*Application Note*

# *对 TI 电池电量监测计进行椭圆曲线加密认证*

*Michael Smith, Garry Elder*

**摘要**

大多数德州仪器 (TI) 电池电量监测计产品都支持一定程度的认证功能，以保护电池组免遭仿冒。本应用手册以 BQ41zxx 系列产品为例，概述了认证功能，并详细介绍了创建和设置椭圆曲线加密 (ECC) 密钥对的流程。

## 内容



## 商标

# 1 简介

椭圆曲线加密 (ECC) 是一种利用椭圆曲线的数学属性生成非对称私钥和公钥对的认证方案。ECC 算法有多种不同的版本，例如 ECDSA（详细信息请参阅 FIPS 186-5）和 EC-KCDSA。BQ41Zxx 系列 TI 电池电量监测计使用基于韩国证书的椭圆曲线数字签名算法 (EC-KCDSA)，且该算法基于 KCDSA 任务组发布的一篇论文予以实施。

BQ41zxx 系列器件所用的实施方案 提供基于 B-233 的 EC-KCDSA 签名或对质询的响应，并使用 SHA-256 算法进行哈希运算（详细信息请参阅 FIPS 183-4）。该实施方案使用公钥的 X 和 Y 坐标，并填充到正确的长度。

使用 BQ41z50 技术参考手册中详述的 MaufacturerAccess () 命令，通过 SMBus 接口访问电池电量监测计的认证功能。BQ41z50 可通过笔记本电脑等主机设备进行认证，电池电量监测计也可以对主机进行认证，以允许对电池电量监测计进行重新配置或重新编程。

**表 1-1. 使用的 SMBus 命令摘要**

| 类型 | ID | 功能 | 模式 | 访问 |
|---|---|---|---|---|
| MAC | 0x0034 | HostPublicKey( )<br>允许读取和写入主机认证公钥。<br>注 1 - 一旦设置了主机认证公钥，旧有的“两字解封”方法就会被立即禁用。<br>注 2 - 这可以写回全零，以在完全访问 (FULL ACCESS) 模式下禁用主机认证。 | 读取/写入 | R： S/U/F<br>W: F |
| MAC | 0x0036 | GaugeAuthPubKey( )<br>用于对器件进行认证的单个“压缩点”公钥<br>读取返回密钥状态字节和公钥的 30 个字节（使用 LSB 在前进行压缩） | 读取 | S/U/F |
| MAC | 0x0038 | ProdPrivateKey( )<br>用于对电池电量监测计认证私钥（私钥 30 字节+公钥压缩点 30 字节）进行编程 | 只写 | F |
| MAC | 0x003a | ECC_MAC( )<br>用于允许运行主机经认证的解封命令 | 读取/写入 | S/U/F |
| MAC | 0x003c | ECC_R<br>读取会返回最新的电池电量测量计认证结果 *r*（如果可用）。<br>写入用于主机将认证数据作为 ECC_MAC( ) 的一部分写入电池电量监测计。 | 读取/写入 | S/U/F |
| MAC | 0x003d | ECC_S<br>读取会返回最新的电池电量测量计认证结果 *s*（如果可用）。<br>写入用于主机将认证数据作为 ECC_MAC( ) 的一部分写入电池电量监测计。 | 读取/写入 | S/U/F |
| SBS | 0x2f | GaugeAuthentication( )<br>用于将质询写入电池电量监测计以及读取 60 字节 *r* 和 *s*。 | 读取/写入 | S/U/F |

有关相关标准的更多信息，请参阅 节 8。

## 2 认证方案比较

与安全哈希算法 (SHA) 认证方案（例如 SHA-1）相比，ECC 具有若干重要的区别。首先，ECC 使用非对称密钥，因此主机和电池电量监测计不共享单个密钥，必须使用一个密钥对（一个公钥和一个私钥）来对器件进行防伪认证。这两种方案均采用 20 字节的质询长度，以提供随机质询。

两种认证协议之间的一个主要区别在于认证验证。采用 SHA 方案时，主机会与电池电量监测计一起开始验证，因为一旦开始验证，主机就已包含密钥和随机质询，而电池电量监测计会在收到质询后开始验证。ECC 要求主机等待电池电量监测计的响应，以完成验证过程。但是，主机可以在等待该响应时预先启动某些计算。

两种认证协议之间的第二个主要区别是验证密钥编程。当使用相同的密钥和质询时，SHA 会生成相同的响应。因此，质询-响应对可用于验证密钥是否正确编程。采用 ECC 方案时，相同的密钥和相同的质询不会产生相同的响应。必须实施单独的验证功能来验证密钥是否正确编程。

**表 2-1. ECC 与 SHA-1 认证算法比较**

| | SHA-1 HMAC | ECC |
|---|---|---|
| **TI 产品** | BQ40z50 和 BQ41z50 | BQ41z50 |
| **密钥类型** | 对称密钥（共享密钥） | 非对称密钥（公钥和私钥对） |
| **哈希函数** | 160 位 | 256 位 (SHA-2) |
| **密钥长度** | 128 位 | 233 位密钥 |
| **认证响应时间** | <100ms | <100ms |
| **质询长度** | 20 字节 | 8-19 个字节 |
| **响应长度** | 20 字节 | 60 个字节（或 2 x 30 字节） |
| **对给定密钥和质询的确定性响应** | 否 | 是 |
| **在不使用私有数据的情况下验证已编程密钥** | 是<br>使用已知质询响应对 | 是<br>使用公钥验证功能 |

# 3 电池组制造流程中的 ECC 密钥编程

BQ41z50 包含用于不同用途的多组密钥，详情请参阅 表 3-1。

**表 3-1. 密钥对和密钥列表**

| 密钥 | 所有者 | 使用 |
|---|---|---|
| 主机命令密钥（仅限公钥） | 客户 | 用于对主机命令进行认证 |
| 电池电量监测计认证密钥（私钥、公钥） | 客户 | 主机生成并将其编程到 BQ41z50 器件。<br>用于电池主机系统认证。 |

电池电量监测计和主机生产密钥对必须按照特定的程序生成并上传到 BQ41z50。

密钥生成：私钥的随机 233 位值为“x”，生成的公钥为 (x^-1)G，或者生成标准 ECDSA 密钥，然后（ECKCDSA 私钥）=（ECDSA 私钥）^-1

钥匙编程（仅限完全访问）：将私钥（30 个字节、LSB 在前）|| 公钥（30 个字节、LSB 在前、压缩）写入 MAC 0x0038

# 4 BQ41z50 产品系列的电池电量监测计认证流程

电池组制造商或组装厂可以执行认证过程，以确保构建完整且经过认证的电池组。图 4-1 图显示了使用 SMBus ManufacturerAccess( ) (MAC) 命令对电池电量监测计进行认证的流程。

整个流程概述如下：

1. 主机从电池电量监测计读取 ProdKpub
2. 电池电量监测计认证
   - 主机向电池电量监测计发送质询消息
   - 电池电量监测计使用 ECC-233 对消息签名
   - 电池电量监测计向主机提供 r/s
   - 主机验证签名

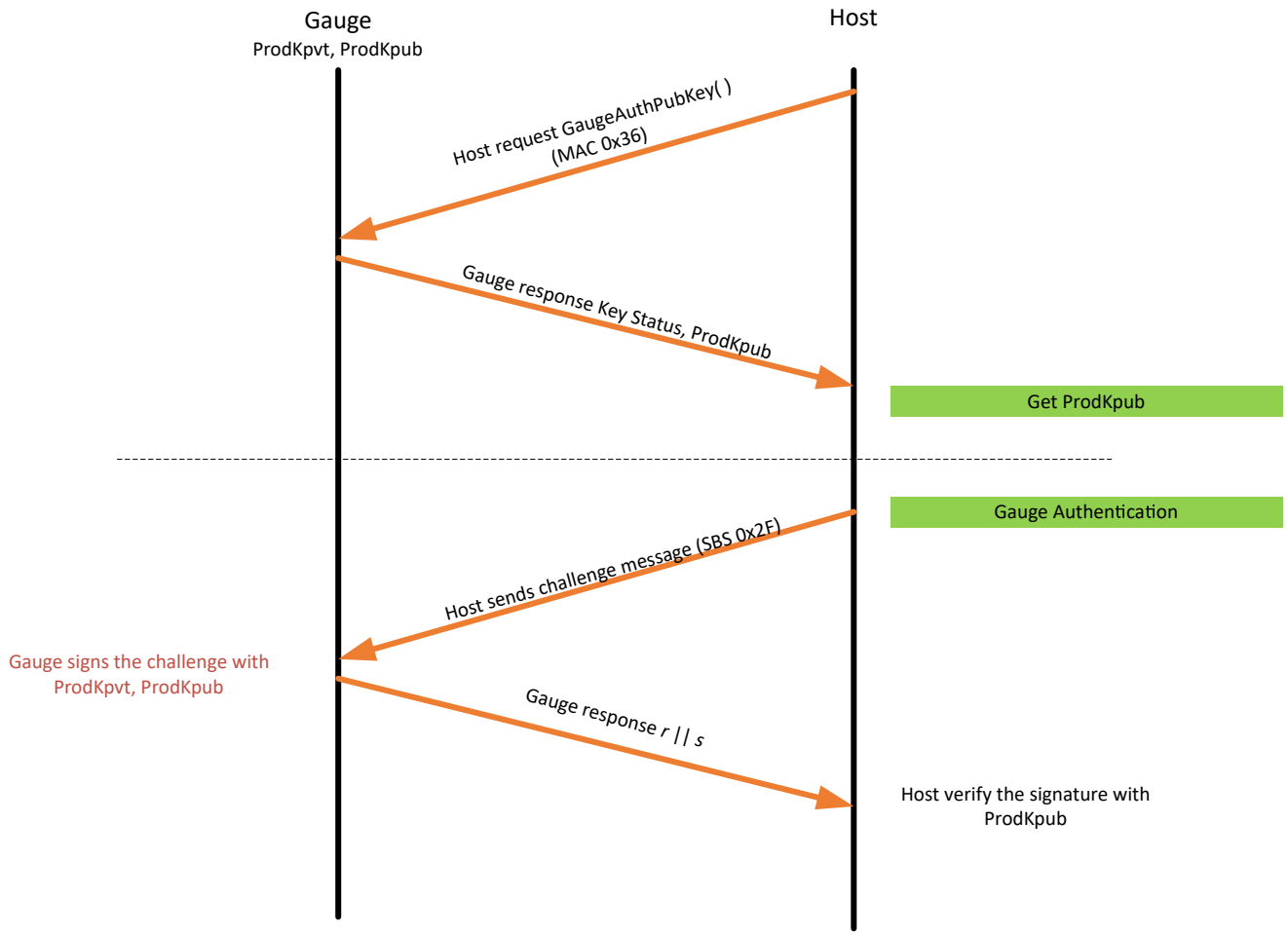
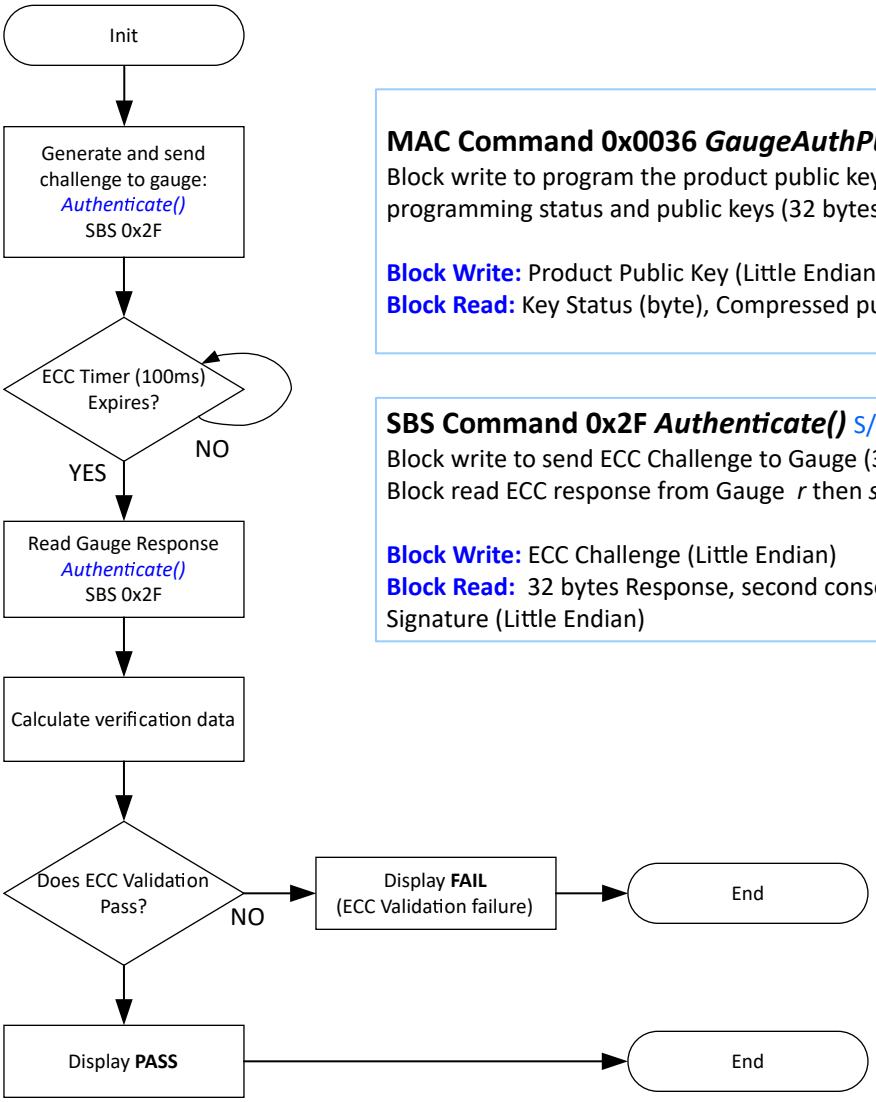



**图 4-1. 电池电量监测计认证概述**

更详细的执行流程图如 图 4-2 所示。




**MAC Command 0x0036 *GaugeAuthPubKey( )*** R: S/U/F, W: U/F
Block write to program the product public key and read back the programming status and public keys (32 bytes)

**Block Write:** Product Public Key (Little Endian)
**Block Read:** Key Status (byte), Compressed public key (30 bytes, LSB first)

**SBS Command 0x2F *Authenticate()*** S/U/F
Block write to send ECC Challenge to Gauge (30 bytes)
Block read ECC response from Gauge *r* then *s.*

**Block Write:** ECC Challenge (Little Endian)
**Block Read:** 32 bytes Response, second consecutive read 32 bytes Signature (Little Endian)

* Command availability under the following Security Modes:
S: Seal Mode
U: Unseal Mode
F: Full Access Mode

**图 4-2. 电池电量监测计认证流程图**

# 5 BQ41z50 产品系列的主机认证流程

为了更好地保护对器件的访问，电池电量监测计还可用于对主机进行认证（允许电池电量监测计更改安全状态），以及将电池电量监测计解锁（允许主机更新电池电量监测计）。为了执行此功能，主机必须首先对经授权公钥进行编程。当电池电量监测计处于“完全访问”状态时，必须通过将 30 个字节的压缩公钥发送到 MAC 子命令 0x0034 来写入公钥。必须读取该相同的命令，以确认当前编程的公钥用于主机认证。

如果没有编程的公钥，则使用旧的“安全密钥”解封操作。然而，一旦对公钥进行编程，旧的解封命令将被禁用。

**备注**

确保在编程后读取公钥，以确认该值已正确存储，然后再发送密封 (SEAL) 命令。如果没有相应的私钥，则无法恢复处于已密封 (SEALED) 状态的器件。

必须按照 图 5-1 图（使用 SMBus ManufacturerAccess()(MAC) 命令对电池电量监测计进行认证）执行该操作程序。

整个流程概述如下：

1. 主机使用以下数据块之一发送带数据的 MAC 子命令 0x003a：
   - 要请求解封 (UNSEAL) 访问操作，请使用数据块 0x14、0x04、0x72、0x36
   - 要请求 FULL_ACCESS 访问操作，请使用数据块 0xff、0xff、0xff、0xff
2. 主机使用 0x003a 读取 MAC 结果，以接收所生成的 8 字节质询代码。
3. 主机将 8 字节质询和命令组合成一条消息，并使用私钥对消息进行签名，生成一个 30 字节 *r* 和 30 字节 *s*。
   - 例如，如果电池电量监测计生成了质询 0x12、0x34、0x56、0x78、0x9a、0xbc、0xde、0xf0，则要为解封 (UNSEAL) 操作签名的完整消息字符串为 0x12、0x34、0x56、0x78、0x9a、0xbc、0xde、0xf0、0x14、0x04、0x72、0x36
4. 主机将生成的 *r* 和 *s* 写入电池电量监测计。
   - ECC_R (0x003c) 子命令接受 30 字节 *r* 值或完整的 60 字节 *r*、*s* 值。
   - ECC_S (0x003d) 子命令接受在将 *r* 值发送到电池电量监测计之后写入的 30 字节 *s* 值。
5. 一旦测量仪同时具有 *r* 和 *s*，测量仪就会验证签名。
6. 如果签名有效，则执行命令所请求的操作。

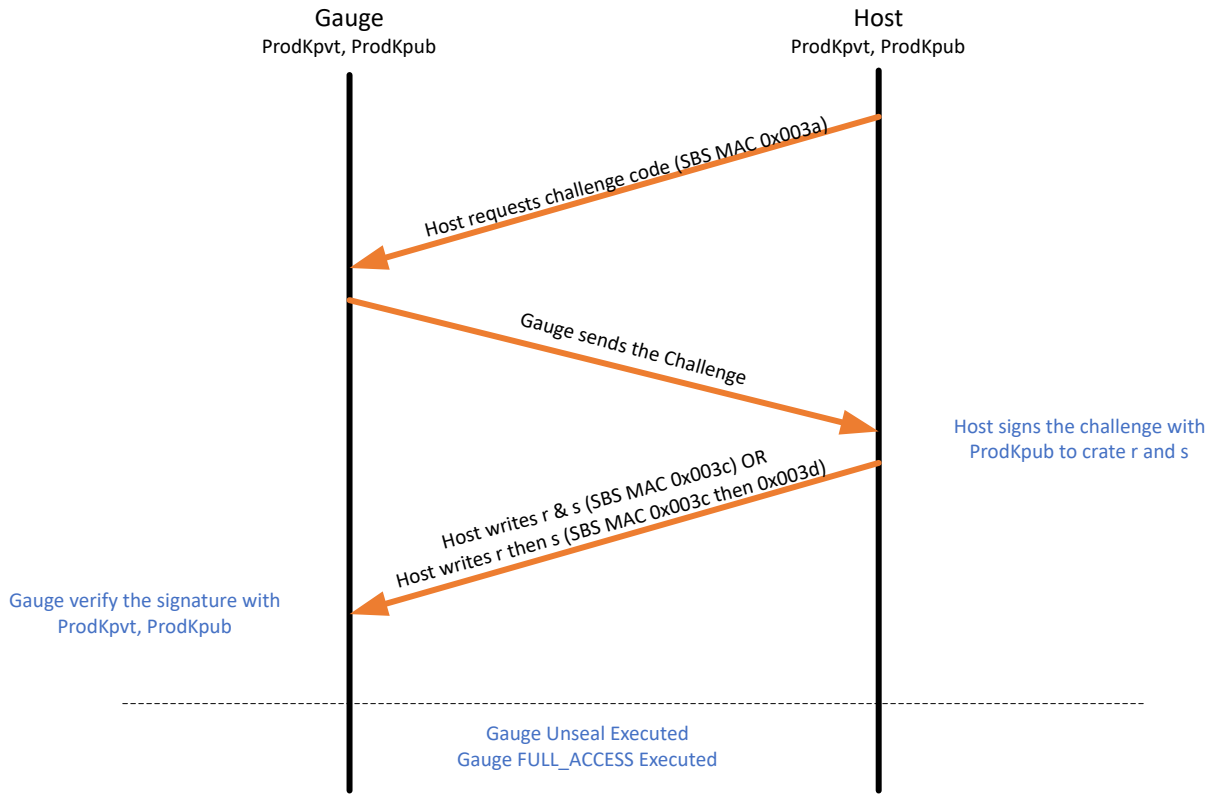
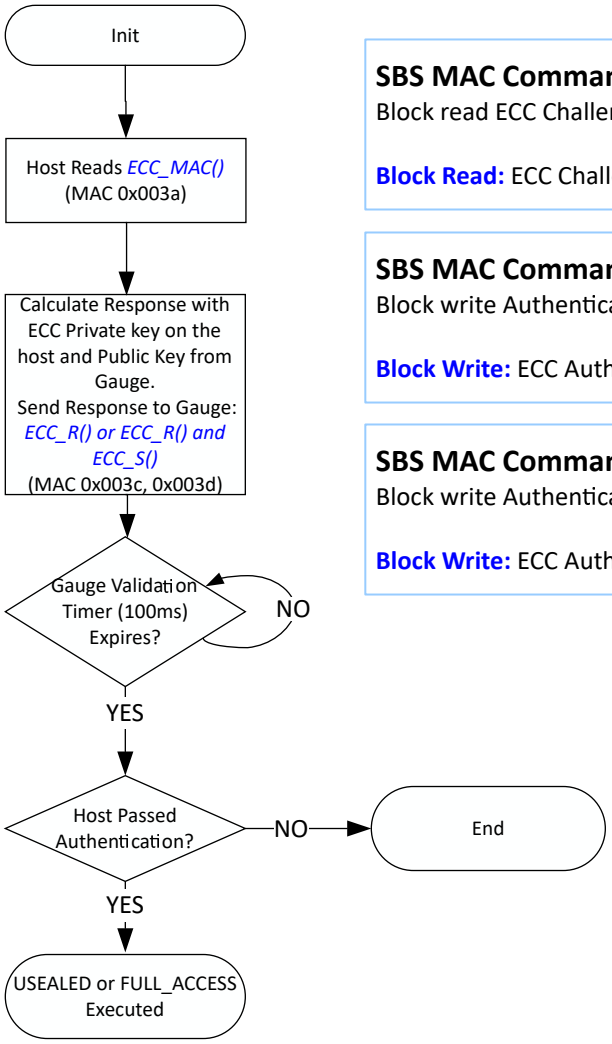



**图 5-1. 主机认证概述**

更详细的执行流程图如 图 5-2 所示。




**SBS MAC Command 0x003a ECC_MAC()** S/U/F
Block read ECC Challenge from Gauge (8 bytes)

**Block Read:** ECC Challenge (Little Endian)

**SBS MAC Command 0x003c ECC_R()** S/U/F
Block write Authentication *r* or *r* & *s* (30 or 60 bytes)

**Block Write:** ECC Authentication *r* or *r* and *s* data (Little Endian)

**SBS MAC Command 0x003d ECC_S()** S/U/F
Block write Authentication *s* (30 bytes)

**Block Write:** ECC Authentication *s* data (Little Endian)

* Command availability under the following Security Modes:
S: Seal Mode
U: Unseal Mode
F: Full Access Mode

**图 5-2. 主机认证流程图**

# 6 BQSTUDIO 中的认证流程

BQSTUDIO 是德州仪器 (TI) 提供的用于与 BQ41z50 通信的工具。为便于实施本文档所述的认证流程，使用了*高级通讯 SMB* 选项卡。图 6-1 列示了本文档中提到的一些关键用户互动。

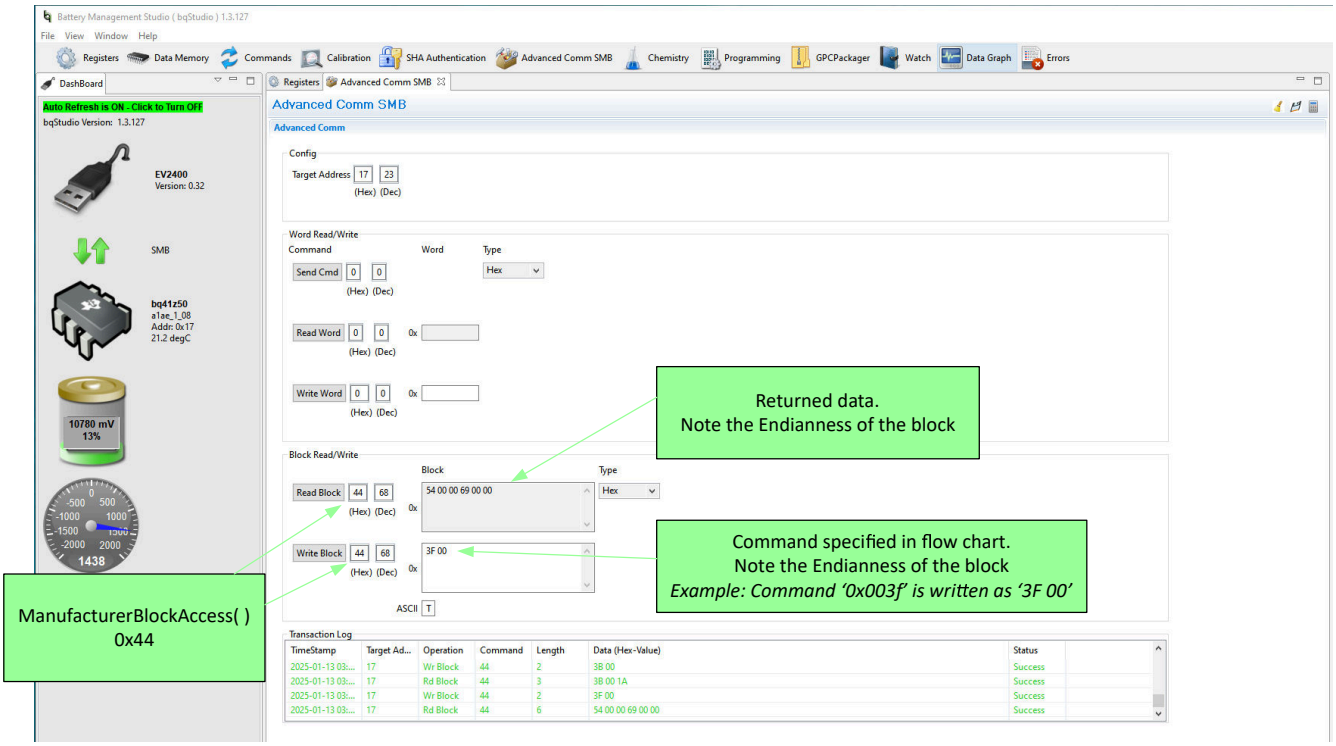



**图 6-1. BQSTUDIO 高级通讯 SMB 选项卡**

## 7 总结

总之，本应用手册介绍了如何生成 BQ41z50 器件的认证密钥，如何将密钥数据编程到器件中，以及如何在电池认证过程中使用已启用 bqBQ41z50 功能的电池。

# 8 参考资料


- KCDSA 任务组，*基于韩国证书的数字签名算法*
- 美国国家标准与技术研究院，*FIPS 186-5 数字签名标准 (DSS)*
- 美国国家标准与技术研究院，*FIPS 180-4 安全哈希标准 (HSS)*
- 国际标准化组织 (ISO)，*ISO/IEC 14888-3：2018 IT 安全技术 — 数字签名*
- 德州仪器 (TI)，*BQSTUDIO Battery Management Studio 软件*
- 德州仪器 (TI)，*BQ40Z50 1-4 节串联锂离子电池组管理器 | 电池电量监测计*
- 德州仪器 (TI)，*BQ41Z50 2-4 节串联锂离子高度集成式电池电量监测计和保护器*


**表 8-1. 算法汇总和注释**

| 算法 | 注释 |
|---|---|
| ECDH | #peer_kbub 为 32 字节<br>#self_kpri 为 32 字节<br>#密钥为 30 字节<br><br>`secret = ecdh(peer_kpub, self_Kpvt)` |
| PBKDF2HMAC | #openssi 的 python 代码示例<br>#Salt 是从电池电量监测计读取的随机数<br>#AES-128 的长度为 16 字节<br>#迭代次数为 128<br>#密钥是 AES-128 密钥<br><br>`from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC`<br>`kdf = PBKDF2HMAC(`<br>`aglorithm = hashes.SHA256( ),`<br>`length = 16,`<br>`salt=bytes(salt),`<br>`iterations = 128,`<br>`backed=backend`<br>`)`<br>`aeskey = bytearray(kdf.derive(bytes(secret)))` |
| AES | #iv 是从电池电量监测计读取的<br>加密的 ProdKpvt ProdKpve 为 32 字节<br><br>`from Crypto.Cipher import AES`<br>`cipher = AES.new(aeskey, AES.MODE_CTR, nonce=bytes(iv[0:8]),`<br>`initial_value=bytes(iv[8:16]))`<br>`CProdKpvt = cipher.encrypt(ProdKpvt)` |
| ECC | ECC-233 |

# 重要通知和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的相关应用。 严禁以其他方式对这些资源进行复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265