AN99209

PSoC® 4 BLE 和 PRoC™ BLE：低功耗蓝牙 4.2 特性

作者： utsv@cypress.com、sasd@cypress.com、ankc@cypress.com

相关器件系列：CYBL11X7X 和 CY8C4XX8-BL5XX

相关应用笔记：要想获取完整列表，请点击此处。

要想获取本应用笔记的最新版本或相关项目文件，请访问 http://www.cypress.com/AN99209。

AN99209 提供了有关低功耗蓝牙（BLE）4.2 的特性、它们的优点以及相关应用的概况。本应用笔记还说明了使用赛普拉斯 PSoC 4/PRoC BLE 4.2 器件的各种应用是如何使用这些特性的。

目录

1 简介 1
2 PSoC/PRoC 资源 2
3 PSoC Creator 3
3.1 PSoC Creator 帮助 3
3.2 代码示例 4
4 BLE 4.2 特性简介 5
5 LE 数据包长度扩展 5
5.1 优点 6
5.2 应用 8
5.3 在 PSoC Creator 中开发使用 LE 数据包长度扩展特性的各种应用 8
6 低功耗安全连接 9
6.1 更新配对过程 10
6.2 优点 13
6.3 应用 13
6.4 通过 PSoC Creator 开发支持 LE 安全连接的应用 13
7 链路层（LL）保密 15
7.1 保密功能简介 15
7.2 保密概念 15
7.3 优点 19
7.4 应用 20
7.5 通过 PSoC Creator 开发使用链路层保密的应用 20
8 汇总 23
9 相关应用笔记 23
A 防御被动窃听 24
B 防御中间人（MITM）攻击 25
B.1 数字比较关联模型 25
B.2 密钥输入关联模型 27
B.3 带外数据（OOB）关联模型 27
文档修订记录 28
全球销售和设计支持 29
产品 29
PSoC®解决方案 29
赛普拉斯开发者社区 29
技术支持 29

1 简介

2014 年 12 月 2 日，蓝牙技术联盟（SIG）发布了蓝牙内核规范版本 4.2。该版本介绍了三个主要特性：LE 数据包长度扩展、链路层保密（也称保密 1.2）和 LE 安全连接。这些特性使低功耗蓝牙（BLE）或称作 Bluetooth Smart 器件变得更加聪明、快捷和保密，并适用于物联网（IoT）。您可以点击此处下载该规范。

赛普拉斯 PRoC BLE（CYBL11X7X）和 PSoC 4 BLE（CY8C4XX8-BL5XX）器件完全符合蓝牙 4.2 规范，并能够支持上述的三种新特性。这些器件还具有一个 DMA 控制器，支持进行数据传输，无需 CPU 的干预。它们还包含 256 KB 的闪存和 32 KB 的 RAM，用于进行空中传送（OTA）的固件更新，无需外部存储器。通过将 PSoC Creator 中的 BLE 组件更新为版本 3.0 或更高版本，可以使传统的 BLE 器件支持 LE 安全连接特性。表 1 总结了赛普拉斯的不同器件所支持的蓝牙 4.2 特性。

表 1. 赛普拉斯器件支持新蓝牙特性

特性	蓝牙 4.1 设备	蓝牙 4.2 设备
LE 数据包长度扩展	不支持	支持
链路层保密	不支持	支持
LE 安全连接	支持	支持

本应用笔记对新蓝牙 4.2 特性和它们的优点进行了简介，并说明了如何在使用赛普拉斯 PRoC BLE 和 PSoC 4 BLE 器件的应用中使用这些特性。本应用笔记假设您已经基本了解 BLE 架构和相关术语。

- 如果您尚未熟悉 BLE 或 PSoC，请参考应用笔记 AN91627 — PSoC® 4 BLE 入门或 AN94020 — PRoC™ BLE 入门。
- 要想了解 PSoC Creator 中的 BLE 组件以及如何通过标准 BLE 服务开发各种应用，请参考应用笔记 AN91184 — 使用 PSoC 4 BLE 设计 BLE 应用。
- 更多有关蓝牙规范的信息，请参考蓝牙 SIG 网站。

2 PSoC/PRoC 资源

赛普拉斯的网站 www.cypress.com 上提供了大量资料，有助于选择符合您设计的 PSoC（可编程片上系统）和 PRoC（可编程片上射频）器件，并能够快速、有效地将该器件集成到您的设计中。有关资源的完整列表，请参考 KBA86521 — 如何使用 PSoC 3、PSoC 4 和 PSoC 5LP 的资源进行设计。下面提供的是 PSoC 4 BLE 和 PRoC BLE 的简要列表：

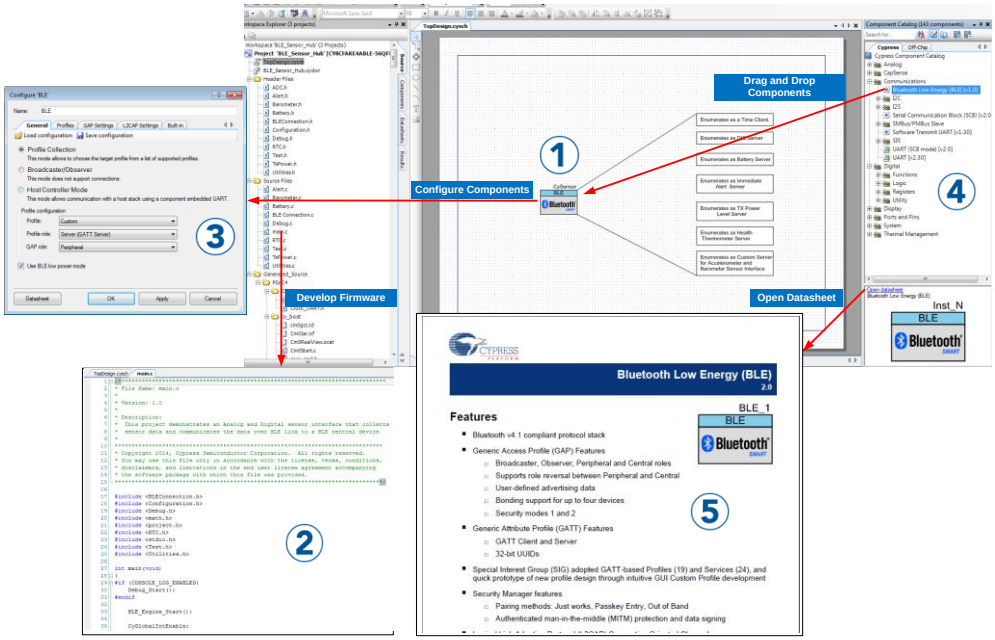
- **概况：**Bluetooth® Low Energy 产品系列、赛普拉斯无线/射频蓝图
- **产品选型器：**PSoC 4 BLE 或 PRoC BLE。此外，PSoC Creator 还包含了一个器件选择工具。
- **数据手册**描述并提供了适用于 PSoC 4 BLE 和 PRoC BLE 器件系列的电气规范。
- **CapSense 设计指南**：了解如何使用 PSoC 4、PSoC 4 BLE 和 PRoC BLE 器件系列的资源来设计电容式触摸感应应用。
- **应用笔记和代码示例**包括了从基本到高级的广泛主题。许多应用笔记还提供了代码示例。
- **技术参考手册（TRM）**详细说明了 PSoC 4 BLE 和 PRoC BLE 器件系列中的架构和寄存器。
- **开发套件：**
  - CY8CKIT-042-BLE：通过 Pioneer 套件，用户能够使用 PSoC 4 BLE 和 PRoC BLE 器件来评估和开发 BLE 应用。
  - CY8CKIT-143A：通过带有蓝牙 4.2 射频、256 KB 大小的 PSoC 4 BLE 模块，用户可以评估 CY8C4XX8-BL5XX 系列器件。
  - CY5676A：通过支持蓝牙 4.2 射频的 256 KB 大小的 PRoC BLE 模块，用户可以评估 CYBL11X7X 系列器件。
  - CY5677：通过 CySmart BLE 4.2 USB 收发器，用户可以使用 CySmart PC 工具来测试和调试 BLE 4.2 特性。
  - CY5682：PRoC BLE 触控鼠标参考设计套件提供了 BLE 触控鼠标的量产实施方案。
  - CY5672： PRoC BLE 遥控参考设计套件提供了 BLE 遥控的量产实施方案。
- **MiniProg3** 器件提供了一个接口，用于进行闪存编程和调试。
- **CySmart** 是一个适用于 Windows PC 的 BLE 主机仿真工具。该工具提供了一个易用的 GUI，用于测试和调试用户的 BLE 外设应用。
- **CySmart — 移动应用**是由赛普拉斯开发的 Android™/iOS®手机应用程序，用于连接和测试不同的 BLE 产品，包括赛普拉斯的 BLE 开发套件。
- **赛普拉斯的自定义 BLE 配置文件和服务：**赛普拉斯定义了一些自定义 BLE 配置文件和服务。这样用户便能够通过 BLE 为不受由蓝牙 SIG 特定的标准 BLE 配置文件和服务支持的各种特性进行数据传输。

3 PSoC Creator

PSoC Creator 是一个基于 Windows 的免费集成开发环境（IDE）。通过它可以同时对 PSoC 3、PSoC 4、PSoC 4 BLE、PRoC BLE 和 PSoC 5LP 器件进行硬件和固件设计。如图 1 所示，通过 PSoC Creator，您可以进行以下操作：

1. 将组件图标拖放到主设计工作区中，以进行您的硬件系统设计。
2. 协作设计您的应用固件和 PSoC 硬件。
3. 使用配置工具来配置各组件。
4. 体验包含 100 多个组件的库。
5. 查看组件数据手册

图 1. PSoC Creator 的原理图输入项和组件



3.1 PSoC Creator 帮助

请访问 PSoC Creator 主页，以下载并安装 PSoC Creator 的最新版本。然后，启动 PSoC Creator，并导航到下列各项：

- **快速入门指南**：依次选择 **Help >Documentation > Quick Start Guide**。本指南提供了与开发 PSoC Creator 项目有关的基本知识。
- **简单的组件代码示例**：依次选择 **File > Code Example**。这些代码示例展示了如何配置和使用 PSoC Creator 组件。
- **系统参考指南**：依次选择 **Help > System Reference Guides**。该指南列出并描述了 PSoC Creator 所提供的系统功能。
- **组件数据手册**：右击组件，然后选择“Open Datasheet”项。请访问 PSoC 4/PRoC BLE 组件数据手册网页，以获取 PSoC 4/PRoC BLE 组件的所有数据手册列表。
- **文档管理工具**：PSoC Creator 提供了一款文档管理工具，便于查找和参考文档资源。要想打开文档管理工具，请依次选择菜单项：**Help >Document Manager**。

3.2 代码示例

PSoC Creator 为您提供了较多的代码示例。可以从 PSoC Creator 的起始页上获取这些项目，如图 2 所示。

通过向您提供完整的设计（并非一个空白设计），代码示例可以加快您的设计进程。代码示例还介绍了如何将 PSoC Creator 组件用于不同的应用中。

在图 3 所示的 **Find Code Example** 对话框中，您可以选择以下选项：

- 可以根据 Architecture（架构）、Device family（器件系列，如：PSoC 4、PSoC 4 BLE、PRoC BLE 等）、Category（类型）或 Keyword（关键词）等选项筛选示例。
- 从 **Filter Options** 的示例菜单中进行选择。共有 30 多个 BLE 代码示例供您参考，如图 3 所示。
- 通过 **Documentation** 选项卡，查看选中的数据手册。
- 查看已选的代码示例。您可以复制该窗口中的代码，然后将其粘贴在您的项目内，从而加快代码开发过程；
- 或根据所选项目创建一个新的项目（需要时可添加新的工作区）。向您提供了一个完整的基本设计，该方式可以加快您的设计进程。然后，您可以根据自己的应用调整该设计。

除了 PSoC Creator 代码示例外，您还可以在赛普拉斯的 GitHub 资料库中查询 BLE 示例项目。

图 2. PSoC Creator 中的代码示例

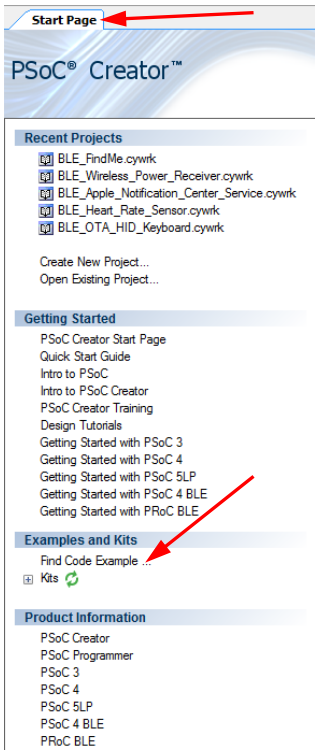
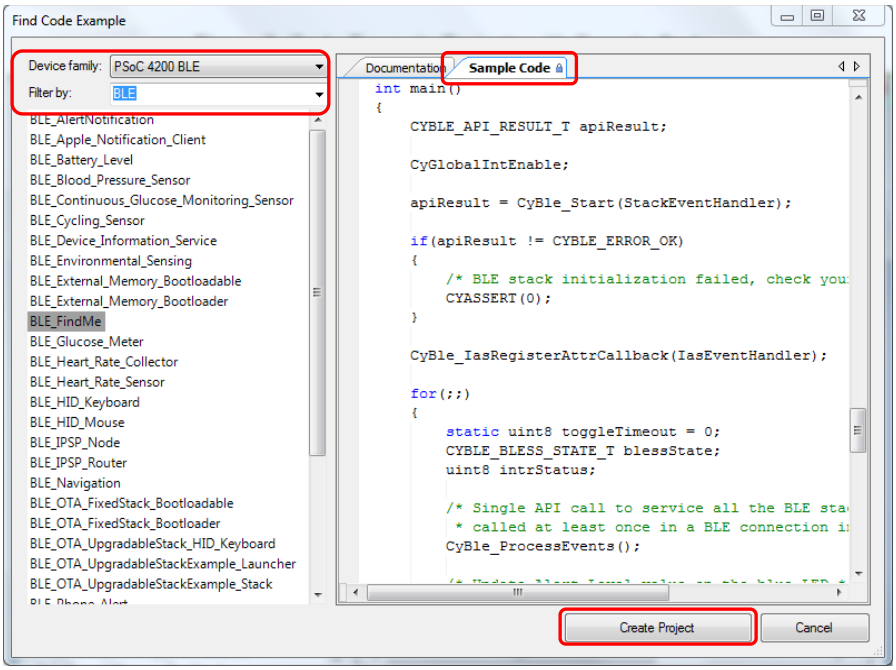


图 3. 带样本代码的示例项目



4 BLE 4.2 特性简介

蓝牙 4.2 向您介绍了以下三个主要特性：LE 数据包长度扩展、链路层（LL）保密和低功耗安全连接。下面各章节对这些新特性进行了详细说明。

5 LE 数据包长度扩展

链路层（LL）是 BLE 协议栈的一部分，用于实现广播、扫描、建立和保持连接。

图 4 显示的是链路层数据包的格式。它包含四个字段：序言、访问地址、协议数据单元（PDU）和循环冗余校验（CRC）。在广播、扫描或建立连接的过程中使用广播通道 PDU 传输数据包。而用于与连接器件交换数据的数据包是通过数据通道 PDU 传输的。

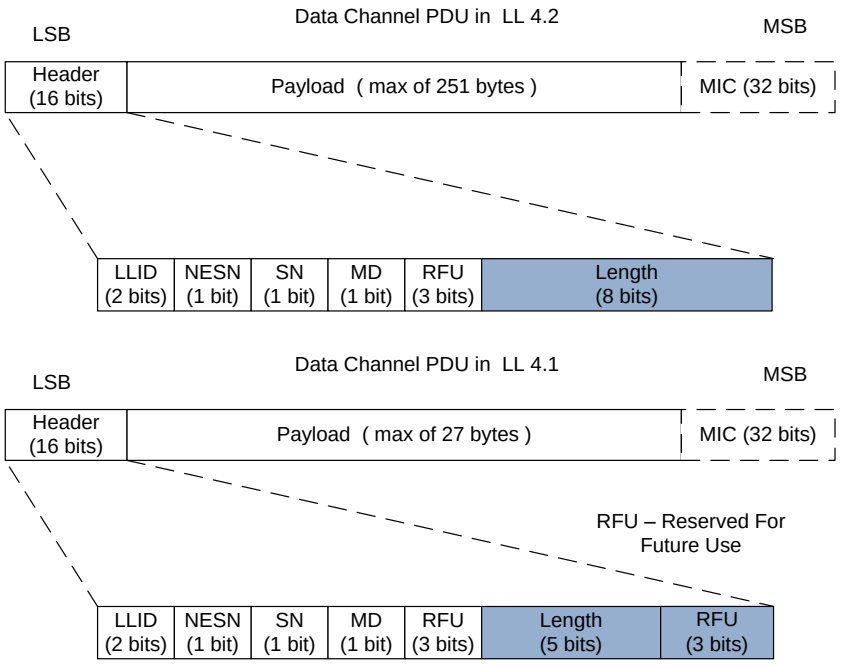
图 4. 链路层数据包格式

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)

数据通道 PDU 包含一个 16 位的头文件、一个长度可调的 payload（有效负载）字段和一个可选的信息完整性检查（MIC）字段。在蓝牙 4.2 规范中，数据通道 PDU 中 payload 字段的最大长度可从 27 字节增加到 251 字节，从而使数据通道的吞吐量大约提高 10 倍（请参考更大的吞吐量一节的内容）。

图 5 显示的是蓝牙 4.2 和蓝牙 4.1 中数据通道 PDU 的差异。

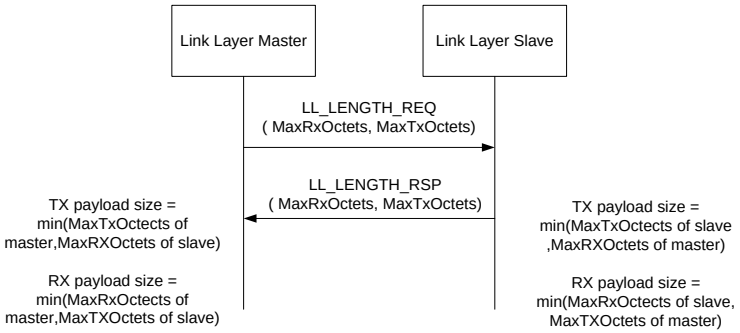
图 5. 蓝牙规范版本 4.2 和 4.1 中的 LE 数据通道 PDU



头文件中的长度字段指定跟随该头文件的数据字节数。头文件中的长度字段从 5 位（蓝牙 4.1）增加到 8 位（蓝牙 4.2），从而使长度字段的值从 31 增加到 255。加密数据包中所使用的信息完整性检查（MIC）的长度为 4 字节。因此，蓝牙 4.2 和蓝牙 4.1 规范中最大可用 payload 字段长度分别为 251 字节和 27 字节。要想了解头文件中的其他字段，请参考蓝牙核心规范版本 4.2 第 6 卷 B 部分中第 2.4 章节的内容。

该链路层使用数据长度更新程序来协商传输和接收方向中所使用的 payload 长度，如图 6 所示。通过两个新添加的链路层控制 PDU（LL_LENGTH_REQ 和 LL_LENGTH_RSP），可以交换设备支持的最大 payload 长度。设备可传输的最大 payload 长度被称为 MaxTxOctets，而设备可接收的最大 payload 长度被称为 MaxRxOctets。实际传输（TX）和接收（RX）的 payload 长度取决于数据长度更新程序。其中，实际 TX 的 payload 长度是局部 MaxTxOctets 和对等设备 MaxRxOctets 参数两者中较小的那个值；同样，实际 RX 的 payload 长度是局部 MaxRxOctets 和对等设备 MaxTxOctets 参数两者中较小的那个值。该链路层使用的 payload 字段长度默认为 27 字节，直到数据长度更新程序完成为止。接收到 LL_LENGTH_REQ PDU 时，不支持该特性的设备会使用 LL_UNKNOWN_RSP PDU 进行响应。然后，链路层将使用长度默认为 27 字节的 payload。

图 6. 数据长度更新程序



5.1 优点

通过 LE 数据包长度扩展特性，各应用可提高吞吐量、降低功耗，并能够使用不对称的带宽。要想获得这些优点，需要满足以下条件：

- 两个 BLE 设备都要支持 LE 数据包长度扩展特性
- 高层协议使用大于默认的最大传输单元（MTU）（23 字节）的尺寸

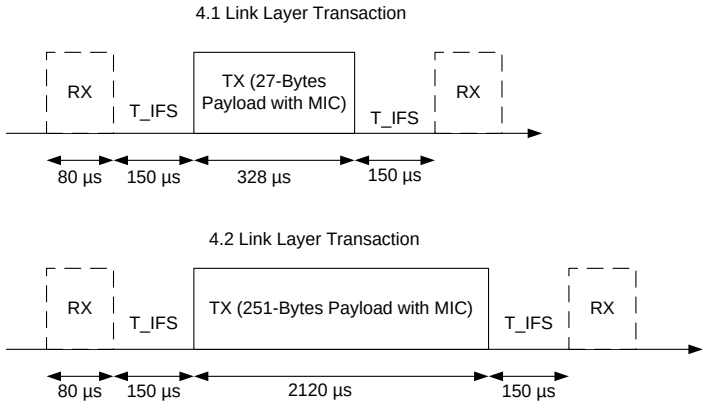
5.1.1 更大的吞吐量

使用 LE 数据包长度扩展特性，通过链路层的吞吐量可提高 2.6 倍。在上面内容中，图 4 显示的是链路层数据包格式，图 5 显示的是数据通道 PDU 中的不同字段。其中，MIC 字段只被附加在非零 payload 数据通道 PDU 中的加密数据包中。

Payload 字段为零时，数据包的最短传输时间为 80 µs。当 payload 字段分别为 27 字节（蓝牙 4.1 设备）和 251 字节（蓝牙 4.2 设备）时，所对应的数据包最长传输时间分别为 328 µs 和 2120 µs。

图 7 显示的是蓝牙 4.1 和 4.2 设备传输数据时采用的典型的链路层传输。单个数据包传输操作包含以下部分：空数据包（payload 大小为 0）的一个 RX、150 µs 的帧间隔（T_IFS）、一个包含最长 payload 的数据包的 TX 以及 T_IFS，直到发生下一个 RX 操作为止。这时，将重复该程序。在下图中第二个 RX 的位置上，第一个 TX 数据包被确认，并开始进行新的传输。

图 7. 链路层传输



该链路层的吞吐量（即 BLE 协议栈中高层位置上可用的吞吐量）被定义为：

吞吐量 = Payload 长度/ 单传输操作时间

在蓝牙 4.1 设备中，payload 长度为 27 字节（216 位），并且单传输操作需要时间为 708 µs。因此，理论上的吞吐量可达 298 kbps。

在蓝牙 4.2 设备中，payload 长度为 251 字节（2008 位），并且传输操作需要时间为 2500 µs。因此，理论上的吞吐量可达 784 kbps。可见，蓝牙 4.2 设备的理论吞吐量是蓝牙 4.1 设备的 2.6 倍。

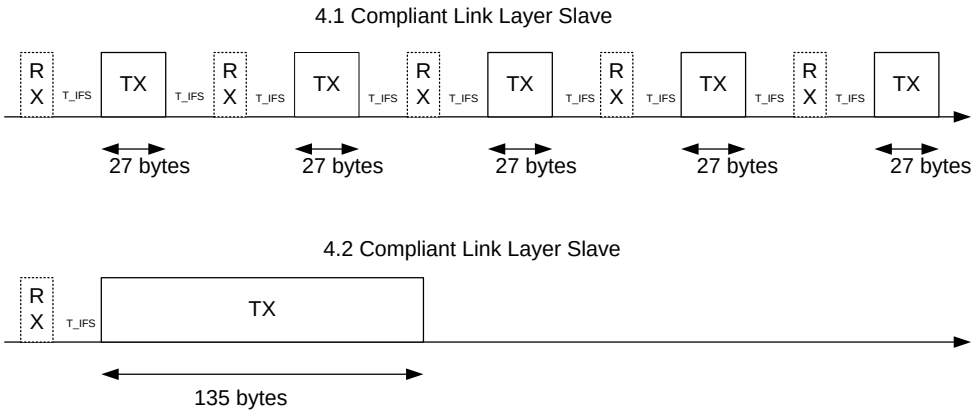
5.1.2 低功耗

在真空理想条件下，通过 LE 数据包长度扩展特性可获得更有效的带宽，从而降低器件功耗。

与蓝牙 4.1 设备相比，蓝牙 4.2 设备需要实现更少的传输操作便能传输给定的数据量。这样可缩短射频收发器处于有效状态的时间，并且设备能够保持低功耗模式的时间更长，从而降低消耗的平均电流。

图 8 介绍了该机制（假设链路层的 payload 长度为 135 字节）在蓝牙 4.1 设备中，该 135 字节长的 payload 字段被分为多个长度为 27 字节的 payload，并通过 5 个传输操作传输。在蓝牙 4.2 的设备中，可以在单个传输操作中发送 135 字节长的 payload。

图 8. 135 字节的数据传输案列



5.1.3 不对称带宽

不对称带宽指的是使用不同的 TX 和 RX 带宽。它有助于空中传送（OTA）固件更新等应用。这些应用要求 RX 方向的带宽较高，并且 TX 方向上的带宽较低。要想获得不对称带宽，您需要为局部 MaxTxOctets 和 MaxRxOctets 选择合适的值。例如，分别将 MaxTxOctets 和 MaxRxOctets 的值设置为 251 字节和 27 字节，便可在传输方向上提供更大带宽。同样，分别将 MaxTxOctets 和 MaxRxOctets 的值设置为 27 字节和 251 字节，便可在接收方向上提供更大带宽。

5.2 应用

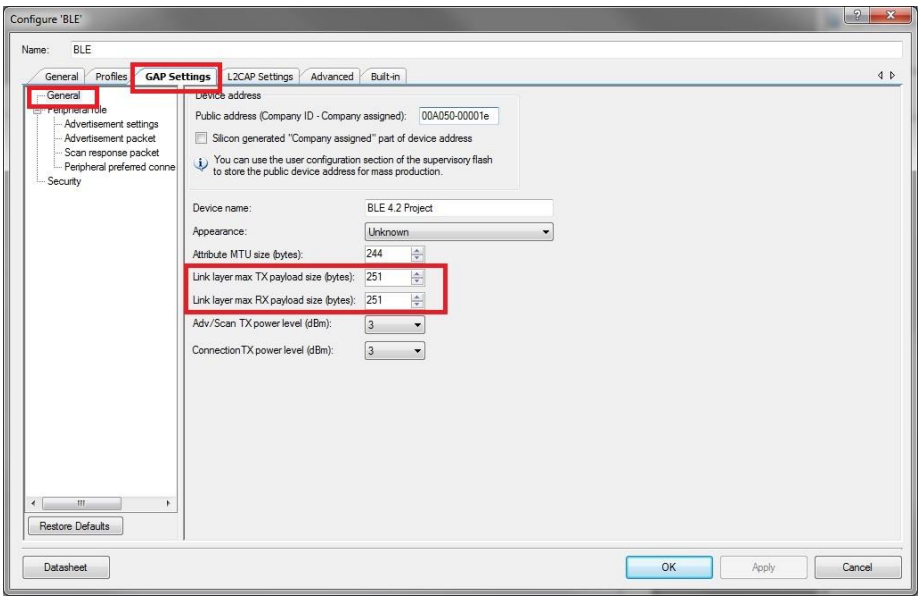
- 通过 BLE 发送音频数据（Audio-over-BLE）能够利用更高的带宽来降低压缩数据所需的功耗。
- 空中传送（OTA）固件更新过程可在更短时间内完成，并能够降低功耗。
- 互联网协议支持配置文件（IPSP）数据包可进行更快的数据交换，从而可以加快检测和传输操作。
- 通过使用更长的数据 payload 字段，可以加快多个传感器中数据记录的速度。

5.3 在 PSoC Creator 中开发使用 LE 数据包长度扩展特性的各种应用

5.3.1 组件配置

要想使用 LE 数据包长度扩展特性，请依次打开 **GAP Settings** > **General** 项，然后分别在 **Link Layer max TX payload size (bytes)**和 **Link Layer max RX payload size (bytes)**框中选择适合 BLE 组件的 MaxTxOctets 和 MaxRxOctets 数值（如图 9 所示）。

图 9. 配置 BLE 组件中的 LE 数据包长度扩展参数



5.3.2 应用处理

建立连接后，BLE 堆栈将立即自动根据组件配置与对等设备协商 TX 和 RX 的 payload 长度。表 2 总结了各种 BLE 堆栈事件名称、事件说明以及使能 LE 数据包长度扩展特性所需进行的操作。

表 2. BLE 堆栈事件以及使能 LE 数据包长度扩展特性所需进行的操作

BLE 堆栈事件名称	事件说明	事件处理操作
CYBLE_EVT_GAP_DATA_LENGTH_CHANGE	报告已协商好的 TX 和 RX 长度	信息事件

通过 CYBLE_EVT_GAP_DATA_LENGTH_CHANGE BLE 堆栈事件，可将该连接已协商好的最大传输和接收的 payload 尺寸通知给应用。通过该事件，应用固件会知道该连接上最大 TX 和 RX 的 payload 尺寸的变化。

表 3 提供了用于支持 LE 数据包长度扩展特性的新 API 列表（以及相关的说明内容）。

表 3. 支持 LE 数据包长度扩展特新的新 API

API	说明
CyBle_GapSetDataLength	设置新的 TX payload 尺寸，用于初始化新的数据长度更新程序。

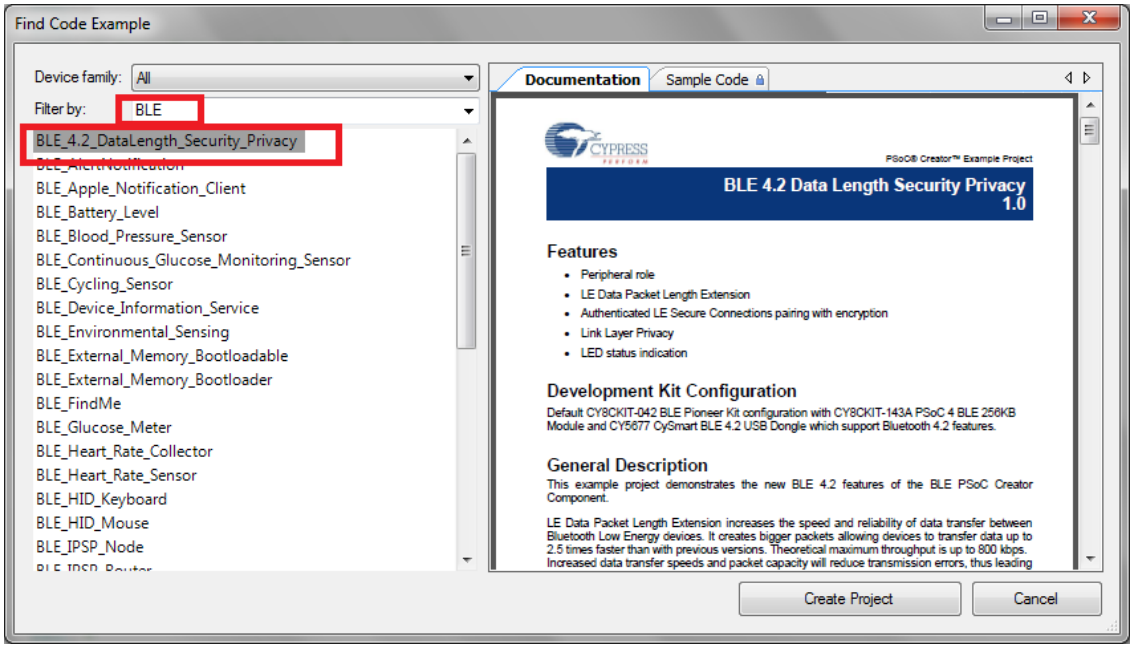
建立连接后，通过使用 CyBle_GapSetDataLength API，您可以随时更改 MaxTxOctets 参数。该 API 初始化一个新的数据包长度更新程序。该程序完成后，实际的传输和接收的 payload 尺寸将通过 CYBLE_EVT_GAP_DATA_LENGTH_CHANGE 事件被通知给应用。

更多有关 BLE 协议栈事件和 API 的信息，请参考 BLE 组件数据手册。

5.3.3 示例项目

PSoC Creator 中所提供的 **BLE_4.2_DataLength_Security_Privacy** 示例项目使用了 LE 数据包长度扩展特性。通过依次选择 **PSoC Creator** > **File** > **Code Example** 并将筛选项设置为 **BLE**，可以阅读该示例项目，如图 10 所示。

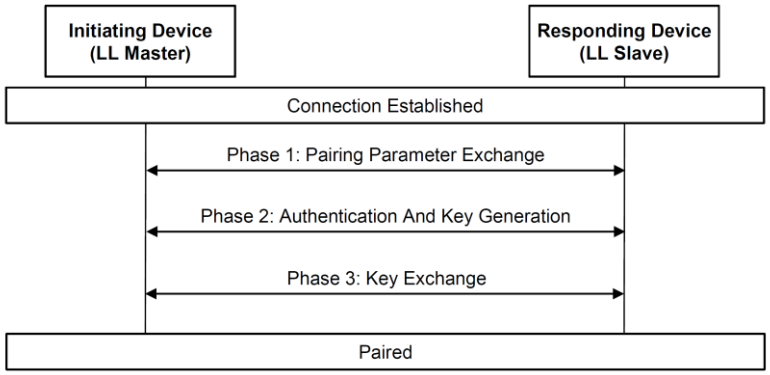
图 10. BLE 4.2 示例项目



6 低功耗安全连接

配对指的是两个 BLE 设备间认证和密钥的交换的过程。该配对过程包括三个阶段，如图 11 所示。LE 安全连接指的是蓝牙 4.2 规范中介绍的一个加强的安全功能。它使用了一个用于生成密钥的符合联邦信息处理标准（FIPS）算法（也称 Elliptic Curve Diffie-Hellman（ECDH））以及用于密钥交换的新程序。BLE 应用中的关联模型指的是根据两个 BLE 设备的输入和输出功能来确定配对方法的模型。蓝牙 4.2 规范向您介绍了一个新的关联模型，即数字比较（NC）。

图 11. 配对过程



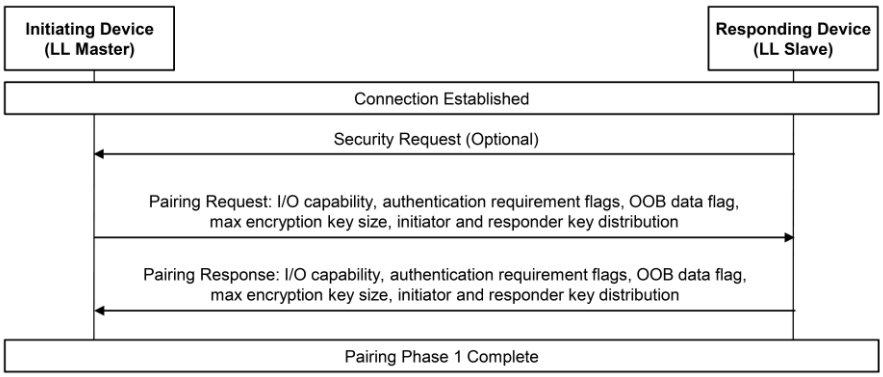
下面各节描述了配对过程的三个阶段，以及 LE 安全连接特性对每个阶段的影响。

6.1 更新配对过程

6.1.1 配对阶段 1

在配对的第一个阶段中，初始化设备和响应设备进行交换配对参数（如输入/输出功能、认证要求标志、加密密钥大小以及频带外（OOB）数据的可用性）。LE 传统配对和 LE 安全连接的第一个配对阶段是相同的（如图 12 所示）。

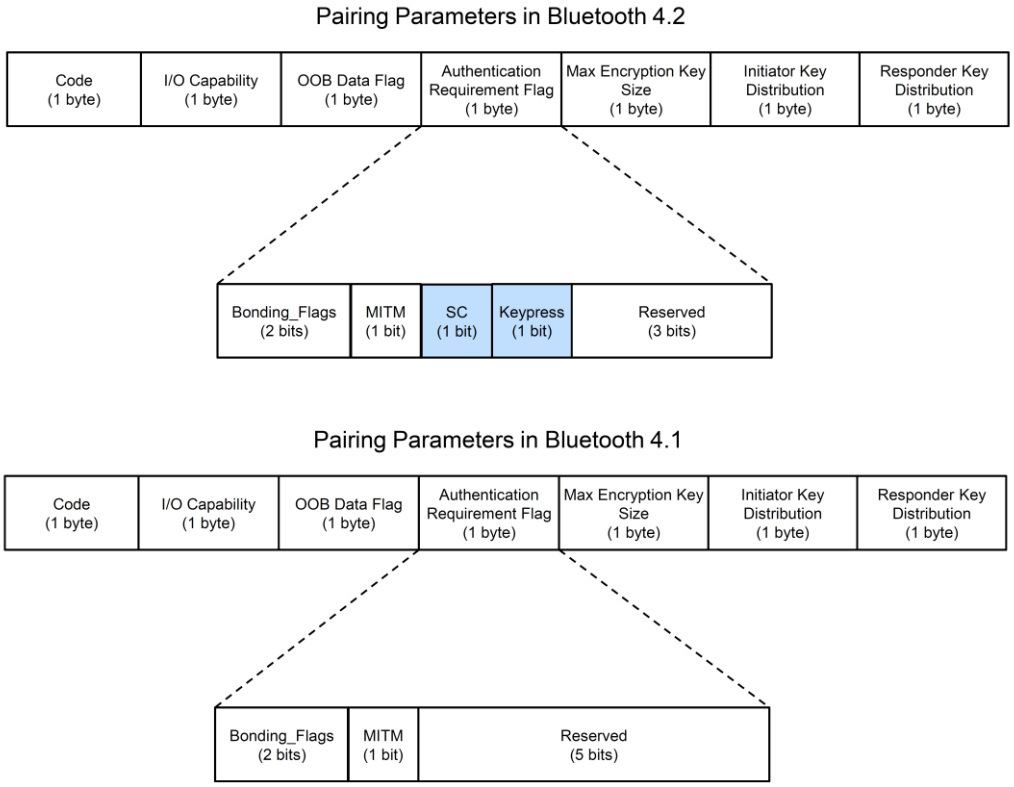
图 12. LE 配对阶段 1



初始化设备（如链路层主设备）通过配对请求命令进行参数交换。响应设备（如链路层从设备）将通过配对响应命令做出响应。该响应设备还可以通过安全请求命令来初始化配对过程。

认证要求标志是配对参数的一部分。在蓝牙 4.2 设备中，更新这些标志可以添加两个新的字段，即安全连接（SC）和按键。图 13 显示的是蓝牙 4.1 和 4.2 设备中的配对参数和认证要求标志。

图 13. 配对参数



第二个配对阶段的配对方式或关联模型取决于第一个阶段中所交换的参数。第二个配对阶段可以采用以下四种配对方法或关联模型：

- Just Works（直接连接）
- Numeric Comparison（数字比较 — 仅适用于 LE 安全连接）
- Passkey Entry（万能钥匙）
- Out Of Band （带外数据 — OOB）

表 4. 确定 LE 安全连接中的关联模型

		初始化设备			
		设置 OOB 数据标志	未设置 OOB 数据标志	设置 MITM	未设置 MITM
响应设备	设置 OOB 数据标志	使用 OOB	使用 OOB		
	未设置 OOB 数据标志	使用 OOB	检查 MITM		
	设置 MITM			使用 I/O 功能	使用 I/O 功能
	未设置 MITM			使用 I/O 功能	使用 “Just Works” 模型

表 4 显示的是：根据第一个阶段中所交换的配对参数，如何在 LE 安全连接中确定第二配对阶段的关联模型。在 LE 安全连接中， 如果初始化和响应设备都具有 Display 和 Yes/No I/O 功能，或者 Display 和 Keyboard I/O 功能，那么可以使用数字比较的关联模型。请参考蓝牙内核规范版本 4.2 第 3 卷 H 部分第 2 章节的内容，深入了解在一个或两个 BLE 设备支持 LE 传统配对特性的情况下，如何根据 I/O 功能确定关联模型。

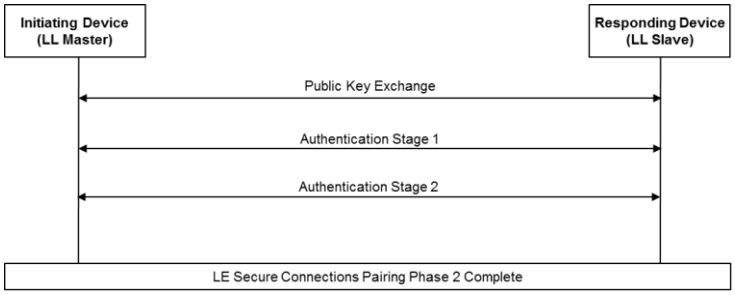
6.1.2 配对阶段 2

第二个配对阶段包括用于防止中间人（MITM）攻击的认证以及用于加密 BLE 链接的密钥生成。

在 LE 的传统配对中，可以使用一个临时密钥（0：Just Works 模型、6 数字或 20 位：Passkey Entry 模型、128 位：OOB 模型）来获得可加密 BLE 链接的密钥。该临时密钥是未通过 BLE 链接交换的随机数据。更多有关 LE 传统配对的信息，请参考蓝牙内核规范版本 4.2 第 3 卷 H 部分中第 2.3.5 章节的内容。

LE 安全连接中的第二个配对阶段包括三个小阶段，如图 14 所示。

图 14. LE 安全连接配对第二阶段



在公有密钥交换阶段中，初始化设备和响应设备将互换它们的公有密钥，并开始计算 Diffie-Hellman 密钥。您可以使用 Elliptic-Curve Diffie-Hellman 功能（P256）来生成 Diffie-Hellman 密钥。该 P256 将对等设备的特定密钥和公有密钥作为输入。Diffie-Hellman 密钥始终不被无线交换，它能够提供随机的 256 位数据。请参考防御被动窃听一节，了解初始化和响应设备如何通过 ECDH 算术来计算出一个公用的 Diffie-Hellman 密钥，并不需要通过 BLE 链接交换密钥。

在认证阶段 1 中，各 BLE 设备将进行互相认证，以防止中间人（MITM）攻击。每个关联模型的认证阶段 1 各不相同。请参考防御中间人（MITM）攻击一节，了解 Numeric Comparison、Passkey Entry 和 OOB 关联模型的认证阶段 1 如何提供更强的防止 MITM 攻击的功能。认证阶段 1 中发生的任何故障都会终止配对过程。

在认证阶段 2 中，各 BLE 设备将计算 Long Term Key（长期密钥，LTK），用于加密链接。可以使用认证阶段 1 中所生成的 Diffie-Hellman 密钥、蓝牙设备地址和 128 位随机数值并通过这些设备的 I/O 功能来生成 LTK。

更多有关 LE 安全连接中认证阶段 1 和 2 的信息，请参考蓝牙内核规范版本 4.2 第 3 卷 H 部分中第 2.3.5.6 章节的内容。

6.1.3 配对阶段 3

在配对阶段 3 中，可以使用配对阶段 2 所生成的 STK（如果使用 LE 传统配对）或 LTK（如果使用 LE 安全连接配对）来加密 BLE 链接。然后，加密链接上将提供以下密钥：

1. Identity Resolving Key（识别解析密钥，IRK） — 指的是一个用于生成和解析随机地址的 128 位密钥。
2. Connection Signature Resolving Key（连接签名解析密钥，CSRK） — 指的是一个用于进行数据签名和验证接收设备上签名的 128 位的密钥。
3. Long Term Key（长期密钥，LTK） — 指的是一个用于为某个加密连接生成共同会话密钥的 128 位的密钥。更多有关信息，请参考 蓝牙内核规范版本 4.2 第 6 卷 B 部分中第 5.1.3 章节的内容。
4. Encrypted Diversifier（加密的变化符，EDIV） — 指的是一个用于识别 LE 传统配对过程中所提供 LTK 的 16 位存储值。每当提供一个唯一的 LTK， 都会生成新的 EDIV。
5. Random Number（随机数值，Rand）— 指的是一个用于识别 LE 传统配对过程中所提供 LTK 的 64 位存储值。每当提供一个唯一的 LTK， 都会生成新的 Rand。

仅在使用 LE 传统配对的情况下提供 LTK、EDIV 和 Rand。

6.2 优点

6.2.1 更强的安全性

与 LE 传统配对相比，LE 安全连接提供了更强的安全性，能够阻止 MITM 攻击和被动窃听。

被动窃听器是第三个设备，用于监控两个 BLE 设备间的通信。被动窃听器需要获得通过 BLE 链接提供的密钥，从而监控加密通信。在 LE 安全连接中，无论使用哪个关联模型，都不能空中交换 256 位 Diffie-Hellman 密钥。因此，被动窃听器无法计算加密用的长期密钥（LTK），并且无法监控 BLE 加密通信。对于 Bluetooth 4.1，只能通过 OOB 关联模型防止被动窃听。另外，它使用了 128 位临时密钥，所以该保护功能相当弱。请查阅防御被动窃听内容，了解两个 BLE 设备是如何计算 LE 安全连接中的 Diffie-Hellman 公钥的。

MITM 攻击使用第三个设备伪装成参与通信的每个设备的对等设备，从而可以修改两个设备所交换的数据。数字比较、密钥输入和 OOB 关联模型能够提供更强的防御 MITM 攻击功能。请查阅防御中间人（MITM）攻击内容，了解这些关联模型如何防御 MITM 攻击。数字比较的配对过程比密钥输入的配对过程快，而且该方法不要求单独的通信链接（OOB 方法需要）。

表 5 汇总了 LE 传统配对和 LE 安全连接配对方法的保护级别。

表 5. LE 传统配对和 LE 安全连接配对的对比

特性	LE 传统配对方法	LE 安全连接配对方法
防御 MITM	密钥和 OOB	数字比较、密钥输入和 OOB
防御被动窃听	OOB	全部

6.2.2 仅支持安全连接模式

该模式强制使用 LE 安全连接进行严格的配对。如果其中某个设备设置了严格配对标志，那么只有两个设备均支持 LE 安全连接并验证要求得到满足时，才进行配对过程的第二个阶段。对安全要求非常高的应用，该模式很有用。

6.3 应用

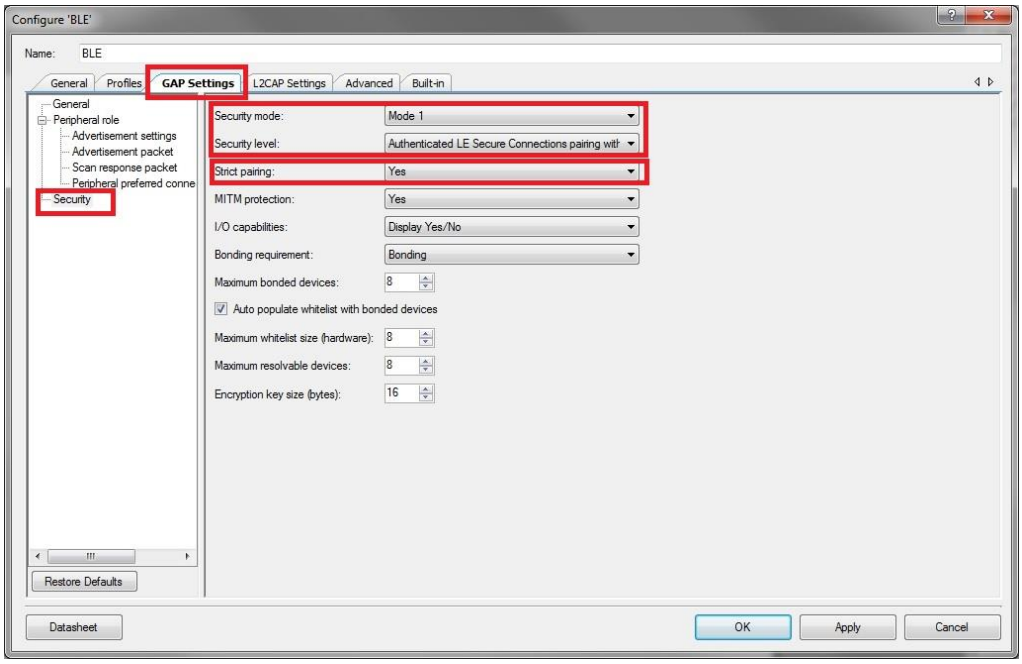
门锁、银行卡和其它的安全要求高的应用可以使用 Bluetooth 4.2 的增强型安全功能。

6.4 通过 PSoC Creator 开发支持 LE 安全连接的应用

6.4.1 组件配置

通过 BLE 组件可以轻松配置安全模式、安全级别、严格配对要求、防御 MITM、I/O 能力、连接要求以及加密密钥长度。要想使用 LE 安全连接，请依次选择 **Gap Settings** > **Security**，然后将 **Security mode** 参数设置为 **Mode 1** 并将 **Security level** 设置为 **Authenticated LE Secure Connections pairing with encryption**。根据应用的要求设置其它参数。

图 15. BLE 组件配置窗口 — 安全设置



6.4.2 应用处理

使用 LE 安全连接功能时，应用固件需要管理以下任务：

- 生成局部的公有和私有密钥对
- 显示数字比较方法中的数值和密钥输入方法中的密钥输入。
- 密钥输入传输状态
- 密钥传输
- 传输使用数字比较方法时所显示的数值是否为正确信息

表 6 列出了使用 LE 安全连接功能时 BLE 堆栈事件、每个事件的描述以及相应的行动。

表 6. 使用 LE 安全连接时 BLE 事件和相应的行动

BLE 堆栈事件名称	事件说明	事件处理程序行动
CYBLE_EVT_GAP_NUMERIC_COMPARISON_REQUEST	提供了数字比较方法所需的 6 数字值	显示 6 数字值。 根据两个设备上所显示的数值来发送接受/拒绝响应信息（针对数字比较方法）
CYBLE_EVT_GAP_KEYPRESS_NOTIFICATION	通知对等设备上的密钥输入状态	检查对等设备的通知是否同该设备上用户所输入的内容相匹配。 如果不匹配，则断开连接
CYBLE_EVT_GAP_OOB_GENERATED_NOTIFICATION	通知 OOB 数据生成已经完成	应用特定的行动
CYBLE_EVT_GAP_SMP_NEGOTIATED_AUTH_INFO	通知所协商的配对参数	应用特定的行动

表 7 提供了 LE 安全连接应用中所使用的新 API 列表。

表 7. LE 安全连接的新 API

API	描述
CyBle_GapSetSecureConnectionsOnlyMode	使能或禁用仅支持安全连接模式
CyBle_GapGenerateLocalP256Keys	生成局部的公有和私有密钥
CyBle_GapAuthSendKeyPress	发送按键状态
CyBle_GapGenerateOobData	生成 OOB 数据

欲更多了解各种事件和 API，请查阅 BLE 组件数据手册。

6.4.3 示例项目

PSoC Creator 所提供的示例项目 BLE_4.2_DataLength_Security_Privacy 使用了 LE 安全连接。通过依次选择 **PSoC Creator** > **File** > **Code Example** 并将筛选项设置为 **BLE**，可以查看该示例项目，如图 10 所示。

7 链路层（LL）保密

7.1 保密功能简介

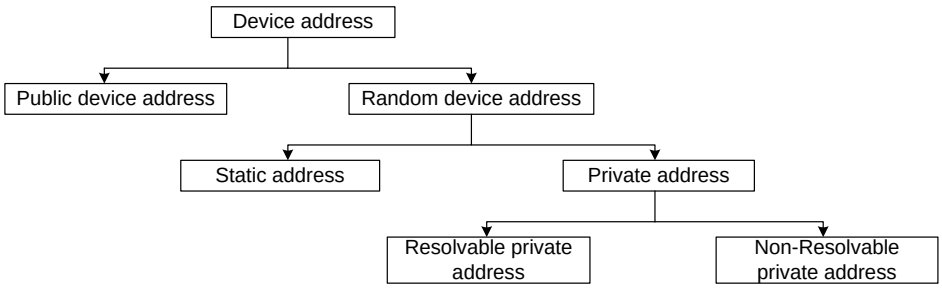
可以通过 48 位设备地址来识别 BLE 设备。设备在广播通道上发送的所有数据包都包含该地址。监听所有三路广播通道的第三个设备通过使用该地址很容易便能够跟踪设备活动。保密功能可以定期生成和修改保密地址，从而降低跟踪 BLE 设备的能力。

7.2 保密概念

7.2.1 蓝牙地址类型

图 16 显示的是 BLE 设备可用的各种地址类型。

图 16. 蓝牙地址类型



有两种设备地址，即是公有地址和随机地址。公有地址包括一个 24 位的公司识别码（基于 IEEE802-2001 标准的组织唯一标识符，简称为 OUI）和一个 24 位的公司分配码（每个设备的号码不一样）。随机设备地址分为两种：静态地址和私有地址。静态地址是随机生成的 48 位地址，其中两个最高有效位被设置为 1。公有地址是固定不变的。静态地址只在重新开机时才被修改。对等设备很容易便能检测和连接使用了其中一种地址的设备。私有地址则定期改变，这样可确保 BLE 设备不被跟踪。每次重新连接时，不可解析的私有地址都会改变。对等设备无法计算不可解析的私有地址，因此连接前需要向对等设备提供该地址。可解析的私有地址（RPA）被定期修改，支持保密功能的设备可以计算并使用它。在本应用笔记中，我们在保密功能背景下讨论有关 RPA 的内容。有关各种地址类型的更多详细信息，请参考蓝牙 4.2 核心规范。

每个 BLE 保密设备都有唯一一个地址，被称为识别（ID）地址。ID 地址是 BLE 设备的公有地址或静态地址。另外，这些设备还有一个身份解析密钥（IRK）。通过使用 IRK，可以生成 BLE 设备的 RPA（由 BLE 设备执行）并解析 RPA（由对等设备执行）。ID 地址和 IRK 均在配对过程的第三个阶段进行交换。BLE 保密设备具有一个解析表，包括对等设备的 ID 地址、BLE 设备生成其 RPA 时所用的局部 IRK 以及用于解析对等设备 RPA 的 IRK。 解析表中的每一项均遵循图 17 中所示的格式。

图 17. 解析表

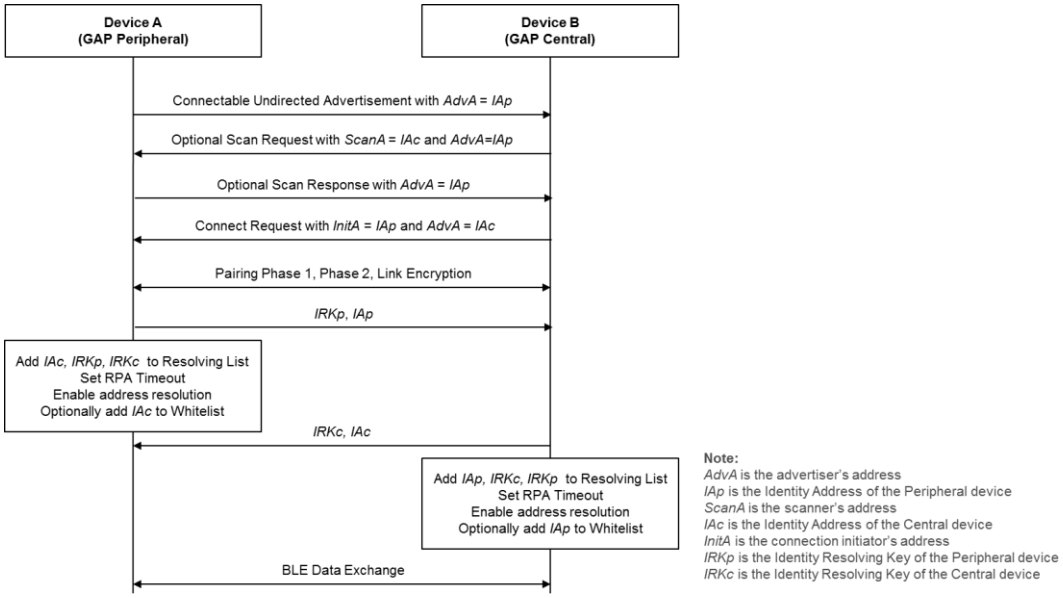
Identity address	Local IRK	Peer IRK

BLE 保密设备定期修改它的 RPA，以防止跟踪。BLE 堆栈配置了链路层的 RPA 超时参数。该值指定了链路层必须生成新 RPA 的时长。

7.2.2 保密流程

图 18 显示的是两个使用保密功能的 BLE 设备间的首次连接。在该图中，一个设备作为通用访问配置文件（GAP）中的外设，另一个设备则作为 GAP 中心。有关 GAP 和蓝牙设备可担任的各种功能的详细信息，请查阅蓝牙 4.2 核心规范的第 3 卷，C 部分，第 2.2.2 节。

图 18. 两个使用保密功能的 BLE 设备间的首次连接



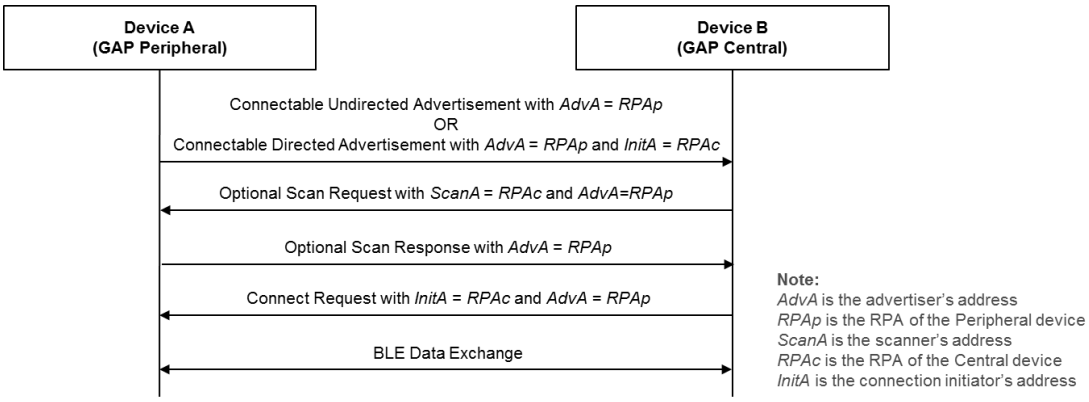
如上面所示，在首次建立连接期间，GAP 外设和 GAP 中心通过广播通道发送的所有数据包中都包含 ID 地址（*IAp* 是外设 ID 地址，*IAc* 是中心 ID 地址）。这是因为在首次连接期间，两个设备都不能确定对等设备的 IRK，因此无法解析对等设备的 RPA。通过广播通道传输的数据包包括：

- 可连接无定向广播：是指不针对特定目标（如特定 GAP 中心）进行广播的数据包。这些广播数据包只有 GAP 外设的地址（即广播者的地址），而不包含 GAP 中心地址。
- 可选的扫描请求和扫描响应：扫描请求在与外设连接前由 GAP 中心发送，从而要求外设的其它信息。扫描响应由外设发送，包括被请求的数据。这两个数据包都是可选的。
- 连接请求：这是 GAP 中心向 GAP 外设发送并要求启动连接的请求。

除了上面各数据包外，所有其它数据包都通过数据通道发送，并且不包含蓝牙设备地址。连接请求数据包是在广播通道上发送的最后数据包。除了 GAP 中心和 GAP 外设的 ID 地址外，该数据包还包含 32 位随机地址（称为访问地址）。访问地址用于识别两个 BLE 设备间的链路层连接。每次建立连接（例如，每个连接请求）期间，都会生成一个新的访问地址。两个 BLE 设备间在数据通道上进行交换的每个数据包（包括配对和数据交换数据包）使用访问地址来识别两个设备间的连接。

在配对过程的第三阶段中（请参考第 6.1 节，了解配对过程的有关信息），GAP 中心和 GAP 外设交换了 IRK 和 ID 地址。这些内容作为配对相关数据包的有效载荷部分。对等设备的 IRK、ID 地址和局部 IRK 被存储在两个设备的解析表中。在该阶段，两个设备都包含用于解析 RPA 的信息，因此它们都设置了 RPA 超时参数，并使能了地址解析。它们也可以选择性地将对等设备的 ID 地址添加到筛选设备用的白名单内。白名单是 BLE 设备的链路层筛选广播者、扫描者和连接发起者时所用的一组蓝牙设备地址。仅在使能设备筛选功能时，才使用白名单。设备在 BLE 数据通道上交换数据。由于设备的解析表具有用于解析对等设备 RPA 的信息，因此重新连接程序将会使用 RPA。图 19 显示的是两个设备成功实现首次连接后被断开，然后正在重新连接。

图 19. 使用 RPA 重新连接

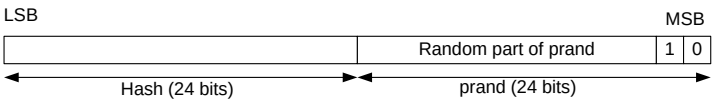


如上面所示，这次，两个设备在广播通道上发送的所有数据包都使用 RPA。因此，两个设备间在广播通道上进行的通信不被任何第三个设备跟踪。请注意，重新连接时，GAP 外设可以使用可连接无定向广播或可连接定向广播。第 7.2.5 节解释了只有蓝牙 4.2 保密设备支持可连接定向广播的原因。仅在 GAP 外设使用可连接无定向广播时，才会使用扫描请求和扫描响应。在 GAP 外设使用可连接定向广播时，GAP 中心只能发送连接请求进行响应。请注意，保密功能防止跟踪 BLE 设备在广播通道上进行的通信。数据通道的数据包所使用的访问地址每次连接都被修改，因此最难跟踪。保密功能不会对数据通道数据包产生影响。

7.2.3 可解析保密地址（RPA）的生成

本节介绍了 BLE 保密设备如何生成 RPA。可解析私有地址的格式遵循蓝牙规范，如图 20 所示。

图 20. 可解析私有地址格式



设备生成 24 位数值（22 位是随机的，2 位是固定的）被称为 *prand*。设备将使用 *prand* 通过 Hash 函数生成 24 位 *hash*：

hash = *e*(*IRK*$_{local}$, *padding* | *prand*)， 截断为 24 位

其中：

IRK$_{local}$ = 128 位局部 IRK

Padding = 向 *prand* 零填充 104 位以得到 128 位

prand = 24 位随机数值（22 位是随机的，两个最高有效位被设置为 0b10）

安全函数‘e’是 128 位 AES 加密函数，该函数在 PSoC 4/ PRoC BLE 设备的链路层硬件中被执行。它使用 128 位 *key* 和 128 位 *plaintextData* 来生成 *encryptedData*，如 FIPS-1971 所定义：

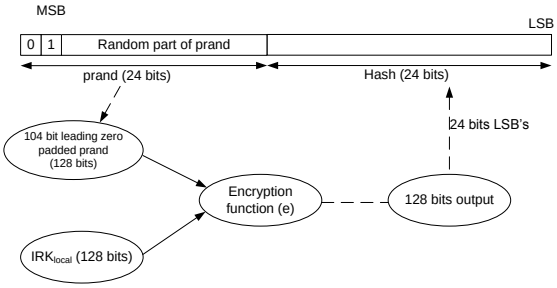
encryptedData = e(key, plaintextData)

按照以下方式将 24 位 *hash* 和 24 位 *prand* 结合起来便得到随机地址（*randomAddress*）：

randomAddress = hash | prand

可解析私有地址的生成如图 21 所示。

图 21. 可解析私有地址的生成



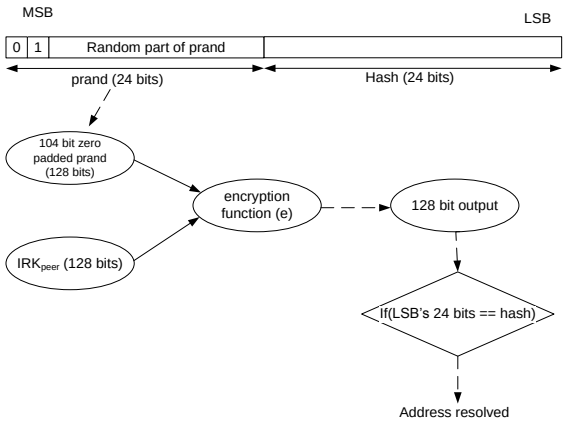
7.2.4 可解析私有地址的解析

本节介绍了 BLE 保密设备如何解析对等设备的 RPA。对等设备提供的 RPA 包括 24 位随机部分（*prand*）和 24 位散列部分（*hash*），如第 7.2.3 节所述。对地址进行解析或解码时，RPA 的最低有效 24 位当作对等设备的 *hash*，地址的最高有效 24 位当作 *prand*。使用上面的 Hash 函数生成 *localHash* 值。其中，函数的输入参数为对等设备所提供的 IRK 和从 RPA 提取得到的 *prand*。

localHash = *e*(*IRK*$_{peer}$, *padding* | *prand*)， 截断为 24 位

将 *localHash* 和从 RPA 提取的 *hash* 进行比较。如果 *localHash* 同所提取的 *hash* 匹配，则表示对等设备的 ID 地址已被解析。地址解析流程如图 22 所示。

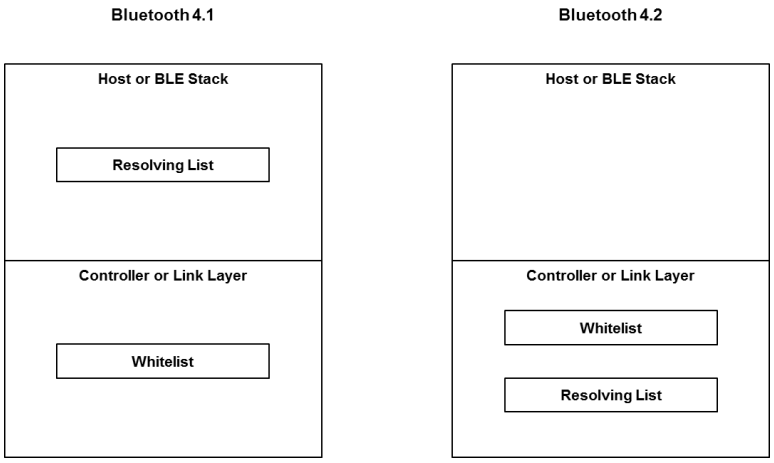
图 22. 可解析私有地址的解析



7.2.5 保密 1.1 与保密 1.2 的对比

蓝牙 4.1 中的保密功能被称为保密 1.1。蓝牙 4.2 中的保密功能被称为保密 1.2 或链路层保密。这是因为在蓝牙 4.2 中，地址解析（如 RPA 解析）由链路层处理。在蓝牙 4.2 中，解析表和白名单都是链路层的一部分，如图 23 所示。

图 23. 蓝牙 4.1 中的保密 1.1 与蓝牙 4.2 中的保密 1.2 的对比



可连接定向广播包含广播端和接收端的 RPA。使用蓝牙 4.2 的链路层保密时，链路层可以通过解析表对 RPA 进行解析。因此链路层可以确定它是否为可连接定向广播的目标。至于 RPA 超时参数的取值，在蓝牙 4.1 和蓝牙 4.2 中也不一样。在蓝牙 4.2 中，RPA 超时的取值范围为 1 秒到 11.5 个小时，默认值为 900 秒。因此在蓝牙 4.1 中，该值被固定设置为 15 分钟。

7.3 优点

7.3.1 重新连接更快

第 7.2.5 节描述了保密设备如何使用可连接定向广播重新连接。在蓝牙 4.1 中，保密连接的设备筛选功能被禁用。链路层不访问解析表，因此，不能将 RPA 解析为 ID 地址，也不能使用白名单来筛选 ID 地址。在蓝牙 4.2 中，解析表是链路层的一部分，如图 23 所示。因此，链路层可以使用解析表将 RPA 解析为 ID 地址，从而使用白名单来筛选 ID 地址。通过蓝牙 4.2 中的设备筛选和可连接定向广播功能，BLE 保密设备可快速重新连接。

7.3.2 节能的 GAP 中心设备

对于使用设备筛选功能的保密 GAP 中心设备，链路层只把解析表和白名单中的对等设备的定向广播和扫描响应发送给 BLE 堆栈。这样可以减少 BLE 堆栈中的处理操作。BLE 设备（如赛普拉斯 PSoC 4 BLE 和 PRoC BLE）将 BLE 堆栈当作在 MCU 上运行的固件，并将链路层当作硬件模块。因此，减少在 BLE 堆栈中的处理操作能够减少 MCU 的工作时间，同时降低系统功耗。

7.3.3 节能型 GAP 外设设备

对于使用设备筛选功能的保密 GAP 外设设备，链路层只将解析表和白名单中的对等设备的扫描请求和连接请求发送给 BLE 堆栈。这样可以减少 BLE 堆栈中的处理操作。BLE 设备（如赛普拉斯 PSoC 4 BLE 和 PRoC BLE）将 BLE 堆栈当作运行在 MCU 上的固件，并将链路层当作硬件模块。因此，减少在 BLE 堆栈中的处理操作也会减少 MCU 的工作量，同时降低系统功耗。

7.3.4 保密性比蓝牙 4.1 更强

如第 7.2.5 节所述，保密 4.1 的 RPA 超时被固定设置为 15 分钟，而保密 4.2 的 RPA 超时可以设置为 1 秒。这样做，RPA 的修改更加频繁，使得蓝牙 4.2 的 BLE 设备更难跟踪。

7.4 应用

许多应用得利于链路层保密功能。

通过保密功能，用户可以在公共场所（如健身房）控制自己可穿戴设备的可见性。可穿戴保密设备与用户的智能手机或健身房设备连接时所进行的广播不会被第三个设备跟踪。用户的可穿戴设备可以防止在公共场所被跟踪。大多数可穿戴设备为 GAP 外设。由于功耗高，它们不使用蓝牙 4.1 中的保密功能。蓝牙 4.2 中的链路层保密支持低功耗性能（如第 7.3.3 节中所述），因此用户可以使用保密功能。

零售应用也受益于保密功能。零售区域中的服务供应商可以使用 BLE 信标通过广播将消息发送到用户智能手机上。如果使用链路层保密，用户的智能手机通过设备筛选功能（如第 7.3.1 节中所述）可以接收优选服务供应商的消息，并忽略其它服务供应商消息。

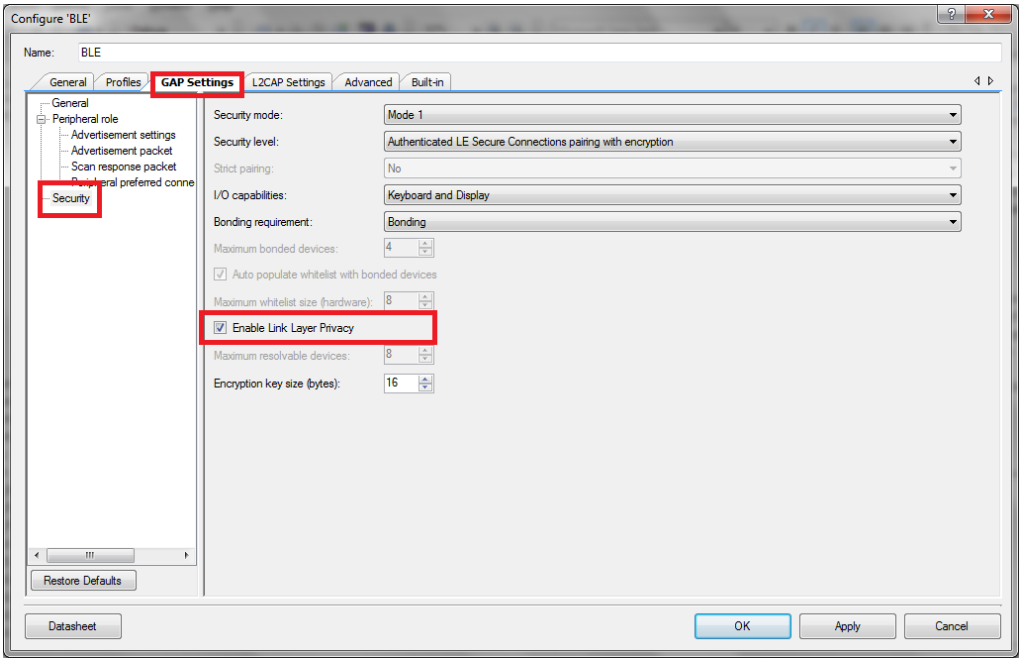
由于链路层保密频繁修改 RPA，因此在公共环境中难以跟踪用户的智能手机。智能手机一般作为 GAP 中心设备使用。链路层保密也能够降低智能手机进行 BLE 通信的功耗（如第 7.3.2 节所述）。

7.5 通过 PSoC Creator 开发使用链路层保密的应用

7.5.1 组件配置

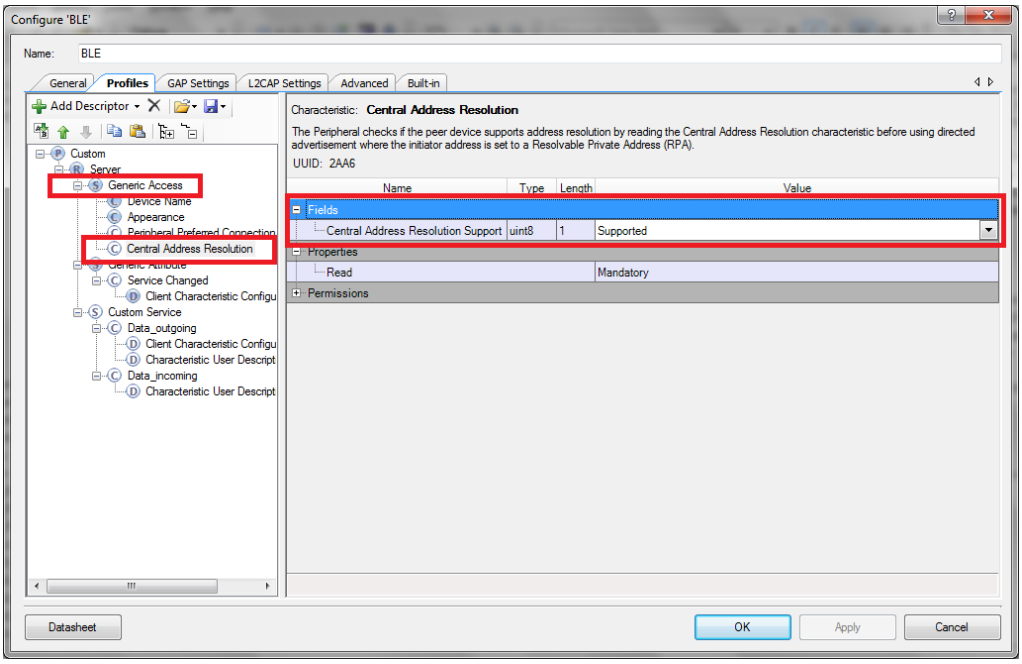
通过使用 BLE 组件配置窗口中 **GAP Settings** > **Security** 下的 **Enable Link Layer Privacy** 选项，可以使能或禁用链路层保密功能和相关 API，如图 24 所示。

图 24. 使能/禁用链路层保密



建立好初次连接后，GAP 外设将读取 GAP 服务中的中心设备地址解析特性。通过读取该特性的值，GAP 外设可以了解 GAP 中心的链路层是否支持地址解析。如果支持，GAP 外设可以使用可连接定向广播重新与 GAP 中心重新连接。通过 **Profiles** > **Generic Access** > **Central Address Resolution** 路径下的下拉菜单，可以设置中心地址解析特性值，如图 25 所示。对于支持链路层保密的设备，需要将该特性值设置为 **Supported**，从而能够向对等设备通知链路层保密得到支持。

图 25. 设置中心地址解析特性值



7.5.2 应用处理

应用固件需要管理保密设备固件的以下任务：

- 使能/禁用地址解析
- 设置 RPA 超时
- 为解析表添加/移除设备
- 设置合适的白名单筛选策略

表 8 列出了各种 BLE 堆栈事件、事件的说明以及事件处理程序需要采取的相应行动。

表 8. 链路层保密的 BLE 事件和相应行动

BLE 堆栈事件名称	事件说明	事件处理程序行动
CYBLE_EVT_STACK_ON	成功完成 BLE 堆栈初始化	填写解析表 使能地址解析 设置 RPA 超时 设置用户的白名单筛选政策
CYBLE_EVT_GAP_KEYINFO_EXCHNGE_CMPLT	完成与对等设备进行交换安全密钥	复制对等设备的 IRK 更新解析表 更新白名单筛选政策
CYBLE_EVT_GAPC_DIRECT_ADV_REPORT	地址解析后收到定向广播	与设备建立连接

表 9 提供了链路层保密应用中所使用的新 API 列表。

表 9. 链路层保密应用中的新 API

API	说明
CyBle_GapAddDeviceToResolvingList	为解析表添加一个设备
CyBle_GapRemoveDeviceFromResolvingList	为解析表移除一个设备
CyBle_GapSetAddressResolutionEnable	使能控制器中的地址解析
CyBle_GapSetResolvablePvtAddressTimeOut	设置 RPA 超时
CyBle_GapReadResolvingList	读取当前的解析表
CyBle_GapReadPeerResolvableAddress	读取对等设备的当前 RPA 地址
CyBle_GapReadLocalResolvableAddress	读取本地设备的当前 RPA 地址
CyBle_GapGetDevSecurityKeyInfo	获取局部 IRK 值

7.5.3 读取中心地址解析特性值

如第 7.5.1 节所述，外设将读取中心地址解析特性，仅在中心保密设备支持链路层保密时，它才发送可连接定向广播。为了读取中心地址解析特性，需要使用 CyBle_GattcReadUsingCharacteristicUuid API，然后输入合适的参数，如下所示。

```
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);
```

如果中心设备具有中心地址解析特性，发生 CYBLE_EVT_GATTC_READ_BY_TYPE_RSP 事件时，特性值和属性地址被传输给应用。通过检查特性值，应用可以决定下次连接是否使用可连接定向广播。

7.5.4 为解析表添加/移除设备

通过使用 CyBle_GapAddDeviceToResolvingList API，可以为解析表（如图 17 所示）添加一个新 BLE 设备。其中，API 的参数为局部 IRK、对等设备 IRK 和对等设备 ID 地址。

```
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);
```

处理 CYBLE_EVT_GAP_KEYINFO_EXCHNGE_CMPLT 事件时，将对等设备 IRK 和对等设备 ID 地址传入到应用中。应用需要保存这些值。通过使用 CyBle_GapGetDevSecurityKeyInfo API，可获得局部 IRK。

要想移除解析表中的某个设备，需要调用 CyBle_GapRemoveDeviceFromResolvingList API，并输入设备的 ID 地址。

欲了解各种事件和 API，请查阅 BLE 组件数据手册。

7.5.5 示例项目

有关使用链路层保密的示例项目信息，请查阅 PSoC Creator 提供的 **BLE_4.2_DataLength_Security_Privacy** 示例项目。通过依次选择 **PSoC Creator** > **File** > **Code Example**，并将筛选项设置为 **BLE**，可以访问该示例项目，如图 10 所示。

8 汇总

本应用笔记介绍了蓝牙 LE4.2 规范的新功能、其优点以及使用这些功能进行开发应用的方法。

9 相关应用笔记

AN94020 — PRoC™ BLE 入门

AN91267 — PSoC® 4 BLE 入门

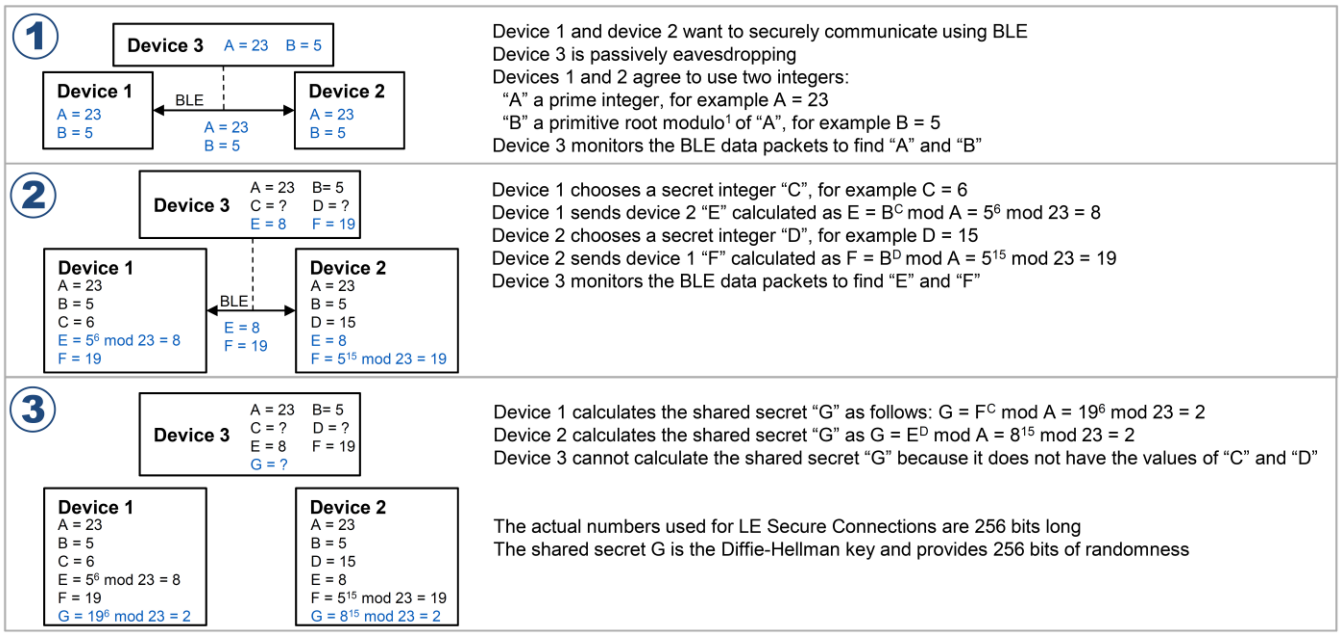
AN97060 — PSoC® 4 BLE 和 PRoC™ BLE：空中传输（OTA）设备固件升级（DFU）指南

AN91184 — PSoC 4 BLE：设计 BLE 应用

A 防御被动窃听

椭圆曲线 Diffie-Hellman（ECDH）算法允许两个 BLE 设备在进行基于 LE 安全连接的配对时建立一个共享密钥。配对过程的第二个阶段（认证阶段 2）将使用共享密钥（即 Diffie-Hellman 密钥）来生成长期密钥（LTK），用以对 BLE 链接进行加密。Diffie-Hellman 密钥提供了随机的 256 位，这些位不会被无线交换，如 图 26 所示。

图 26. 使用 ECDH 建立共享密钥



[1] 欲了解“原根”，请查阅 George E. Andrews 的*数论*（ISBN-10:0486682528）

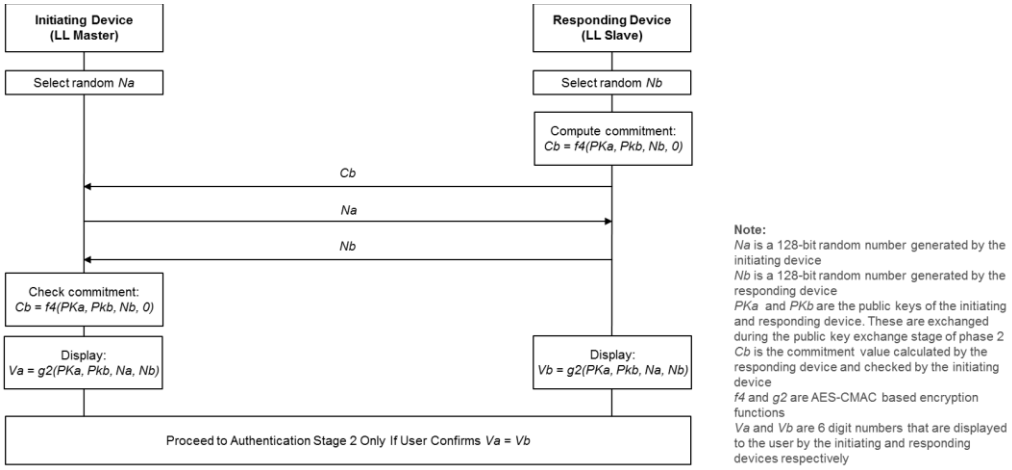
B 防御中间人（MITM）攻击

下面各节解释了在进行基于 LE 安全连接的配对中如何使用数字比较、密钥输入和带外数据（OOB）关联模型防御 MITM 攻击。

B.1 数字比较关联模型

图 27 显示的是配对流程的认证阶段 1，具体是在使用数字比较关联模型进行 LE 安全连接的情况下。

图 27. 数字比较情况下的认证阶段 1

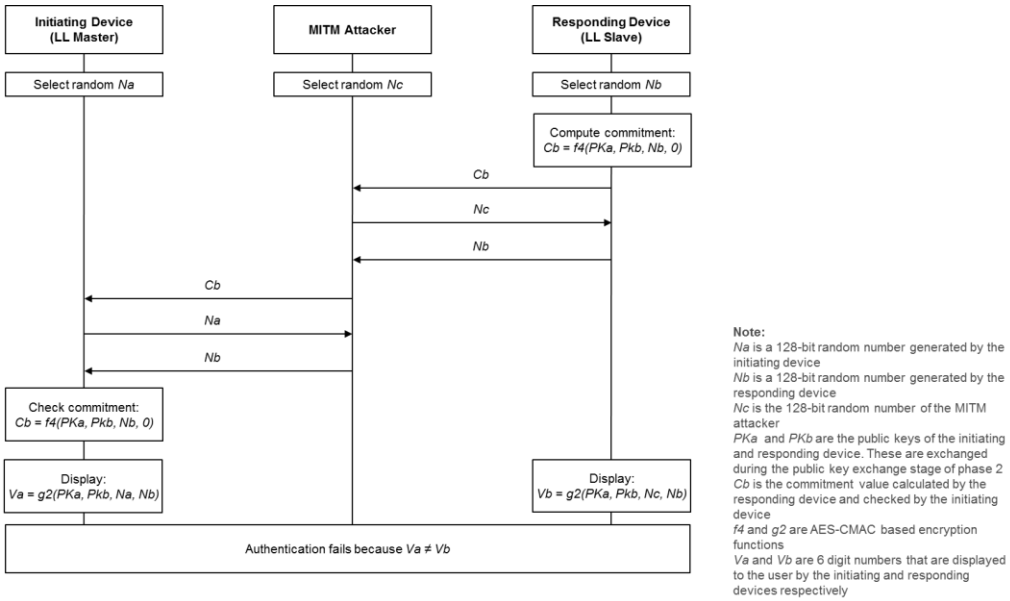


数字比较关联模型使用以下认证措施来防御 MITM 攻击：

- 在接收发起设备的随机数值（*Na*）前，响应设备必须提供使用响应设备随机数值（*Nb*）和两个 BLE 设备的公有密钥计算得到的约定值（*Cb*）。
- 接收响应设备的随机数值（*Nb*）前，发起设备必须分享它的随机数值（*Na*）。
- 接收到响应设备的随机数值（*Nb*）后，发起设备需要检查约定值（*Cb*）。

图 28 显示的是 MITM 攻击设备依次与响应设备和发起设备交换随机值的情况。

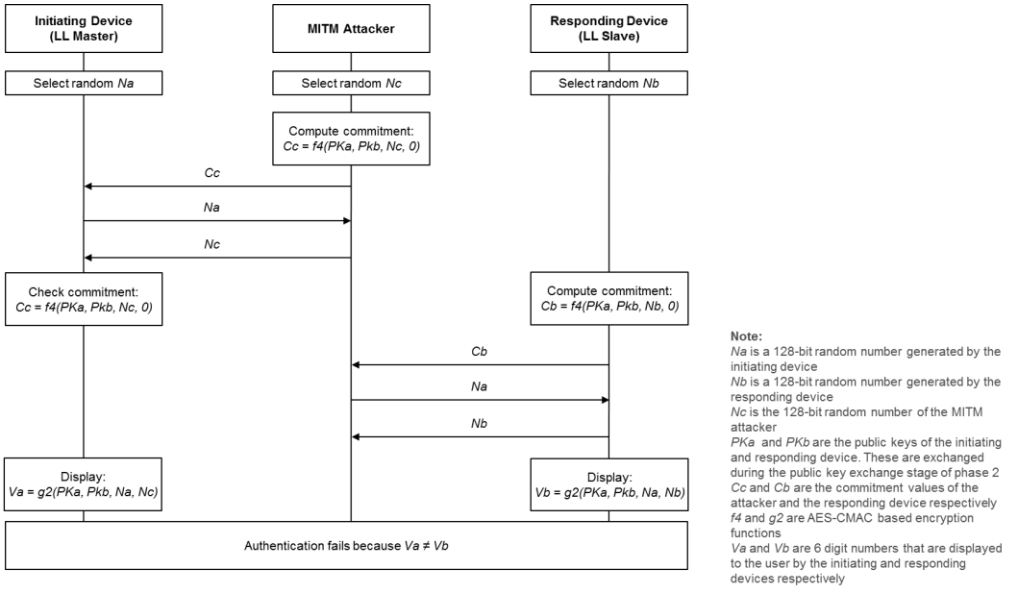
图 28. MITM 攻击设备依次与响应设备和发起设备交换密钥



通过图 28 可知，在获得响应设备的随机值（*Nb*）前，攻击设备需要为响应设备提供它的随机值（*Nc*）。这样，用户检查 BLE 设备所显示的值时会发现不同的 6 数字值，因而认证失败。

图 29 显示的是 MITM 攻击设备依次与发起设备和响应设备交换随机值的情况。

图 29. MITM 攻击设备依次与发起设备和响应设备交换密钥

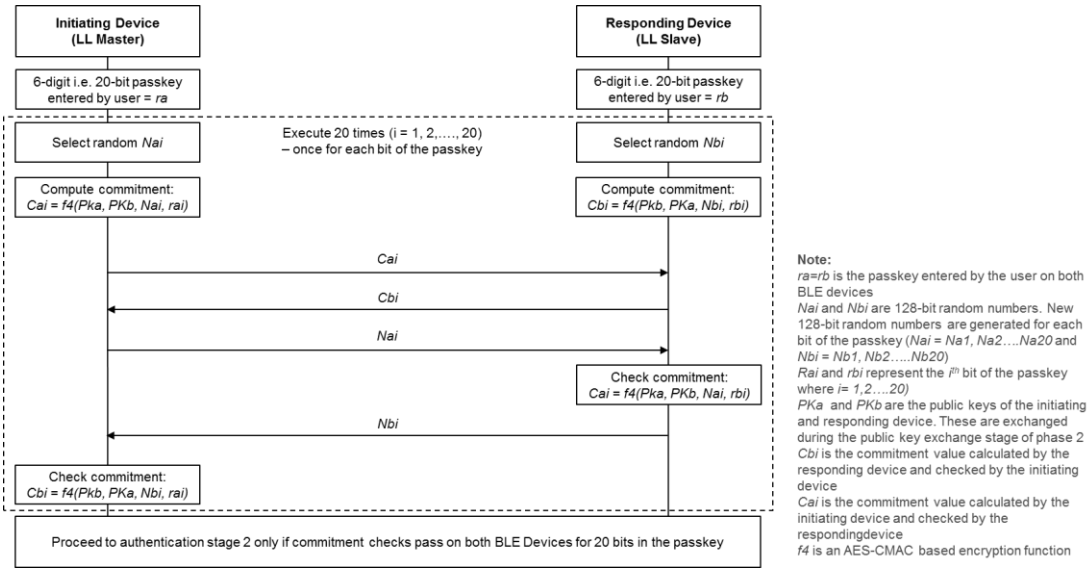


通过图 29 可见，在获得发起设备的随机值（*Na*）前，攻击设备需要为发起设备提供它的约定值（*Cc*）。发起设备将检查约定值，从而可以防止攻击设备修改它的随机值。用户检查 BLE 设备显示的值时将会发现不同的 6 数字值，因而认证失败。

B.2 密钥输入关联模型

图 30 显示的是配对流程的认证阶段 1，具体是在使用密钥输入关联模型进行 LE 安全连接的情况下。

图 30. 密钥输入情况下的认证阶段 1



密钥输入关联模型使用以下认证措施来防御 MITM 攻击：

1. 两个 BLE 设备都接收到用户输入的公有 6 数字或 20 位密钥（*ra* 和 *rb*）
2. 对于密钥中的每一位都需要重复执行第 3 到第 7 步（例如，*i = 1, 2,….20*）
3. 两个 BLE 设备选择 128 位随机值（*Nai* 和 *Nbi*）
4. 发起设备提供使用两个 BLE 设备的公有密钥（*PKa* 和 *PKb*）计算得到的约定值（*Cai*）、128 位随机值（*Nai*）以及密钥的第 *i* 位（*rai*）
5. 发起设备提供使用两个 BLE 设备的公有密钥（*PKa* 和 *PKb*）计算得到的约定值（*Cai*）、128 位随机值（*Nai*）以及密钥的第 *i* 位（*rai*）
6. 发起设备为响应设备提供它的 128 位随机值（*Nai*）
7. 响应设备使用发起设备的 128 位随机值（*Nai*）来检查收到的约定值（*Cai*）。如果该约定值正确，则发起设备将为响应设备提供它的 128 位随机值（*Nai*）
8. 发起设备使用响应设备的 128 位随机值（*Nai*）来检查收到的约定值（*Cai*）。如果两个值相互匹配，则发起设备继续进行配对流程

密钥输入关联模型的中心是密钥逐渐或逐位被公开。MITM 攻击设备与发起和响应设备接合时，它只能获得密钥的两位，然后 BLE 设备会检测到约定值不正确，并中止配对流程。与数字比较关联模型相比，该模型的缺点是需要进行 20 次认证（密钥的每一位需要进行一次），因此很耗时。

B.3 带外数据（OOB）关联模型

如果 OOB 通信能防御 MITM 攻击，那么 OOB 关联模型也能防御 MITM 攻击。OOB 关联模型的主要缺点是除了 BLE 接口外，两个 BLE 设备必须配备 OOB 接口，用以进行通信。OOB 接口使 BLE 设备成本增加。有关 OOB 关联模型的更详细信息，请查阅蓝牙 4.2 核心规范，第 3 卷，部分 H，第 2.3.5.6 节。

文档修订记录

文档标题：AN99209 — PSoC® 4 BLE 和 PRoC™ BLE：低功耗蓝牙 4.2 特性

文档编号： 002-15738

版本	ECN	变更者	提交日期	变更说明
**	5403976	ROWA	08/18/2016	本文档版本号为 Rev**，译自英文版 001-99209 Rev**。

全球销售和设计支持

赛普拉斯公司具有一个由办事处、解决方案中心、厂商代表和经销商组成的全球性网络。要想查找离您最近的办事处，请访问赛普拉斯所在地。

产品

ARM® Cortex®微控制器	cypress.com/arm
汽车级产品	cypress.com/automotive
时钟与缓冲区	cypress.com/clocks
接口	cypress.com/interface
照明与电源控制	cypress.com/powerpsoc
存储器	cypress.com/memory
PSoC	cypress.com/psoc
触摸感应	cypress.com/touch
USB 控制器	cypress.com/usb
无线/射频	cypress.com/wireless

PSoC®解决方案

PSoC 1 | PSoC 3 | PSoC 4 |PSoC 5LP

赛普拉斯开发者社区

论坛 | 项目 | 视频 | 博客 | 培训 | 组件

技术支持

cypress.com/support

PSoC 是赛普拉斯半导体公司的注册商标，且 PSoC Creator 是赛普拉斯半导体公司的商标。此处引用的所有其他商标或注册商标归其各自所有者所有。

赛普拉斯半导体公司
198 Champion Court
San Jose, CA 95134-1709

电话 ：408-943-2600
传真 ：408-943-4730
网址 ：www.cypress.com

© 赛普拉斯半导体公司，2016 年。本文件是赛普拉斯半导体公司及其子公司，包括 Spansion LLC（“**赛普拉斯**”）的财产。本文件，包括其包含或引用的任何软件或固件（“**软件**”），根据全球范围内的知识产权法律以及美国与其他国家签署条约由赛普拉斯所有。除非在本款中另有明确规定，赛普拉斯保留在该等法律和条约下的所有权利，且未就其专利、版权、商标或其他知识产权授予任何许可。如果软件并不附随有一份许可协议且贵方未以其他方式与赛普拉斯签署关于使用软件的书面协议，赛普拉斯特此授予贵方属人性质的、非独家且不可转让的如下许可（无再许可权）（1）在赛普拉斯特软件著作权项下的下列许可权（一）对以源代码形式提供的软件，仅出于在赛普拉斯硬件产品上使用之目的且仅在贵方集团内部修改和复制软件，和（二）仅限于在有关赛普拉斯硬件产品上使用之目的将软件以二进制代码形式的向外部最终用户提供（无论直接提供或通过经销商和分销商间接提供），和（2）在被软件（由赛普拉斯公司提供，且未经修改）侵犯的赛普拉斯专利的权利主张项下，仅出于在赛普拉斯硬件产品上使用之目的制造、使用、提供和进口软件的许可。禁止对软件的任何其他使用、复制、修改、翻译或汇编。

在适用法律允许的限度内，赛普拉斯未对本文件或任何软件作出任何明示或暗示的担保，包括但不限于关于适销性和特定用途的默示保证。赛普拉斯保留更改本文件的权利，届时将不另行通知。在适用法律允许的限度内，赛普拉斯不对因应用或使用本文件所述任何产品或电路引起的任何后果负责。本文件，包括任何样本设计信息或程序代码信息，仅为供参考之目的提供。文件使用人应负责正确设计、计划和测试信息应用和由此生产的任何产品的功能和安全性。赛普拉斯产品不应被设计为、设定为或授权用作武器操作、武器系统、核设施、生命支持设备或系统、其他医疗设备或系统（包括急救设备和手术植入物）、污染控制或有害物质管理系统中的关键部件，或产品植入之设备或系统故障可能导致人身伤害、死亡或财产损失其他用途（“**非预期用途**”）。关键部件指，若该部件发生故障，经合理预期会导致设备或系统故障或会影响设备或系统安全性和有效性的部件。针对由赛普拉斯产品非预期用途产生或相关的任何主张、费用、损失和其他责任，赛普拉斯不承担全部或部分责任且贵方不应追究赛普拉斯之责任。贵方应赔偿赛普拉斯因赛普拉斯产品任何非预期用途产生或相关的所有索赔、费用、损失和其他责任，包括因人身伤害或死亡引起的主张，并使之免受损失。

赛普拉斯、赛普拉斯徽标、Spansion、Spansion 徽标，及上述项目的组合，及 PSoC、CapSense、EZ-USB、F-RAM 和 Traveo 应视为赛普拉斯在美国和其他国家的商标或注册商标。请访问 cypress.com 获取赛普拉斯商标的完整列表。其他名称和品牌可能由其各自所有者主张为该方财产。