Application Brief

TMP1827 的密钥生成和身份验证机制

Amit Ashara

Temperature and Humidity Sensing

控制系统通常依赖于传感器的输入，这些传感器可以是底盘上子系统或模块的一部分，也可以是非板载元件。这些元件可以是超高精度负温度系数 (NTC) 热敏电阻或铂电阻温度检测器 (RTD)，这通常很昂贵，需要额外的工程时间和资源进行校准。在需要精确温度补偿的关键工业应用中，通常使用 AA 类 RTD 或容差为 0.01% 的 NTC 热敏电阻。但是，使用现成的 RTD 或 NTC 热敏电阻可以轻松替换这些昂贵的元件。此外，终端设备（如应用或特定于供应商的电池包、医疗耗材和可更换产品）需要一种机制，主机控制器可以通过该机制确保插件模块为原装模块。为了应对认证的挑战和要求，TI 开发了 TMP1827，这是一款带有集成 2048 位 EEPROM 和 SHA-256-HMAC 认证引擎且基于单线 ±0.3°C 精度的温度传感器，而且具有以下特性：

- 以符合 FIPS 180-4 的安全散列标准实施
- 以符合 FIPS 198-1 标准的 HMAC 算法实施
- EEPROM 的已认证写保护模式
- NIST 可追溯出厂编程不可擦除 64 位标识号
- IEC 61000-4-2 ESD 用于 8kV 接触放电，适用于插件应用

质询-响应

如前所述，主机控制器无法区分此类替换器件，可能会出现很大的误差，并可能对安全应用造成危害。这在必须满足严格标准的医疗应用中变得更加重要。检测此类替换的理想方法是使用 TMP1827 为替换器件添加身份验证。主机可以向目标器件发出质询消息（通常是一组随机数据字节）并接收响应（即消息的散列签名）。通过验证接收到的对预期响应的响应，主机现在可以验证温度传感器是否真实，数字值是否可信。

但是，主机和目标必须共享一个公共密钥，以便两个器件可以生成相同的数字签名。一种常见的方法是对所有目标使用相同的密钥，这会导致以下问题：如果提取一个目标器件密钥，则可能会影响整个目标器件批次。因此，始终建议每个目标器件使用唯一的密钥，这在提供增强安全性的同时会使密钥生成过程更加复杂。

密钥生成

图 1 展示了一种方法，通过使用加密方法来确保每个目标器件的密钥生成是唯一的。为了简化加密方案，使用了 SHA-256-HMAC 示例。主机读取出厂时编程的 64 位唯一标识符，然后将标识符与用户特定的机密消息和密钥混合。这会为每个 TMP1827 生成唯一的 256 位哈希，然后可将其安全地编程回器件并由 TMP1827 提供保护。但是，由于并非每个主机 MCU 都可以具有 SHA-256-HMAC 模块，因此 TMP1827 的 SHA-256-HMAC 引擎可以在安全环境中用于生成密钥。否则，请使用此处提供的软件实现。

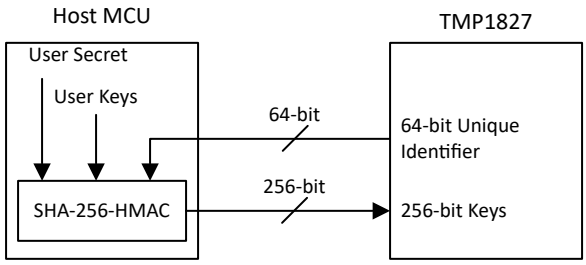

图 1. 密钥生成流程

密钥验证

通过生成密钥并对其进行编程，现场部署现在变得更加轻松。如图 2 所示，主机现在可以使用相同的过程来重新生成密钥，然后在写入 TMP1827 或从 TMP1827 验证哈希时使用密钥来生成哈希，而无需交换密钥。通过为每个事务使用新的质询/响应数据负载，主机可以动态地更改目标器件的预期，从而抵消重放攻击模型。

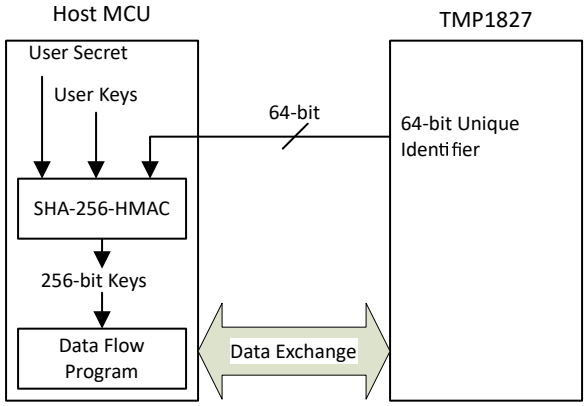

图 2. 密钥再生和数据流模型

总结

TMP1827 是一款独特的 ±0.3°C 精度温度传感器，具有集成的 SHA-256-HMAC 认证引擎，可支持热分配表和冷端补偿等工业应用，依靠精确的温度测量来安全地读取温度并更新 2048 位 EEPROM 中的关键系统校准内容，同时防止假冒和篡改终端设备。

重要声明和免责声明

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 产品的应用。严禁对这些资源进行其他复制或展示。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