

DX81 安全 EEPROM

I2C/SPI Secure EEPROM With SHA1 Anti-Clone Authentication

1. 产品概述

在传统的 24/25 系列串行 EEPROM 存储功能的基础上增加了：每颗芯片 wafer 制造的唯一 SN 序列号，用户可一次性编程写入的 UID，Host 防克隆安全认证，用户区数据的可编程安全访问模式等安全功能。

DX81 系列：

Part	Interface	EEPROM	Zones	Voltage	Package	Status	Description
DX81C01	I2C/SPI	1K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	I2C/SPI Interface Security EEPROM With SHA1 Authentication
DX81C02	I2C/SPI	2K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	
DX81C04	I2C/SPI	4K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	
DX81C08	I2C/SPI	8K bits	8	1.8-5.5V	1,2,3,4	Sample	
DX81C16	I2C/SPI	16K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX81C32	I2C/SPI	32K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX81C64	I2C/SPI	64K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX81C128	I2C/SPI	128K bits	16	1.8-5.5V	1,2,3	Sample	
DX81C256	I2C/SPI	256K bits	16	1.8-5.5V	1,2,3	Sample	

2. 基本特性

- DX81-I2C 兼容标准 I2C 总线协议，最高 1Mbps
- DX81-SPI 兼容标准 SPI 总线协议，最高 10Mbps
- 配置区 Memory
 - 每颗芯片通过 wafer 制造定制唯一 ROM SN 序列号
 - 内置 56 bits OTP 用户 UID，用于产品生产和流通管理
 - 64 bits 芯片配置密钥，对用户进行认证
 - 128 bits Host 认证密钥
- 用户 EEPROM 数据区（1Kb---256Kb）
 - 分成 4--16 个独立的访问区

- 每个区单独设置 128bits 密钥长度
- 每个区独立进行双向认证
- 每个区具有灵活的可编程访问模式：

只读模式 PGO (Program Only) 模式

普通模式 认证模式 加密模式

- 支持单字节、多字节和页编程写入
- 擦写次数：100K Cycles
- 数据保持：10 Years

- Host Anti-Clone 认证：

- 国际通用 SHA1 算法
- 128 bits 密钥长度
- 每次计算的结果动态随机，即使相同的挑战输入

- 其他安全特性

- 数据传输流加密和 CRC 校验
 - 有效防止传输线上的数据被干扰和截获
- EEPROM 物理访问地址 Scramble，与 SN 相关
- EEPROM 物理数据存储加密，与 SN 相关
- 相同地址的相同数据，存储在每颗芯片的物理地址和值都不一样
 - 有效防止 EEPROM 被物理复制
- 内置真随机数发生器
- 内置 POR 和 OSC 电路
- 高低压检测

- 电压：1.8 — 5.5V

- 温度：-40°C -- +85°C

- ESD：4KV

- Sleep 电流：< 15uA

- 封装类型：SOP8/TSSOP8/UDFN8/MSOP8/SOT23-6

DX81-I2C 系列 Pin-to-Pin 兼容 24 系列串行 EEPROM

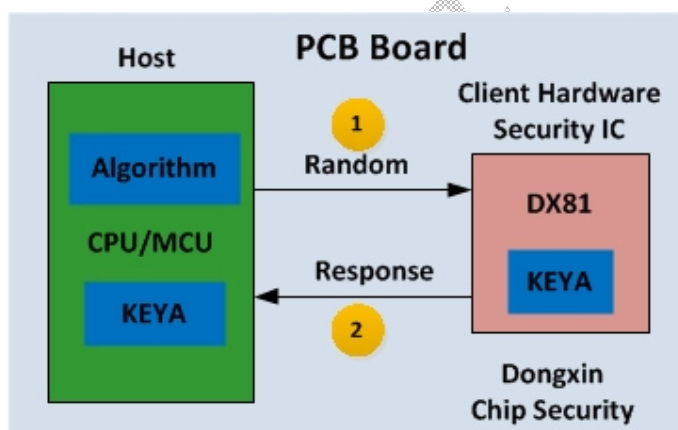
DX81-SPI 系列 Pin-to-Pin 兼容 25 系列串行 EEPROM

- 技术支持：

- 烧录设备和软件
- 定制主机库文件和 SDK
- 支持 Android 操作系统
- 应用：
 - 兼容传统 24/25 系列串行 EEPROM 功能，Pin-to-Pin
 - 防抄板认证，硬件 PCB 认证保护
- 电子设备的外设、配件、附件等的防山寨认证
- 电子产品代工生产数量控制，代理商出货、窜货管理，售后服务认证
- 电子设备的软件版权管理和授权
- 电子产品多项付费功能的开通、禁止授权
- 电子设备敏感参数和安全数据及密钥存储
- 用户密钥认证及校验，密码不会暴露在数据线上
- 可用于手机附件，打印机墨盒，原装电池，医疗设备配件，
机顶盒，游戏机，GPS 导航仪，视频监控设备等

2. 应用方案

PCB 防抄板典型应用方案



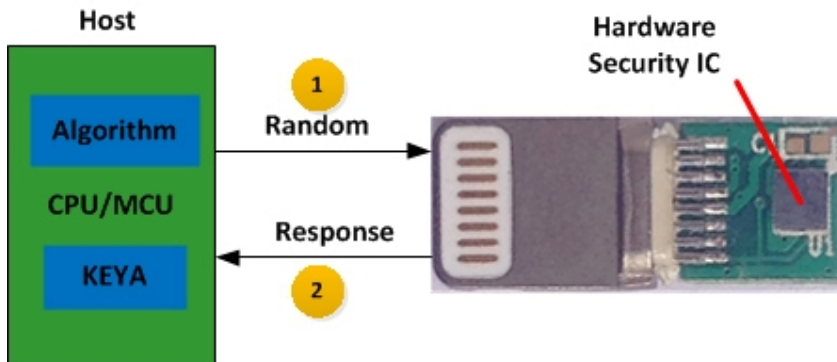
通过在 PCB 电路板上嵌入 DX81 芯片(如果原电路板有 24 系列串行 EEPROM,可以直接替代),并预先烧录好 128bits 认证密钥 KEYA,然后在主机软件中嵌入认证程序,实现主机对芯片的认证。即便盗版者复制了 PCB 板,并且从存储器中直接 copy 出了 CPU 的 binary code,将代码烧录进被复制的存储器中,由于烧录的程序会不时的与 DX81 芯片进行挑战---应答的认证,因为盗版者无法获得厂商定制烧录认证密钥 KEYA 的 DX81 芯片,认证就无法通过,因此系统将无法运行。

产品在进行代工生产的时候,也可以通过控制烧录认证密钥的 DX81 芯片数量来有效控制代工

为开微电子 2014年 发布 版权所有

生产的出货数量，以防假冒产品流入市场。

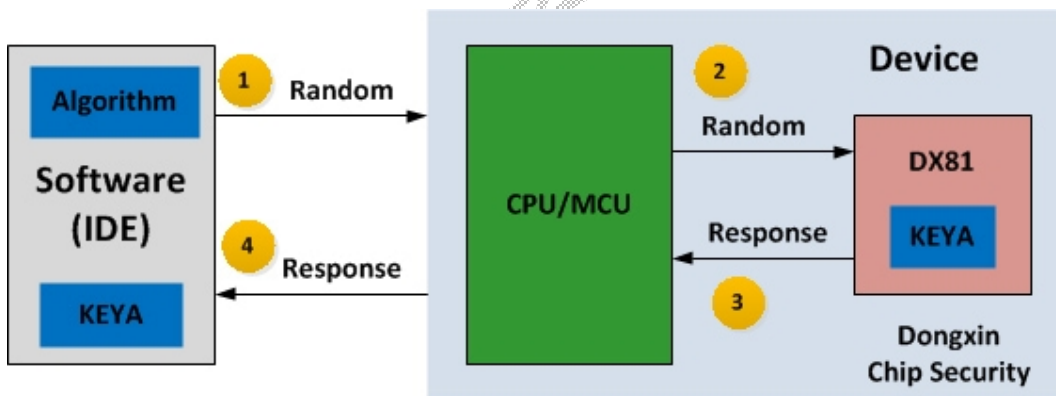
电子配件原装认证方案



此方案需要将 DX81 芯片嵌入到原装配件中，当原装的配件与主机相应接口相连时，设置主机软件启动认证流程，对配件上的芯片进行认证，只有认证通过后才允许配件正常工作，否则配件将无法使用，这样可以通过 DX81 芯片来防止劣质配件的仿冒。

应用市场：移动设备电池、打印机墨盒、充电线、手机皮套等等

电子设备系统接入控制



此解决方案与 PCB 防复制不同的是，防克隆认证的流程在外部系统软件计算完成（如远程服务器），被认证设备即可以在本地、也可以是远程的。当设备接入系统或者网络时，系统软件通过本地接口或者网络发送随机数挑战验证设备，设备收到挑战后传给 DX81 进行计算，芯片完成计算后将结果通过设备传输给系统软件，软件将收到的结果与自己计算的结果进行比较，正确则允许设备接入系统或者网络，否则设备将被拒之门外。应用市场：各类电子产品的防伪认证、医疗设备配件认证、售后服务认证、授权接入控制等