基于国密算法的设备安全认证系统设计

Design of device secure authentication system base on SM2

许小波 （上海交通大学电子系，上海 200240）

摘 要：本文针对电子产品主机与设备之间的安全认证，提出国密算法用于安全认证，设计出通过两次签名验证完成主机对设备和设备对主机的认证方法，并以手机主机对电池的认证进行示例演示。

关键词：国密；SM2；安全认证

0 引言

我们日常生活中使用的电子产品常常是主机带有设备，如打印机与墨盒，苹果手机与数据线。这些主机与设备之间一般都有一个安全认证过程，即认证该设备是否合法，只有合法的设备接入主机才允许使用，以此保证产品安全可靠地运行。在安全认证方法上，文献 [1] 中讨论了使用国际安全算法 SHA−256 和 ECDSA 的实现方式，并且只包含了主机对设备的安全认证，并没有设备对主机的安全认证，属于单向认证。本文首先讨论了基于国密算法的设备安全认证方式，然后设计出基于国密算法的设备单、双向安全认证系统。

1 国密算法安全认证方式

国密算法中包含对称密钥算法 SM1、SM4 等和非对称密钥算法 SM2[2]，对称算法即消息发送和接收双方使用相同的密钥进行运算，其好处是运算速度快，缺点是需要严格保管好该密钥。非对称密钥算法即消息发送和接收双方使用不同的密钥进行运算，消息发送方使用私钥签名，消息接收方使用公钥验证签名，其特点与对称密钥算法正好相反，运算速度稍慢，但只需要保管好私钥就行了，公钥是可以公开的。基于上述特点，在我们的讨论的主机与设备的安全认证中，若是采用对称算法，即主机与设备都使用相同的的密钥，这就要求设备端的密钥不能被窃取，大大增加设备端的安全保护难度。因此，我们采用国密非对称算法 SM2。

2 国密算法安全认证系统设计

首先，预置认证公钥。我们产生一对认证的 SM2 密钥对 Authentication_Private_Key 和 Authentication_Public_Key。在设备生产工厂的安全环境下，将认证公钥 Authentication_Public_Key 预置到设备里，其次，用认证私钥对设备唯一性数据进行签名。设备里产生一对设备的 SM2 密钥对 Device_Private_Key 和 Device_Public_Key。导出设备的 Device_Public_Key 和设备序列号等设备唯一性数据，由认证私钥 Authentication_Private_Key 对其签名，将签名信息再置入到设备里，预置后的设备所含数据如图 1 所示。以上两步都是设备生产工厂的安全环境下进行，同时要求设备出厂后对置入的认证公钥和签名信息、设备的 SM2 密钥对、设备序列号等唯一性数据不可更改。最后，设备出厂后认证方法如下。

主机端预置认证公钥证书 Authentication_Public_Key，读取设备里的认证公钥信息进行比较，不一致则认证失败；若一致则继续读取设备里的设备公钥 Device_Public_Key、序列号等唯一性数据和签名信息，进行 SM2 签名验证。若签名验证失败则设备认证失败；若签名验证通过，则进一步地向设备发送一个设备认证随机数，设备端用设备私钥 Device_Private_Key 对该随机数进行 SM2 签名，返回该随机数的签名信息给主机，主机端用前面读取的设备公钥 Device_Public_Key 对其进行 SM2 签名验证。若签名验证失败则设备认证失败；

作者简介：许小波（1982—），男，硕士生，主要研究方向为嵌入式系统安全，Email: xuxiaobo1997@163.com。

若签名验证通过，则主机对设备认证成功。整个处理流程如图 2 所示。

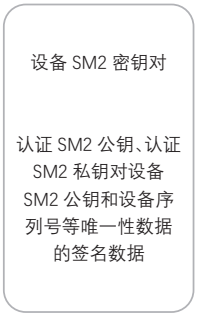

图1 在工厂安全环境下预置数据到设备

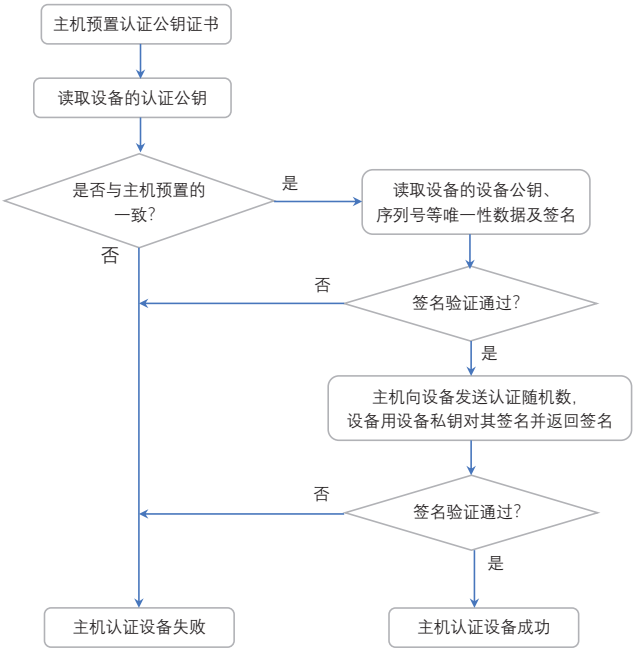

图2 主机认证设备流程图

对于更高安全级别的系统，设备端也可以对主机进行认证，即双向认证系统，其方法为：主机端除了预置认证公钥证书 Authentication_Public_Key，还预置有一对主机端的 SM2 密钥对 Host_Private_Key 和 Host_Public_Key，并且预置认证私钥 Authentication_Private_Key 对 Host_Public_Key 的签名信息。然后，主机将 Host_Public_Key 和该签名信息发送给设备进行 SM2 签名验证。若验证通过，主机再向设备请求一个主机认证随机数，然后主机端用主机端的 SM2 私钥 Host_Private_Key 对该随机数进行 SM2 签名，再将其发送给设备进行 SM2 签名验证。若验证通过，则完成了设备对主机认证。整个处理流程如图 3 所示。

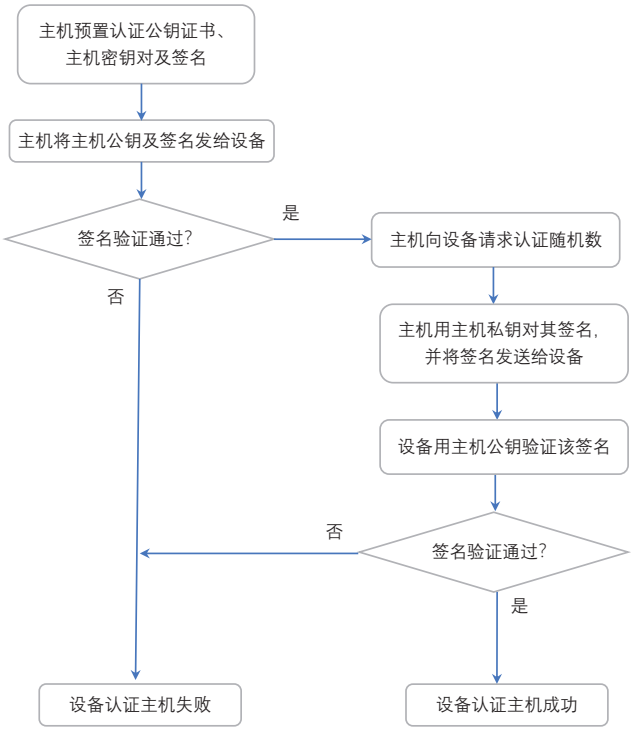

图3 设备认证主机流程图

3 国密算法认证系统示例

我们以手机主机对电池认证为例，在手机开机或充电时手机主机对电池设备进行安全认证，只有认证成功之后手机才能开机运行或对其充电。为此，我们需要在电池设备里增加一颗国密安全芯片，用于和手机主机进行数据交互，预置公钥的安全存储和国密算法的签名验签等操作。这里我们选用上海爱信诺航芯电子科技有限公司的国密安全芯片 ACL16，它采用 32 位 ARM Cortex−M0 内核，最高主频 48 MHz，集成国密、国际算法等多种安全算法模块，电压、频率、温度等安全检测功能和主动金属屏蔽层保护、总线加密串扰等多种保护功能，拥有 USB、SPI、UART、I²C 等丰富的外设接口，内置 RC 振荡器，专门面向低成本、低功耗的应用领域[3]。

硬件方面，我们采用两线的 I²C 做为手机主机与 ACL16 的通讯接口，手机主机做为 I²C 主设备，ACL16 做为 I²C 从设备，再加上电源和地线接口，ACL16 这边

就完成了。由于两边 I/O 口电压不同，还需要在手机主机端增加一颗电压转换芯片，以实现 1.8~3.3 V 的电压转换。整个硬件框图如图 4 所示。

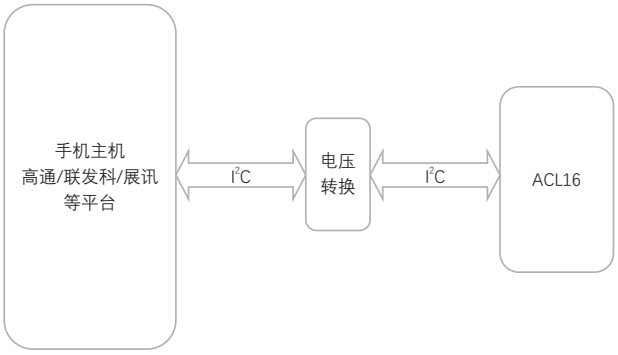

图4 手机主机与ACL16的硬件连接框图

软件方面包括 ACL16 的安全固件和手机主机软件，我们先来看 ACL16 这边的安全固件。ACL16 在上电后，首先进行系统初始化，开启各安全检测模块，初始化 I2C 接口，然后等待接收手机主机发送的命令。待接收完一包命令数据后，对命令数据进行完整性校验，只有校验通过后才对命令进行处理。最后，待命令处理完成，将命令响应数据发送给手机主机。

手机主机方面的软件分包括，处理与 ACL16 通讯的 Linux 驱动和 Android Java 应用层代码。在 Linux 驱动里，主要完成向 I²C 总线驱动上注册驱动，注册字符设备和在 /dev 目录创建设备文件 authenticator，以使应用层对设备文件 authenticator 的读写操作时进而对 ACL16 进行发送命令和接收命令响应。Android 应用层代码包括 JNI 的 so 库和 Java 应用，其中 so 库主要完成对 authenticator 设备的打开、读写操作，为 Java 层提供操作接口。Android Java 应用则主要通过调用 so 库的接口，实现手机主机对电池的认证操作流程和电池对主机的认证操作流程。对于 JAVA 上的 SM2 签名、验签操作，其相关接口采用的是 Bouncy Castle 加密库 bcprov-jdk15to18-168.jar 中 的 SM2 接 口。Bouncy Castle 加密库是澳大利亚非营利组织 Bouncy Castle 编写的轻量级加密 API[4]，非常适合在手机上使用，最新版本为 Version 1.68，包含了对最新 CVE 漏洞的修复，以及对 TLS 1.3 版本的支持。我们在手机演示界面上添加三个按钮，分别执行主机认证设备、设备认证主机和清除显示日志操作。其中点击完“主机认证设备”按钮后的界面如图 5 所示，点击完“设备认证主机”按钮后的界面如图 6 所示。

图5 点击主机认证设备按钮后的界面

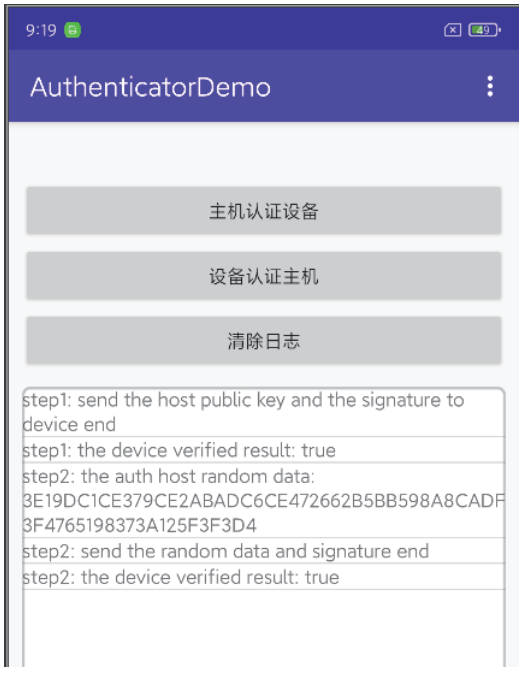

图6 点击设备认证主机按钮后的界面

(下转第56页)

表 5 中，280 h 前为产品早期故障期，20 年后为损耗故障期。中间部分为正常使用的有效寿命期，这一阶段产品故障率相对稳定。由此可知，我们的产品在出厂前要做好老化工作，让其度过早期故障期。

3.5 参照标准[5]

参照 ISO13849 对 *MTTFFd*(等同于这里的 *MTTF*) 的失效风险评估（如表 7）。

表7 ISO13849关于失效时间的定义

每个通道的平均危险失效时间（**MTTFd**）

每个通道的指标	每个通道的范围
低	**MTTFd<10**年
中	**MTTFd<30**年
高	**MTTFd<100**年

注意：每个通道**MTTFd**范围的选择基于该领域内最新技术的失效率，这种技术构建了一种适合对数**PL**标度的对数标度，现实中**SRP/CS**的**MTTFd**值预期不能小于**3**年，否则这意味着一年以后市场上**30%**的系统不合格且需要更换，每个通道的**MTTFd**值大于**100**年也不合适，因为高风险下的**SRP/CS**不宜只依靠零件的可靠性，为了加强**SRPCS**预防系统性和随机失效的能力，推荐采用附加方法，例如:要求冗余和实验，为了更可行，范围的数量限制在**3**个内，**MTTFd**值最大为**100**年的每个通道的限制应参考执行安全功能的**SRP/CS**的单个通道，更高的**MTTFd**值可用于单个零件

4 结语

新产品的寿命模拟评估已经引起了很多单位的重视，未来会将 *MTTF* 计算系统与高温老化设备及电脑终端组建自动化测试系统，将使产品寿命模拟测试更加直观和智能化。

参考文献：

[1] 胡志山.射频印刷电感替代低值空心电感的探索[J].电子产品世界,2015(1):54-56.
[2] 胡志山.射频宽带产品的指压调试法[J].电子世界,2014(17):139-140.
[3] 朱晓燕,曹晋红.浴盆曲线在可靠性设计和管理中的应用[J].中国质量,2007(7):25.
[4] 江玉彬.浴盆曲线在通信电源设备管理中的应用[J].通信电源技术，2013(1):11.
[5] 国际标准化组织.控制系统中与安全[S].ISO 13849-1-2006.

(上接第38页)

4 结语

具有国内自主知识产权的国密算法已经在金融领域开展使用，并逐步替代国际安全算法。本文提出了基于国密算法用于设备的安全认证系统，可取代现有的国际算法安全认证，并可在更广泛的物联网领域进行实际推广应用。

参考文献：

[1] D’ONOFRI M.通过设备认证杜绝造假[J].电子技术及信息科学,2015(01):32-34.
[2] 国家密码管理局.SM2椭圆曲线公钥密码算法[R/OL].[2010-12-17].https://www.oscca.gov.cn/sca/xxgk/2010-12/17/content_1002386.shtml.
[3] ACL16_Datasheet_V2.0.pdf[Z].
[4] Bouncy Castle Cryptography Library[R/OL].https://www.bouncycastle.org/java.html.

(上接第43页)

4 结语

利用激光高速扫描的特点，能够精确检测到跟车驶入时两车的间隙位置，并对跟车的车辆进行准确的分离及准确的对应车辆的轮廓信息，保证检测数据与车辆的一一对应关系，保证车辆队列的正确性，不多车，不漏车；可广泛地应用于固定式治超站、高速公路入口治超站、非现场执法站的车辆长超宽超高检测。

参考文献：

[1] 李明,康静秋,贾智平.嵌入式TCP/IP协议栈的研究与开发[J].计算机工程与应用,2002,38(16):118-121.
[2] 黄克亚.ARM Cortex-M3嵌入式原理及应用——基于STM32F103微控制器[M].北京:清华大学出版社,2020.
[3] STEVENS W R.TCP/IP详解 卷1:协议[M].2版.译:范建华,等.北京:机械工业出版社,2000.