AN99209

PSoC® 4 BLE および PRoC™ BLE: Bluetooth LE 4.2 の特長

著者: utsv@cypress.com; sasd@cypress.com; ankc@cypress.com

関連製品ファミリ: CYBL11X7X および CY8C4XX8-BL5XX

関連アプリケーション ノート: 完全な一覧については、こちらをクリックしてください。

本アプリケーション ノートの最新版または関連プロジェクト ファイルについては、http://www.cypress.com/AN99209 をご覧ください。

本アプリケーション ノート (AN99209) は、Bluetooth Low Energy (BLE) 4.2 の機能、利点、およびアプリケーションの概要を説明します。また、アプリケーションがサイプレスの PSoC 4／PRoC BLE 4.2 デバイスを用いてこれらの機能を使用する方法についても説明します。

目次

1 はじめに 1
2 PSoC／PRoC リソース 2
3 PSoC Creator 3
3.1 PSoC Creator ヘルプ 3
3.2 サンプル コード 4
4 BLE 4.2 機能のご紹介 5
5 LE データ パケット長拡張 5
5.1 利点 6
5.2 アプリケーション 8
5.3 PSoC Creator における LE データ パケット長拡張機能を使用したアプリケーション開発 8
6 Low Energy セキュア コネクション 9
6.1 ペアリング プロセスへのアップデート 10
6.2 利点 13
6.3 アプリケーション 13
6.4 PSoC Creator で LE セキュア コネクションを使用したアプリケーション開発 13
7 Link Layer (LL) プライバシー 15
7.1 プライバシーのご紹介 15
7.2 プライバシー コンセプト 15
7.3 利点 19
7.4 アプリケーション 20
7.5 Link Layer プライバシーを採用したアプリケーションの PSoC Creator による開発 20
8 まとめ 23
9 関連アプリケーション ノート 23
A 受動的盗聴に対する防止 24
B 中間者 (MITM) 攻撃に対する防止 25
B.1 数値比較アソシエーション モデル 25
B.2 パスキー入力アソシエーション モデル 27
B.3 帯域外 (OOB) アソシエーション モデル 27
改訂履歴 28
ワールドワイドな販売と設計サポート 29

1 はじめに

2014 年 12 月 2 日に、Bluetooth スペシャル インタレスト グループ (SIG) は Bluetooth コア仕様バージョン 4.2 をリリースしました。このバージョンでは次の 3 つの主な機能を紹介しました: LE データ パケット長拡張機能、Link Layer プライバシー機能 (Privacy 1.2 とも呼ばれる)、および LE セキュア コネクション機能です。この 3 つの機能により、Bluetooth Low Energy (BLE; Bluetooth Smart とも呼ばれる) デバイスがよりスマートで、より速く、より安全になり、モノのインターネット (IoT) には最適です。仕様書をこちらからダウンロードしていただけます。

サイプレスの PRoC BLE (CYBL11X7X) および PSoC 4 BLE (CY8C4XX8-BL5XX) デバイスは Bluetooth 4.2 仕様に完全に準拠しており、これら 3 つの新機能をサポートします。また、これらのデバイスは、CPU の介入なしにデータ転送を可能にする DMA コントローラーも備えます。さらに、256KB のフラッシュおよび 32KB の RAM を内蔵しており、外部メモリを必要とせずに無線 (OTA) ファームウェアの更新を実現できます。レガシーBLE デバイスは、PSoC Creator 内の BLE コンポーネントをバージョン 3.0 以降にアップグレードすることにより LE セキュア コネクション機能をサポートします。表 1 は、サイプレスの異なるデバイスがサポートする Bluetooth 4.2 の機能をまとめています。

表 1. サイプレスのデバイスでサポートされる Bluetooth の新機能

機能	Bluetooth 4.1 対応のデバイス	Bluetooth 4.2 対応のデバイス
LE データ パケット長拡張	無	有
Link Layer プライバシー	無	有
LE セキュア コネクション	有	有

本アプリケーション ノートは、Bluetooth 4.2 の新機能、利点、およびサイプレスの PRoC BLE と PSoC 4 BLE デバイスを用いてアプリケーションで使用する方法の基本を説明します。本資料は、読者が BLE アーキテクチャおよび関連技術用語についての基礎知識を持っていることを前提とします。

- BLE または PSoC の初心者である場合、アプリケーション ノート「AN91627 - Getting Started with PSoC® 4 BLE」または「AN94020 - Getting Started with PRoC™ BLE」を参照してください。
- PSoC Creator における BLE コンポーネントを理解し、標準 BLE サービスに基づいてアプリケーションを開発する方法を学ぶには、アプリケーション ノート「AN91184 - PSoC 4 BLE Designing BLE Applications」を参照してください。
- Bluetooth 仕様については、Bluetooth SIG ウェブサイトをご覧ください。

2 PSoC／PRoC リソース

サイプレスは、www.cypress.com に大量のデータを掲載しており、ユーザーがデザインに適切な PSoC (プログラマブル システムオンチップ) および PRoC (プログラマブル ラジオオンチップ) デバイスを選択し、迅速かつ効率的にデバイスをデザインに統合する手助けをします。リソースの包括的なリストについては、「KBA86521 - How to Design with PSoC 3, PSoC 4, and PSoC 5LP」を参照してください。以下は PSoC 4 BLE および PRoC BLE のリソースの要約です。

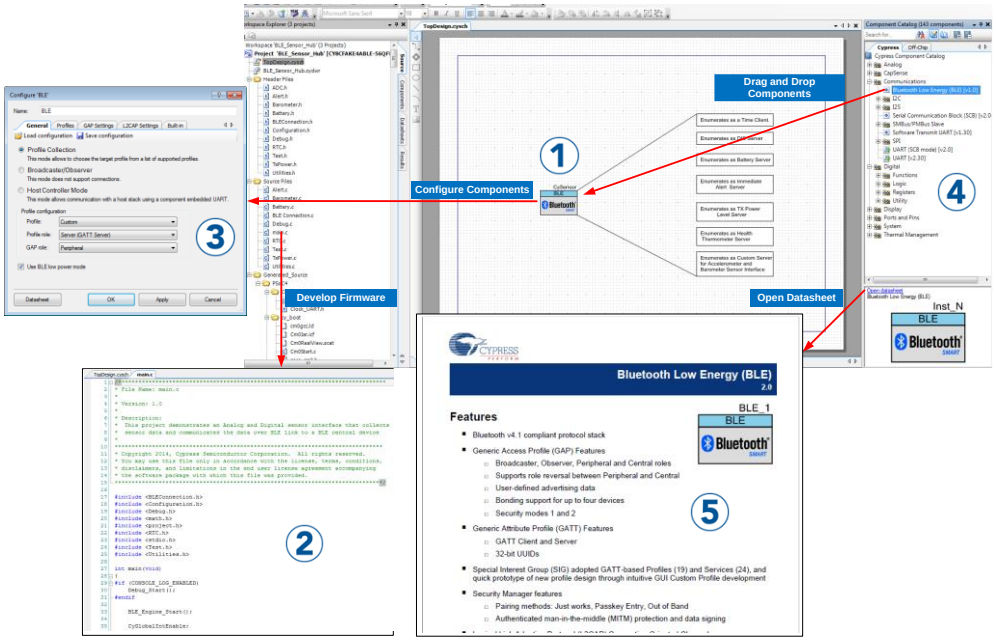
- **概要:** Bluetooth® Low Energy ポートフォリオ、サイプレス ワイヤレス／RF ロードマップ
- **製品セレクター:** PSoC 4 BLE または PRoC BLE。また、PSoC Creator にはデバイス選択ツールも含まれます。
- **データシート**は PSoC 4 BLE および PRoC BLE デバイス ファミリの電気的仕様を説明します。
- **CapSense 設計ガイド:** PSoC 4、PSoC 4 BLE、および PRoC BLE ファミリのデバイスを使用して静電容量タッチ センシング アプリケーションを設計する方法について説明します。
- **アプリケーション ノートおよびサンプル コード**は基本的なレベルから高度なレベルまでの幅広いトピックに触れます。多くのアプリケーション ノートはサンプル コードを含みます。
- **テクニカル リファレンス マニュアル (TRM)** は PSoC 4 BLE および PRoC BLE デバイスのアーキテクチャとレジスタについて詳細に説明します。
- **開発キット:**
  - CY8CKIT-042-BLE の BLE Pioneer Kit により、ユーザーは PSoC 4 BLE および PRoC BLE デバイスを使用して BLE アプリケーションを評価および開発できます。
  - Bluetooth 4.2 ラジオを搭載している CY8CKIT-143A の PSoC 4 BLE 256KB モジュールにより、ユーザーは CY8C4XX8-BL5XX ファミリのデバイスを評価できます。
  - Bluetooth 4.2 ラジオを搭載している CY5676A の PRoC BLE 256KB モジュールにより、ユーザーは CYBL11X7X ファミリのデバイスを評価できます。
  - CY5677 の CySmart BLE 4.2 USB ドングルにより、ユーザーは CySmart PC ツールで BLE 4.2 の機能をテストおよびデバッグできます。
  - CY5682 の PRoC BLE タッチ マウス リファレンス デザイン キット (RDK) を使用し、BLE タッチ マウスの完全な量産品の開発が可能です。
  - CY5672 の PRoC BLE リモコン リファレンス デザイン キット (RDK) を使用し、BLE リモコンの完全な量産品の開発が可能です。
- **MiniProg3** デバイスは、フラッシュのプログラミングとデバッグ用のインターフェースを提供します。
- **CySmart** は Windows PC 用の BLE ホスト エミュレーション ツールです。このツールはユーザーが BLE ペリフェラル アプリケーションをテストおよびデバッグするために使いやすい GUI を提供します。
- **モバイル アプリケーションの CySmart** はサイプレスにより開発される Android™／iOS®アプリケーションです。これらのアプリケーションは、サイプレスの BLE 開発キットを含む、様々な BLE 製品に接続し検証するために使用されます。
- **サイプレスのカスタム BLE プロファイルおよびサービス:** サイプレスはいくつかの BLE プロファイルおよびサービスを定義しました。これにより、ユーザーは Bluetooth SIG によって指定された標準 BLE プロファイルおよびサービスがサポートしていない機能に対して BLE を介してデータを送信できます。

3 PSoC Creator

PSoC Creator は無料で利用できる Windows ベースの統合開発環境 (IDE) です。これは、PSoC 3、PSoC 4、PSoC 4 BLE、PRoC BLE、および PSoC 5LP ベース システムのハードウェアとファームウェアの同時設計を可能にします。図 1 に示すように、PSoC Creator を使用すれば、以下のことができます。

1. コンポーネントをドラッグ &ドロップして、メイン デザイン ワークスペースでハードウェア システム デザインを構築
2. アプリケーションのファームウェアと PSoC ハードウェアを相互設計
3. コンフィギュレーション ツールを用いてコンポーネントを設定
4. 100 以上のコンポーネントを含むライブラリを利用
5. コンポーネント データシートをレビュー

図 1. PSoC Creator の回路図エントリ入力コンポーネント



3.1 PSoC Creator ヘルプ

PSoC Creator ホームページへアクセスし、PSoC Creator の最新版をダウンロードしてインストールしてください。次に、PSoC Creator を起動して、以下の項目を開きます。

- **Quick Start Guide** (クイック スタート ガイド): **Help** > **Documentation** > **Quick Start Guide** を選択します。このガイドは PSoC Creator プロジェクトを開発するための基礎知識を提供します。
- **Simple Component Code Examples** (シンプルなコンポーネントのサンプル コード): **File** > **Code Example** を選択します。これらのサンプル コードは、PSoC Creator のコンポーネントの設定と使用方法を示します。
- **System Reference Guide** (システム リファレンス ガイド): **Help** > **System Reference Guide** を選択します。このガイドは、PSoC Creator が提供するシステム機能を記載し説明します。
- **Component datasheets** (コンポーネント データシート): コンポーネントを右クリックして「Open Datasheet」を選択します。すべての PSoC 4／PRoC BLE コンポーネント データシートの一覧を表示するには、PSoC 4／PRoC BLE コンポーネント データシート ページをご覧ください。
- **Document Manager** (ドキュメント マネージャー): PSoC Creator が提供するドキュメント マネージャーにより、ドキュメント リソースを容易に検索し、レビューできます。Document Manager を開くには、メニューから **Help** > **Document Manager** を選択します。

3.2 サンプル コード

PSoC Creator は多数のサンプル コードを提供します。これらのプロジェクトは、図 2 に示すように、PSoC Creator のスタート ページから利用可能です。

サンプル コードにより、空のページの代わりに完成した設計から始めることで設計時間を短縮させることができます。サンプル コードはまた、PSoC Creator コンポーネントを様々なアプリケーションに使用する方法を示します。

図 3 に示す **Find Example Project** ダイアログにはいくつかのオプションがあります。

- アーキテクチャ、デバイス ファミリ (PSoC 4、PSoC 4 BLE、PRoC BLE など)、カテゴリまたはキーワードで絞り込んでサンプル コードを検索します。
- **Filter Options** に基づいて提供されたサンプル プロジェクトのメニューから選択します。図 3 に示すように、ご参考のための 30 以上の BLE サンプル コードがあります。
- 選択したデータシートをレビューします (**Documentation** タブ)。
- 選択したサンプル コードをレビューします。このウィンドウからコードをプロジェクトにコピー＆ペーストして、コード開発時間を短縮させることができます。
- さらに、選択に応じて新規プロジェクト (また、必要な場合は新規ワークスペース) を作成できます。完成した基本的設計から開始することで設計時間を短縮できます。その後、設計をアプリケーションに適合させることができます。

PSoC Creator のサンプル コードに加えて、サイプレスの GitHub リポジトリから BLE サンプル プロジェクトを見ることもできます。

図 2. PSoC Creator のサンプル コード

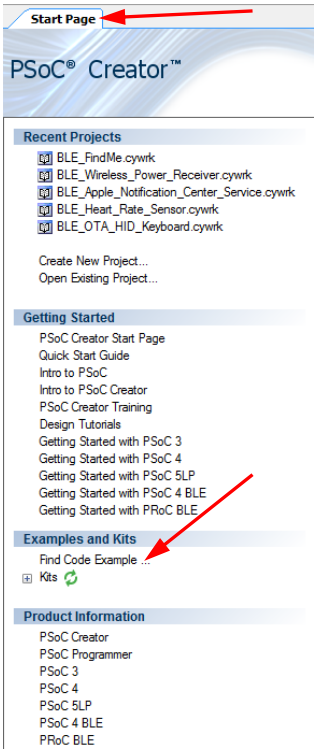
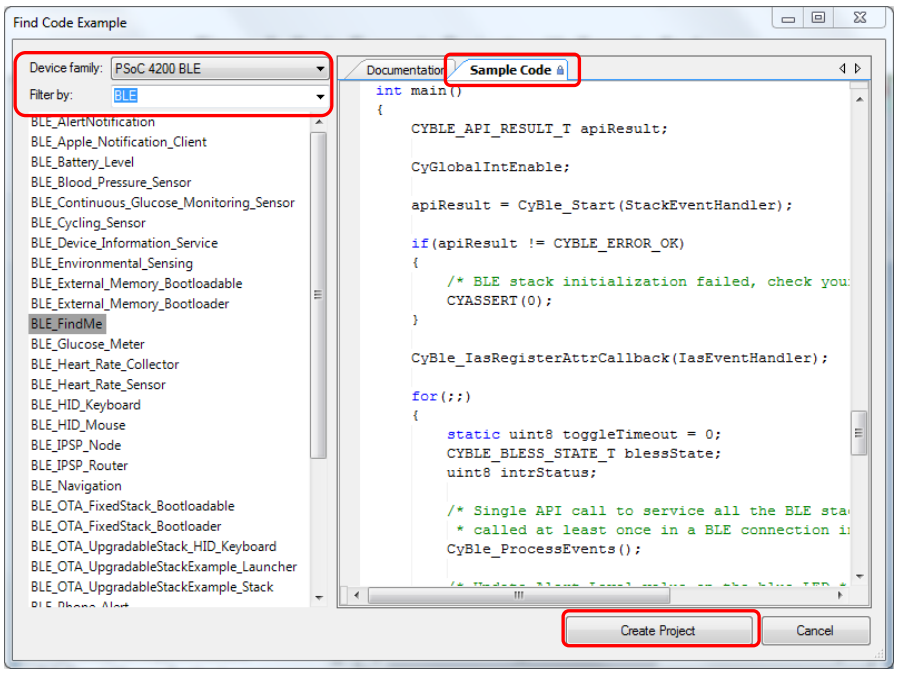


図 3. コード例およびサンプル コード



4 BLE 4.2 機能のご紹介

Bluetooth 4.2 は、LE データ パケット長拡張、Link Layer (LL) プライバシー、および Low Energy セキュア コネクションという 3 つの主な機能を紹介しました。次の節では、それぞれの新機能を詳細に説明します。

5 LE データ パケット長拡張

Link Layer (LL) は BLE プロトコル スタックの一部分であり、宣伝、スキャン、接続の確立および保持を行います。

Link Layer パケットのフォーマットは図 4 に示されます。それぞれのパケットには 4 つのフィールドが含まれます。プリアンブル、アクセス アドレス、プロトコル データ ユニット (PDU)、および巡回冗長検査 (CRC) です。宣伝、スキャン、または接続の確立手順中に送信されるパケットは宣伝チャネル PDU を使用します。接続されたデバイスにデータを共有するために送信されるパケットはデータ チャネル PDU を使用します。

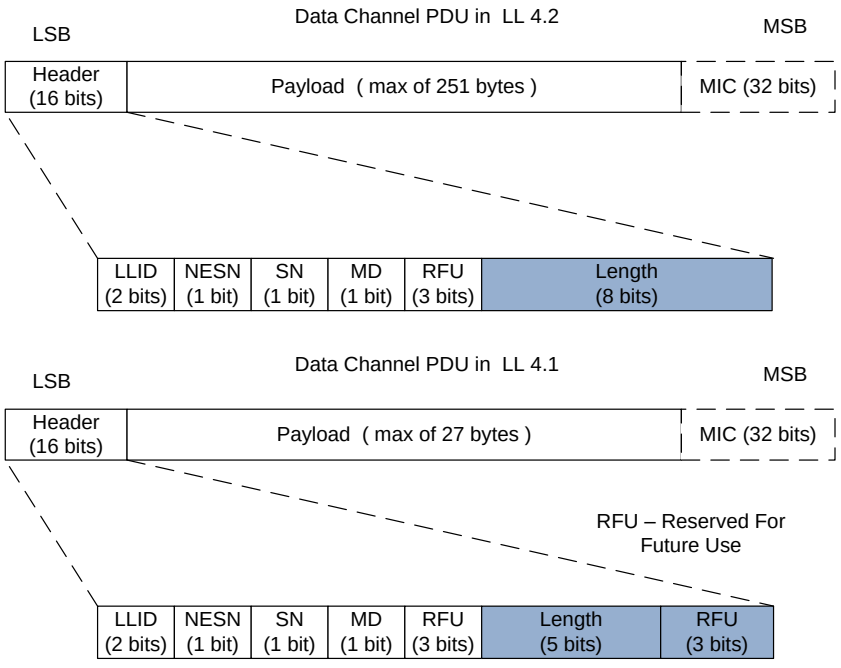
図 4. Link Layer パケットのフォーマット

Preamble (1 byte)	Access Address (4 bytes)	Data Protocol Data Unit (PDU) (2 to 257 bytes in BLE 4.2 & 2 to 33 bytes in BLE 4.1)	CRC (3 bytes)

データ チャネル PDU は、16 ビットのヘッダー、サイズ可変なペイロード フィールド、およびオプションのメッセージ インテグリティ チェック (MIC) フィールドを含みます。Bluetooth 4.2 仕様では、データ チャネル PDU 内のペイロード フィールドの最大サイズが 27 バイトから 251 バイトに増えるため、データ チャネル自体の容量も約 10 倍になります (より高いスループットを参照してください)。

図 5 は、Bluetooth 4.2 と Bluetooth 4.1 におけるデータ チャネル PDU の違う点を示します。

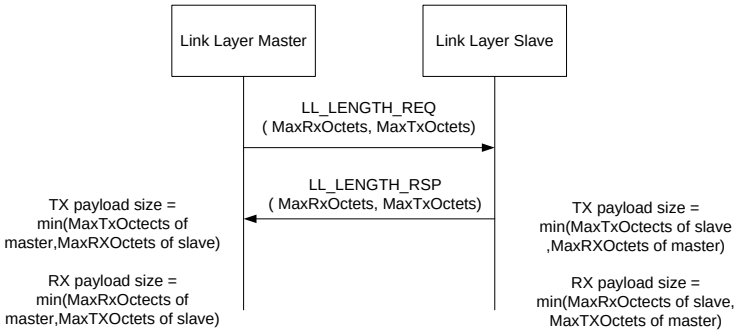
図 5. Bluetooth 仕様バージョン 4.2 と 4.1 における LE データ チャネル PDU



ヘッダーにある長さフィールドはヘッダーの後に続くデータ バイト数を指定します。ヘッダーにある長さフィールドのサイズは、Bluetooth 4.1 仕様では 5 ビットであるが、Bluetooth 4.2 仕様では 8 ビットに増えるため、長さフィールドの値範囲が 31 から 255 に増えます。暗号化されたパケットで使用されるメッセージ インテグリティ チェック (MIC) の長さは 4 バイトです。そのため、可能な最大ペイロード サイズは Bluetooth 4.2 では 251 バイトで、Bluetooth 4.1 では 27 バイトです。ヘッダー部の他のフィールドについては、「Bluetooth Core Specification Version 4.2」、第 6 巻、第 B 部、2.4 節を参照してください。

Link Layer は、図 6 に示すように、データ長更新手順を使用して送信方向および受信方向で使用されるペイロード サイズを調整します。新規に追加された 2 つの Link Layer 制御 PDU である LL_LENGTH_REQ および LL_LENGTH_RSP は、デバイスによりサポートされる最大ペイロード サイズを交換するために使用されます。デバイスにより送信される最大ペイロード サイズは MaxTxOctets、デバイスにより受信される最大ペイロード サイズは MaxRxOctets と呼ばれます。送信 (TX) および受信 (RX) の実際のペイロード サイズはデータ長更新手順により判定されます。実際の TX ペイロード サイズはローカルの MaxTxOctets とピアの MaxRxOctets パラメーターの最小値であり、同様に、実際の RX ペイロード サイズはローカルの MaxRxOctets とピアの MaxTxOctets パラメーターの最小値です。Link Layer は、データ長更新手順が完了するまで、27 バイトのデフォルトのペイロード サイズを使用します。この機能をサポートしないデバイスは、LL_LENGTH_REQ の PDU を受信した際に LL_UNKNOWN_RSP の PDU で応答します。その場合、Link Layer は 27 バイトのデフォルト ペイロード サイズを使用します。

図 6. データ長更新手順



5.1 利点

LE データ パケット長拡張機能により、アプリケーションはより高いスループット、より低い消費電力、および非対称の帯域幅を実現できます。これらの利点は、以下の条件を満たした場合にのみ実現できます。

- 両方の BLE デバイスが LE データ パケット長拡張機能をサポート
- 上位層のプロトコルが最大伝送単位 (MTU) サイズのデフォルト値 (23 バイト) よりも大きなサイズを使用

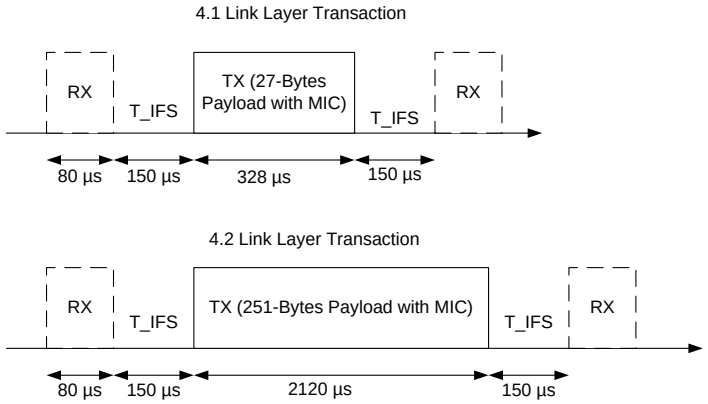
5.1.1 より高いスループット

LE データ パケット長拡張機能により、Link Layer を介して約 2.6 倍のより高いスループットを実現できます。図 4 は Link Layer パケットのフォーマットを示し、図 5 はデータ チャネル PDU の様々なフィールドを示します。MIC フィールドは、ペイロード サイズが 0 でないデータ チャネル PDU の暗号化されたパケットのみに追加されます。

ペイロード サイズが 0 バイトの場合、パケットの最短転送時間が 80µs です。Bluetooth 4.1 では、パケットの最長転送時間は 328µs (ペイロード サイズが 27 バイト) です。Bluetooth 4.2 では、パケットの最長転送時間は 2120µs (ペイロード サイズが 251 バイト) です。

図 7 には、Bluetooth 4.1 および Bluetooth 4.2 それぞれの場合のデータ転送中の一般的な Link Layer トランザクションを示します。単一のデータ パケットのトランザクションは、パケットを含まない RX (ペイロード サイズ=0)、150µs のフレーム間隔時間 (T_IFS)、ペイロード サイズが最大なパケットの TX、および T_IFS から構成されます。次の RX 動作が行われると 1 つのトランザクションが終了します。その時点で手順が繰り返されます。図に示している 2 番目の RX は、最初の TX パケットが認識され、新しいトランザクションが開始するところです。

図 7. Link Layer のトランザクション



Link Layer のスループット (すなわち、BLE プロトコル スタックの上位層に利用可能なスループット) は以下のように定義されます。

スループット = ペイロード サイズ / 単一トランザクションの時間

Bluetooth 4.1 では、ペイロード サイズが 27 バイト (216 ビット) であり、単一トランザクションの合計時間が 708µs です。よって、理論上のスループットが 298kbps になります。

Bluetooth 4.2 では、ペイロード サイズが 251 バイト (2008 ビット) で、合計時間が 2500µs であるため、理論的なスループットが 784kbps になります。これで、Bluetooth 4.1 のデバイスに比べて、 Bluetooth 4.2 のデバイスでは約 2.6 倍のスループットが得られます。

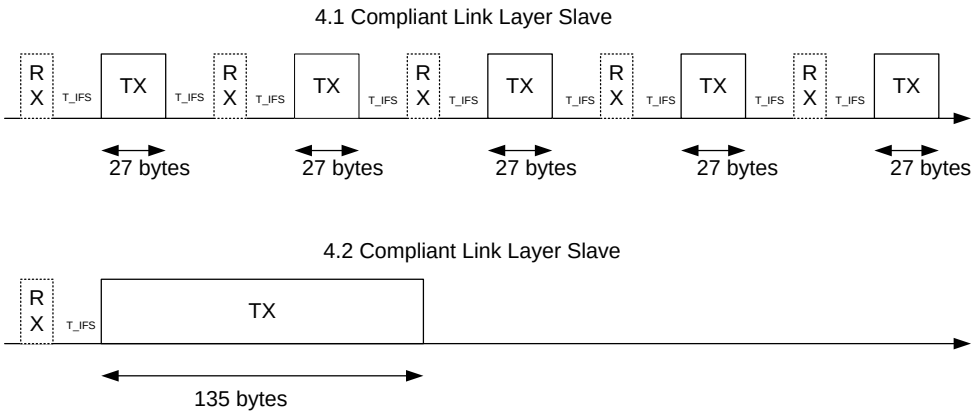
5.1.2 低消費電力

エア干渉がないという理想的な状況下では、LE データ パケット長拡張機能は、帯域幅をより効率良く使用することで消費電力を削減するのに役立ちます。

Bluetooth 4.2 では、一定のデータを転送するのに必要なトランザクションの数は Bluetooth 4.1 に比べて少ないです。これは、ラジオがアクティブ状態にある時間を減少させ、デバイスが低電力モードにある時間を長めにすることで、平均電流消費量を削減します。

図 8 に示しているのは、135 バイトの Link Layer ペイロードを仮定した場合のメカニズムです。Bluetooth 4.1 では、135 バイトのペイロードが 27 バイトのペイロードに分割され、5 つのトランザクションで送信されます。Bluetooth 4.2 では、135 バイトのペイロードが単一のトランザクション内で送信されます。

図 8. 135 バイトのデータ転送例



5.1.3 非対称の帯域幅

非対称の帯域幅とは TX と RX の帯域幅が同じでないことを意味します。RX 方向でより高い帯域幅を、TX 方向でより低い帯域幅を必要とする無線 (OTA) ファームウェア アップグレード等のようなアプリケーションには有用です。MaxTxOctets および MaxRxOctets パラメーターに適切な値を選択することで非対称の帯域幅を取得できます。例えば、MaxTxOctets を 251 バイトに、MaxRxOctets を 27 バイトに設定すれば、送信方向の帯域幅が増幅されます。同様に、MaxTxOctets を 27 バイトに、MaxRxOctets を 251 バイトに設定することで受信方向の帯域幅が増幅されます。

5.2 アプリケーション

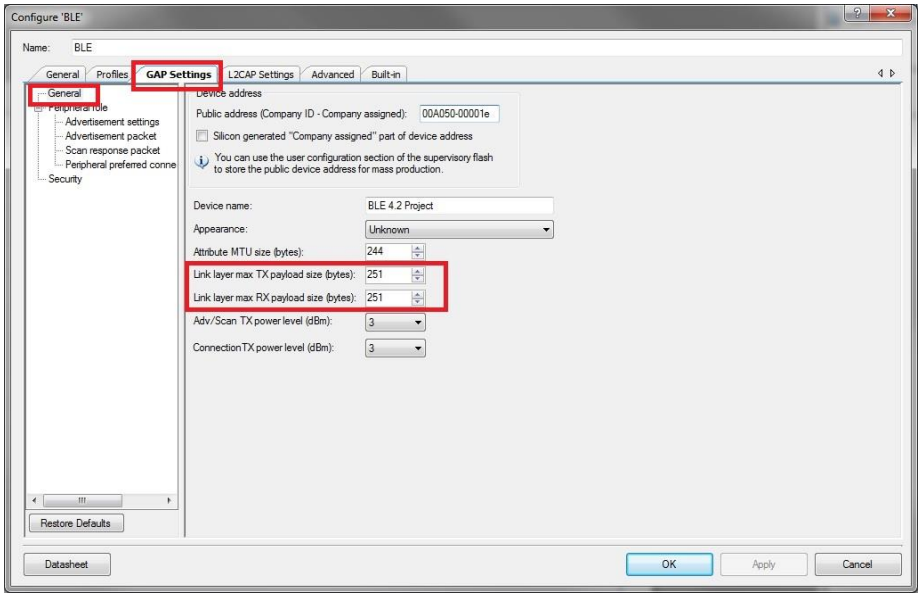
- BLE 経由の音声送信は、高帯域幅を利用してデータを圧縮するのに必要な処理電力を低減させられます。
- 無線 (OTA) ファームウェア アップグレードは低消費電力で、より短い時間で完了できます。
- インターネット プロトコル サポート プロファイル (IPSP) パケットはより迅速に交換され、その結果、より高速な検出とトランザクションに繋がります。
- 複数のセンサーからのデータは、データ ペイロード サイズの増加に伴ってより迅速にログすることができます。

5.3 PSoC Creator における LE データ パケット長拡張機能を使用したアプリケーション開発

5.3.1 コンポーネントの構成

LE データ パケット長拡張機能を使用するには、図 9 に示しているとおりに、**GAP Settings** > **General** セクションで **Link Layer max TX payload size (bytes)**パラメーターの MaxTxOctets、**Link Layer max RX payload size (bytes)** パラメーターの MaxRxOctets の適切な値で BLE コンポーネントを設定しなければなりません。

図 9. BLE コンポーネントで LE データ パケット長拡張機能を設定



5.3.2 アプリケーションの取り扱い

BLE スタックは、ピア デバイスとの接続が確立した後、直ちにコンポーネントの設定に基づいて自動的に TX と RX のペイロード サイズを調整します。表 2 は、BLE スタック イベントの説明および LE データ パケット長拡張機能を活用するのに取るべきアクションをまとめたものです。

表 2 BLE スタック イベントおよび LE データ パケット長拡張機能に対するアクション

BLE スタック イベント名	イベントの説明	イベント ハンドラの応答処理
CYBLE_EVT_GAP_DATA_LENGTH_CHANGE	調整された TX と RX の長さをレポートする	参考になるイベント

通信に調整された送信と受信の最大ペイロード サイズは CYBLE_EVT_GAP_DATA_LENGTH_CHANGE BLE スタック イベントを介してアプリケーションにレポートされます。アプリケーション ファームウェアはこのイベントを使用して通信に対する TX および RX の最大ペイロード サイズの変更を確認できます。

表 3 は、LE データ パケット長拡張機能をサポートする新しい API の一覧 (説明欄付き) を示します。

表 3. LE データ パケット長拡張機能用の新 API

API	説明
CyBle_GapSetDataLength	TX ペイロード サイズを新しく設定し、新規のデータ長更新手順を開始する

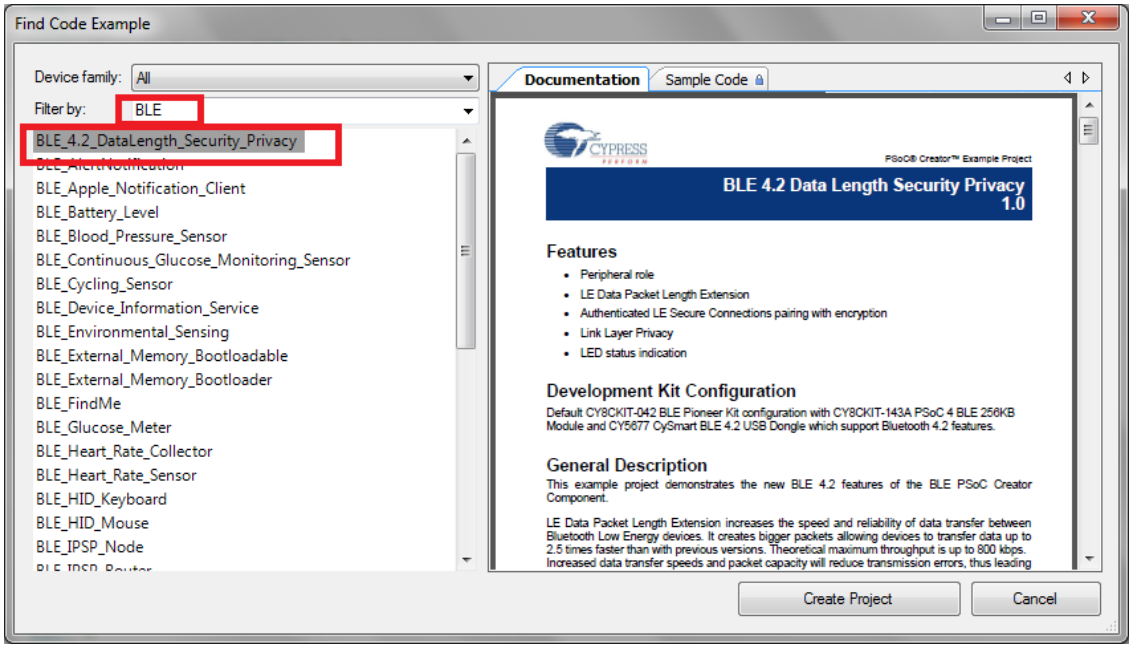
接続後、MaxTxOctets パラメーターは CyBle_GapSetDataLength の API を使用することによりいつでも変更できます。この API は新規のデータ長更新手順を開始し、その手順が完了した後に実際に送受信されたペイロード サイズが CYBLE_EVT_GAP_DATA_LENGTH_CHANGE イベント経由でアプリケーションにレポートされます。

BLE プロトコル スタック イベントおよび API の詳細については、BLE コンポーネント データシーを参照してください。

5.3.3 サンプル プロジェクト

PSoC Creator で利用可能な **BLE_4.2_DataLength_Security_Privacy** サンプル プロジェクトは LE データ パケット長拡張機能を使用します。図 10 に示すように、**PSoC Creator** > **File** > **Code Example** で **BLE** に絞り込むことでサンプル プロジェクトにアクセスできます。

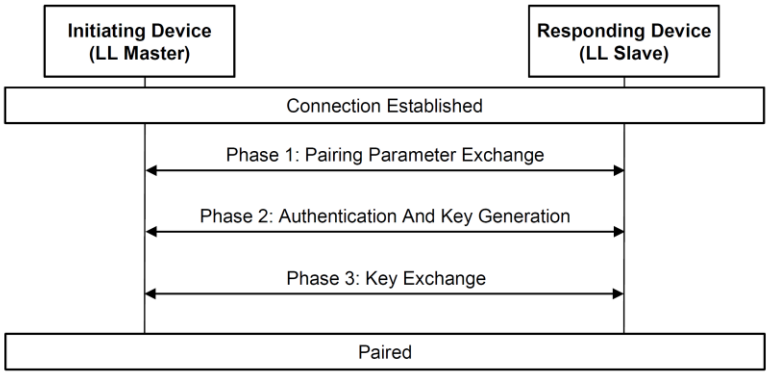
図 10. BLE 4.2 サンプル プロジェクト



6 Low Energy セキュア コネクション

ペアリングは、2 つの BLE デバイス間の認証およびキー共有プロセスです。図 11 に示すように、ペアリングは 3 段階プロセスです。LE セキュア コネクションは、Bluetooth 4.2 で紹介されている拡張セキュリティ機能です。キーを生成するためには楕円曲線ディフィー ヘルマン (ECDH) と呼ばれる連邦情報処理標準 (FIPS) に準拠するアルゴリズムを使用し、およびキーを共有するためには新たな手順を使用します。BLE におけるアソシエーション モデルは、2 つの BLE デバイスの入出力機能に基づいてペアリング方法を定義するモデルです。Bluetooth 4.2 は数値比較 (NC) と呼ばれる新しいアソシエーション モデルを紹介します。

図 11. ペアリング プロセス



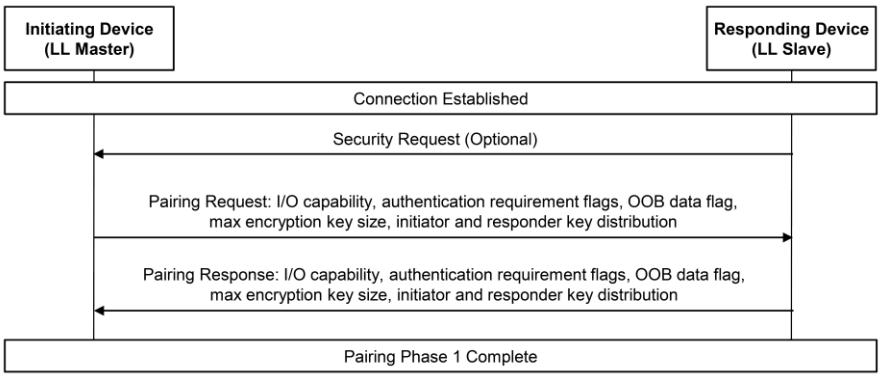
次の節では、ペアリングの 3 段階プロセス、および LE セキュア コネクション機能のそれぞれのフェーズへの影響を説明します。

6.1 ペアリング プロセスへのアップデート

6.1.1 ペアリング第 1 フェーズ

フェーズ 1 においては、発信デバイスおよび応答デバイスは入出力機能、認証要求フラグ、暗号化キーのサイズ、および帯域外 (OOB) データの可用性等のペアリング パラメーターを共有します。図 12 に示しているように、ペアリング プロセスのフェーズ 1 は LE レガシー ペアリングおよび LE セキュア コネクションの間で共通です。

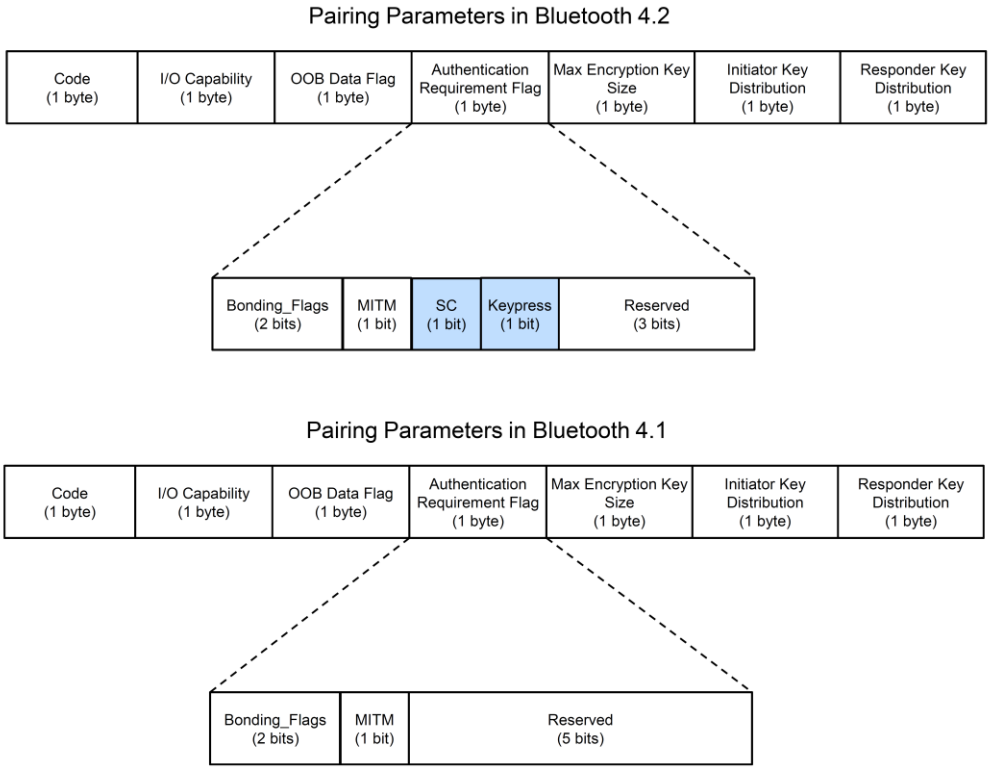
図 12. LE ペアリング第 1 フェーズ



発信デバイス (Link Layer マスター) はペアリング リクエストのコマンドを使用してパラメーターの交換を開始します。応答デバイス (Link Layey スレーブ) はペアリング レスポンスのコマンドで応答します。また、応答デバイスはセキュリティ リクエストのコマンドを使用してペアリング プロセスも開始できます。

認証要求フラグはペアリング パラメーターの一部です。Bluetooth 4.2 では、これらのフラグはセキュア コネクション (SC) およびキープレスと言った 2 つの新規フィールドを追加するために更新されます。図 13 には Bluetooth 4.1 および 4.2 それぞれのペアリング パラメーターと認証要求フラグを示します。

図 13. ペアリング パラメーター



フェーズ 2 のペアリング方法またはアソシエーション モデルはフェーズ 1 の間に交換されたパラメーターにより判定されます。以下がフェーズ 2 に使用できる 4 つのペアリング方法またはアソシエーション モデルです。

- Just Works (ジャスト ワーク)
- Numeric Comparison (数値比較;LE セキュア コネクション専用)
- Passkey Entry (パスキー入力)
- Out Of Band (帯域外;OOB)

表 4. LE セキュア コネクションにおけるアソシエーション モデルの判定

		発信デバイス			
		OOB データ フラグが設定済み	OOB データ フラグが未設定	MITM が設定済み	MITM が未設定
応答デバイス	OOB データ フラグが設定済み	OOB を使用	OOB を使用		
	OOB データ フラグが未設定	OOB を使用	MITM をチェック		
	MITM が設定済み			I/O 機能を使用	I/O 機能を使用
	MITM が未設定			I/O 機能を使用	ジャスト ワークを使用

表 4 では、LE セキュア コネクションにおいてアソシエーション モデルがフェーズ 1 で交換されたペアリング パラメーターに基づいてフェーズ 2 でどのように判定されるかを示します。LE セキュア コネクションでは、発信デバイスおよび応答デバイスの両方とも表示機能と「はい／いいえ」I/O 機能、または表示機能とキーボード I/O 機能を内蔵している場合、数値比較のアソシエーション モデルが使用されます。I/O 機能に基づきアソシエーション モデルがどのように判定されるか、そして片方の BLE デバイスまたは両方の BLE デバイスが LE レガシー ペアリングのみをサポートする場合の詳細情報については、Bluetooth Core Specification Version 4.2、第 3 巻、第 H 部、2 節をご覧ください。

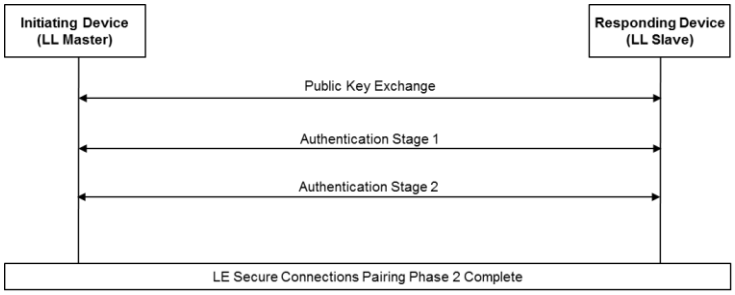
6.1.2 ペアリング第 2 フェーズ

ペアリング プロセスのフェーズ 2 は、中間者 (MITM) 攻撃を防止するための認証、および BLE リンクを暗号化するために使用されるキーの生成に関連します。

LE レガシー ペアリング方法では、一時キー (ジャスト ワーク モデルの場合は 0、パスキー入力モデルの場合は 6 桁または 20 ビット、OOB モデルの場合は 128 ビット) は BLE リンクを暗号化するキーを取得するために使用されます。この一時キーは、BLE リンクをとおって交換されない唯一のランダム データです。LE レガシー ペアリング方法の詳細については、「Bluetooth Core Specification Version 4.2」、第 3 巻、第 H 部、2.3.5 節を参照してください。

図 14 に示すように、LE セキュア コネクションにおけるフェーズ 2 は 3 つの過程を含みます。

図 14. LE セキュア コネクション ペアリングにおけるフェーズ 2



公開キー交換の過程では、発信デバイスおよび応答デバイスはお互いの公開キーを共有し、ディフィー ヘルマン キーを計算し始めます。ディフィー ヘルマン キーは楕円曲線ディフィー ヘルマン機能、P256 で生成されたキーです。P256 はデバイス固有の秘密キーとペア デバイスの公開キーを入力として取り扱います。ディフィー ヘルマン キーは決して無線で交換されず、256 ビットの乱数を提供します。ECDH アルゴリズムが秘密キーを BLE リンク経由で交換することなく発信デバイスおよび応答デバイスの両方を有効にし、共通のディフィー ヘルマン キーを計算する方法を理解するには、受動的盗聴に対する防止を参照してください。

認証過程 1 では、中間者 (MITM) 攻撃を防ぐために BLE デバイス同士が相互に認証し合います。認証過程 1 はそれぞれのアソシエーション モデルによって異なります。数値比較、パスキー入力、および OOB のアソシエーション モデルを使用する認証過程 1 で MITM 攻撃に対して高度な保護を提供する方法を理解するには、中間者 (MITM) 攻撃に対する防止を参照してください。認証過程 1 で何らかの誤りが発生するとペアリング プロセスもそこで終了してしまいます。

認証過程 2 では、BLE デバイスはリンクを暗号化するために使用される Long Term Key (長期キー;LTK) を計算します。認証過程 1 で生成されたディフィー ヘルマン キー、Bluetooth デバイス アドレス、128 ビットの乱数、およびデバイスの I/O 機能は LTK を生成するために使用されます。

LE セキュア コネクションにおける認証過程その 1 と 2 の詳細については、「Bluetooth Core Specification Version 4.2」、第 3 巻、第 H 部、2.3.5.6 節をご覧ください。

6.1.3 ペアリング第 3 フェーズ

ペアリングの第 3 フェーズでは、BLE リンクは、フェーズ 2 で生成された STK (LE レガシー ペアリングの場合) または LTK (LE セキュア コネクション ペアリングの場合) を使用して暗号化されます。そして、以下のキーが暗号化されたリンクをとおして配布されます。

1. Identity Resolving Key (IRK) - ランダムのアドレスを生成し、解読するために使用される 128 ビットのキー
2. Connection Signature Resolving Key (CSRK) - データを署名し、受信側でその署名を検証するために使用される 128 ビットのキー
3. Long Term Key (LTK) - 暗号化された通信に対してセッション キーを生成するために使用される 128 ビットのキー詳細は、「Bluetooth Core Specification Version 4.2」、第 6 巻、第 B 部、5.1.3 節を参照
4. Encrypted Diversifier (EDIV) - LE レガシー ペアリング中に配布された LTK を識別するために使用される 16 ビットの保持値。ユニークな LTK が配布される度に新しい EDIV が生成される
5. Random Number (Rand) - LE レガシー ペアリング中に配布された LTK を識別するために使用される 64 ビットの保持値。ユニークな LTK が配布される度に新しい Rand が生成される

LTK、EDIV および Rand は LE レガシー ペアリングの場合にのみ配布されます。

6.2 利点

6.2.1 より良いセキュリティ

LE セキュア コネクションは、LE レガシー ペアリングより、MITM 攻撃および受動的盗聴に対するセキュリティ性が高いです。

受動的盗聴者は、2 つの BLE デバイス間の通信を盗聴する第三者です。受動的盗聴者は暗号化された通信を盗聴するために、BLE リンク経由で配布されたキーを横取りする必要があります。LE セキュア コネクションのあらゆるアソシエーション モデルでは、256 ビットのディフィー ヘルマン キーは無線で交換されることは決してありません。そのため、受動的盗聴者は暗号化用に使われる Long Term Key (LTK) を計算できず、その結果、暗号化された BLE 通信を盗聴することもできなくなります。Bluetooth 4.1 では、受動的盗聴への防止は OOB アソシエーション モデル経由でのみ可能になり、128 ビットの一時キーを使用するため防止能力そのものが低いです。LE セキュア コネクションにおいて 2 つの BLE デバイスがどのように共通のディフィー ヘルマン キーを計算できるかを理解するには、受動的盗聴に対する防止を参照してください。

MITM 攻撃は、通信に接続しようとするデバイスに対してピア デバイスに扮する第三者の攻撃です。ピア デバイスに扮することにより 2 つのデイバス間で交わされているデータを変更します。数値比較、パスキー入力、および OOB のアソシエーション モデルは MITM 攻撃に対してより高度な保護を提供します。これらのアソシエーション モデルがどのように MITM 攻撃から保護できるかを理解するには、中間者 (MITM) 攻撃に対する防止を参照してください。数値比較はパスキー入力よりも高速なペアリングを可能にし、OOB のように独立した通信リンクを必要としません。

表 5 では、LE レガシー ペアリングおよび LE セキュア コネクションそれぞれの異なるペアリング方法の保護レベルをまとめます。

表 5. LE レガシー ペアリングおよび LE セキュア コネクション ペアリングの比較

機能	LE レガシー ペアリング方法	LE セキュア コネクション ペアリング方法
MITM に対する防止	パスキーと OOB	数値比較、パスキー入力、OOB
受動的盗聴に対する防止	OOB	すべて

6.2.2 セキュア コネクション専用モード

このモードは LE セキュア コネクションを使用して厳密なペアリングを強制的に行います。どちらか一方のデバイスが厳格なペアリング フラグを設定した場合、ペアリング プロセスのフェーズ 2 は、双方のデバイスが LE セキュア コネクションをサポートし、認証要件を満たした時にのみ行われます。これは高度なセキュリティが必要とされるアプリケーションには非常に有用です。

6.3 アプリケーション

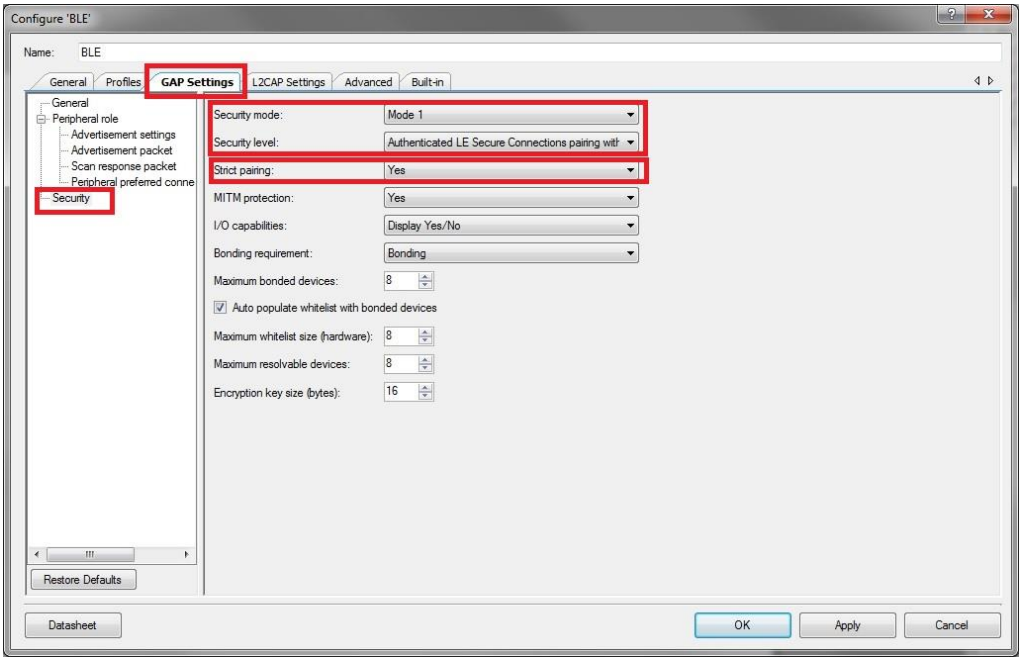
ドア ロック、銀行カード、および高度なセキュリティを求める他のアプリケーションは Bluetooth 4.2 の強化されたセキュリティ機能を活用できます。

6.4 PSoC Creator で LE セキュア コネクションを使用したアプリケーション開発

6.4.1 コンポーネントの構成

BLE コンポーネントは、セキュリティ モード、セキュリティ レベル、厳格なペアリング要求、MITM への防止、I/O 機能、ボンディング要求、および暗号化キー サイズを設定するための簡単な方法を提供します。アプリケーションで LE セキュア コネクションを使用するには、**Gap Settings** > **Security** に移動し、**Security mode** パラメーターを **Mode 1** に、**Security level** パラメーターを **Authenticated LE Secure Connections pairing with encryption** に設定します。他のパラメーターは対象アプリケーションの要求に応じて設定できます。

図 15. BLE コンポーネントのコンフィギュレーション: セキュリティ設定



6.4.2 アプリケーションの処理

LE セキュア コネクション機能を使用する際に、アプリケーション ファームウェアは以下の作業を管理する必要があります。

- ローカルの公開キーと秘密キーのペアの生成
- 数値比較の場合は数値の表示;パスキー入力の場合はパスキーの表示・入力
- パスキー入力状態の送信
- パスキーの送信
- 数値比較の場合に表示される数値に対する採否情報の送信

表 6 は、BLE スタック イベントそれぞれの説明、および LE セキュア コネクション機能を使用する際に取るべきアクションをまとめたものです。

表 6. LE セキュア コネクションにおける BLE イベントおよび応答処理

BLE スタック イベント名	イベントの説明	イベント ハンドラの応答処理
CYBLE_EVT_GAP_NUMERIC_COMPARISON_REQUEST	数値比較に表示される 6 桁の数値を提供する	6 桁の数値を表示する 数値比較に双方のデバイスに表示される数値を元に採否情報を送信する
CYBLE_EVT_GAP_KEYPRESS_NOTIFICATION	ピア側のパスキー入力状態を通知する	ピア側から通知された数値と対象デバイスでユーザーが入力した数値が一致するか確認する 一致しない場合は通信を切断する
CYBLE_EVT_GAP_OOB_GENERATED_NOTIFICATION	OOB データの生成が完了した旨を通知する	アプリケーション特有のアクション
CYBLE_EVT_GAP_SMP_NEGOTIATED_AUTH_INFO	調整されたペアリング パラメーターを通知す	アプリケーション特有のアクション

表 7 は、LE セキュア コネクションが有効なアプリケーションで使用される新しい API を一覧化したものです。

表 7. LE セキュア コネクション用の新 API

API	説明
CyBle_GapSetSecureConnectionsOnlyMode	セキュア コネクション専用モードを有効化または無効化
CyBle_GapGenerateLocalP256Keys	ローカルの公開キーと秘密キーを生成
CyBle_GapAuthSendKeyPress	キープレス状態を送信
CyBle_GapGenerateOobData	OOB データを生成

イベントおよび API の詳細については、BLE コンポーネント データシートをご覧ください。

6.4.3 サンプル プロジェクト

PSoC Creator で利用可能な BLE_4.2_DataLength_Security_Privacy サンプル プロジェクトは LE セクイア コネクションを使用します。図 10 に示すように、**PSoC Creator** > **File** > **Code Example** で **BLE** に絞り込むことでサンプル プロジェクトにアクセスできます。

7 Link Layer (LL) プライバシー

7.1 プライバシーのご紹介

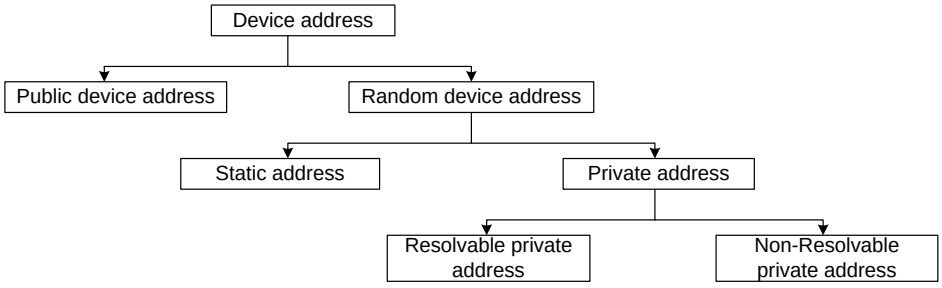
BLE デバイスは 48 ビットのデバイス アドレスを用いて識別されます。このデバイス アドレスは宣伝チャネルでデバイスにより送信されたすべてのパケットの一部です。3 つの宣伝チャネルでリッスンしている第三者はデバイス アドレスを使用することでそのデバイスのアクティビティーを容易に追跡できます。プライバシーは、一定の間隔で生成され変更されるプライベートなアドレスを使用して BLE デバイスを追跡する能力を低下させる機能です。

7.2 プライバシー コンセプト

7.2.1 Bluetooth アドレス タイプ

図 16 には、BLE デバイスの異なるアドレス タイプを示します。

図 16. Bluetooth アドレス タイプ



デバイス アドレスはパブリック デバイス アドレスかランダム デバイス アドレスのいずれかです。パブリック デバイス アドレスは、24 ビットの企業 ID (IEEE 802-2001 標準に準拠した企業のユニークな識別子または OUI) および企業が割り振る 24 ビットの数値 (デバイス固有) から構成されます。ランダム デバイス アドレスにはスタティック アドレスとプライベート アドレスの 2 種類があります。スタティック アドレスは、ランダムに生成される 48 ビットのアドレスであり、その 48 ビット アドレスの最上位の 2 ビットが 1 に設定されます。パブリック デバイス アドレスは時間を経ても変わらないものです。スタティック アドレスはデバイスの電源を一度切って再投入した時にのみ変更できます。これらいずれかのアドレスを使用しているデバイスはピア デバイスにより容易に検出され、接続できます。プライベート アドレスは、BLE デバイスが追跡されないことを確保するために、一定の間隔で変更します。解読不可能なプライベート アドレスは再接続する度に変更します。解読不可能なプライベート アドレスは、ピア デバイスにより解読されず、前の通信中にピア デバイスと共有しなければなりません。解読可能なプライベート アドレス (RPA) は一定の間隔で変更し、解読でき、プライバシーが有効なデバイスにより使用されます。本アプリケーション ノートでは、プライバシー機能の範囲内で RPA について説明します。異なるアドレス タイプの詳細については、Bluetooth Core Specification Version 4.2 を参照してください。

プライバシー機能が有効なすべての BLE デバイスには、アイデンティティー アドレスと呼ばれるユニークなアドレスがあります。そのアイデンティティー アドレスは BLE デバイスのパブリック アドレスまたはスタティック アドレスです。また、プライバシー機能が有効なあらゆる BLE デバイスは Identity Resolving Key (IRK) を持ちます。IRK は RPA を生成するために BLE デバイスにより使用され、BLE デバイスの RPA を解読するためにピア デバイスにより使用されます。アイデンティティー アドレスと IRK の両方ともペアリング プロセスの 3 番目の過程で交換されます。プライバシーが有効な BLE デバイスは、ピア デバイスのアイデンティティー アドレス、RPA を生成するために BLE デバイスにより使用されるローカル IRK、およびピア デバイスの RPA を解読するために使用されるピア デバイスの IRK を含むリストを保持します。それは Resolving List と呼ばれます。Resolving List に入力する際は、図 17 に示しているフォーマットに従います。

図 17. Resolving List

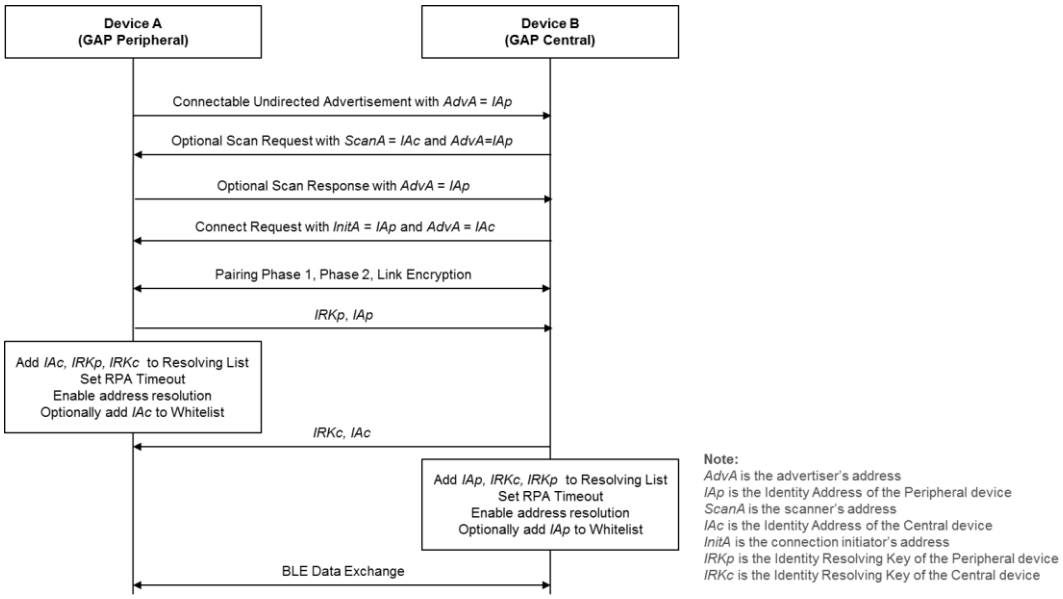
Identity address	Local IRK	Peer IRK

プライバシーが有効な BLE デバイスは追跡を回避するために RPA を周期的に変更します。BLE スタックは RPA タイムアウトと呼ばれる値で Link Layer を設定します。このタイムアウト時間が満了すると Link Layer は新しい RPA を生成しなければなりません。

7.2.2 プライバシーの流れ

図 18 は、プライバシー機能を使用しようとする 2 つの BLE デバイス間に確立される初期接続を示します。この図を見れば分かるように、片方のデバイスが Generic Access Profile (GAP) のペリフェラル役割を、残りの片方のデバイスが GAP セントラルの役割を果たします。GAP および Bluetooth デバイスで利用可能な様々な役割の詳細については、Bluetooth Core Specification Version 4.2、第 3 巻、第 C 部、2.2.2 節をご覧ください。

図 18. プライバシー機能を使用しようとするデバイス間に確立された初期接続



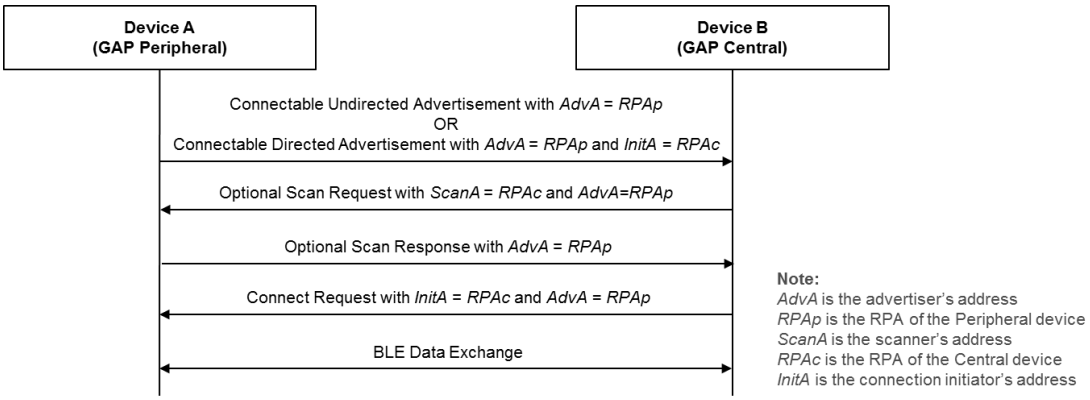
上の図に見られるように、初期の接続を確立している間に GAP ペリフェラルおよび GAP セントラルは宣伝チャネル経由で送信されるすべてのパケットにおいてアイデンティティー アドレス (ペリフェラルの場合は *IAp*、セントラルの場合は *IAc*) を使用します。これはもともと両方のデバイスともピア デバイスの IRK を意識しなかったため、ピア デバイスの RPA を解読できなくなるからです。宣伝チャネル経由で送信されるパケットは以下のとおりです。

- 接続可能無向宣伝: これは特定の受信者 (すなわち、特定の GAP セントラル) に向けていない宣伝パケットです。これらの宣伝は GAP セントラルのアドレスを含まず、GAP ペリフェラル、すなわち、宣伝側のアドレスのみを含みます。
- 任意のスキャン要求およびスキャン応答: スキャン要求は GAP セントラルにより送信され、ペリフェラルに接続する前にペリフェラルに対してデータを追加するように要求します。スキャン応答はペリフェラルにより送信され、要求されたデータを含みます。これら両方のパケットは任意です。
- 接続要求: これは通信を開始するために GAP セントラルから GAP ペリフェラルへ送信する要求です。

上記以外の他のすべてのパケットはデータ チャネル上で送信され、Bluetooth デバイス アドレスを含みません。接続要求パケットは宣伝チャネルで送信される最後のパケットです。GAP セントラルおよび GAP ペリフェラルのアイデンティティー アドレスの他に、接続要求パケットはアクセス アドレスと呼ばれる 32 ビットの乱数も含んでいます。アクセス アドレスは 2 つの BLE デバイス間の Link Layer 通信を識別します。接続が確立される度に、すなわち、接続要求が送信される度に新しいアクセス アドレスが生成されます。データ チャネル上で交換される BLE デバイス間のすべてのパケットはアクセス アドレスを使用し、その 2 つのデバイス間の通信を識別します。それはペアリングおよびデータ交換用のパケットです。

ペアリング プロセスの 3 番目の過程 (ペアリング プロセスの詳細は 6.1 を参照) では、GAP セントラルおよび GAP ペリフェラルは IRK とアイデンティティー アドレスをペアリングに関連するパケットのペイロードの一部として交換します。両方のデバイスは、ローカルの IRK と共にピアの IRK とアイデンティティー アドレスを Resolving List に格納します。この過程では、両方のデバイスは RPA を解読するのに必要な情報を持っているため、両方とも RPA タイムアウトを設定し、アドレス ソリューションを有効にします。双方のデバイスは、デバイスをフィルタリングするために、ピア デバイスのアイデンティティー アドレスを Whitelist に追加することもできます。Whitelist は、Bluetooth デバイス アドレス一式です。BLE デバイスの Link Layer はそのデバイス アドレスを使用し、宣伝者、スキャナー、および通信のイニシエーターをフィルタリングします。Whitelist はデバイス フィルタリング機能が有効な場合にのみ使用されます。その場合、デバイスは BLE データ チャネル上でデータを交換します。この時、デバイスは Resolving List のピア RPA を解読するのに必要な情報を持っているため、再接続手順ではその RPA を使用します。図 19 は、デバイスが初期接続の確立後に一旦切断してまた接続するというシナリオを示します。

図 19. RPA を使用した再接続

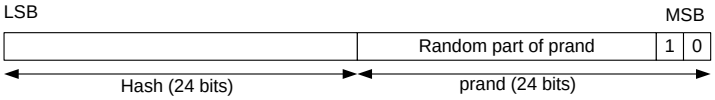


上述のとおりに、ここでデバイスは宣伝チャネル経由で送信されるあらゆるパケットで RPA を使用します。そのため、宣伝チャネル上のデバイス間の通信は第三者のいかなるデバイスによりも追跡されません。GAP ペリフェラルは再接続するために接続可能無向宣伝または接続可能有向宣伝を使用できることに注意してください。7.2.5 節では、Bluetooth 4.2 を搭載しているプライバシー機能が有効なデバイスが接続可能有向宣伝のみをサポートする理由を説明します。スキャン要求およびスキャン応答パケットは、GAP ペリフェラルが接続可能無向広報を使用する時にのみ使用されます。GAP ペリフェラルが接続可能無向宣伝を使用する場合、GAP セントラルは接続要求でのみ応答できます。プライバシーは、宣伝チャネル上の通信による BLE デバイスのトラッキングを防止することにご注意ください。データ チャネル パケットは、接続が確立されるたびに生成されるランダムのアクセス アドレスを使用するため、トラッキングに影響されません。プライバシーはデータ チャネル パケットに影響を与えません。

7.2.3 解読可能プライベート アドレス (RPA) の生成

本節では、プライバシー機能を備えた BLE デバイスがどのように RPA を生成するかを説明します。解読可能プライベート アドレスのフォーマットは Bluetooth 仕様書に記述されており、図 20 に示されます。

図 20. 解読可能プライベート アドレス フォーマット



デバイスは、*prand* と呼ばれる 24 ビットの数値 (22 ビットはランダムで、2 ビットは固定) を生成します。デバイスは *prand* を使用して hash 関数により 24 ビットの *hash* を生成します。

$hash = e(IRK_{local}, padding \mid prand)$、24 ビットに切り捨てられる

ここで、

IRK_{local} = 128 ビットのローカル IRK

Padding = *prand* を 128 ビットに拡張するための 104 ビットのゼロ パディング

prand = 24 ビットの乱数 (22 ビットはランダムで、最上位 2 ビットは 0b10 にセットされる)

セキュリティ関数「e」は、PSoC 4／PRoC BLE デバイスの Link Layer ハードウェアに実施された 128 ビット暗号化関数です。これは、FIPS-1971 で定義されたように、128 ビットの *key* と 128 ビットの *plaintextData* から 128 ビットの *encryptedData* を生成します。

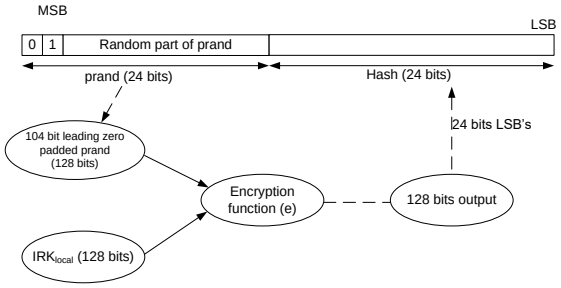
encryptedData = *e(key, plaintextData)*

24 ビット *hash* と 24 ビット *prand* は連結られ、以下のようにランダム アドレス *(randomAddress)* を生成します。

randomAddress = *hash* | *prand*

解読可能プライベート アドレスの生成は図 21 に示されます。

図 21. 解読可能プライベート アドレスの生成



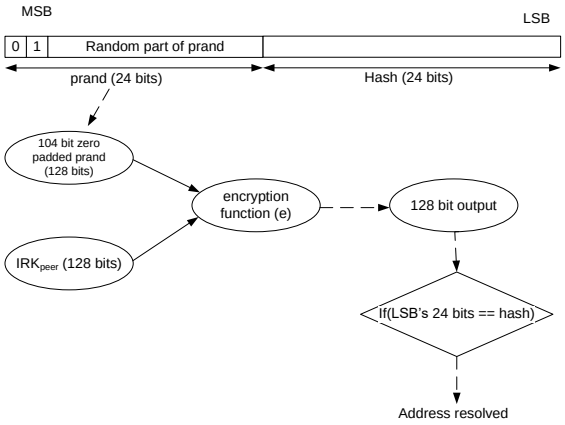
7.2.4 解読可能プライベート アドレスの解読

本節では、プライバシー機能を備えた BLE デバイスがどのようにピア デバイスの RPA を解読するかを説明します。ピア デバイスから受信された RPA は、7.2.3 節で説明されたように、24 ビットのランダム部分 (*prand*) と 24 ビットの hash 部分 (*hash*) から成ります。アドレスを解読／復号するために、RPA の最下位 24 ビットと最上位 24 ビットそれぞれはピア デバイスの *hash* と *prand* に抽出されます。その後、前述された hash 関数により *localHash* 値が生成されます。hash 関数では、入力パラメータはピア デバイスから受信された IRK にセットされ、入力パラメータ *prand* 値は RPA から抽出されます。

localHash = *e*(*IRK_{peer}*, *padding* | *prand*)、24 ビットに切り捨てられる

localHash 値は、RPA から抽出された *hash* 値と比較されます。*localHash* 値が抽出された *hash* 値と一致したら、ピア デバイスのアイデンティティは解読されたとみなされます。アドレスの解読は図 22 に示されます。

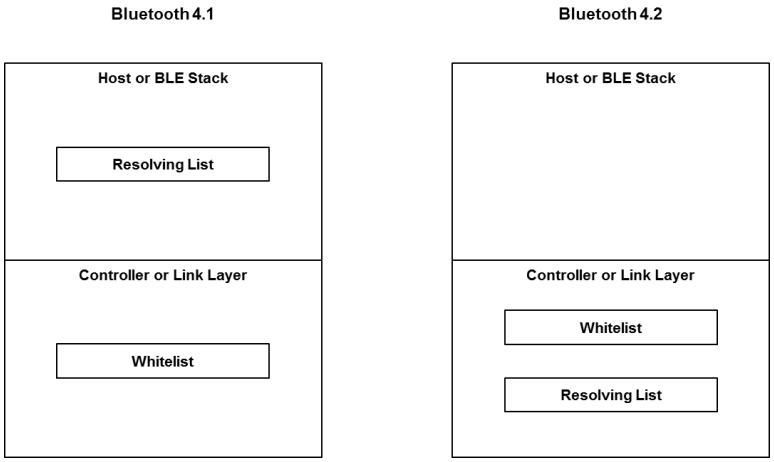
図 22. 解読可能プライベート アドレスの解読



7.2.5 プライバシー1.1 とプライバシー1.2 の比較

Bluetooth 4.1 において、プライバシー機能はプライバシー1.1 と呼ばれます。Bluetooth 4.2 においては、プライバシー機能はプライバシー1.2 (Link Layer プライバシー) と呼ばれます。理由は、Bluetooth 4.2 ではアドレスの解読 (すなわち、RPA の解読) は Link Layer によって処理されるためです。図 23 に示されるように、Bluetooth 4.2 では、Resolving List および Whitelist は Link Layer の一部です。

図 23. Bluetooth 4.1 のプライバシー1.1 と Bluetooth 4.2 のプライバシー1.2 の比較



接続可能有向宣伝は、宣伝側および受信側の RPA を含みます。Bluetooth 4.2 の Link Layer プライバシー機能により、Link Layer は Resolving List を使用して RPA を解読できます。そのため、Link Layer は受信側が接続可能有向宣伝の対象となる受信側であるかを理解できます。また、Bluetooth 4.1 と Bluetooth 4.2 は RPA タイムアウトの許容値で違います。Bluetooth 4.2 では、RPA タイムアウトの値は 1 秒～11.5 時間の任意の値であり、デフォルト値は 900 秒です。Bluetooth 4.1 では、RPA タイムアウトは 15 分に固定されます。

7.3 利点

7.3.1 高速な再接続

7.2.5 節では、プライバシー機能を備えたデバイスが再接続のために接続可能有向宣伝をどのように使用するかを説明しました。Bluetooth 4.1 では、プライバシー機能によるデバイス フィルタリングはできません。Link Layer は Resolving List へのアクセスがありません。そのため、Link Layer は RPA をアイデンティティー アドレスに解読することも、Whitelist を使用してアイデンティティー アドレスをフィルタリングすることもできません。Bluetooth 4.2 では、図 23 に示すように、Resolving List は Link Layer の一部です。そのため、Link Layer は Resolving List を使用して RPA をアイデンティティー アドレスに解読してから、Whitelist を使用してアイデンティティー アドレスをフィルタリングできます。Bluetooth 4.2 における接続可能有向宣伝によるデバイス フィルタリングにより、プライバシー機能を備えた BLE デバイスのより高速な再接続が可能です。

7.3.2 電力効率の良い GAP セントラル デバイス

デバイス フィルタリングを使用する、プライバシー機能を備えた GAP セントラル デバイスに対しては、Link Layer は Resolving List と Whitelist にリストアップされたピア デバイスからの有向宣伝およびスキャン応答をのみ BLE スタックに送信します。これにより、BLE スタックでの必要な処理が減少されます。サイプレスの PSoC 4 BLE と PRoC BLE のような BLE デバイスは、BLE スタックを MCU で実行されるファームウェアとして、Link Layer をハードウェア ブロックとして実装します。そのため、BLE スタックでの必要な処理が減少されることにより、MCU のアクティブ時間が短縮され、システムの消費電力も減少されます。

7.3.3 電力効率の良い GAP ペリフェラル デバイス

デバイス フィルタリングを使用する、プライバシー機能を備えた GAP ペリフェラル デバイスに対しては、Link Layer は Resolving List と Whitelist にリストアップされたピア デバイスからのスキャン要求および接続要求をのみ BLE スタックに送信します。これにより、BLE スタックでの必要な処理が減少されます。サイプレスの PSoC 4 BLE と PRoC BLE のような BLE デバイスは、BLE スタックを MCU で実行されるファームウェアとして、Link Layer をハードウェア ブロックとして実装します。そのため、BLE スタックでの必要な処理が減少されることにより、MCU のアクティブ時間が短縮され、システムの消費電力も減少されます。

7.3.4 Bluetooth 4.1 よりプライベート

7.2.5 節に記述したように、Bluetooth 4.1 におけるプライバシー機能は固定された 15 分の RPA タイムアウトを使用しますが、Bluetooth 4.2 における RPA タイムアウトは最小 1 秒です。これにより、Bluetooth 4.2 では RPA がより頻繁に変化し、BLE デバイスのトラッキングは困難になります。

7.4 アプリケーション

Link Layer プライバシー機能を採用する応用は多くあります。

プライバシー機能により、利用者は体育館などの公共の環境でウェアラブル機器の可視性を制御できます。プライバシー機能を備えたウェアラブル機器が利用者のスマートフォンや体育館の設備に接続しようとする時、それからの宣伝は 3 番目のデバイスによってトラッキングされることはできません。これにより、公共の場所で利用者はウェアラブル機器をとおしてトラッキングされることは防げます。ほとんどのウェアラブル機器は GAP ペリフェラルであり、消費電力が大きいため Bluetooth 4.1 におけるプライバシー機能を使用しません。Bluetooth 4.2 における Link Layer プライバシー機能により、7.3.3 節で説明したように消費電力が減少されるため、ウェアラブル機器はプライバシー機能を使用できます。

小売業アプリケーションもプライバシー機能によって利益を得られます。小売業環境で、サービス提供者は BLE ビーコンを採用して広告を介して利用者のスマートフォンにオファーを送信します。Link Layer プライバシー機能に対応したスマートフォンは、デバイス フィルタリングを (7.3.1 節で説明したように) 使用して望ましいサービス提供者からのオファーのみを受信し、他のサービス提供者を無視します。

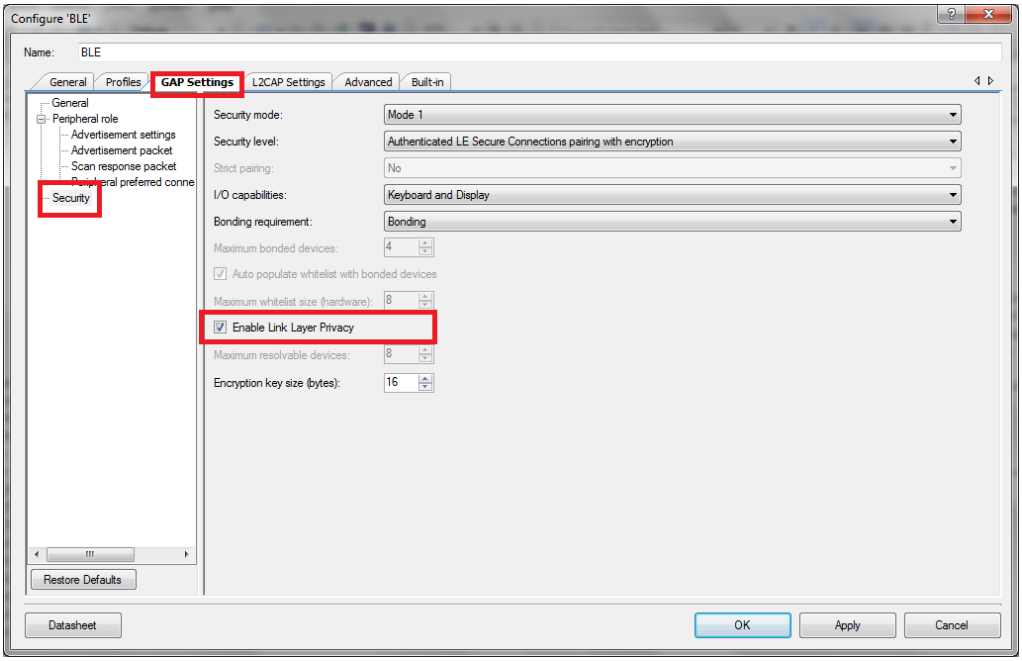
Link Layer プライバシー機能により、RPA が頻繁に変化するため公共の場所で利用者のスマートフォンをトラッキングすることが困難になります。一般的には、スマートフォンは GAP セントラル デバイスとして動作します。また、Link Layer プライバシーにより、(7.3.2 節で説明したように) スマートフォンの BLE 通信に消費される電力量は減少されます。

7.5 Link Layer プライバシーを採用したアプリケーションの PSoC Creator による開発

7.5.1 コンポーネントのコンフィギュレーション

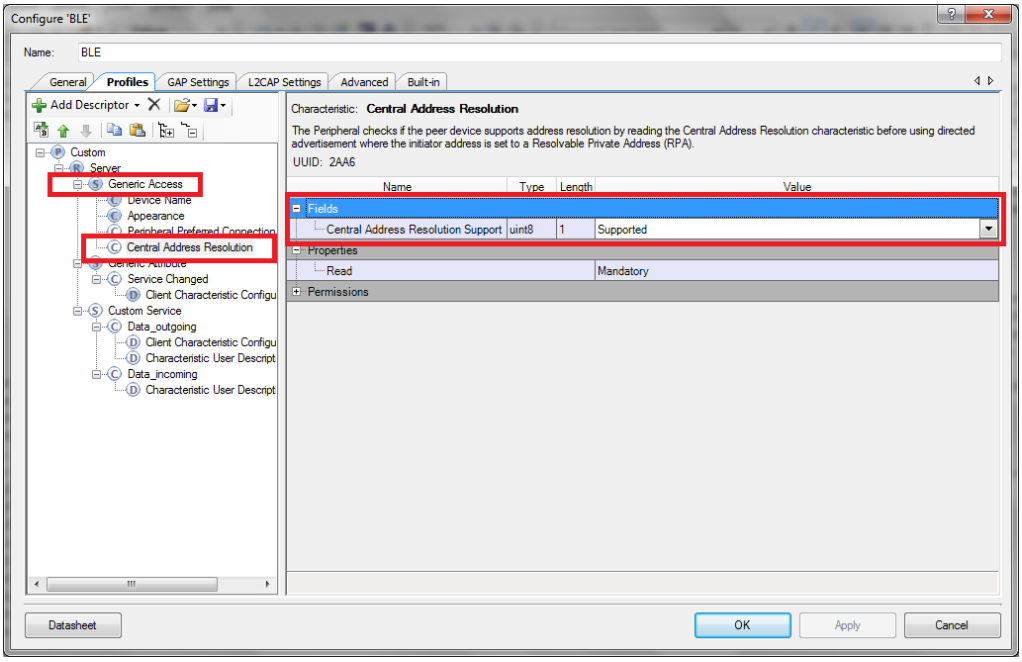
Link Layer プライバシー機能および関連する API は、図 24 に示すように **GAP Settings** > **Security** の下の BLE コンポーネント コンフィギュレーション ウィンドウ内の **Enable Link Layer Privacy** オプションで有効／無効にできます。

図 24. Link Layer プライバシーの有効化／無効化



GAP サービスのセントラル アドレス解読キャラクタリスティックは、初期の接続確立の後に GAP ペリフェラル デバイスによって読み出されます。このキャラクタリスティックの値により、GAP ペリフェラルは GAP セントラルが Link Layer でのアドレス解読をサポートするかを理解できます。Link Layer でアドレス解読がサポートされる場合、GAP ペリフェラルは GAP セントラルとの再接続のために接続可能有向宣伝を使用できます。セントラル アドレス解読キャラクタリスティックの値は、図 25 に示すように、**Profiles** > **Generic Access** > **Central Address Resolution** の下のドロップダウン メニューでセットできます。Link Layer プライバシーに対応したデバイスは、この機能がサポートされることをピア デバイスに通知するためにこのキャラクタリスティック値を **Supported** にセットする必要があります。

図 25. セントラル アドレス解読キャラクタリスティック値の設定



7.5.2 アプリケーションの処理

アプリケーション ファームウェアは、プライバシー機能を備えたデバイスのファームウェアで以下のタスクを管理する必要があります。

- アドレス解読の有効化／無効化
- RPA タイムアウトの設定
- Resolving List に／からのデバイスの追加／除外
- 適切な Whitelist フィルター ポリシーの設定

表 8 では、BLE スタック イベント、イベントの説明、およびイベント ハンドラで行うべき応答処理をリストアップします。

表 8. LL プライバシー用の BLE イベントおよび措置

BLE スタック イベント名	イベントの説明	イベント ハンドラの応答処理
CYBLE_EVT_STACK_ON	BLE スタックの初期化が正常に完了	Resolving List に入力 アドレス解読を有効化 RPA タイムアウトを設定 Whitelist フィルター ポリシーを設定
CYBLE_EVT_GAP_KEYINFO_EXCHNGE_CMPLT	ピア デバイスとのセキュリティ キー交換が完了	ピア デバイスの IRK をコピー Resolving List を更新 Whitelist フィルター ポリシーを更新
CYBLE_EVT_GAPC_DIRECT_ADV_REPORT	アドレス解読の後に有向宣伝を受信	デバイスに接続

表 9 は、LL プライバシーに対応したアプリケーションで使用される新しい API を一覧化したものです。

表 9. LL プライバシー機能に対応したアプリケーションの新しい API

API	説明
CyBle_GapAddDeviceToResolvingList	Resolving List にデバイスを追加
CyBle_GapRemoveDeviceFromResolvingList	Resolving List からデバイスを除外
CyBle_GapSetAddressResolutionEnable	コントローラーでアドレス解読を有効化
CyBle_GapSetResolvablePvtAddressTimeOut	RPA タイムアウトを設定
CyBle_GapReadResolvingList	現時点の Resolving List を読み出す
CyBle_GapReadPeerResolvableAddress	ピア デバイスの現時点の RPA アドレスを読み出す
CyBle_GapReadLocalResolvableAddress	ローカル デバイスの現時点の RPA アドレスを読み出す
CyBle_GapGetDevSecurityKeyInfo	ローカル IRK 値を取得

7.5.3 セントラル アドレス解読キャラクタリスティックの読み出し

7.5.1 節に記述したように、ペリフェラル デバイスはプライバシー機能を備えたセントラル デバイスが Link Layer プライバシーをサポートする場合にのみ、セントラル アドレス解読キャラクタリスティックを読み出し接続可能有向宣伝を送信します。セントラル アドレス解読キャラクタリスティックを読み出すために、以下に示すように CyBle_GattcReadUsingCharacteristicUuid API を適切なパラメーターで使用できます。

```
CYBLE_GATTC_READ_BY_TYPE_REQ_T read_by_type_req;
read_by_type_req.range.startHandle = CYBLE_GATT_ATTR_HANDLE_START_RANGE;
read_by_type_req.range.endHandle = CYBLE_GATT_ATTR_HANDLE_END_RANGE;
read_by_type_req.uuid.uuid16 = CYBLE_UUID_CHAR_CENTRAL_ADDRESS_RESOLUTION;
read_by_type_req.uuidFormat = CYBLE_GATT_16_BIT_UUID_FORMAT;
CyBle_GattcReadUsingCharacteristicUuid(cyBle_connHandle,&read_by_type_req);
```

セントラル デバイスがセントラル アドレス解読キャラクタリスティックを持っている場合、キャラクタリスティックおよびアトリビュートハンドルは CYBLE_EVT_GATTC_READ_BY_TYPE_RSP イベントでアプリケーションに渡されます。アプリケーションは、キャラクタリスティックの値をチェックして、次の再接続に接続有向宣伝を使用するかを決定します。

7.5.4 Resolving List に／からのデバイスの追加／除外

新しい BLE デバイスは、ローカル IRK、ピア IRK、ピア アイデンティティー アドレスをパラメーターとした CyBle_GapAddDeviceToResolvingList API により、図 17 に示した Resolving List に追加できます。

```
CYBLE_GAP_RESOLVING_DEVICE_INFO_T rpaInfo;

memcpy(&rpaInfo.bdAddr,&peer_ID_Addr[1],CYBLE_GAP_BD_ADDR_SIZE);
rpaInfo.type = smp_key->idAddrInfo[0];
memcpy(rpaInfo.localIrk,local_irk,CYBLE_GAP_SMP_IRK_SIZE);
memcpy(rpaInfo.peerIrk,smp_key->irkInfo,CYBLE_GAP_SMP_IRK_SIZE);

/* Add device to resolving list */
CyBle_GapAddDeviceToResolvingList(&rpaInfo);
```

ピア IRK およびピア アイデンティティー アドレスは CYBLE_EVT_GAP_KEYINFO_EXCHNGE_CMPLT イベントでアプリケーションに渡されます。アプリケーションはこれらの値を保存しなければなりません。ローカル IRK は CyBle_GapGetDevSecurityKeyInfo API で取得できます。

デバイスを Resolving List から除外するために、デバイスのアイデンティティー アドレスで CyBle_GapRemoveDeviceFromResolvingList API を呼び出します。

これらのイベントおよび API の詳細については、BLE コンポーネントのデータシートを参照してください。

7.5.5 サンプル プロジェクト

Link Layer プライバシーを採用したサンプル プロジェクトについては、PSoC Creator で提供されるサンプル プロジェクト **BLE_4.2_DataLength_Security_Privacy** を参照してください。図 10 に示すように、**PSoC Creator** > **File** > **Code Example** で **BLE** に絞り込むことでサンプル プロジェクトにアクセスできます。

8 まとめ

本アプリケーション ノートは Bluetooth LE 4.2 仕様で紹介される新しい機能とそれらの利点、およびそれらを採用したアプリケーションを開発する方法について説明しました。

9 関連アプリケーション ノート

AN94020 - Getting Started with PRoC™ BLE

AN91267 - Getting Started with PSoC® 4 BLE

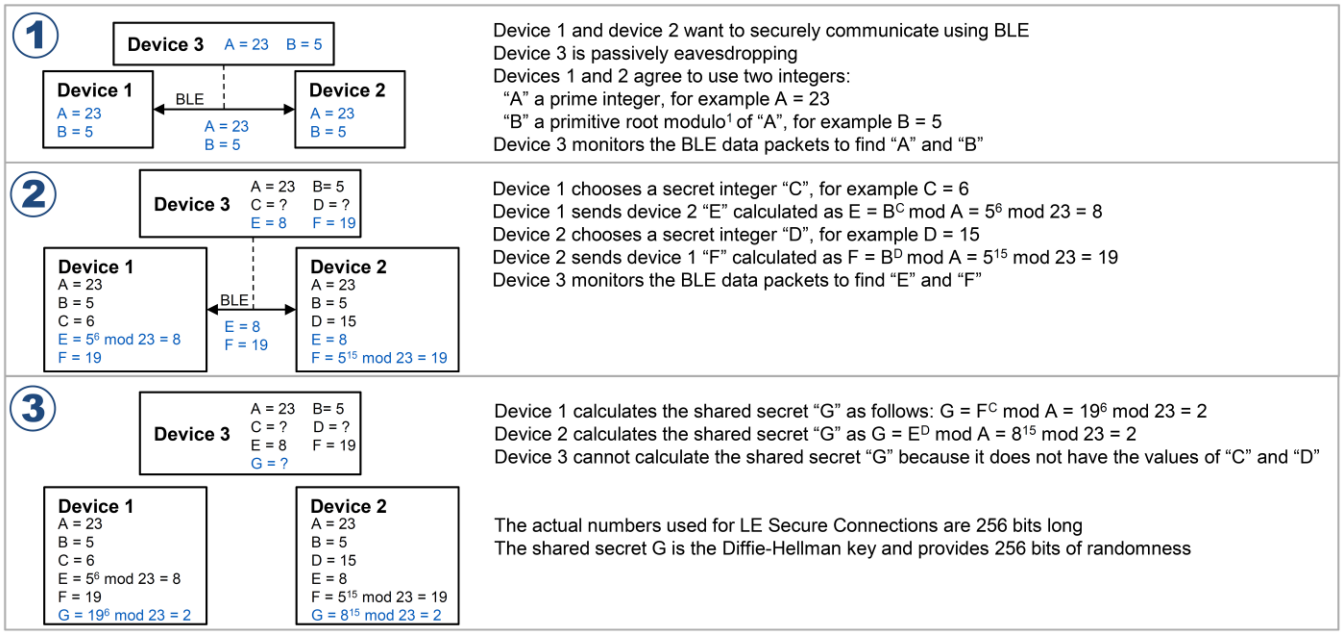
AN97060 - PSoC® 4 BLE and PRoC™ BLE - Over-The-Air (OTA) Device Firmware Upgrade (DFU) Guide

AN91184 - PSoC 4 BLE - Designing BLE Applications

A 受動的盗聴に対する防止

楕円曲線ディフィー ヘルマン (ECDH) アルゴリズムにより、2 つの BLE デバイスは LE セキュア コネクションに基づいたペアリングを使用して共有秘密キーを確立できます。共有秘密キー (ディフィー ヘルマン キー) は、BLE リンクを暗号化する長期キー (LTK) を生成するために、ペアリング プロセスの第 2 フェーズ (認証ステージ 2) で使用されます。ディフィー ヘルマン キーは 256 ビットの乱数を提供し、図 26 に示すように無線で交換されません。

図 26. 共有秘密キーの ECDH による確立



[1]「primitive root modulo」については、George E. Andrews 著『*Number Theory*』(ISBN-10:0486682528) を参照してください。

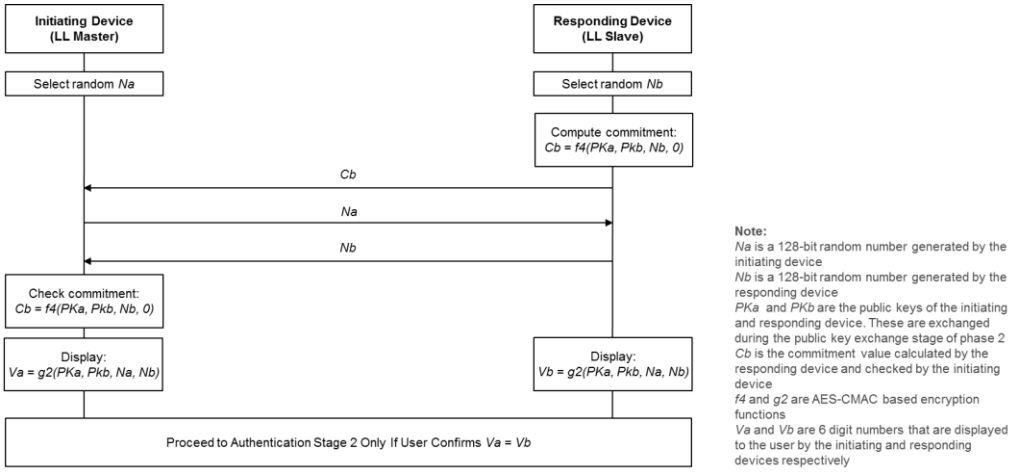
B 中間者 (MITM) 攻撃に対する防止

以下の節は、LE セキュア コネクション ベースのペアリングの数値比較、パスキー入力、および帯域外 (OOB) アソシエーション モデルがどのように MITM の攻撃を防ぐかについて説明します。

B.1 数値比較アソシエーション モデル

図 27 には、数値比較アソシエーション モデルが LE セキュア コネクションに使用される時のペアリング プロセスの認証ステージ 1 を示します。

図 27. 数値比較の認証ステージ 1



数値比較アソシエーション モデルは、MITM の攻撃を防止するために以下の認証手段を使用します。

- 応答デバイスは、発信デバイスの乱数 (*Na*) を受信する前に、応答デバイスの乱数 (*Nb*) と両方の BLE デバイスの公開キーで計算されたコミットメント値 (*Cb*) を共有しなければなりません。
- 発信デバイスは、応答デバイスの乱数 (*Nb*) を受信する前に、発信デバイスの乱数 (*Na*) を共有しなければなりません。
- 発信デバイスは、応答デバイスの乱数 (*Nb*) を受信した後、コミットメント値 (*Cb*) をチェックしなければなりません。

図 28 には、MITM 攻撃者がまず応答デバイスと乱数を交換してから、発信デバイスと乱数を交換するシナリオを示します。

図 28. MITM 攻撃者がまず応答デバイスと乱数を交換してから、発信デバイスと乱数を交換

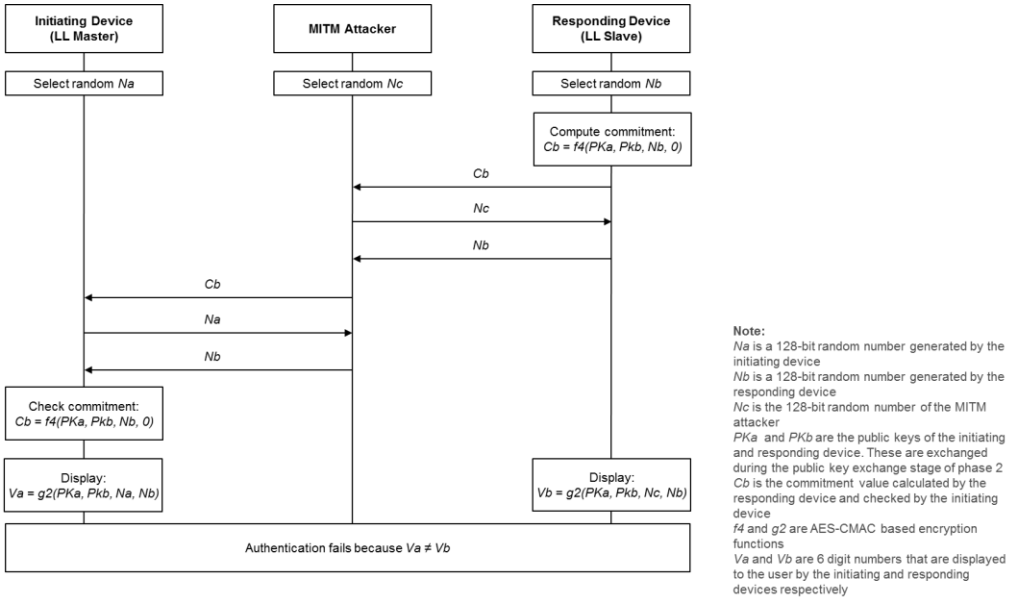


図 28 からわかるように、攻撃者は応答デバイスの乱数 (*Nb*) にアクセスする前に、攻撃者の乱数 (*Nc*) を応答デバイスと共有しなければなりません。このため、両方の BLE デバイスは異なる 6 桁の値を表示し、その結果、ユーザーが表示された値を確認する時に認証失敗となります。

図 29 には、MITM 攻撃者がまず発信デバイスと乱数を交換してから、応答デバイスと乱数を交換するシナリオを示します。

図 29. MITM 攻撃者がまず発信デバイスと乱数を交換してから、応答デバイスと乱数を交換

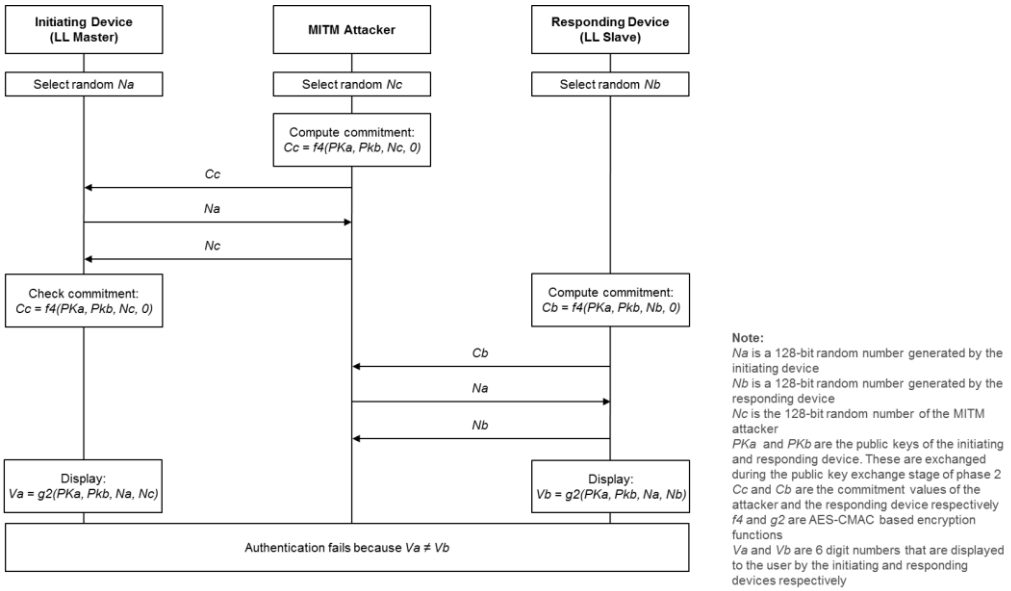
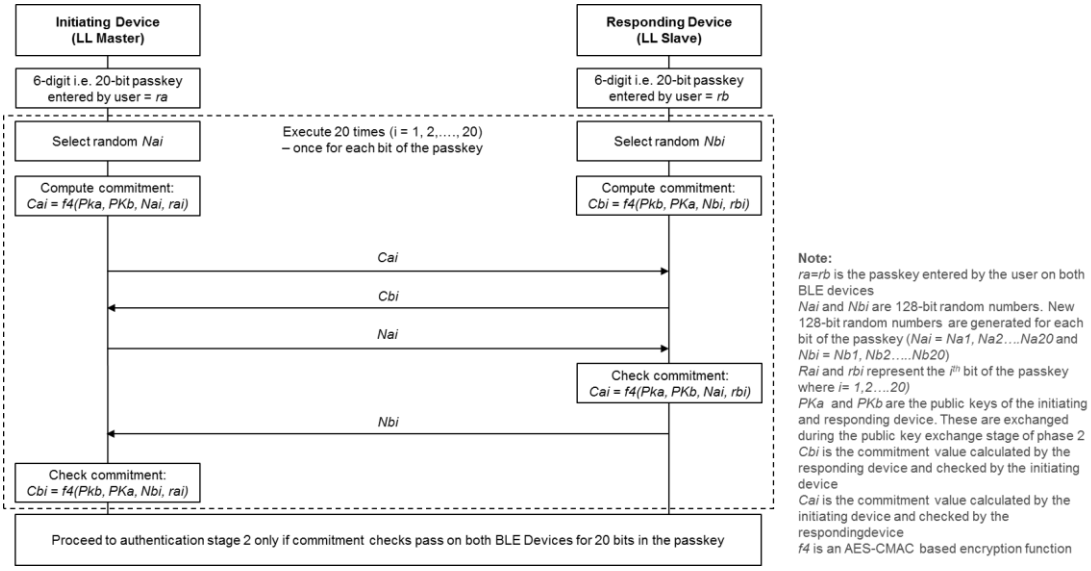


図 29 からわかるように、攻撃者は発信デバイスの乱数 (*Na*) にアクセスする前に、攻撃者のコミットメント値 (*Cc*) を発信デバイスと共有しなければなりません。発信デバイスはコミットメント値をチェックすることで、攻撃者が発信デバイスの乱数を変更しないようにします。このため、両方の BLE デバイスは異なる 6 桁の値を表示し、その結果、ユーザーが表示された値を確認する時に認証失敗となります。

B.2 パスキー入力アソシエーション モデル

図 30 には、パスキー入力アソシエーション モデルが LE セキュア コネクションに使用される時のペアリング プロセスの認証ステージ 1 を示します。

図 30. パスキー入力の認証ステージ 1



パスキー入力アソシエーション モデルは、MITM の攻撃を防止するために以下の認証手段を使用します。

1. 両方の BLE デバイスは、ユーザー入力として共通の 6 桁または 20 ビットのパスキー (*ra* と *rb*) を受信します。
2. ステップ 3～7 は、パスキー内のそれぞれのビット (すなわち、*i = 1, 2,….20*) に対して繰り返されます。
3. 両方の BLE デバイスは 128 ビットの乱数 (*Nai* と *Nbi*) を選択します。
4. 発信デバイスは、両方の BLE デバイスの公開キー (*PKa* と *PKb*)、128 ビットの乱数 (*Nai*) およびパスキーの *i* 番目のビット (*rai*) で計算されたコミットメント値 (*Cai*) を共有します。
5. 応答デバイスは、両方の BLE デバイスの公開キー (*PKa* と *PKb*)、128 ビットの乱数 (*Nbi*) およびパスキーの *i* 番目のビット (*rbi*) で計算されたコミットメント値 (*Cbi*) を共有します。
6. 発信デバイスは 128 ビットの乱数 (*Nai*) を応答デバイスと共有します。
7. 応答デバイスは、発信デバイスの 128 ビット乱数 (*Nai*) を使用して発信デバイスから受信したコミットメント値 (*Cai*) をチェックします。チェックが合格した場合、応答デバイスは 128 ビット乱数 (*Nbi*) を発信デバイスと共有します。
8. 発信デバイスは、応答デバイスの 128 ビット乱数 (*Nbi*) を使用して応答デバイスから受信したコミットメント値 (*Cbi*) をチェックします。チェックが合格した場合、発信デバイスはペアリング プロセスを継続します。

パスキー入力アソシエーション モデルの中心は、パスキーの少しずつ (ビットずつ) の公開です。発信デバイスおよび応答デバイスと関わり合う MITM 攻撃者は、BLE デバイスがコミットメント値のチェックの不合格を検出してペアリング プロセスを中止する前に、パスキーの 2 ビットにのみアクセスできます。数値比較アソシエーション モデルに比べると、パスキー入力アソシエーション モデルのデメリットは、認証手段の 20 回の繰り返し (パスキーのビットごとに 1 回) のためペアリング プロセスに時間がかかることです。

B.3 帯域外 (OOB) アソシエーション モデル

OOB 通信が MITM 攻撃に対して耐性があるため、OOB アソシエーション モデルも MITM 攻撃に対して耐性があります。OOB アソシエーション モデルの主なデメリットは、両方の BLE デバイスが通信のために BLE インターフェースに加えて OOB インターフェースを備えなければならないことです。OOB インターフェースのため、BLE デバイスのコストは増加します。OOB アソシエーション モデルの詳細については、「Bluetooth Core Specification Version 4.2」の第 3 巻、第 H 部、2.3.5.6 節を参照してください。

改訂履歴

文書名: AN99209- PSoC® 4 BLE および PRoC™ BLE: Bluetooth LE 4.2 の特長

文書番号: 002-15739

版	ECN	発行日	変更内容
**	5403984	08/22/2016	これは英語版 001-99209 Rev. **を翻訳した日本語版 002-15739 Rev. **です。
*A	6930940	07/22/2020	これは英語版 001-99209 Rev. *A を翻訳した日本語版 002-15739 Rev. *A です。

ワールドワイドな販売と設計サポート

サイプレスは、事業所、ソリューション センター、メーカー代理店、および販売代理店の世界的なネットワークを保持しています。お客様の最寄りのオフィスについては、サイプレスのロケーション ページをご覧ください。

製品

Arm® Cortex® Microcontrollers	cypress.com/arm
車載用	cypress.com/automotive
クロック&バッファ	cypress.com/clocks
インターフェース	cypress.com/interface
IoT(モノのインターネット)	cypress.com/iot
メモリ	cypress.com/memory
マイクロコントローラ	cypress.com/mcu
PSoC	cypress.com/psoc
電源用 IC	cypress.com/pmic
タッチ センシング	cypress.com/touch
USB コントローラー	cypress.com/usb
ワイヤレス	cypress.com/wireless

PSoC®ソリューション

PSoC 1 | PSoC 3 | PSoC 4 | PSoC 5LP | PSoC 6 MCU

サイプレス開発者コミュニティ

コミュニティ | サンプルコード | Projects | ビデオ | ブログ | トレーニング | Components

テクニカル サポート

cypress.com/support

本書で言及するその他すべての商標または登録商標は、それぞれの所有者に帰属します。

Cypress Semiconductor
An Infineon Technologies Company
198 Champion Court
San Jose, CA 95134-1709

© Cypress Semiconductor Corporation、2016-2020. 本書面は，Cypress Semiconductor Corporation 及び Spansion LLC を含むその子会社（以下「Cypress」という。）に帰属する財産である。本書面（本書面に含まれ又は言及されているあらゆるソフトウェア若しくはファームウェア（以下「本ソフトウェア」という。）を含む）は，アメリカ合衆国及び世界のその他の国における知的財産法令及び条約に基づき Cypress が所有する。Cypress はこれらの法令及び条約に基づく全ての権利を留保し，本段落で特に記載されているものを除き，その特許権，著作権，商標権又はその他の知的財産権のライセンスを一切許諾しない。本ソフトウェアにライセンス契約書が伴っておらず，かつ Cypress との間で別途本ソフトウェアの使用方法を定める書面による合意がない場合，Cypress は，（1）本ソフトウェアの著作権に基づき，（a）ソースコード形式で提供されている本ソフトウェアについて，Cypress ハードウェア製品と共に用いるためにのみ，かつ組織内部でのみ，本ソフトウェアの修正及び複製を行うこと，並びに（b）Cypress のハードウェア製品ユニットに用いるためにのみ，（直接又は再販売者及び販売代理店を介して間接のいずれかで）本ソフトウェアをバイナリーコード形式で外部エンドユーザーに配布すること，並びに（2）本ソフトウェア（Cypress により提供され，修正がなされていないもの）が抵触する Cypress の特許権のクレームに基づき，Cypress ハードウェア製品と共に用いるためにのみ，本ソフトウェアの作成，利用，配布及び輸入を行うことについての非独占的で譲渡不能な一身専属的ライセンス（サブライセンスの権利を除く）を付与する。本ソフトウェアのその他の使用，複製，修正，変換又はコンパイルを禁止する。

適用される法律により許される範囲内で，Cypress は，本書面又はいかなる本ソフトウェア若しくはこれに伴うハードウェアに関しても，明示又は黙示をとわず，いかなる保証（商品性及び特定の目的への適合性の黙示の保証を含むがこれらに限られない）も行わない。いかなるコンピューティングデバイスも絶対に安全ということはない。従って，Cypress のハードウェアまたはソフトウェア製品に講じられたセキュリティ対策にもかかわらず，Cypress は，Cypress 製品への権限のないアクセスまたは使用といったセキュリティ違反から生じる一切の責任を負わない。加えて，本書面に記載された製品には，エラッタと呼ばれる設計上の欠陥またはエラーが含まれている可能性があり，公表された仕様とは異なる動作をする場合がある。適用される法律により許される範囲内で，Cypress は，別途通知することなく，本書面を変更する権利を留保する。Cypress は，本書面に記載のある，いかなる製品若しくは回路の適用又は使用から生じる一切の責任を負わない。本書面で提供されたあらゆる情報（あらゆるサンプルデザイン情報又はプログラムコードを含む）は，参照目的のためのみに提供されたものである。この情報で構成するあらゆるアプリケーション及びその結果としてのあらゆる製品の機能性及び安全性を適切に設計，プログラム，かつテストすることは，本書面のユーザーの責任において行われるものとする。Cypress 製品は，兵器，兵器システム，原子力施設，生命維持装置若しくは生命維持システム，蘇生用の設備及び外科的移植を含むその他の医療機器若しくは医療システム，汚染管理若しくは有害物質管理の運用のために設計され若しくは意図されたシステムの重要な構成部分としての使用，又は装置若しくはシステムの不具合が人身傷害，死亡若しくは物的損害を生じさせるようなその他の使用（以下「本目的外使用」という。）のためには設計，意図又は承認されていない。重要な構成部分とは，それの不具合が装置若しくはシステムの不具合を生じさせるか又はその安全性若しくは実効性に影響すると合理的に予想できるような装置若しくはシステムのあらゆる構成部分をいう。Cypress 製品のあらゆる本目的外使用から生じ，若しくは本目的外使用に関連するいかなる請求，損害又はその他の責任についても，Cypress はその全部又は一部をとわず一切の責任を負わず，かつ Cypress はそれら一切から本書により免除される。Cypress は Cypress 製品の本目的外使用から生じ又は本目的外使用に関連するあらゆる請求，費用，損害及びその他の責任（人身傷害又は死亡に基づく請求を含む）から免責補償される。

Cypress，Cypress のロゴ，Spansion，Spansion のロゴ及びこれらの組み合わせ，WICED，PSoC，CapSense，EZ-USB，F-RAM，及び Traveo は，米国及びその他の国における Cypress の商標又は登録商標である。Cypress のより完全な商標のリストは，cypress.com を参照すること。その他の名称及びブランドは，それぞれの権利者の財産として権利主張がなされている可能性がある。