

ALPU的蓝牙应用

Neowine ALPU加密芯片介绍
—深圳市天浩旭科技有限公司

ALPU蓝牙应用说明

■ 背景

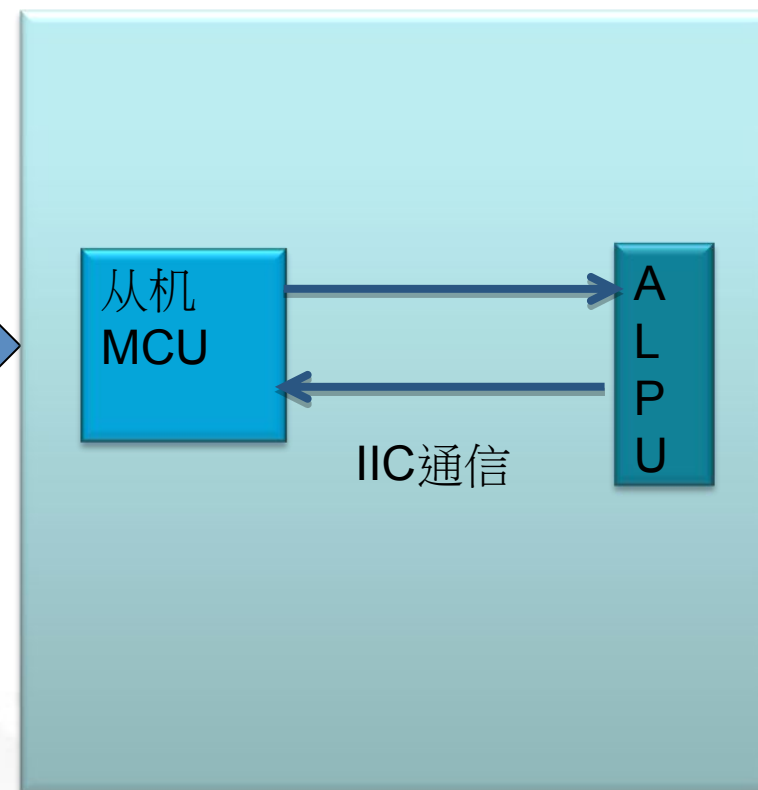
随着物联网时代的到来，越来越多的远程控制，远程操作的智能设备大量涌现。随之而来也出现了大量的认证操作。根据现有几个客户的使用案例，下面对ALPU在蓝牙设备上的使用进行简要的说明。

■ 蓝牙，作为一种支持设备短距离通信（一般10m内）的无线电技术。具有发送端，接收端两个方面进行数据交换。通过现有案例发现，客户多将认证存放在接收端，通过发送端进行校验。具体原理如下。

蓝牙主机认证端



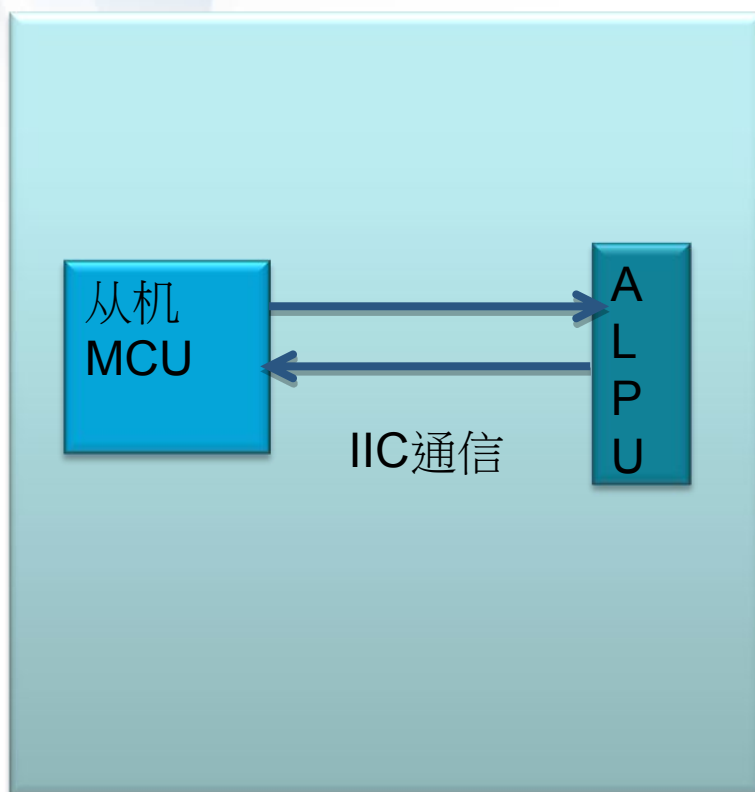
蓝牙从机接收端



主机端嵌入加密库文件，从机接收端搭载ALPU并通过IIC和从机MCU进行通信

相关细节说明

从机接收端



硬件：1.从机MCU 型号没有特殊要求，但需要支持蓝牙信息的传输及IIC通信。

软件：对系统没有要求，可以无系统。但需能执行IIC读写操作，及蓝牙相关操作。

本端作用：

- 1.从机MCU通过蓝牙接收主机端读写命令。
- 2.通过IIC执行对ALPU的读写操作。
- 3.通过蓝牙发送 ALPU的读取数据。

主机端说明



硬件：无特殊要求。

软件：无特殊要求。其中加密库需要嵌入到程序中。

本端作用：

- 1.主机MCU通过蓝牙发送lib中需要的读写命令。
- 2.通过蓝牙接收从机端得到的读取数据。
- 3.Lib进行加密验证。

工作流程

■1. 蓝牙连接，且蓝牙协议握手成功。

- a) 主机端，需要对从机端进行认证时，调用加密库。MCU将加密库中需要执行的读写命令通过蓝牙发送给从机MCU
- b) 从机端，MCU接收到读写命令，通过IIC和ALPU进行读写操作，并将读出数据发送给主机
- c) 主机端，接收到读取数据后，经lib加密处理并进行验证。
- d) 主机端，进行验证后的相关操作。

■2. 蓝牙连接，蓝牙协议并未进行握手操作

具体操作同上，验证值以蓝牙握手协议进行传输校验。如不通过，则蓝牙无法与具体的APP连接。

ALPU的远程认证流程如下：

主设备端MCU加密

system
data

明文X

签名X

lib

明文X

AES加密

密文X

会话密文A

WiFi/bluetooth
传输

WiFi/
bluetooth

比较是
否一致，
若一
致表明
信息可
靠，认
证通过。

明文X

system
data

密文Z

lib

签名Y

解密

加解密

AES加密

密文X

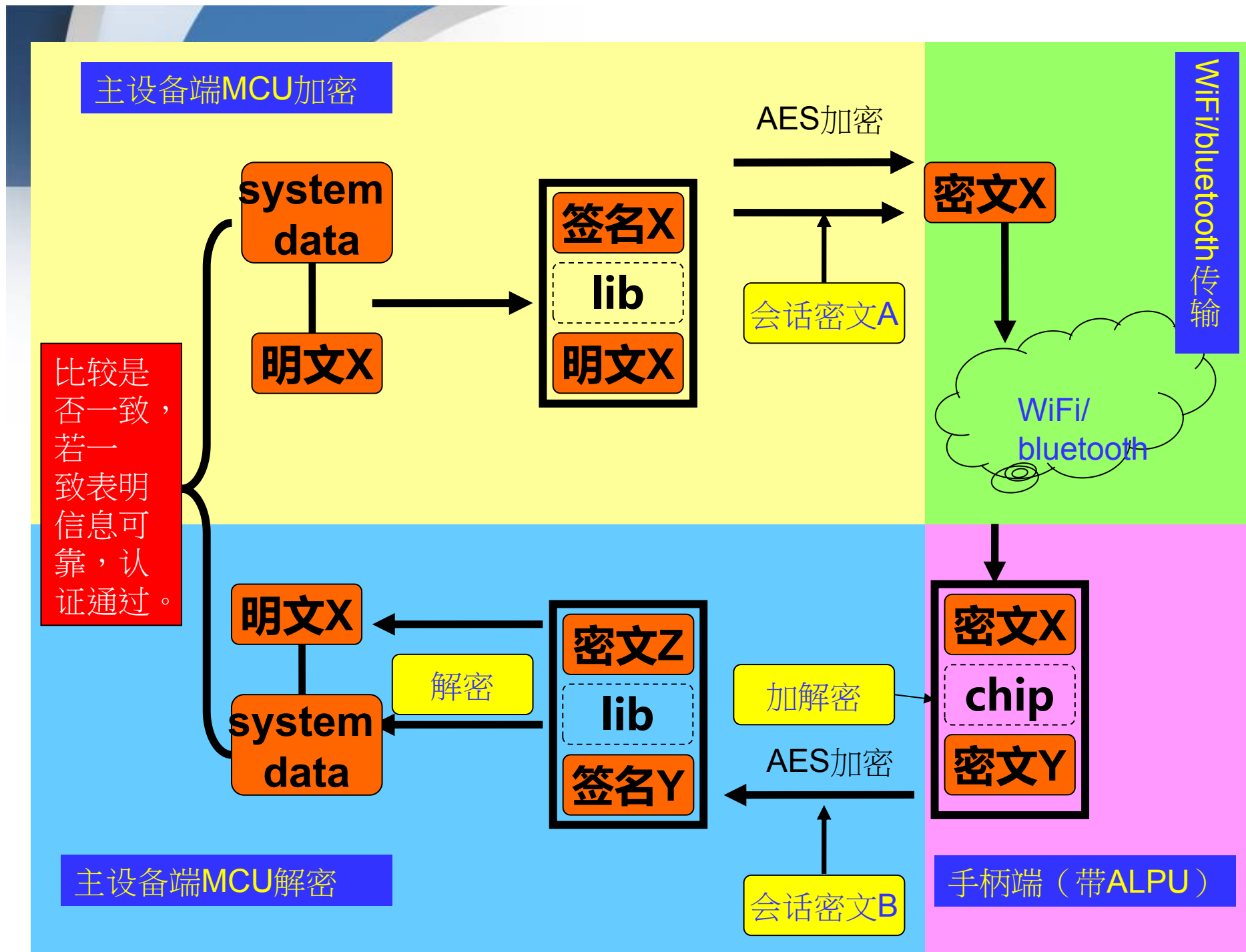
chip

密文Y

主设备端MCU解密

会话密文B

手柄端（带ALPU）



蓝牙操作的问题细节

一、稳定性，存在稳定因素

由于采用蓝牙传输中存在较多不稳定因素，这样会导致部分加密认证失败。-----现有解决方法，多次调用加密，以校验成功次数判断加密认证。

二、同步性。

从上面看到，加密库与芯片并不是在同一平台，需要进行lib和芯片的异步化操作 -----MP的已经实现

三、数据转换

从现有案例看，蓝牙传输多搭载在android系统进行，这就涉及到数据格式的转换与调用 -----MP的已经实现

ALPU在蓝牙上的使用方案

一、配套设备的附件认证。

将**ALPU**搭载附件上，通过主机端认证确保附件的不可替代性。
(附件如蓝牙手柄，手表，遥控器等)

二、智能家居的主从机端认证

将**ALPU**搭载在智能家居中，通过手机或其他支持蓝牙设备的**APP**对家居设备进行控制。

a)通过软件认证设备

b)通过设备认证软件，如软件不配套，蓝牙无法连通

传输方式以及应用的衍生

1.传输方式上

蓝牙的应用衍生出入WIFI传输，网络传输，局域网互联，**2G/3G**链接 等，都可以使用

2.应用方式上

除了验证设备，还可用来验证配套软件。

总结

通过异步加密流程的实现，先已具备了可以进行远程认证的应用方式。

随着**WIFI**等链接方式的普及 和**Android**的广泛应用，移动软件认证智能设备，也会出现这一趋势。前景非常广泛。



THE END

THXTEK天浩旭科技

0755-86583632 sales@thxtek.com