージの一部に含める事ができます。MAC レスポンス出力は GenDig 計算で使われるデータと MAC コマンドからの秘密鍵の両方を含むため、ダイジェストは Data および/または OTP ゾーンに保存されているデータの認証用に使えます。

© 2019 Microchip Technology Inc.

2. 後続の Read または Write コマンドは、ダイジェストを使ってデータに認証および/または機密性を提供できます。この場合、ダイジェストはデータ保護ダイジェストと呼びます。
3. このコマンドは、トランスポート鍵配列からの値を使う事により、セキュア パーソナライズ用に使えます。結果として得られるデータ保護ダイジェストは、Write コマンドによって使われます。

ゾーンが 2 (Data)かつ SlotID が 15 以下である場合、GenDig コマンドは TempKey.GenData を 1 に設定し、TempKey.SlotID を入力 SlotID に設定します。これ以外の場合、TempKey.GenData は 0 に設定されます。

結果のダイジェストがどのように計算されたかに関係なく、ダイジェストをデバイスから読み出す事は決してできません。

TempKey.Valid が無効の場合、このコマンドはエラーを返します。コマンドの実行が完了すると、TempKey.Valid ビットがセットされ、ダイジェストが書き込まれて使用可能である事が示されます。次のコマンドの実行時に TempKey.Valid ビットはクリアされます。詳細は**「スタティック RAM (SRAM)」**を参照してください。

0x8000 未満の全ての SlotID 値に対し、デバイスは SlotID の最下位 4 ビットを使って、EEPROM の Data ゾーン内のどのスロットから鍵値を取得するのか指定します。0x8000 以上の SlotID 値は、設計マスクに保存された鍵を参照します。いずれの場合も、デバイスへの入力として SlotID の 16 ビット全てが SHA-256 計算において Param2 として使われます。

ゾーン パラメータメータが Configuration ゾーンを指している場合、Configuration ゾーンがアンロック状態であれば、このコマンドはエラーを返します。

GenDig への入力で指定された鍵の CheckOnly ビットがセットされている場合、GenDig はクライアントの CryptoAuthentication デバイスで DeriveKey コマンドを使って生成された鍵と一致する一時鍵を生成できます。鍵の CheckOnly ビットがセットされているという事は、そのデバイスがホストとして動作しているという状況を表します。この場合、SHA 計算に通常含まれるオペコードおよびパラメータ バイトは、入力ストリームからのバイトで置き換えられます。

表 8-15. 入力パラメータ

	名称	サイズ	注釈
Opcode	GenDig	1	0x15
Param1	ゾーン	1	0x00 (Configuration ゾーン)の場合、SlotID を使って Configuration ゾーンの最初の 256 ビットブロック(SlotID = 0)または 2 番目の 256 ビットブロック(SlotID = 1)を指定します。 0x01 (OTP ゾーン)の場合、SlotID を使って OTP ゾーン内の最初の 256 ビットブロックまたは 2 番目の 256 ビットブロックを指定します。 0x02 (Data ゾーン)の場合、SlotID は Data ゾーン内のスロットまたはハードウェア配列内のトランスポート鍵を指定します。
Param2	SlotID	2	使用する鍵の ID 番号または OTP ブロックの選択
Data	OtherData	4 または 0	CheckOnly 鍵を使う場合、SHA 計算向け 4 バイトデータ (その他の場合は無視される)

表 8-16. 出力パラメータ

名称	サイズ	注釈
Success	1	正常に実行されると、ATSHA204A は値「0」を返します。

© 2019 Microchip Technology Inc.

ゾーンが Data かつ SlotConfig<SlotID>.CheckOnly が「1」の場合、新しい TempKey を生成するために使われる SHA-256 メッセージボディは以下のバイトで構成されます。

32 バイト	Slot<SlotID>
4 バイト	OtherData
1 バイト	SN<8>
2 バイト	SN<0:1>
25 バイト	全ビットが「0」
32 バイト	TempKey 値

その他の全ての条件では、TmpKey の生成に使われるメッセージは以下のバイトで構成されます。

32 バイト	Config<SlotID>、OTP<SlotID>、Data.slot<SlotID>、TransportKey<SlotID>のいずれか
1 バイト	Opcode
1 バイト	Param1
2 バイト	Param2
1 バイト	SN<8>
2 バイト	SN<0:1>
25 バイト	全ビットが「0」
32 バイト	TempKey 値

8.5.9 HMAC コマンド

HMAC コマンドは、デバイス内に保存されている鍵の HMAC/SHA-256 ダイジェスト、チャレンジ、デバイス上のその他の情報を計算します。このコマンドの出力は、この鍵とメッセージに対して計算された HMAC アルゴリズムの出力です。メッセージにデバイスのシリアル番号が含まれる場合、レスポンスは「Diversify」されたとなります。
このコマンドを使うための通常のコマンドフローは以下の通りです。

1. Nonce コマンドを実行して入力チャレンジをロードします。オプションにより、このチャレンジに生成された乱数を組み合わせる事ができます。この演算の結果は、ノンスとしてデバイス内部に保存されます。
2. 必要に応じ、GenDig コマンドを実行する事で、デバイス内の 1 つまたは複数の EEPROM 位置に保存されている値をノンスと組み合わせる事ができます。その結果は、デバイス内部に保存されます。
3. この HMAC コマンドを実行して上記ステップ 1 (および必要に応じてステップ 2) の出力と EEPROM 鍵を組み合わせる事で、出力レスポンスを生成します。

ステップ 2 は複数鍵使用モデルに対応します。EEPROM 内のデータが鍵である場合、GenDig は複数の秘密鍵を使ってチャレンジを認証する効果を持ちます。スロットの内容がデータ (データは秘密でなくても構わない)である場合、GenDig はその位置に保存されている値を認証する効果を持ちます。

表 8-17. 入力パラメータ

	名称	サイズ	注釈
Opcode	HMAC	1	0x11
Param1	Mode	1	メッセージで使うデバイス内のフィールドを指定します。
Param2	SlotID	2	レスポンスを生成するために使う鍵を指定します。

© 2019 Microchip Technology Inc.

	名称	サイズ	注釈
			スロットの選択には Param2<3:0>だけが使われますが、HMAC メッセージ内では 16 ビットの全てが使われます。
Data	—	0	—

表 8-18. 出力パラメータ

名称	サイズ	注釈
Response	32	HMAC ダイジェスト

HMAC ダイジェストは、SlotID にある鍵をメッセージに対する HMAC 鍵として使って計算されます。このメッセージは以下の情報により構成されます。

32 バイト	全ビットが「0」
32 バイト	TempKey
1 バイト	Opcode (常に 0x11)
1 バイト	Mode
2 バイト	SlotID
8 バイト	OTP<0:7>または全ビットが「0」(表 8-19 参照)
3 バイト	OTP<8:10>または全ビットが「0」(表 8-19 参照)
1 バイト	SN<8>
4 バイト	OTP<4:7>または全ビットが「0」(表 8-19 参照)
2 バイト	SN<0:1>
2 バイト	OTP<2:3>または全ビットが「0」(表 8-19 参照)

SHA-256、HMAC 鍵、適切なパディングを使って各種ダイジェストを計算する詳細な方法を記載した規格文書については**「HMAC/SHA-256」**を参照してください。

表 8-19. モードの指定

Bit	意味
7	0 である事が必要
6	**0 =** SN<2:3>と SN<4:7>に対応する 48 ビットを「0」に設定する **1 =** メッセージに SN<2:3>と SN<4:7>に対応する 48 ビットを含める
5	**0 =** OTP<0>～OTP<7>に対応する 64 ビットを「0」に設定する **1 =** メッセージに最初の 64 OTP ビット(8 バイト: OTP<0>～OTP<7>)を含める Mode<4>がセットされている場合、このモードビットの値は無視されます。
4	**0 =** OTP<0>～OTP<10>に対応する 88 ビット(11 バイト)を「0」に設定する **1 =** メッセージに最初の 88 OTP ビット(11 バイト: OTP<0>～OTP<10>)を含める
3	0 である事が必要

© 2019 Microchip Technology Inc.

Bit	意味
2	このビットの値は、TempKey.SourceFlag 内の値と一致する必要があります。一致しない場合、コマンドはエラーを返します。
1 – 0	0b00 である事が必要

8.5.10 Lock コマンド

指定されたゾーンのパーミッションを変更するために LockConfig または LockValue に 0x00 を書き込みます。そのゾーンがロック済みである場合、このコマンドは失敗します。
デバイスをロックする前に、ATSHA204A は CRC-16 アルゴリズムを使って、そのゾーンのサマリー ダイジェストを生成します。計算方法は、入力および出力ブロックに対する CRC 計算と同じです。

- **Configuration ゾーン:** CRC は 88 バイトの全てに対して計算されます。
- **Data および OTP ゾーン**: これらのゾーンの内容は、順番通り(Data が先、OTP が後)に連結されて CRC アルゴリズムへの入力を形成します。

入力サマリーがデバイス上での計算値に一致しない場合、エラーが返されます。その場合、パーソナライズ処理を再実行する必要があります。

表 8-20. 入力パラメータ

	名称	サイズ	注釈
Opcode	Lock	1	0x17.
Param1	Zone	1	**Bit 7:** 0 = ゾーンがロックされた時に CRC を確認する 1 = メモリの状態に関係なく、CRC 検査を無視してゾーンをロックする このモードは使わない事を推奨します。 **Bit 6-1:** 全てのビットは「0」である事が必要です。 **Bit 0:** 0 = Configuration ゾーン 1= Data および OTP ゾーン
Param2	Summary	2	指定されたゾーンのサマリー ダイジェストです。Zone<7>がセットされている場合、0x0000 である事が必要です。
Data	—	0	—

表 8-21. 出力パラメータ

名称	サイズ	注釈
Success	1	正常に実行されると、ATSHA204A は値「0」を返します。

8.5.11 MAC コマンド

MAC コマンドは、デバイスに保存されている鍵の SHA-256 ダイジェスト、チャレンジ、デバイス上のその他の情報を計算します。このコマンドの出力は、このメッセージのダイジェストです。メッセージにデバイスのシリアル番号が含まれる場合、レスポンスは「diversify」されたとなります。

このコマンドを使うための通常のコマンドフローは以下の通りです。

1. Nonce コマンドを実行して入力チャレンジをロードします。オプションにより、このチャレンジに生成された乱数を組み合わせる事ができます。この演算の結果は、ノンスとしてデバイス内部で TempKey に保存されます。

© 2019 Microchip Technology Inc.

2. 必要に応じ、GenDig コマンドを実行する事で、デバイス内の 1 つまたは複数の EEPROM 位置に保存されている値をノンスと組み合わせる事ができます。その結果は、デバイス内の TempKey に保存されます。この機能により、複数の鍵をレスポンス生成の一部として使う事ができます。
3. この MAC コマンドを実行して上記ステップ 1 (および必要に応じてステップ 2)の出力と EEPROM 鍵を組み合わせる事で、出力レスポンス(またはダイジェスト)を生成します。

表 8-22. 入 力パラメータ

	名称	サイズ	注釈
Opcode	MAC	1	0x08
Param1	Mode	1	メッセージで使うデバイス内のフィールドを指定します。
Param2	SlotID	2	レスポンスを生成するために使う内部鍵を指定します。 スロットの選択には bit 3-0 だけが使われますが、SHA-256 メッセージ内では 16 ビットの全てが使われます。
Data	Challenge	0 または 32	ダイジェスト化されるメッセージの入力部分。 Mode<0> = 「1」の場合に無視されます。

表 8-23. 出力パラメータ

名称	サイズ	注釈
Response	32	SHA-256 ダイジェスト

SHA-256 アルゴリズムによりハッシュ化されるメッセージは以下の情報を含みます。

32 バイト	key<SlotID>または TempKey(表 8-24 参照)
32 バイト	チャレンジまたは TempKey(表 8-24 参照)
1 バイト	Opcode (常に 0x08)
1 バイト	Mode
2 バイト	Param2
8 バイト	OTP<0:7>または全ビットが「0」(表 8-24 参照)
3 バイト	OTP<8:10>または全ビットが「0」(表 8-24 参照)
1 バイト	SN<8>
4 バイト	SN<4:7>または全ビットが「0」(表 8-24 参照)
2 バイト	SN<0:1>
2 バイト	SN<2:3>または全ビットが「0」(表 8-24 参照)

表 8-24. モードの指定

Bit	意味
7	0 である事が必要
6	**0 =** SN<2:3>と SN<4:7>に対応するビットを「0」に設定する **1 =** メッセージに SN<2:3>と SN<4:7>に対応する 48 ビットを含める
5	Mode<4>がセットされた場合、このモードビットの値は無視されます。 **0 =** 対応する 64 OTP ビットを「0」に設定する

© 2019 Microchip Technology Inc.

Bit	意味
	1 = メッセージに最初の 64 OTP ビット(OTP<0>～OTP<7>)を含める
4	**0 =** 対応する 88 OTP ビットを「0」に設定する **1 =** メッセージに最初の 88 OTP ビット(OTP<0>～OTP<10>)を含める
3	0 である事が必要
2	Mode<0>または Mode<1>のどちらかがセットされている場合、Mode<2>は TempKey.SourceFlag 内の値と一致する必要があります。一致しない場合、コマンドはエラーを返します。
1	**0 =** SHA メッセージの最初の 32 バイトをデータスロットの 1 つからロードする **1 =** 最初の 32 バイトに TempKey を書き込む
0	**0 =** SHA メッセージの 2 番目の 32 バイトは入力チャレンジ パラメータから取り込む **1 =** 2 番目の 32 バイトに TempKey の値を書き込む このモードは、全ての使用条件に推奨します。

8.5.12 Nonce コマンド

Nonce コマンドは、内部生成した乱数とシステムからの入力値を組み合わせる事により、後続の GenDig、MAC、HMAC、Read、Write コマンドによって使われるノンスを生成します。生成されたノンスは TempKey に内部保存され、生成された乱数がシステムへ返されます。

入力値は、ホストに対するリプレイ攻撃を防ぐ事を目的とします。この値は、システムによってデバイスの外部で生成され、コマンドを使ってデバイスに渡される必要があります。この値には、常に変化する任意の値(不揮発性カウンタ、現在の時刻等)が使えます。外部で生成される乱数も使えます。

後続の暗号処理コマンドにノンス値を提供するため、以下の情報に従って、入力値と出力乱数が一緒にハッシュ化されます。結果のダイジェスト (ノンス)は常に TempKey レジスタに保存され、TempKey.Valid がセットされ、TempKey.SourceFlag が「Rand」に設定されます。このノンスは後続の GenDig、Read、Write、HMAC、MAC コマンドで使えます。従って、これらのコマンドを実行するには、システムがこのダイジェスト値を外部で計算し、その値を外部に保存する必要があります。

後続のコマンドが固定されたノンスを要求する場合、Nonce コマンドはパススルー モードで実行できます。この場合、入力値は 32 バイト長である事が必要です。この値は、変更されずに直接 TempKey に渡されます。SHA-256 は計算されず、TempKey.SourceFlag は「Input」に設定されます。TempKey 内のノンス値を Read または Write コマンドで使う事はできません。このモードで同じ入力値が繰り返し使われる場合、デバイスはリプレイ攻撃に対する防御を提供しません。

テストを容易にするため、Configuration ゾーンがロックされるまで、RNG は 32 バイト値(0xFF FF 00 00 FF FF 00 00...)を生成します。 このテスト値は、前述の方法で入力値と組み合わされます。

© 2019 Microchip Technology Inc.

表 8-25. 入力パラメータ

	名称	サイズ	注釈
Opcode	Nonce	1	0x16
Param1	Mode	1	内部 RNG とシード更新の方法を制御します。
Param2	0	2	0x0000 である事が必要です。
Data	NumIn	20,32	システムからの入力値

表 8-26. 出力パラメータ

名称	サイズ	注釈
RandOut	1 または 32	RNG の出力、または、Mode<0:1> = 3 の場合は値が 0 の 1 バイト

Mode<1:0>が 0b00 または 0b01 である場合、NumIn パラメータは 20 バイト長である事が必要です。その場合、TempKey に内部保存されるノンスを生成するための SHA-256 メッセージ ボディは以下により構成されます。

32 バイト	RandOut
20 バイト	入力ストリームからの NumIn
1 バイト	Opcode (常に 0x16)
1 バイト	Mode
1 バイト	Param2 の LSb (常に 0x00 である事が必要)

コマンドの完了時に、TempKey.SourceFlag は「Rand」に設定されます。

Mode<1:0>が 0b11 である場合、このコマンドはパススルー モードで動作します。この場合、32 バイト長の入力パラメータ(NumIn)を TempKey に書き込む必要があります。SHA-256 は計算されず、システムにデータは返されません。TempKey.SourceFlag は「Input」に設定されます。

Mode<1:0> = 0b01 の場合、シードは自動的に更新されません。詳細は**「乱数生成器(RNG)」**を参照してください。セキュリティを最大限に高めるため、Mode<1:0>は 0b00 に設定する事を推奨します。

表 8-27. モードの指定

Bit	意味
7 – 2	0 である事が必要
1 – 0	**00 =** 新しい乱数と NumIn を組み合わせて TempKey に保存する (必要な場合にのみ、乱数生成前に自動的に EEPROM シードを更新します。セキュリティを最高にするために推奨します) **01 =** 新しい乱数と NumIn を組み合わせて TempKey に保存する (EEPROM シードを更新せず、既存の EEPROM シードを使って乱数を生成します) **10 =** 無効な状態 **11 =** パススルーモードで動作し、TempKey に NumIn を書き込む (32 バイトである事が必要です)

8.5.13 Pause コマンド

Configuration ゾーン内の Selector バイトが入力セレクタ パラメータと一致しないバイス上の全てデバイスはアイドル状態に移行させます。このコマンドは、複数の ATSHA204A が同じバスを共有するシステムでのバス競合を防ぐために使います。

© 2019 Microchip Technology Inc.

Pause コマンドの動作はアイドル フラグ/シーケンスとは異なります。すなわち、Pause コマンドを使うと単線式バス上の個々のデバイスを選択してアイドル状態へ移行させる事ができますが、アイドルフラグはバス上の全ての CryptoAuthentication デバイスをアイドル状態に移行させます。

EEPROM Selector バイトが入力セレクタ パラメータと一致しない場合、そのデバイスは直ちにアイドル状態へ移行します。Configuration ゾーン内の Selector バイトが入力セレクタ パラメータと一致した場合、そのデバイスは一致を示すコードとして 0x00 を返します。

Pause コマンドを使ってデバイスをスリープ状態に移行させる事はできません。

表 8-28. 入力パラメータ

	名称	サイズ	注釈
Opcode	Pause	1	0x01
Param1	Selector	1	この値に一致しない全てのデバイスはアイドル状態に移行します。
Param2	0	2	0x0000 である事が必要です。
Data	—	0	—

表 8-29. 出力パラメータ

名称	サイズ	注釈
Success	1	Pause コマンドの入力セレクタ パラメータと一致した(すなわちアイドルに移行しない) ATSHA204A は値 0x00 を返します。アイドルに移行するデバイスは値を返しません。

8.5.14 Random コマンド

Random コマンドは、システムによって使われる乱数を生成します。

乱数は、ハードウェア RNG の出力と、EEPROM または SRAM に保存されている内部シード値の組み合わせから生成されます。外部システムは、Nonce また Random コマンドによる乱数生成の前に、内部保存されている EEPROM シード値を更新するかどうか選択できます。セキュリティを最大限に高めるため、EEPROM シード値は常に更新する事を推奨します。

Random コマンドは、入力値と内部保存シード値を組み合わせる機能を提供しません。この機能が必要な場合、システムは Nonce コマンドを使う必要があります(生成されたノンスは無視する)。

テストを容易にするため、Configuration ゾーンがロックされるまで、RNG は 32 バイト値(0xFF、0xFF、0x00、0x00、0xFF、0xFF、0x00、0x00...)を生成します。

Nonce コマンドと Random コマンドの両方に同じ内部保存シード値が使われます。必要に応じ、Mode<0>を使って EEPROM シードを更新します。

表 8-30. 入力パラメータ

	名称	サイズ	注釈
Opcode	Random	1	0x1B
Param1	Mode	1	内部 RNG とシード更新の方法を制御します。

	名称	サイズ	注釈
Param2	0	2	0x0000 である事が必要です。
Data	—	0	—

表 8-31. 出力パラメータ

名称	サイズ	注釈
RandOut	32	RNG の出力

表 8-32. モードの指定

Bit	意味
7 – 1	0 である事が必要
0	**0 =** 必要な場合にのみ乱数生成前に自動的に EEPROM シードを更新する セキュリティを最高にするために推奨します。 **1 =** EEPROM シードを更新せず既存の EEPROM シードを使って乱数を生成する

8.5.15 Read コマンド

Read コマンドは、デバイスのメモリゾーンの 1 つからワード(1 つの 4 バイトワードまたは 1 つの 8 ワードブロック(32 バイト))を読み出します。オプションにより、システムへ返すデータを暗号化できます。Data ゾーンのバイトおよびワード アドレス情報は**「EEPROM Data ゾーン」**を参照してください。

SlotConfig.EncryptRead がセットされているスロットから読み出す場合、Read コマンドを実行する前に GenDig コマンドを実行して暗号化に使う鍵を生成しておく必要があります。スロット番号が偶数である場合、またはこのスロットに対応する CheckMacSource ビットが「0」である場合、GenDig に対する入力ノンスは乱数である事が必要です。また、GenDig の計算には SlotConfig.ReadKey で指定された鍵を使う必要があります。

デバイスは、EEPROM から読み出した各バイトと TempKey からの対応するバイトの間で XOR を取る事により、読み出しデータを暗号化します。Configuration ゾーンおよび OTP ゾーンからの暗号化された読み出しは許可されません。

読み出しバイトのアドレスは、デバイスへ渡す前に 4 で除算する(最下位 2 ビットを切り落とす)必要があります。32 バイトを読み出す場合、入力アドレスの最下位 3 ビットは無視されます。指定されたゾーンの終端を越えるアドレスは無視されます。

各ゾーンに対して以下の制約が適用されます。

- **Data**
  Data ゾーンがアンロック状態の場合、Read コマンドはエラーを返します。 ロック状態の場合、対応する SlotConfig ワード内の値によってデータスロットへのアクセスが制御されます。SlotConfig.IsSecret がセットされている場合に 4 バイト読み出しが試みられると、デバイスはエラーを返します。EncryptRead がセットされている場合、Read コマンドは前述の通りにデータを暗号化します。IsSecret がセットされ EncryptRead がクリアされている場合、Read コマンドはエラーを返します。IsSecret と EncryptRead の両方がクリアされている場合、Read コマンドは要求されたスロットのデータを平文で返します。
- **Configuration**
  このゾーン内のワードは、LockConfig.Read の値に関係なく、Read コマンドを使って常時読み出せます。

© 2019 Microchip Technology Inc.

- **OTP**
  OTP ゾーンがアンロック状態の場合、Read コマンドはエラーを返します。OTP モードが Legacy に設定されていない場合、OTP ゾーンがロックされた後は全てのワードが読み出せます。OTP モードが Legacy に設定されている場合、4 バイト読み出しのみが許可され、0 または 1 のアドレスはエラーを返します。

表 8-33. 入力パラメータ

	名称	サイズ	注釈
Opcode	Read	1	0x02
Param1	Zone	1	**Bit 7:** 0 = 4 バイトを読み出す 1 = 32 バイトを読み出す (OTP ゾーンから Legacy モードで読み出す場合、「0」である事が必要です) **Bit 6-2:** 全てのビットは「0」である事が必要です。 **Bit 1-0:** ゾーン(Config、OTP、Data のいずれか)を選択します。「ゾーンの指定」を参照してください。
Param2	Address	2	ゾーンから読み出す最初のワードのアドレスを指定します。「アドレスの指定」を参照してください。
Data	—	0	—

表 8-34. 出力パラメータ

名称	サイズ	注釈
Contents	4 または 32	指定されたメモリ位置の内容です。

8.5.15.1 Data ゾーン内の読み出し動作

Data ゾーン内の読み出し動作は、下表に示す通り、IsSecret と EncryptRead に基づきます。

表 8-35. 読み出し動作の許可

IsSecret	EncryptRead	概要
0	0	このスロットからは常に平文読み出しが可能です。 この状態に設定されたスロットを鍵ストレージとして使ってはいけません。 4 バイトまたは 32 バイトが一度に読み出せます。
0	1	この設定は使用禁止です。 このコードを使うと、スロットのセキュリティは保証されません。
1	0	このスロットからの読み出しは常に禁止されます。 この状態に設定したスロットは鍵ストレージとして使えます。
1	1	このスロットからの読み出しは、「Read コマンド」に記載したアルゴリズムを使って暗号化されます。 ReadKey によって指定されたスロット内にある暗号化鍵が使われます。 4 バイトの読み書きは禁止されます。

Data ゾーンから読み出す場合、対応する SlotConfig ワード内で EncryptRead ビットがセットされていると、データを暗号化するために以下の対応が取られます。

- 全ての TempKey レジスタビットは、以下の通りに正しく設定する必要があります。そうしないと、このコマンドはエラーを返します。

```
TempKey.Valid == 1

TempKey.GenData == 1
```

© 2019 Microchip Technology Inc.

```
TempKey.SlotID == SlotConfig.ReadKey
```

- 偶数番号スロットから読み出す場合、TempKey.SourceFlag は「RAND」である事が必要です。
- 奇数番号スロットから読み出す場合、TempKey.SourceFlag はそのスロットに対応する Config.CheckMacSource 内の値と一致する必要があります。
- メモリゾーンからのデータと TempKey の間で XOR が取られます。「Contents」として返されます。

8.5.16 SHA コマンド

SHA コマンドは、システムが汎用的に使う SHA-256 ダイジェストを計算します。メッセージの長さに制限はありません。システムは、最後のブロックで the pad and length バイト(長さを揃えるためのパディング バイト)を送信する必要があります。

ダイジェストの計算は以下の 2 ステップで発生します。

1. **Init**
   TempKey の現在の値に初期化定数を上書きする事により、SHA-256 計算エンジンをセットアップします。TempKey フラグは、Nonce(Fixed)コマンドの後の TempKey の状態と一致するように設定します。このモードはメッセージバイトを一切受け付けません。
2. **Compute**
   SHA コマンドをこのモードで任意回数呼び出す事で、メッセージにバイトを追加できます。このモードの各繰り返しは 64 バイトのメッセージを含む必要があります。出力バッファは常にダイジェストを格納しますが、これは必要に応じて無視できます。ダイジェストは TempKey にも書き込まれます。

SHA(Init)コマンドは、SHA(Compute)コマンドがデバイスに受け入れられる前に実行する必要があります。システムは、SHA(Compute)コマンドをダイジェストの計算に必要な回数だけ実行できます。SHA(Init)と最後の SHA(Compute)の間で SHA 以外のコマンドが実行されると、エラーが返されます。Mode バイトの値が 0x00 または 0x01 ではない場合、このコマンドは構文解析エラーを返します。

SHA コマンドの繰り返し中にデバイスがスリープに移行した場合、またはウォッチドッグ タイマがタイムアウトした場合、TempKey に保存されているダイジェストの中間結果は無効になります。システム ソフトウェアは、1 回の復帰/ウォッチドッグ周期中に完全なメッセージを送信するか、SHA コマンドと SHA コマンドの間に適切なアイドル シーケンスを挿入する必要があります。

表 8-36. 入力パラメータ

	名称	サイズ	注釈
Opcode	SHA	1	0x47
Param1	Mode	1	**Bit 7-1:** 0 である事が必要 **Bit 0:** 0 = (Init): TempKey に SHA-256 の初期値を書き込む メッセージバイトは受け付けません(メッセージの長さは 0 である事が必要)。 1 = (Compute): SHA コンテクストへのメッセージ パラメータに 64 バイトを追加し、ダイジェストを返す
Param2	Param2	2	0x0000 である事が必要
Data	Message	0 または 64	ハッシュ演算に含める 64 バイトのデータ Mode<0> = 0 の場合は無視されます。

© 2019 Microchip Technology Inc.

表 8-37. 出力パラメータ

名称	サイズ	注釈
Response	1 または 32	Mode<0> = 1 の場合、SHA-256 ダイジェスト Mode<0> = 0 の場合、成功を示す 0x00 またはエラーコード

8.5.17 UpdateExtra コマンド

UpdateExtra コマンドは、Configuration ゾーンがロックされた後に Configuration ゾーン内の 2 つの追加バイト (アドレス 84 および 85)を更新するために使います。 このコマンドを使うと、鍵に割り当てられた使用制限カウンタを適切なタイミングで素早くデクリメントする事もできます。

Mode<1>がセットされている場合、このコマンドは、特定の鍵に割り当て可能な使用制限カウンタの高速デクリメント(一度に複数ステップのデクリメントが可能)を実装します。「NewValue」パラメータによって指定されたスロットが使用制限付きの鍵を格納していない場合、このコマンドは何もアクションを取らずに戻ります。指定されたスロットが残回数のなくなった使用制限付き鍵を格納している場合、コマンドはエラーを返します。コマンドは、そのスロットに対応する Config.UpdateCount を変更しません。

Mode パラメータがアドレス 84 の UserExtra を指定している場合:

- UserExtra (Configuration ゾーン内のバイト 84)内の値が 0 である場合、UpdateExtra コマンドはこのバイトに NewValue の LSB を書き込み、成功を示すコードを返します。
- UserExtra 内の値が非 0 である場合、UpdateExtra コマンドは実行エラーを返します。

Mode パラメータがアドレス 85 の UserExtra を指定している場合:

- SelectorMode (Configuration ゾーン内のバイト 19)が非 0 かつ Selector バイト(Configuration ゾーン内のバイト 85)が 0 である場合、UpdatExtra コマンドは Selector バイトに NewValue の LSB を書き込み、成功を示すコードを返します。一度非 0 値が書き込まれると、Selector バイトは後続の更新に対してロックされます。
- SelectorMode の値が 0 (現在の Selector のチェックなし)である場合、UpdateExtra コマンドは常に Selector の更新に成功します。

表 8-38. 入力パラメータ

	名称	サイズ	注釈
Opcode	UpdateExtra	1	0x20
Param1	Mode	1	**Bit 7..2:** 0 である事が必要 **Bit 1:** 0 = Configuration ゾーンのバイト 84 または 85 を更新する 1 = bit 0 を無視し、スロット「NewValue」内の鍵に対応する使用制限カウンタをデクリメントする **Bit 0:** 0 = Configuration ゾーンのバイト 84 を更新する 1 = Configuration ゾーンのバイト 85 を更新する
Param2	NewValue	2	**LSB:** 必要に応じて Configuration ゾーンのバイト 84 または 85 に書き込む値 **MSB:** 0x00 である事が必要
Data	—	0	—

© 2019 Microchip Technology Inc.

表 8-39. 出力パラメータ

名称	サイズ	注釈
Success	1	このコマンドは、メモリバイトが更新された場合に 0x00 を返し、更新されなかった場合に実行エラーを返します。

8.5.18 Write コマンド

Write コマンドは、デバイスの EEPROM ゾーンの 1 つに 4 バイトワードまたは 8 ワードブロック(32 バイト)を書き込みます。スロットの WriteConfig バイトの値に応じて、システムはデバイスへ送信する前にデータを暗号化する必要があります。

Write コマンドを使った各ゾーンへの書き込みには以下の制限が適用されます。

- **Data ゾーン**: Configuration ゾーンがロック状態かつ Data ゾーンがアンロック状態である場合、32 バイト書き込みを使って Data ゾーン内の全てのバイトに平文または暗号データを書き込めます。Data ゾーンがロックされた後は、WriteConfig バイト内の値によってデータスロットへのアクセスが制御されます。スロットに対応する WriteConfig ビットが「always」に設定されている場合、入力データは平文でデバイスに渡す必要があります。SlotConfig<14>が「1」に設定されている場合、入力データを暗号化し、入力 MAC を計算する必要があります。
- **Configuration ゾーン:** Configuration ゾーンがロックされている場合、または Zone<6>がセットされている場合、Write コマンドはエラーを返します。これ以外の場合、バイトは要求通りに書き込まれます。書き込みが恒久的に禁止されているバイト(**「EEPROM Data ゾーン」**参照)への書き込みが試みられると、コマンドエラーが発生し、EEPROM の内容は変更されません。
- **OTP ゾーン**: OTP ゾーンがアンロック状態である場合、Write コマンドを使って全てのバイトに書き込めます。OTP ゾーンがロック状態かつ OTPmode バイトが「read-only」または「legacy」である場合、Write コマンドはエラーを返します。OTPmode が「consumption」の場合、Write コマンドは入力パラメータ値内の「0」のビットに対応する OTP ゾーン内のビットを「0」に設定します。OTP ゾーンがロック状態である場合、OTPmode に関係なく、OTP ゾーンへの暗号化された書き込みは禁止されます。

以下の 4 つの条件の全てが真である場合、Data ゾーンと OTP ゾーンでは 4 バイト書き込みのみが許可されます。

- SlotConfig.IsSecret = 0
- SlotConfig.WriteConfig = always
- 入力データは平文
- Data/OTP ゾーンはロック状態

1 つでも条件が満たされない場合、4 バイト書き込みはエラーを返します。

Param2 の最下位 3 ビット(Address<2:0>)は、ブロック内のワードを指定します(32 バイトブロック全体が書き込まれる場合は無視されます)。Address<6:3>は、Data ゾーンへの書き込み時にスロット番号を格納し、Configuration または OTP ゾーンへの書き込み時にブロック番号を格納します。アドレス値が指定されたゾーンのサイズを超えている場合、コマンドはエラーを返します。

Configuration ゾーンがロックされる前に OTP または Data ゾーンへの書き込みが試みられると、デバイスはエラーコードを返します。

8.5.18.1 入力データの暗号化

パーソナライズ中またはシステム動作中にバスの傍聴を防ぐため、入力データは暗号化できます。システムは、平文と TempKey 内の現在の値との間で XOR を取る事により、データを暗号化する必要があります。デバイスは、データ受信時に EEPROM へ書き込む前に、入力データと TempKey の間で XOR を取る事により平文へ復号します。

© 2019 Microchip Technology Inc.

入力データが暗号化されている場合、Data ゾーンへの書き込み時に認証用入力 MAC が常に要求されます。この MAC は以下の通りに計算されます。

SHA-256 (TempKey、Opcode、Param1、Param2、SN<8>、SN<0:1>、<25 バイトの「0」>、PlainTextData)

OTP/Data ゾーンがロックされる前は、入力データが暗号化されているかどうかをデバイスに示すために Zone<6>が使われます。OTP/Data ゾーンがロックされた後は、Zone<6>は無視され、入力データが暗号化されているかどうかの判定には、書き込み先のスロットに対応する SlotConfig<14>のみが使われます。

データの暗号化が指定された場合、`Write` コマンドが呼び出される前に TempKey が有効であり `GenDig` の結果を格納している事が必要です。具体的には、TempKey.Valid と TempKey.GenDig の両方が「`1`」に設定されている必要があります。
Data ゾーンがロックされる前は、任意の鍵を使って TempKey を生成できます。ロック後は、TempKey の生成用に `GenDig` によって使われ TempKey.SlotID に保存された最後のスロットは、SlotConfig.WriteKey 内のスロットと一致する必要があります。偶数番号のスロットに書き込む場合、TempKey.SourceFlag は「RAND」である事が必要です。
奇数番号のスロットに書き込む場合、TempKey.SourceFlag はそのスロットに対応する Config.CheckMacSource 内の値と一致する必要があります。

表 8-40. 入力パラメータ

	名称	サイズ	注釈
Opcode	Write	1	0x12
Param1	Zone	1	**Bit 7:** `0` = 指定されたゾーンに 4 バイトのデータを書き込む `1` = 指定されたゾーンに 32 バイトのデータを書き込む **Bit 6:** `0` = データを平文で書き込む `1` = 入力データを暗号化する Data/OTP ゾーンがロックされている場合、「`0`」である事が必要です。 **Bit 5-2:** `0` である事が必要 **Bit 1-0:** ゾーン(Config、OTP、Data のいずれか)を選択します。
Param2	Address	2	ゾーン内に書き込む最初のワードのアドレスです。 **「アドレスの指定」**を参照してください。
Data_1	Value	4 または 32	ゾーンに書き込む内容です(暗号化可能)。
Data_2	Mac	0 または 32	アドレスとデータを検証するためのメッセージ認証コードです。

表 8-41. 出力パラメータ

名称	サイズ	注釈
Success	1	正常に完了すると、ATSHA204A は値 `0x00` を返します。

© 2019 Microchip Technology Inc.

9. 互換性

ATSHA204A は全てのホスト、クライアント、パーソナライズ動作で ATSHA204 と完全互換となるよう設計されています。以下は、ATSHA204A に適用された重要な改良点です。

- 動作時消費電力が低減されています。
- 外付けダイオードを必要とせずに 2 線式接続モードをサポートします。
- 新しい SHA コマンドにより、ホストで暗号ソフトウェアを必要とせずに SHA ダイジェストの一般的計算が可能です。
- 介入者攻撃を防ぐため、パーソナライズ中の書き込み動作は、MAC がデバイスに渡される事を常に要求します(ATSHA204 の一部のバージョンは、Data ゾーンがアンロック状態の時に、書き込み時の MAC を無視しました)。
- マルチステップ カウントが必要な場合に `UpdateExtra` コマンド使って使用制限カウンタを高速にデクリメントできるようになりました。
- `CheckMac` コマンドの Copy モードが固定ノンスを使って実行できるようになりました。これにより、保護されたセキュアブート検証と関連するタスクの実装が簡素化されます。
- OTP ゾーン向けの新しい Consumption モードにより、使用状況の追跡能力が向上しました。
- OTP ゾーンまたは Data ゾーンに対する書き込み動作は、Configuration ゾーンがロック状態かつ OTP/Data ゾーンがアンロック状態の時に 32 バイト書き込みを要求します。ATSHA204 では、このロック状態で 4 バイト書き込みを許容しました。

© 2019 Microchip Technology Inc.

10. パッケージとピン配置

10.1 ピン配置

本デバイスは以下のパッケージで提供しています。

- 8 ピン UDFN
- 3 ピン SOT23
- 8 ピン SOIC
- 8 ピン TSSOP (ST)(Note)
- 3 ピン CONTACT (はんだ付けしない機械接点向け)

ピン配置は以下の通りです。

表 10-1. パッケージのピン配置

名称	3 ピン SOT23	8 ピン SOIC、8 ピン TSSOP(Note)、8 ピン UDFN	3 ピン CONTACT
SDA	1	5	1
SCL	—	6	—
VCC	2	8	3
GND	3	4	2
NC	—	1, 2, 3, 7	—

Note: 新規設計には非推奨

11. パッケージのマーキング情報

Microchip 社の全体的なセキュリティ対応の一貫として、全ての暗号デバイスの製品マーキングは意図的に曖昧にされています。パッケージ上面のマークは、デバイスのタイプやデバイスの製造者に関する情報を一切提供しません。パッケージ上の英数字コードは製造情報を提供し、アセンブリロットに応じて異なります。パッケージのマークは、お客様の受領検査の項目に含めないでください。

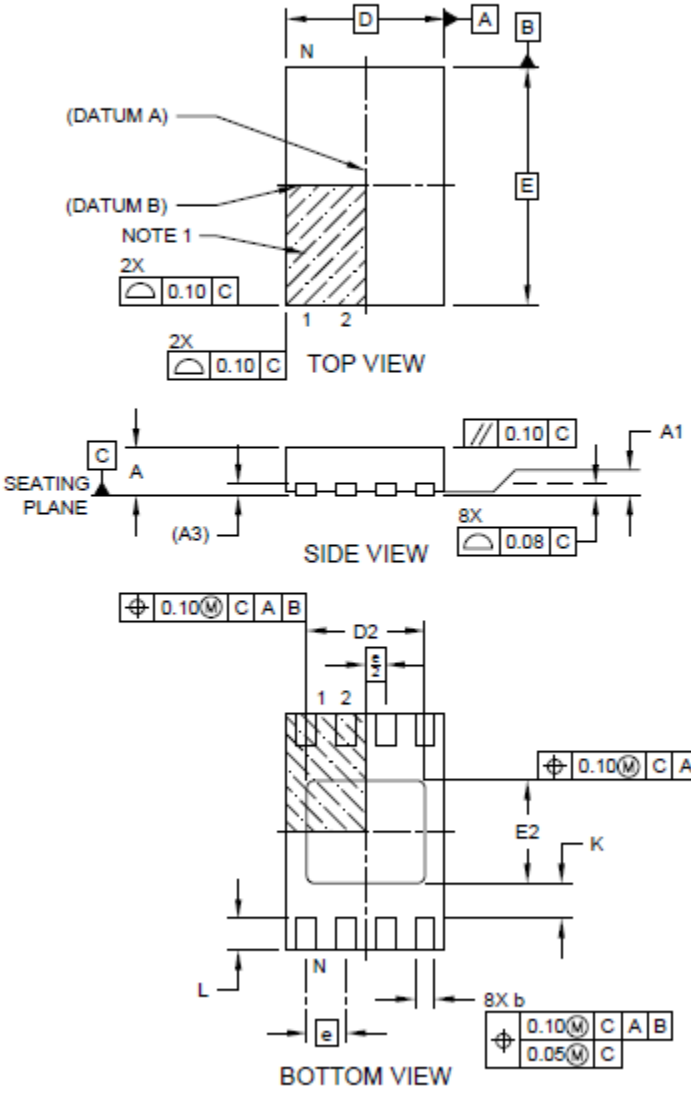
© 2019 Microchip Technology Inc.

12. パッケージ図面

12.1 8 ピン UDFN

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

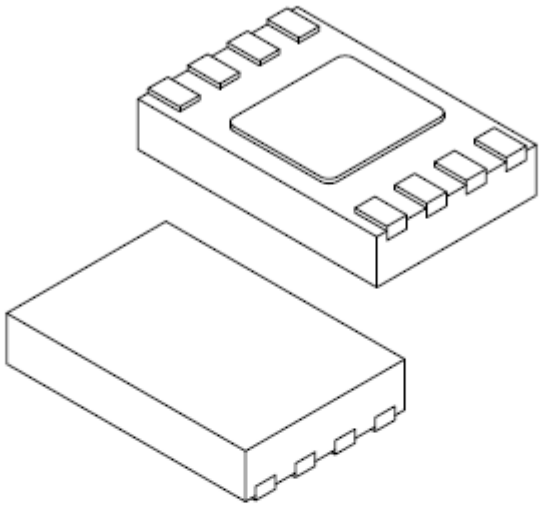
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21355-Q4B Rev A Sheet 1 of 2

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		8	
Pitch	e		0.50 BSC	
Overall Height	A	0.50	0.55	0.60
Standoff	A1	0.00	0.02	0.05
Terminal Thickness	A3		0.152 REF	
Overall Length	D		2.00 BSC	
Exposed Pad Length	D2	1.40	1.50	1.60
Overall Width	E		3.00 BSC	
Exposed Pad Width	E2	1.20	1.30	1.40
Terminal Width	b	0.18	0.25	0.30
Terminal Length	L	0.35	0.40	0.45
Terminal-to-Exposed-Pad	K	0.20	-	-

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Package is saw singulated
3. Dimensioning and tolerancing per ASME Y14.5M

   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

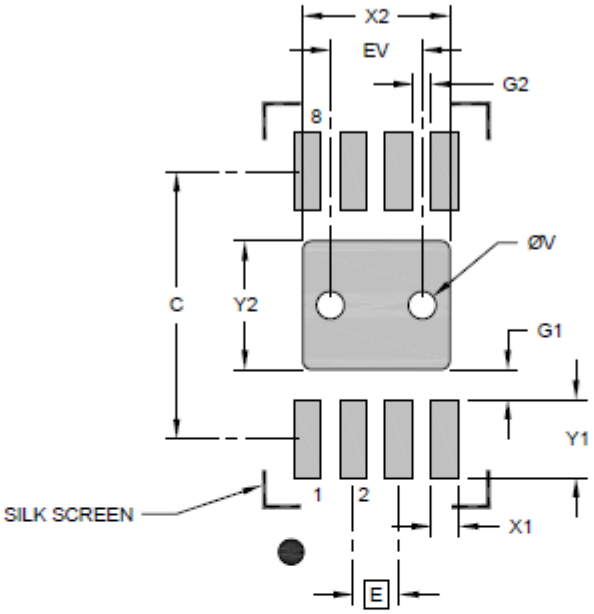
   REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-21355-Q4B Rev A Sheet 2 of 2

© 2019 Microchip Technology Inc.

8-Lead Ultra Thin Plastic Dual Flat, No Lead Package (Q4B) - 2x3 mm Body [UDFN]
Atmel Legacy YNZ Package

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.50 BSC	
Optional Center Pad Width	X2			1.60
Optional Center Pad Length	Y2			1.40
Contact Pad Spacing	C		2.90	
Contact Pad Width (X8)	X1			0.30
Contact Pad Length (X8)	Y1			0.85
Contact Pad to Center Pad (X8)	G1	0.20		
Contact Pad to Contact Pad (X6)	G2	0.33		
Thermal Via Diameter	V		0.30	
Thermal Via Pitch	EV		1.00	

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
2. For best soldering results, thermal vias, if used, should be filled or tented to avoid solder loss during reflow process

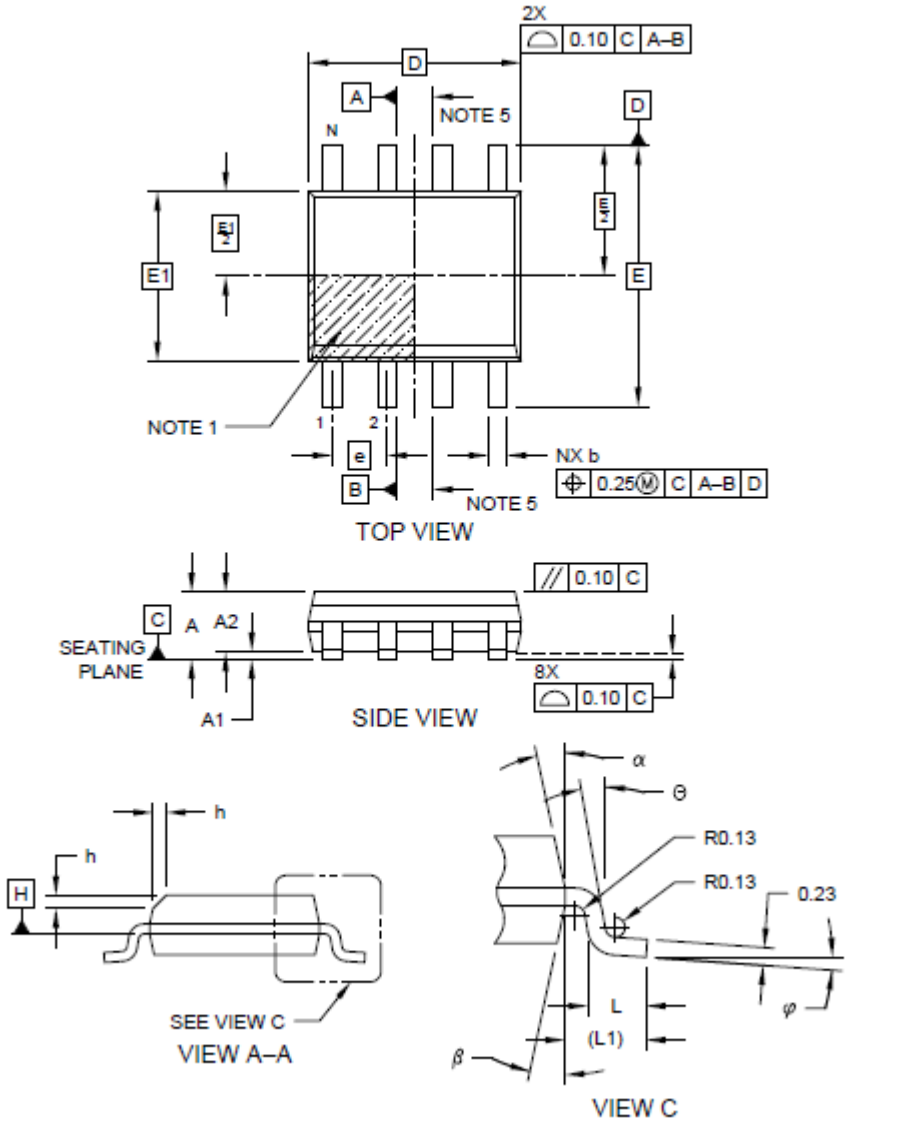
Microchip Technology Drawing C04-21355-Q4B Rev A

© 2019 Microchip Technology Inc.

12.2 8 ピン SOIC

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

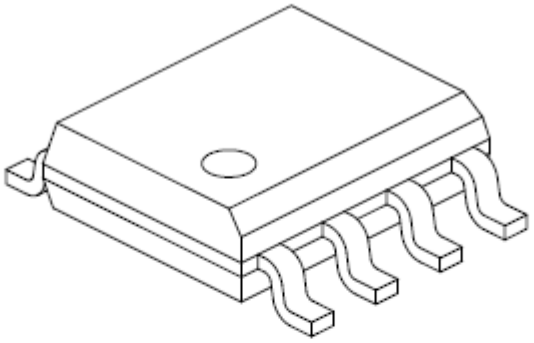
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing No. C04-057-Atmel Rev D Sheet 1 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		1.27 BSC	
Overall Height	A	-	-	1.75
Molded Package Thickness	A2	1.25	-	-
Standoff §	A1	0.10	-	0.25
Overall Width	E		6.00 BSC	
Molded Package Width	E1		3.90 BSC	
Overall Length	D		4.90 BSC	
Chamfer (Optional)	h	0.25	-	0.50
Foot Length	L	0.40	-	1.27
Footprint	L1		1.04 REF	
Foot Angle	φ	0°	-	8°
Lead Thickness	c	0.17	-	0.25
Lead Width	b	0.31	-	0.51
Mold Draft Angle Top	α	5°	-	15°
Mold Draft Angle Bottom	β	5°	-	15°

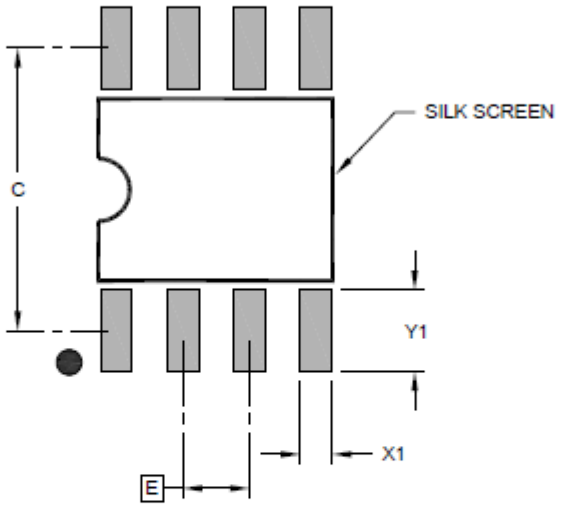
Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. § Significant Characteristic
3. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15mm per side.
4. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.
5. Datums A & B to be determined at Datum H.

Microchip Technology Drawing No. C04-057-OA Rev D Sheet 2 of 2

8-Lead Plastic Small Outline - Narrow, 3.90 mm (.150 In.) Body [SOIC]
Atmel Legacy

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		1.27 BSC	
Contact Pad Spacing	C		5.40	
Contact Pad Width (X8)	X1			0.60
Contact Pad Length (X8)	Y1			1.55

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.

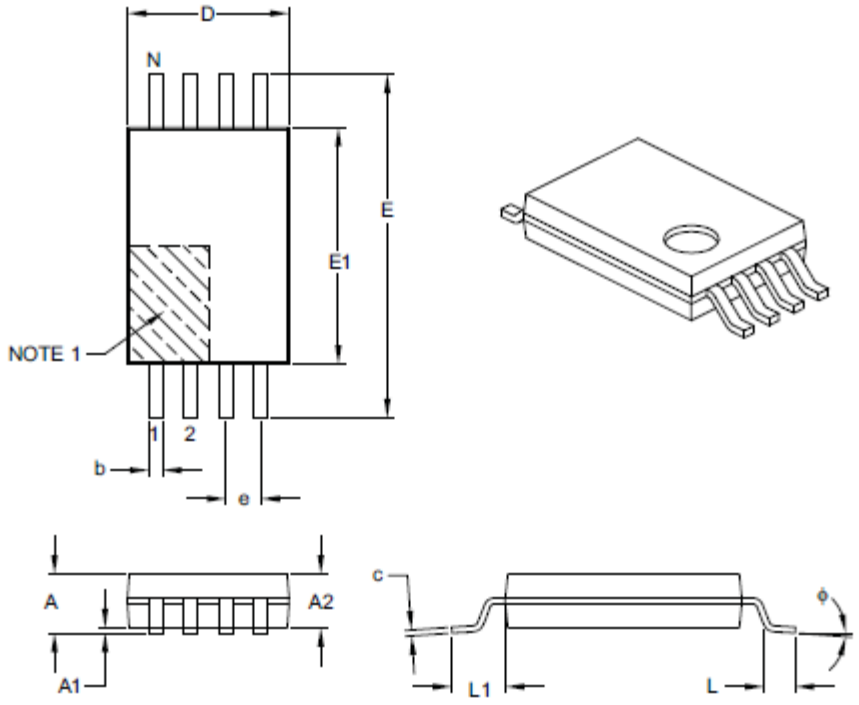
Microchip Technology Drawing C04-2057-M6B Rev B

© 2019 Microchip Technology Inc.

12.3 8 ピン TSSOP

8-Lead Plastic Thin Shrink Small Outline (ST) – 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		8	
Pitch	e		0.65 BSC	
Overall Height	A	–	–	1.20
Molded Package Thickness	A2	0.80	1.00	1.05
Standoff	A1	0.05	–	0.15
Overall Width	E		6.40 BSC	
Molded Package Width	E1	4.30	4.40	4.50
Molded Package Length	D	2.90	3.00	3.10
Foot Length	L	0.45	0.60	0.75
Footprint	L1		1.00 REF	
Foot Angle	ϕ	0°	–	8°
Lead Thickness	c	0.09	–	0.20
Lead Width	b	0.19	–	0.30

Notes:

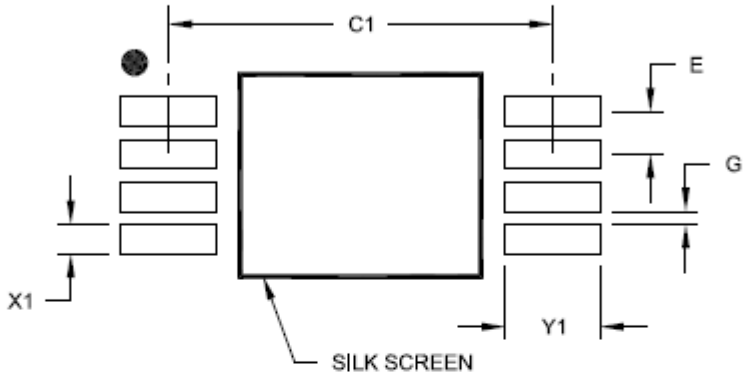
1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.15 mm per side.
3. Dimensioning and tolerancing per ASME Y14.5M.
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

Microchip Technology Drawing C04-086B

© 2019 Microchip Technology Inc.

8-Lead Plastic Thin Shrink Small Outline (ST) – 4.4 mm Body [TSSOP]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.65 BSC	
Contact Pad Spacing	C1		5.90	
Contact Pad Width (X8)	X1			0.45
Contact Pad Length (X8)	Y1			1.45
Distance Between Pads	G	0.20		

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

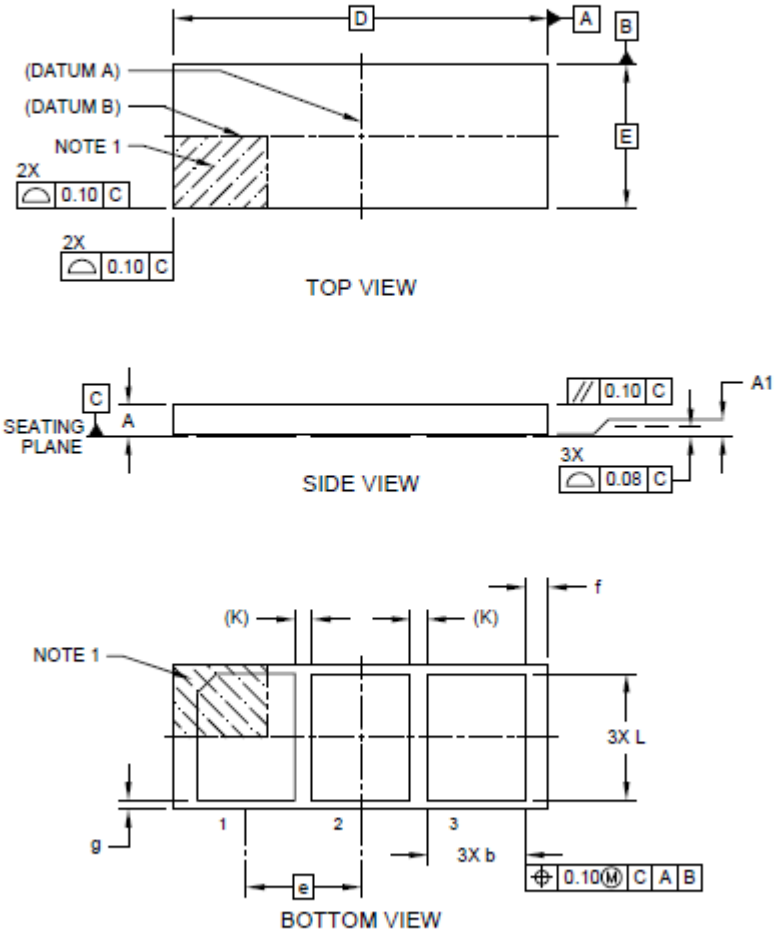
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2086A

12.4 3 ピン CONTACT

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

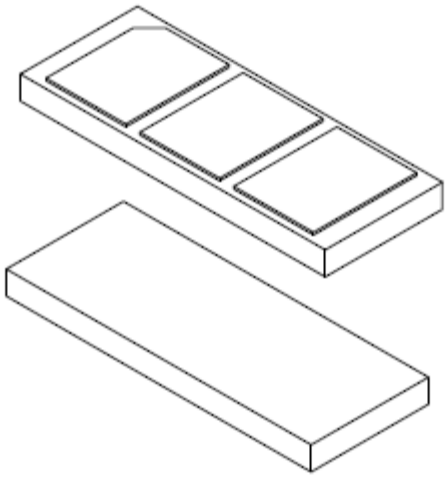
Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Microchip Technology Drawing C04-21303 Rev A Sheet 1 of 2

3-Lead Contact Package (LAB) - 6.54x2.5 mm Body [Contact]
Atmel Legacy Global Package Code RHB

Note:	For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Terminals	N		3	
Pitch	e		2.00 BSC	
Overall Height	A	0.45	0.50	0.55
Standoff	A1	0.00	0.02	0.05
Overall Length	D		6.50 BSC	
Overall Width	E		2.50 BSC	
Terminal Width	b	1.60	1.70	1.80
Terminal Length	L	2.10	2.20	2.30
Terminal-to-Terminal Spacing	K		0.30 REF	
Package Edge to Terminal Edge	f	0.30	0.40	0.50
Package Edge to Terminal Edge	g	0.05	0.15	0.25

Notes:

1. Pin 1 visual index feature may vary, but must be located within the hatched area.
2. Dimensioning and tolerancing per ASME Y14.5M
   BSC: Basic Dimension. Theoretically exact value shown without tolerances.
   REF: Reference Dimension, usually without tolerance, for information purposes only.

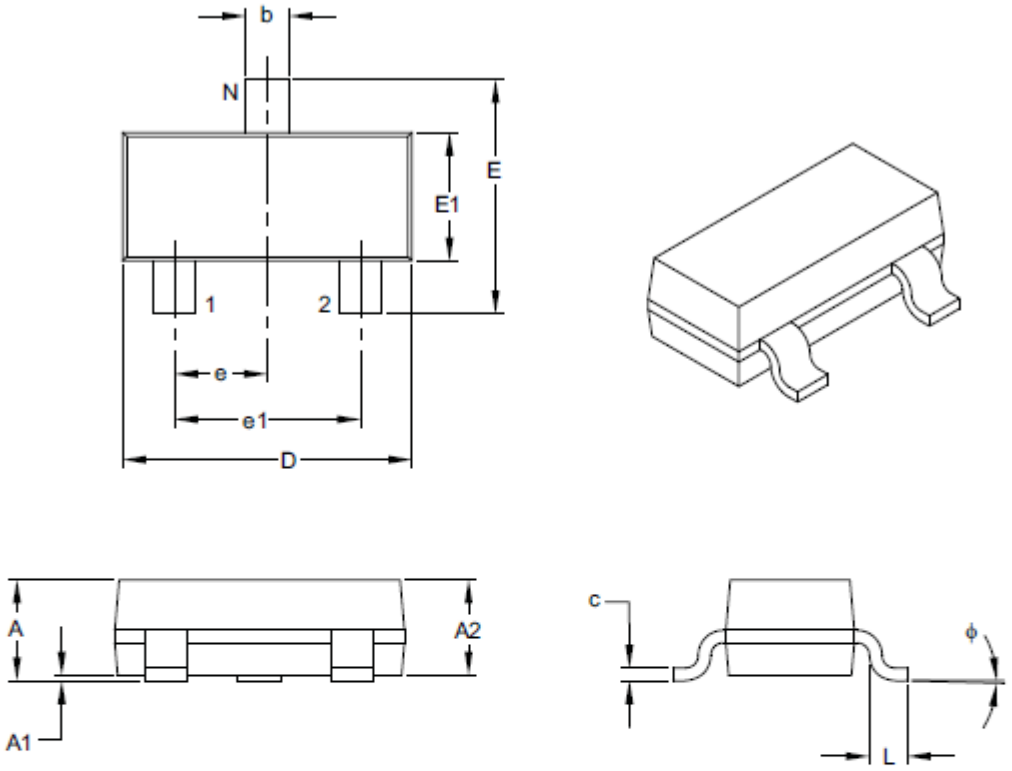
Microchip Technology Drawing C04-21303 Rev A Sheet 2 of 2

© 2019 Microchip Technology Inc.

12.5 3 ピン SOT23

3-Lead Plastic Small Outline Transistor (NB) [SOT-23]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		3	
Lead Pitch	e		0.95 BSC	
Outside Lead Pitch	e1		1.90 BSC	
Overall Height	A	0.89	–	1.12
Molded Package Thickness	A2	0.79	0.95	1.02
Standoff	A1	0.01	–	0.10
Overall Width	E	2.10	–	2.64
Molded Package Width	E1	1.16	1.30	1.40
Overall Length	D	2.67	2.90	3.05
Foot Length	L	0.13	0.50	0.60
Foot Angle	ϕ	0°	–	10°
Lead Thickness	c	0.08	–	0.20
Lead Width	b	0.30	–	0.54

Notes:

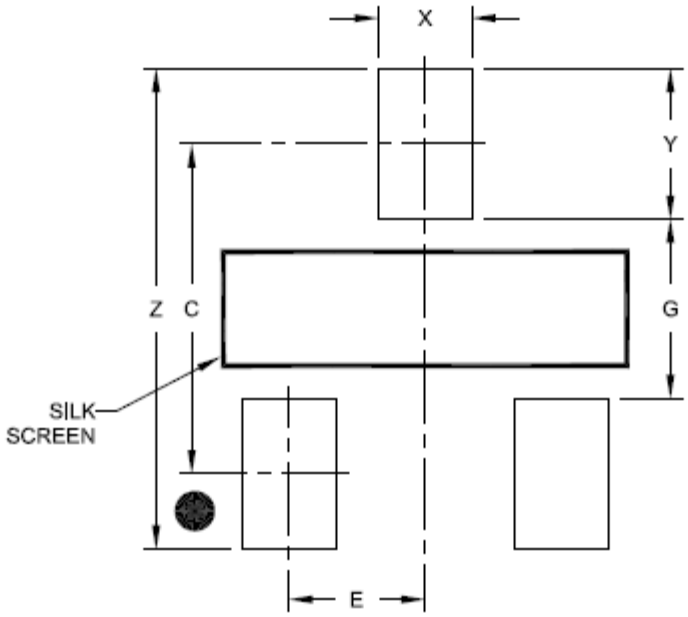
1. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.25 mm per side.
2. Dimensioning and tolerancing per ASME Y14.5M.

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-104B

3-Lead Plastic Small Outline Transistor (NB) [SOT-23]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E		0.95 BSC	
Contact Pad Spacing	C		2.30	
Contact Pad Width (X3)	X			0.65
Contact Pad Length (X3)	Y			1.05
Distance Between Pads	G	1.25		
Overall Width	Z			3.35

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

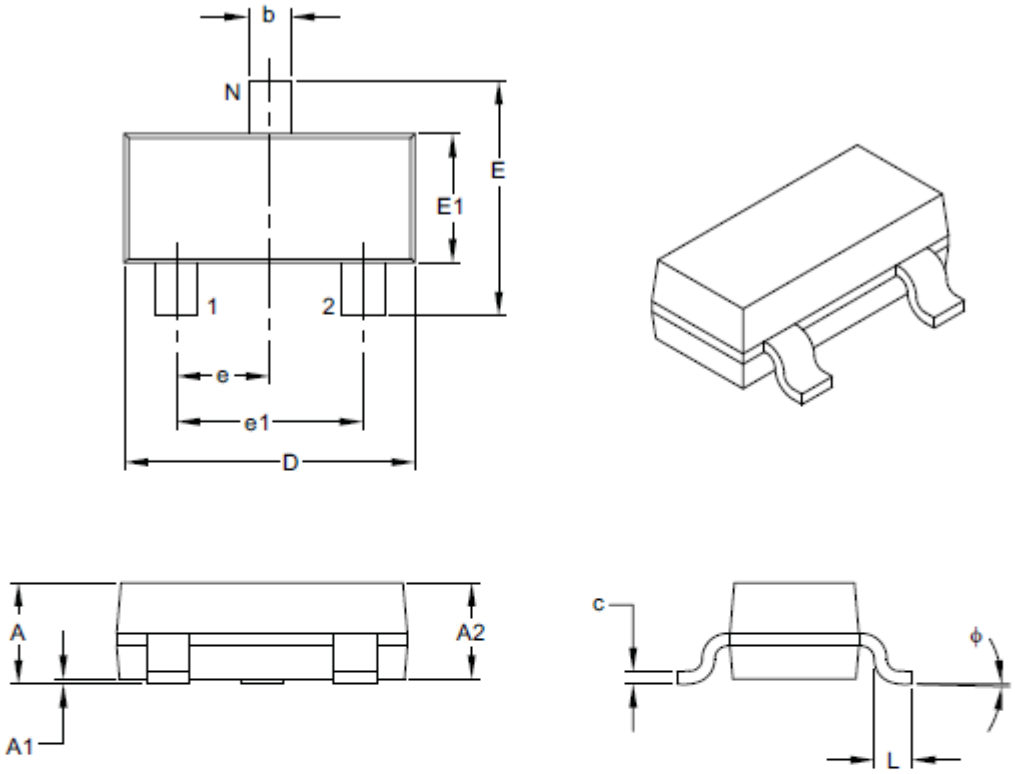
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2104A

© 2019 Microchip Technology Inc.

3-Lead Plastic Small Outline Transistor (TT) [SOT-23]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Number of Pins	N		3	
Lead Pitch	e		0.95 BSC	
Outside Lead Pitch	e1		1.90 BSC	
Overall Height	A	0.89	–	1.12
Molded Package Thickness	A2	0.79	0.95	1.02
Standoff	A1	0.01	–	0.10
Overall Width	E	2.10	–	2.64
Molded Package Width	E1	1.16	1.30	1.40
Overall Length	D	2.67	2.90	3.05
Foot Length	L	0.13	0.50	0.60
Foot Angle	ϕ	0°	–	10°
Lead Thickness	c	0.08	–	0.20
Lead Width	b	0.30	–	0.54

Notes:

1. Dimensions D and E1 do not include mold flash or protrusions. Mold flash or protrusions shall not exceed 0.25 mm per side.
2. Dimensioning and tolerancing per ASME Y14.5M.

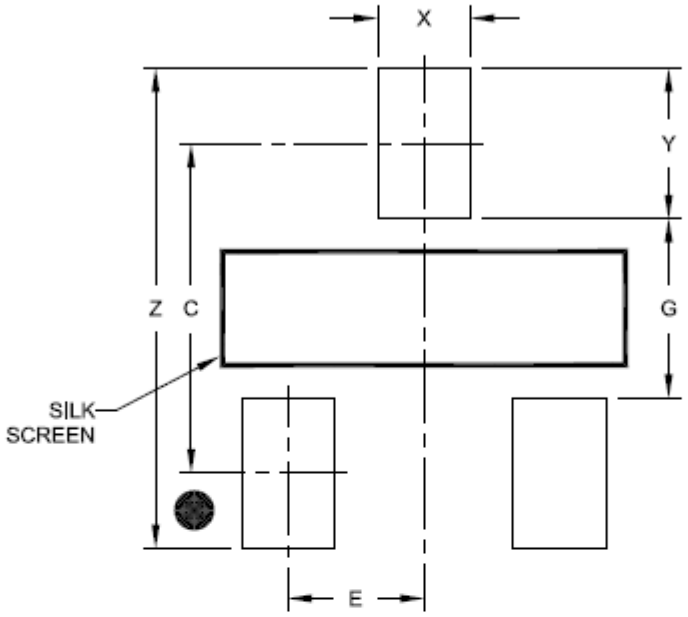
BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing C04-104B

© 2019 Microchip Technology Inc.

3-Lead Plastic Small Outline Transistor (TT) [SOT-23]

Note: For the most current package drawings, please see the Microchip Packaging Specification located at http://www.microchip.com/packaging



RECOMMENDED LAND PATTERN

Units		MILLIMETERS		
Dimension Limits		MIN	NOM	MAX
Contact Pitch	E	0.95 BSC		
Contact Pad Spacing	C		2.30	
Contact Pad Width (X3)	X			0.65
Contact Pad Length (X3)	Y			1.05
Distance Between Pads	G	1.25		
Overall Width	Z			3.35

Notes:

1. Dimensioning and tolerancing per ASME Y14.5M

BSC: Basic Dimension. Theoretically exact value shown without tolerances.

Microchip Technology Drawing No. C04-2104A

© 2019 Microchip Technology Inc.

13. 参考資料とアプリケーション ノート

以下で詳細に説明する通り、ATSHA204A は SHA-256 または HMAC/SHA-256 のどちらかを使ってチャレンジ-レスポンス プロトコルを実装します。レスポンスは常に 256 ビットのダイジェストです。

Nonce コマンド(「Nonce コマンド」参照)は、システムからの入力チャレンジを承認し、必要に応じて入力チャレンジと内部生成した乱数を組み合わせて計算用にノンス(例: 一度だけ使われる番号)を生成します。この組み合わせがシードであり、これは全ての暗号コマンド(例: MAC、HMAC、Read、Write、GenDig)向け認証計算の一部として秘密鍵と組み合わされます。入力チャレンジは MAC コマンドに直接渡す事もできます。

システム入力は一意である場合も一意でない場合もあるため、本デバイスは、本デバイスの RNG 出力が計算に含まれる場合にのみ、ノンスの一意性を保証できます。各ランダムノンスは以前の全てのノンスと比較した場合に一意である事が保証され、これにより各トランザクションの一意性が常に確保されます。

13.1 SHA-256

ATSHA204A の MAC コマンドは、チャレンジまたはノンスと連結した秘密鍵のダイジェストを計算します。必要に応じて、デバイスに保存されているその他の情報をダイジェスト化したメッセージに含める事ができます。

ATSHA204A は、以下の文書に記載されているアルゴリズムに基づいて SHA-256 ダイジェストを計算します。

http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf

ATSHA204A によって処理される完全な SHA-256 メッセージは、このアルゴリズムを使う各コマンドの説明に記載しています。このアルゴリズムの最も標準的なソフトウェア実装は、自動的にこのメッセージに適切な数のパディング ビットを追加する事で、デバイス内部の演算に適合させます。

ATSHA204A は、SHA コマンドを使って SHA-256 ダイジェストを計算する事もできます。呼び出し側がメッセージにパディング バイトを提供します。メッセージサイズは、パディング バイトを含めて 64 の整数倍バイトである事が必要です。

SHA-256 アルゴリズムは、ハッシュ アルゴリズムの出力ダイジェストと平文データの間の XOR によってサイファーテキストを生成する事により、暗号化用に使われます。復号はこの逆の動作であり、サイファー テキストとダイジェストの間の XOR によって平文が得られます。

13.2 HMAC/SHA-256

チャレンジに対するレスポンスは、以下の文書に記載されている SHA-256 に基づく HMAC アルゴリズムを使って計算する事もできます。

http://csrc.nist.gov/publications/fips/fips198/fips-198a.pdf

HMAC コマンドは MAC コマンドほど柔軟ではなく、計算が複雑であるため計算時間も増加します。ダイジェストのセキュリティを確保する上で HMAC シーケンスは必須ではありませんが、各種ソフトウェア パッケージとの互換性を確保するために用意されています。

© 2019 Microchip Technology Inc.

13.3 鍵の値

SHA204A 内の全ての鍵は 256 ビット長です。ATSHA204A は、これらの鍵を MAC、CheckMac、HMAC、GenDig コマンドでハッシュ化されるメッセージの一部として使います。EEPROM の Data ゾーン内の全てのスロットが鍵の保存用に使えます。しかし、SlotConfig (IsSecret ビットを含む)内で読み書き許可が適切に設定されている場合にのみ、値の機密性が保たれます。

GenDig コマンドを除き、SlotID パラメータの最下位 4 ビットを除く全てのビットは、鍵データのソースの指定用に使われません。最下位の 4 ビットのみが、Data ゾーンのスロットの 1 つを選択するために使われます。GenDig による他の SlotID 値の使用法については**「トランスポート鍵」**を参照してください。

SHA-256 計算に Param2 が使われる場合、全てのケースで SlotID の 16 ビット全体が入力としメッセージに含まれます。

13.3.1 鍵の Diversify

ホストまたは検証の対象が秘密鍵を安全に保存する場所を有している場合、EEPROM スロットに保存された鍵の値はデバイスに書き込まれているシリアル番号(SN<0:8>)を使って diversify できます。これにより全てのクライアント デバイスが一意の鍵を持つ事ができ、既知平文攻撃に対する防御を強化できると共に、漏洩したシリアル番号を識別してブラックリストに入れる事ができます。

これを実装するには、パーソナライズ中に何らかの暗号アルゴリズムを使ってルート秘密鍵とデバイスのシリアル番号を外部で組み合わせ、その結果を ATSHA204A の鍵スロットに書き込みます。

ATSHA204A の CheckMac コマンドは、diversify された鍵を安全に生成および比較するための仕組みを提供します(ホストシステムからこれを提供する必要はありません)。

詳細は、以下のアプリケーション ノートを参照してください。

http://ww1.microchip.com/downloads/en/appnotes/doc8666.pdf

13.3.2 鍵のローリング

同じ鍵値が繰り返し使われる事を防ぐため、ATSHA204A は鍵のローリングをサポートします。通常、同じ鍵が決められた回数(最小で 1 回)使われた後に、現在の鍵値は、現在の鍵値と何らかのオフセット(定数、現在のシステムに関連する値(例: シリアル番号またはモデル番号)、乱数のいずれか)を組み合わせた SHA-256 ダイジェストに置き換えられます。

この機能は、DeriveKey コマンドを使って実装します。DeriveKey コマンドの実行前に、Nonce コマンドを実行して TempKey にオフセットを書き込んでおく必要があります。スロット 0～7 に対してローリング動作が実行されるたびに、スロットの UpdateCount フィールドがインクリメントします。

この機能の用途の 1 つは、元の鍵をデバイスから恒久的に削除し、特定の環境でのみ使える鍵に置き換える事です。鍵がローリングされた後に以前の値を取得する方法は存在しないため、システムのセキュリティが向上します。

Roll モードでの DeriveKey コマンドの実行中に停電した場合、鍵または UpdateCount の値は未知となります。SlotConfig の bit 14 を使ってスロットへの書き込みを有効にした場合、Write コマンドを使ってそのような鍵を暗号化/認証された形態で書き込む事ができます。あるいは、鍵の複数の複製を複数のスロットに保存する事で、1 つのスロットでの障害によってシステムの正常機能が損なわれる事を防げます。

© 2019 Microchip Technology Inc.

13.3.3 鍵の生成

全てのクライアント向けに一意の使い捨て鍵をサポートするため、ATSHA204A は鍵の生成もサポートします。この機能では、「ペアレント」鍵(SlotConfig.writeKey により指定)と固定または乱数ノンスの組み合わせから一意鍵を生成します。この鍵は、任意の暗号目的で使われます。

一意鍵の生成機能は、ペアレント鍵に使用制限がある場合に特に便利です(後述の **13.3.4「鍵の使用制限(スロット 0〜7)」**と **13.3.5「鍵の使用制限(スロット 15)」**参照)。このモードでは、使用制限付きのペアレント鍵を使って使用制限なしのチャイルド鍵を生成できます。チャイルド鍵は、この特定のホスト-クライアント ペアに対してのみ使えるため、その値が攻撃された場合の被害を軽減できます。

この機能も DeriveKey コマンドを使って実装します。DeriveKey コマンドの実行前に、Nonce コマンドを実行して TempKey にノンス値を書き込んでおく必要があります。スロット 0〜7 に対して鍵の生成動作が実行されるたびに、スロットの UpdateCount フィールドがインクリメントします。

13.3.4 鍵の使用制限(スロット 0〜7)

EEPROM の Data セクション内のスロット 0〜7 では、対応する SlotID 値によってそのスロットに保存されている鍵の使用回数を制限できます。この機能は、SlotConfig フィールド内の LimitedUse ビットがセットされている場合に有効です。スロット 8〜14 の LimitedUse ビットは無視されます。使用可能な残りの回数は、そのスロットに対応する UseFlag バイト内にビットマップとして保存されます。

そのスロットを鍵として使う全ての暗号コマンドの実行前に、以下を実行する必要があります。

- SlotConfig<SlotID>.LimitedUse がセットされ、かつ UseFlag<SlotID>が 0x00 である場合、デバイスはエラーを返します。
- UseFlag<SlotID>の bit 7 から下位に向かって最初に見つかる「1」のビットを「0」にクリアします。

実際には、この手順は DeriveKey コマンドを使った「リフレッシュ」と「リフレッシュ」の間に LimitedUse 鍵が 8 回使われる事を許可します。この機能を有効にした鍵を参照するコマンドの実行中に停電が発生した場合、コマンドが完了しなかったにもかかわらず UseFlag 内のビットの 1 つがクリアされる可能性があります。このため、鍵は 1 回だけ使う事を推奨します。この場合、他のビットはエラー時の安全マージンを提供します。

通常は、8 個の UseFlag バイトの全てを 0xFF に初期化します。これにより、各鍵の使用回数は 8 回以下に制限されます。これらのバイトは 0xFF (8 回)または 0x7F (7 回)、0x3F (6 回)、0x1F (5 回)、0x0F (4 回)、0x07 (3 回)、0x03 (2 回)、0x01 (1 回)のいずれかに初期化する必要があります。これら以外の値に初期化する事は禁止されます。

鍵の使用制限に関連する Read、Write、DeriveKey コマンドの動作は、以下で説明する通り、互いに少し異なります。

- **Read、Write**
  これらのコマンドは LimitedUse ビットの状態を無視します。これらのコマンドが実行されても UseFlag バイトは変化しません。SlotConfig による制限が適切であれば、UseFlag の値が 0x00 (残回数なし)になっても使用制限されたスロットは読み書きできますが、そのスロット内の値を暗号コマンド用の鍵として使う事はできなくなります。

  スロット X の SlotConfig.WriteKey が X 自身を指し、かつ UseFlag<X>が 0x00 (残回数なし)である場合、先に実行された GenDig コマンドは使用制限のためにエラーを返すため、そのスロットに対する暗号化された書き込みは失敗します。同様の状況は ReadKey を使う読み出しでも発生します。鍵として使われるスロットでは、IsSecret = 「0」または WriteConfig = 「always」に設定しない事が必要です。
- **DeriveKey**
  ペアレント鍵が認証用またはソースとして使われる場合、ペアレント鍵の limitedUse = 「1」かつ UseFlag = 0x00 であれば、DeriveKey コマンドはエラーを返します。ターゲット鍵の LimitedUse ビットと UseFlag ビットは無視されます。実行に成功した場合、DeriveKey は常に

© 2019 Microchip Technology Inc.

ターゲット鍵の UseFlag を 0xFF にリセットします。これが UseFlag をリセットする唯一の機能です。

DeriveKey コマンドの使用は必須ではありません。このスロット向けに WriteConfig<13>がセットされている場合にのみ、このコマンドを実行する必要があります。状況によっては、単純に 8 回使用可能な鍵を使うと都合が良い場合があります。その場合、その他の暗号コマンドは UseFlag 内のビットを一度に 1 つずつクリアし、全てのビットがクリアされた時点で鍵は無効になります。

13.3.5 鍵の使用制限(スロット 15)

Slot<15>.LimitedUse がセットされている場合、鍵 15 の使用は、前記の使用制限(スロット 0～7 にのみ適用)と異なる方法で制限されます。

暗号コマンドによって鍵 15 が使われる前に、以下が実行されます。

- LastKeyUse 内の全てのバイトが 0x00 である場合、エラーが返されます。
- LastKeyUse の最初のバイト(Configuration ゾーン内のバイト 68)の bit 7 から下位に向かって最初に見つかる「1」のビットを「0」にクリアします。バイト 68 が 0x00 である場合、バイト 69 の bit 7 がチェックされます。この手順は、バイト 83 に達するまで繰り返されます。鍵 15 の使用前に 1 つずつビットがクリアされます。

この使用制限にはリセットする仕組みはありません。使用回数が 128(またはパーソナライズで「1」にセットされた LastKeyUse 内のビットの数)に達した後、鍵 15 は恒久的に無効になります。この機能は、停電の影響をあまり受けません。コマンドの実行中に停電が発生しても、LastKeyUse 内の 1 個のビットが未知になるだけであり、LastKeyUse 内の他のビットは変更されず、鍵は変更されません。

鍵 15 の使用回数を 128 よりも少なく設定する場合、この配列内の一部のバイトを 0xFF に初期化しません。UseFlag と同様に、このフィールド内のバイトの値は、0xFF または 0x7F、0x3F、0x1F、0x0F、0x07、0x03、0x01、0x00 のいずれかである事が必要です。「1」にセットされたビットの総数が使用可能回数に対応します。

例: 使用回数を 16 に設定する場合

0xFF, 0xFF, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00,

0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00, 0x00

LimitedUse ビットは Read および Write コマンドによって無視され、それらのコマンドを実行しても LastKeyUse は変化しません。 LimitedUse bit は CheckMac コマンドの複製機能によって無視されます。 LimitedUse ビットは、DeriveKey コマンド内でペアレント鍵向けに使われますが、ターゲット鍵向けには無視されます。

13.3.6 パスワードの検証

多くのアプリケーションでは、各種機能(保存データの復号等)を有効にするために、ユーザはパスワードを入力する必要があります。通常、パスワードはメモリに保存されるため、パスワードが盗まれる恐れがあります。ATSHA204A はパスワードを安全に保存し、パスワードに対して各種の便利な演算を実行します。パスワードが平文の状態でデバイスに渡される事は決してなく、デバイスからパスワードを読み出す事はできません。パスワードは、デバイスに渡される前にシステム ハードウェア内で乱数を使ってハッシュ化されます。TempKey 内のノンスは、トランスポート鍵が使われる時に必ず内部 RNG を使って生成済みである事が必要です。

CheckMac コマンドの複製機能は、以下のパスワード検査オプションを有効にします。

1. CheckMac は内部で有効パスワードとの比較を行い、入力されたパスワードが正しいかどうかを示す論理値をシステムに返します。

2. 入力されたパスワードが正しいとデバイスが判断した場合、必要に応じてパスワード値と保存値または一時値を組み合わせる事で、システムがデータ保護用に使う鍵を生成できます。
3. 入力されたパスワードが正しいとデバイスが判断した場合、必要に応じてデバイスは第 2 の高エントロピ秘密鍵を生成できます。この鍵を使う事で、データを総当たり攻撃から保護できます。
4. パスワードが喪失した場合、ペアレント鍵の値を知っていれば、必要に応じてスロットに新しいパスワードを書き込む事ができます。必要に応じ、ペアレント鍵を使って現在の値を暗号化してデバイスから読み出す事ができます。

パスワードは偶数番号のスロットに保存する必要があります。パスワードに第 2 の値(上のステップ 3 参照)を割り当てた場合、この値を格納したターゲット スロットは次に番号の大きなスロット (パスワード スロット番号+1)に配置されます。そうではない場合、ターゲット スロットはパスワード スロットと同じです。

この機能を有効にするには、ターゲット スロットの ReadKey を 0x0 に設定する必要があります。この機能の不正な使用または偶発的な使用を防ぐため、この CheckMac/Copy 機能が特に必要ではない限り、どのスロットも ReadKey を 0x0 に設定しない事が必要です。特に、特定スロット向けのコンフィグレーション ワード内の他のビットが ReadKey = 0x0 によって有効にされたこの機能を無効にすると期待してはいけません。

この機能は、CheckMac に対する Mode パラメータの値が 0x01 または 0x05 であり、かつ TempKey.SourceFlag が Mode<2>に一致する場合にのみ有効です。

Note: Mode 0x05 を使う場合、システムはリプレイ攻撃の危険に曝されるため、注意が必要です。しかし、システム コンフィグレーションによっては、この設定が都合の良い場合もあります。

- SHA-256 メッセージの最初の 32 バイトは、EEPROM 内のデータスロットに保存されます(パスワード)。
- SHA-256 メッセージの次の 32 バイトは、TempKey レジスタ内のランダムに生成されたノンスである事が必要です。

上記の条件が成立し、かつ入力レスポンスが内部生成されたダイジェストと一致する場合、ターゲット鍵の内容が TempKey へ複製されます。TempKey レジスタの他のビットは以下の通りに設定されます。

- SourceFlag = 「1」 (非ランダム)
- GenData = 「0」(GenData コマンドによって生成されない)
- CheckFlag = 「0」(TempKey は CheckMac コマンドに対して制限されない)
- Valid = 「1」

13.3.7 トランスポート鍵

ATSHA204A は、Data セクションがロックされる前のセキュア パーソナライズ向けに鍵のハードウェア配列を備えています。ハードウェア鍵の値は秘密ですが、Microchip 社は要求に応じて有資格のお客様に鍵の値を開示します。これらの鍵は、GenDig コマンドでのみ使用でき、0x8000 以上の SlotID 値により指定されます。

GenDig コマンドを含む全てのコマンドにおいて、0x8000 未満の SlotID 値は EEPROM の Data ゾーン内に保存されている鍵を参照します。これらの場合、SlotID の最下位 4 ビットだけがスロット番号を指定するために使われます。SHA-256 メッセージの計算では、SlotID の 16 ビット全てが入力として使われます。

© 2019 Microchip Technology Inc.

14. 改訂履歴

リビジョン A (2018 年 4 月)
Microchip 社の書式による初版です。

本リビジョンは、Atmel 社文書(リビジョン 8885H、2015 年 11 月)に置き換わります。

© 2019 Microchip Technology Inc.

Microchip 社のウェブサイト

Microchip 社はウェブサイト(www.microchip.com)を通してオンライン サポートを提供しています。当ウェブサイトでは、お客様に役立つ情報やファイルを簡単に見つけ出せます。インターネット ブラウザから以下の内容がご覧になれます。

- **製品サポート** - データシートとエラッタ、アプリケーション ノートとサンプル プログラム、設計リソース、ユーザガイドとハードウェア サポート文書、最新のソフトウェアと過去のソフトウェア
- **技術サポート** – よく寄せられる質問(FAQ)、技術サポートのご依頼、オンライン ディスカッション グループ、Microchip 社のコンサルタント プログラムおよびメンバーリスト
- **ご注文とお問い合わせ** - 製品セレクタと注文ガイド、最新プレスリリース、セミナー/イベントの一覧、お問い合わせ先(営業所/販売代理店)の一覧

顧客変更通知サービス

Microchip 社の顧客変更通知サービスは、お客様に Microchip 社製品の最新情報をお届けする配信サービスです。ご興味のある製品ファミリまたは開発ツールに関する変更、更新、リビジョン、エラッタ情報をいち早くメールにてお知らせします。

Microchip 社ウェブサイト(http://www.microchip.com/)にアクセスし、[DESIGN SUPPORT]メニューの下の[Product Change Notification]からご登録ください。

カスタマサポート

Microchip 社製品をお使いのお客様は、以下のチャンネルからサポートをご利用になれます。

- 販売代理店
- 弊社営業所
- フィールド アプリケーション エンジニア(FAE)
- 技術サポート

サポートは販売代理店、販売担当者、フィールド アプリケーション エンジニア(FAE)にお問い合わせください。各地の営業所もご利用になれます。本書の最後のページには各国の営業所の一覧を記載しています。

技術サポートは以下のウェブページからもご利用になれます。http://www.microchip.com/support

© 2019 Microchip Technology Inc.

製品識別システム

ご注文や製品の価格、納期につきましては弊社または販売代理店にお問い合わせください。

PART NO. -XXX XX -X

Device Package I/O Type Tape and Reel

デバイス	ATSHA204A: セキュアなハードウェア ベース鍵ストレージを備えた暗号コプロセッサ	
パッケージ	SSH	= 8S1、8 ピン(0.150 インチ幅ボディ)、Plastic Gull Wing Small Outline (JEDEC SOIC)パッケージ
	MAH	= 8MA2、8 ピン 2x3x0.6 mm ボディ、熱的に強化された Plastic Ultra Thin Dual Flat No- Lead (UDFN)パッケージ
	RBH	= 3RB、3 ピン 2.5x6.5 mm ボディ、2.0 mm ピッチ、CONTACT パッケージ(Sawn)
I/O タイプ	CZ	= 単線式インターフェイス
	DA	= I^2C インターフェイス
テープ&リール オプション	B	= チューブ
	T	= ラージリール (サイズはパッケージタイプに応じて異なります)
	S	= スモールリール(MAH 向けにのみ提供)

例:

- ATSHA204A-SSHCZ-T: 単線式、テープ&リール、リールあたり 4,000 個、8 ピン SOIC パッケージ
- ATSHA204A-SSHCZ-B: 単線式、チューブ、チューブあたり 100 個、8 ピン SOIC パッケージ
- ATSHA204A-SSHDA-T: I^2C、テープ&リール、リールあたり 4,000 個、8 ピン SOIC パッケージ
- ATSHA204A-SSHDA-B: I^2C、チューブ、チューブあたり 100 個、8 ピン SOIC パッケージ
- ATSHA204A-MAHCZ-T: 単線式、テープ&リール、リールあたり 15,000 個、8 ピン UDFN パッケージ
- ATSHA204A-MAHDA-T: I^2C、テープ&リール、リールあたり 15,000 個、8 ピン UDFN パッケージ
- ATSHA204A-MAHCZ-S: 単線式、テープ&リール、リールあたり 3,000 個、8 ピン UDFN パッケージ
- ATSHA204A-MAHDA-S: I^2C、テープ&リール、リールあたり 3,000 個、8 ピン UDFN パッケージ
- ATSHA204A-RBHCZ-T: 単線式、テープ&リール、リールあたり 5,000 個、3 ピン Contact パッケージ
- ATSHA204A-RBHCZ-B: 単線式、チューブ、チューブあたり 56 個、3 ピン Contact パッケージ
- ATSHA204A-STUCZ-T: 単線式、テープ&リール、リールあたり 5000 個、3 ピン SOT-23 パッケージ
- ATSHA204A-XHDA-T: I^2C、テープ&リール、リールあたり 5000 個、 8 ピン TSSOP パッケージ
- ATSHA204A-XHCZ-T: 単線式、テープ&リール、リールあたり 5000 個、8 ピン TSSOP パッケージ

© 2019 Microchip Technology Inc.

Note:

1. テープ&リールの識別情報は、カタログの製品番号説明に記載しています。これは製品の注文時に使う識別情報であり、デバイスのパッケージには印刷していません。テープ&リールが選択できるパッケージの在庫/供給状況は、弊社にお問い合わせください。
2. 小型パッケージ オプションがご利用になれる場合があります。小型パッケージについては http://www.microchip.com/ packaging をご覧になるか、弊社または代理店までお問い合わせください。

Microchip 社のデバイスコード保護機能

Microchip 社製デバイスのコード保護機能について以下の点にご注意ください。

- Microchip 社製品は、該当する Microchip 社データシートに記載の仕様を満たしています。
- Microchip 社では、通常の条件ならびに仕様に従って使用した場合、Microchip 社製品のセキュリティ レベルは、現在市場に流通している同種製品の中でも最も高度であると考えています。
- しかし、コード保護機能を解除するための不正かつ違法な方法が存在する事もまた事実です。弊社の理解では、こうした手法は全て、Microchip 社データシートにある動作仕様書以外の方法で Microchip 社製品を使用する事になります。このような行為は知的所有権の侵害に該当する可能性が非常に高いと言えます。
- Microchip 社は、コードの保全性に懸念を抱いているお客様と連携し、対応策に取り組んでいきます。
- Microchip 社を含む全ての半導体メーカーで、自社のコードのセキュリティを完全に保証できる企業はありません。コード保護機能とは、Microchip 社が製品を「解読不能」として保証するものではありません。

コード保護機能は常に進歩しています。Microchip 社では、常に製品のコード保護機能の改善に取り組んでいます。Microchip 社のコード保護機能の侵害は、デジタル ミレニアム著作権法に違反します。そのような行為によってソフトウェアまたはその他の著作物に不正なアクセスを受けた場合、デジタル ミレニアム著作権法の定める所により損害賠償訴訟を起こす権利があります。

法律上の注意点

本書に記載されているデバイス アプリケーション等の情報は、ユーザの便宜のためにのみ提供されるものであり、更新によって無効とされる事があります。お客様のアプリケーションが仕様を満たす事を保証する責任は、お客様にあります。Microchip 社は、明示的、暗黙的、書面、口頭、法定のいずれであるかを問わず、本書に記載されている情報に関して、状態、品質、性能、商品性、特定目的への適合性をはじめとする、いかなる類の表明も保証も行いません。
Microchip 社は、本書の情報およびその使用に起因する一切の責任を否認します。Microchip 社の明示的な書面による承認なしに、生命維持装置あるいは生命安全用途に Microchip 社の製品を使用する事は全て購入者のリスクとし、また購入者はこれによって発生したあらゆる損害、クレーム、訴訟、費用に関して、Microchip 社は擁護され、免責され、損害をうけない事に同意するものとします。特に明記しない場合、暗黙的あるいは明示的を問わず、Microchip 社が知的財産権を保有しているライセンスは一切譲渡されません。

商標

Microchip 社の名称とロゴ、Microchip ロゴ、 AnyRate、AVR、AVR ロゴ、AVR Freaks、BeaconThings、BitCloud、CryptoMemory、CryptoRF、dsPIC、FlashFlex、flexPWR、Heldo、JukeBlox、KeeLoq、KeeLoq ロゴ、Kleer、LANCheck、LINK MD、maXStylus、maXTouch、MediaLB、megaAVR、MOST、MOST ロゴ、MPLAB、OptoLyzer、PIC、picoPower、PICSTART、PIC32 ロゴ、Prochip Designer、QTouch、RightTouch、SAM-BA、SpyNIC、SST、SST ロゴ、SuperFlash、tinyAVR、UNI/O、XMEGA は米国およびその他の国における Microchip Technology Incorporated の登録商標です。

© 2019 Microchip Technology Inc.

ClockWorks、The Embedded Control Solutions Company、EtherSynch、Hyper Speed Control、HyperLight Load、IntelliMOS、mTouch、Precision Edge、Quiet-Wire は米国における Microchip Technology Incorporated 社の登録商標です。

Adjacent Key Suppression、AKS、Analog-for-the-Digital Age、Any Capacitor、AnyIn、AnyOut、BodyCom、chipKIT、chipKIT ロゴ、CodeGuard、CryptoAuthentication、CryptoCompanion、CryptoController、dsPICDEM、dsPICDEM.net、Dynamic Average Matching、DAM、ECAN、EtherGREEN、In-Circuit Serial Programming、ICSP、Inter-Chip Connectivity、JitterBlocker、KleerNet、KleerNet ロゴ、Mindi、MiWi、motorBench、MPASM、MPF、MPLAB Certified ロゴ、MPLIB、MPLINK、MultiTRAK、NetDetach、Omniscient Code Generation、PICDEM、PICDEM.net、PICkit、PICtail、PureSilicon、QMatrix、RightTouch ロゴ、REAL ICE、Ripple Blocker、SAM-ICE、Serial Quad I/O、SMART-I.S.、SQI、SuperSwitcher、SuperSwitcher II、Total Endurance、TSHARC、USBCheck、VariSense、ViewSpan、WiperLock、Wireless DNA、ZENA は、米国およびその他の国における Microchip Technology Incorporated の商標です。

SQTP は、米国における Microchip Technology Incorporated のサービスマークです。

Silicon Storage Technology は、米国以外の国における Microchip Technology Inc.の登録商標です。

GestIC は、米国以外の国における Microchip Technology Inc.の子会社である Microchip Technology Germany II GmbH & Co. KG の登録商標です。

その他の商標は各社に帰属します。

© 2018, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

ISBN: 978-1-5224-4383-4

DNV による品質管理システム認証

ISO/TS 16949

Microchip 社では、Chandler および Tempe(アリゾナ州)、Gresham(オレゴン州)の本部、設計部およびウェハー製造工場そしてカリフォルニア州とインドのデザイン センターが ISO/TS-16949:2009 認証を取得しています。Microchip 社の品質システムプロセスおよび手順は、PIC® MCU および dsPIC® DSC、KEELOQ®コード ホッピング デバイス、シリアル EEPROM、マイクロペリフェラル、不揮発性メモリ、アナログ製品に採用されています。さらに、開発システムの設計と製造に関する Microchip 社の品質システムは ISO 9001:2000 認証を取得しています。

各国の営業所とサービス

北米	アジア/太平洋	アジア/太平洋	ヨーロッパ
本社 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel:480-792 -7200 Fax:480-792 -7277 技術サポート: http://www.microchip.com/ サポート URL: www.microchip.com **アトランタ** Duluth, GA Tel:678-957 -9614 Fax:678-957-1455 **オースティン、TX** Tel:512-257 -3370 **ボストン** Westborough, MA Tel:774-760 -0087 Fax:774-760-0088 **シカゴ** Itasca, IL Tel:630-285 -0071 Fax:630-285-0075 **ダラス** Addison, TX Tel:972-818 -7423 Fax:972-818-2924 **デトロイト** Novi, MI Tel:248-848 -4000 **ヒューストン、TX** Tel:281-894 -5983 **インディアナポリス** Noblesville, IN Tel:317-773 -8323 Fax:317-773-5453 Tel:317-536 -2380 **ロサンゼルス** Mission Viejo, CA Tel:949-462 -9523 Fax:949-462-9608 Tel:951-273 -7800 **ローリー、NC** Tel:919-844 -7510 **ニューヨーク、NY** Tel:631-435 -6000 **サンノゼ、CA** Tel:408-735 -9110 Tel:408-436 -4270 **カナダ - トロント** Tel:905-695-1980 Fax:905-695-2078	**オーストラリア - シドニー** Tel:61-2-9868-6733 **中国 - 北京** Tel:86-10-8569-7000 **中国 - 成都** Tel:86-28-8665-5511 **中国 - 重慶** Tel:86-23-8980-9588 **中国 - 東莞** Tel:86-769-8702-9880 **中国 - 広州** Tel:86-20-8755-8029 **中国 - 杭州** Tel:86-571-8792-8115 **中国 - 香港 SAR** Tel:852-2943 -5100 **中国 - 南京** Tel:86-25-8473-2460 **中国 - 青島** Tel:86-532-8502-7355 **中国 - 上海** Tel:86-21-3326-8000 **中国 - 瀋陽** Tel:86-24-2334-2829 **中国 - 深圳** Tel:86-755-8864-2200 **中国 - 蘇州** Tel:86-186-6233-1526 **中国 - 武漢** Tel:86-27-5980-5300 **中国 - 西安** Tel:86-29-8833-7252 **中国 - 厦門** Tel:86-592 -2388138 **中国 - 珠海** Tel:86-756 -3210040	**インド - バンガロール** Tel:91-80-3090-4444 **インド - ニューデリー** Tel:91-11-4160-8631 **インド - プネ** Tel:91-20-4121-0141 **日本 - 大阪** Tel:81-6-6152-7160 **日本 - 東京** Tel:81-3-6880- 3770 **韓国 - 大邱** Tel:82-53-744-4301 **韓国 - ソウル** Tel:82-2-554-7200 **マレーシア - クアラルンプール** Tel:60-3-7651-7906 **マレーシア - ペナン** Tel:60-4-227-8870 **フィリピン - マニラ** Tel:63-2-634-9065 **シンガポール** Tel:65-6334 -8870 **台湾 - 新竹** Tel:886-3-577-8366 **台湾 - 高雄** Tel:886-7-213-7830 **台湾 - 台北** Tel:886-2-2508-8600 **タイ - バンコク** Tel:66-2-694-1351 **ベトナム - ホーチミン** Tel:84-28-5448-2100	**オーストリア - ヴェルス** Tel:43-7242-2244-39 Fax:43-7242-2244-393 **デンマーク - コペンハーゲン** Tel:45-4450 -2828 Fax:45-4485-2829 **フィンランド - エスポー** Tel:358-9-4520-820 **フランス - パリ** Tel:33-1-69-53-63-20 Fax:33-1-69-30-90-79 **ドイツ - ガーヒング** Tel:49-8931 -9700 **ドイツ - ハーン** Tel:49-2129 -3766400 **ドイツ - ハイルブロン** Tel:49-7131-67-3636 **ドイツ - カールスルーエ** Tel:49-721 -625370 **ドイツ - ミュンヘン** Tel:49-89-627-144-0 Fax:49-89-627-144-44 **ドイツ - ローゼンハイム** Tel:49-8031-354-560 **イスラエル - ラーナナ** Tel:972-9-744-7705 **イタリア - ミラノ** Tel:39-0331 -742611 Fax:39-0331-466781 **イタリア - パドヴァ** Tel:39-049 -7625286 **オランダ - ドリューネン** Tel:31-416 -690399 Fax:31-416-690340 **ノルウェー - トロンハイム** Tel:47-7289 -7561 **ポーランド - ワルシャワ** Tel:48-22 -3325737 **ルーマニア - ブカレスト** Tel:40-21-407-87-50 **スペイン - マドリッド** Tel:34-91-708-08-90 Fax:34-91-708-08-91 **スウェーデン - ヨーテボリ** Tel:46-31-704-60-40 **スウェーデン - ストックホルム** Tel:46-8-5090-4654 **イギリス - ウォーキンガム** Tel:44-118-921-5800 Fax:44-118-921-5820

© 2019 Microchip Technology Inc.