

DX82 加密 EEPROM

I2C/SPI Secure EEPROM

With Identity Authentication and Encryption

1. 产品概述

为了满足物联网设备安全认证的应用需求，在 DX81 系列的基础上，DX82 系列增加了对称标识认证单元，不仅兼容 DX81 系列的功能，而且实现了基于联网设备标识的安全认证和加密功能：同域设备间，只需知道标识，即可完成相互的鉴别认证和加密数据传输。

- 无需建立复杂的密钥管理中心。
- 无需主机 CPU 计算能力
- 主机只需流程控制和数据传输

DX82 系列:

Part	Interface	EEPROM	Zones	Voltage	Package	Status	Description
DX82C01	I2C/SPI	1K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	I2C/SPI Security EEPROM With Identity Authentication and Encryption
DX82C02	I2C/SPI	2K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	
DX82C04	I2C/SPI	4K bits	4	1.8-5.5V	1,2,3,4/5(I2C)	Production	
DX82C08	I2C/SPI	8K bits	8	1.8-5.5V	1,2,3,4	Sample	
DX82C16	I2C/SPI	16K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX82C32	I2C/SPI	32K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX82C64	I2C/SPI	64K bits	16	1.8-5.5V	1,2,3,4	Sample	
DX82C128	I2C/SPI	128K bits	16	1.8-5.5V	1,2,3	Sample	
DX82C256	I2C/SPI	256K bits	16	1.8-5.5V	1,2,3	Sample	

2. 基本特性

- DX82-I2C 系列兼容标准 I2C 协议，最高 1Mbps
- DX82-SPI 系列兼容标准 SPI 总线协议，最高 30Mbps

支持高清图像实时加解密

- 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，支持写入手机号、QQ 号等，不仅规范产品编号，

进行生产、出货、窜货管理，同时也便于产品接入物联网或者移动互联网

--- 64 bits 芯片配置密钥，对用户进行认证

--- 64 bits 标识域（群）密钥

--- 128 bits Host 认证密钥

- 用户 EEPROM 数据区（4Kb---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

--- 密钥长度每次计算的结果动态随机，即使相同的挑战输入

- 标识认证特性：

--- 每颗芯片内置对称标识密钥算法单元

 无需建立复杂的密钥管理中心，无需主机 CPU 计算能力

--- 支持端到端的签名认证

--- 支持一对一、一对多、多对多实时加解密，一人一次一密

--- 芯片内部 3DES 加解密速度达 30MBytes/s

--- 内置一个公共域和一个可配置 64bits 密钥的私有域

--- 支持用户数据 3DES 和 SHA1 的计算

- 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：-400C -- +850C
- ESD：4000V
- Sleep 电流：< 15uA
- 封装类型：SOP8/TSSOP8/UDFN8/MSOP8/SOT23-6

DX82-I2C 系列兼容 24 系列串行 EEPROM

DX82-SPI 系列兼容 25 系列串行 EEPROM

- 技术支持：

--- 烧录设备和软件

--- 定制主机 SDK

--- 支持 Android 操作系统

- 应用：

--- 兼容 24/25 系列串行 EEPROM，Pin-to-Pin

--- 物联网设备相互识别和认证

--- 物联网设备间数据传输加密

DX82-I2C 系列外部加解密速度可达 1Mbps

DX82-SPI 系列外部加解密速度可达 30Mbps（支持高清图像实时加解密）

--- 物理、网络及计算机访问控制

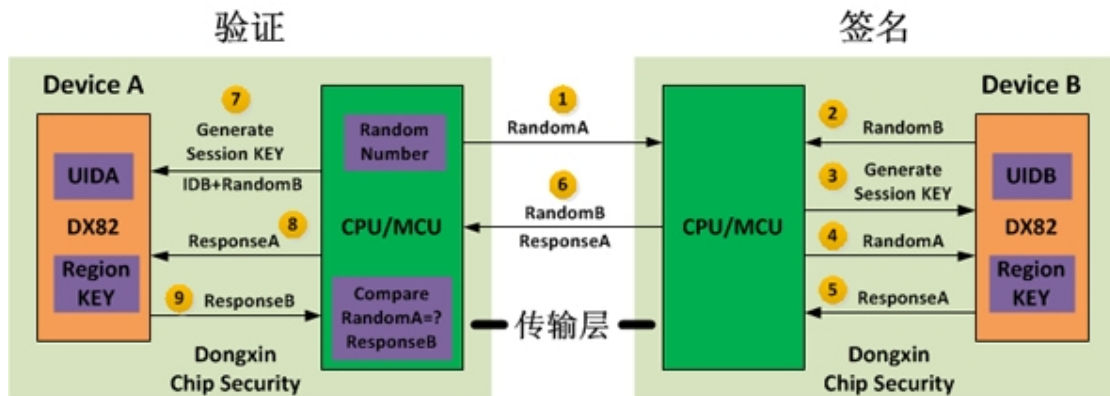
--- 网络机顶盒、车载 GPS

--- 智能家居、网络摄像头、视频监控、传感器设备

--- 物安全路由器，等等

3. 应用方案

M2M 动态签名认证方案

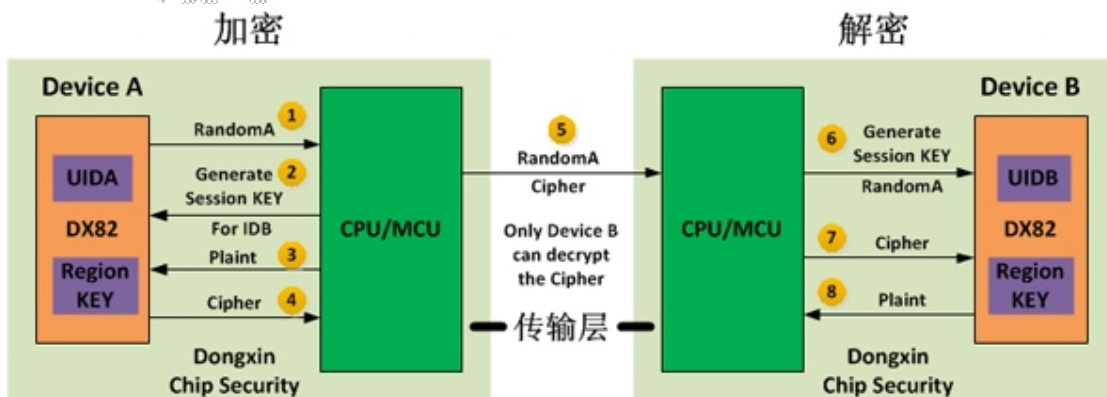


此方案实现了端到端直接认证，多颗 DX82 芯片只需设置相同的群密钥，这样嵌入相同群密钥芯片的设备间，只需知道其他设备该芯片的 SN 和 UID，无需任何其他密钥，就可以实现相互鉴别和认证，防止非法假冒的设备接入系统和网络。

DX82 芯片内嵌了对称标识认证算法单元，签名时芯片内部会根据设置的群密钥、自身芯片唯一的 SN 和 UID，每次动态产生随机的签名密钥，然后用此签名密钥对挑战数据进行签名，即便每次相同的挑战数据，签名的结果都会不同，并且签名密钥在芯片内部只参与中间计算，永远不会出芯片，外部无法获取，这样可以有效的防止第三方设备伪造签名。

此方案无需主机建立复杂的密钥管理中心，只需设置芯片的群密钥，所有密钥计算和签名验证计算都在芯片内部完成，无需主机计算能力，主机只需流程控制和数据传输。

M2M 动态加密数据传输方案



此方案实现了端到端传输数据的直接加解密，多颗 DX82 芯片只需设置相同的群密钥，这样嵌

入相同群密钥芯片的设备间，只需相互知道该芯片的 SN 和 UID，无需任何其他密钥，就可以实现相互通信数据的直接加解密，有效防止传输线上的明文数据被非法窃取。

DX82 芯片内嵌了对称标识加解密算法单元，加密时芯片内部会根据设置的群密钥、接收设备该片的 SN 和 UID，每次动态产生随机的加密密钥，然后用此加密密钥对传输数据进行加密，即便每次传输相同的数据，加密的结果都会不同，加密密钥在芯片内部只参与中间计算，永远不会出芯片，外部无法获取，并且由于加密密钥是根据唯一接收设备的标识产生，只有拥有此标识的接收设备才能恢复同样的解密密钥对数据进行解密，这样可以有效的防止第三方设备窃取其他设备的密文数据进行解密。

此方案无需主机建立复杂的密钥管理中心，只需设置芯片的群密钥，所有密钥计算和数据加解密都在芯片内部完成，无需主机计算能力，主机只需此方案的流程控制和数据传输。