

信息安全领域

AES128算法

AES128是一种对称加密算法，使用128位密钥对数据进行多轮混淆和扩散，以其卓越的性能和高度的安全性脱颖而出，成为了全球广泛应用的加密技术之一。但是AES128算法在通用处理器上面临着明显的性能瓶颈，本文采用隼瞻科技ArchitStudio™工具，为AES128算法定制了一级加速和二级加速指令扩展方案，这些指令可直接在硬件层级执行单轮加密的核心操作，将原本需要大量内存访问和逻辑运算的操作压缩为少数几个时钟周期完成，最终在少量硬件开销的前提下获得13.6倍和50倍的性能收益。



隼瞻科技
WingSemi Technology

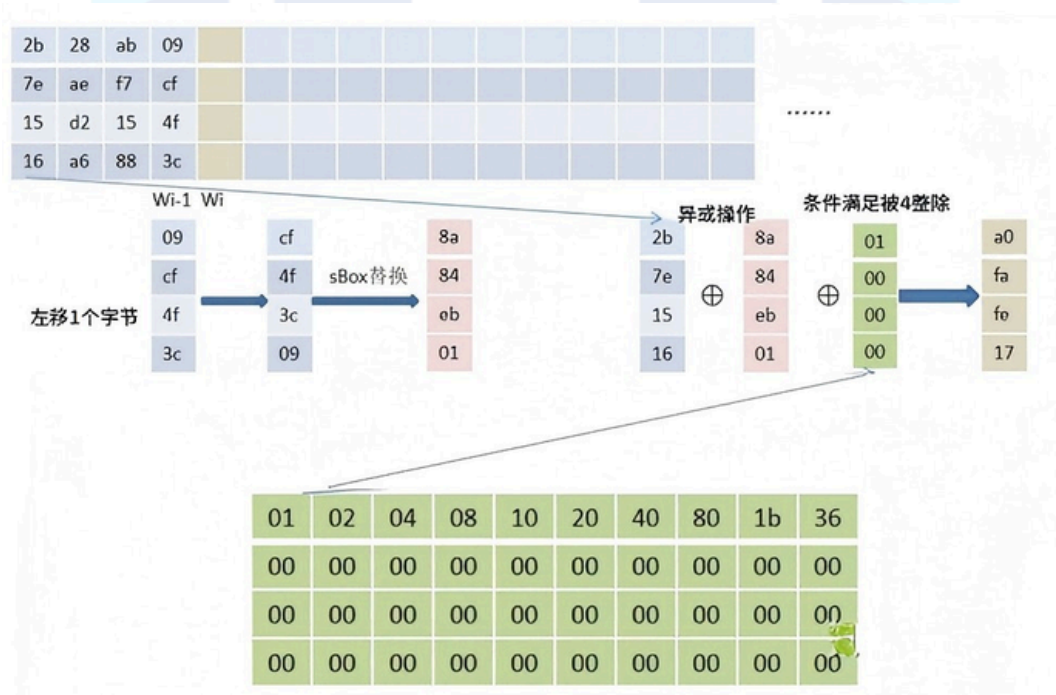
一、背景介绍

在物联网安全、数据传输加密、嵌入式设备身份认证等现代信息安全应用场景中，AES128对称分组加密算法凭借128位密钥的高安全性、轻量型的计算特性，成为终端设备端到端加密、数据存储加密的核心算法标准。AES128算法已广泛应用于智能硬件、工业控制终端、车载通信、消费电子等领域，这类场景对加密解密的实时性、硬件资源开销、功耗有着严苛要求，既需要保证加解密的处理速度满足业务流的实时性需求，又要求适配嵌入式设备的有限硬件资源与低功耗设计准则。

二、问题与挑战

1) AES128算法介绍

AES128算法以128 bit为一个明文/密文处理块，并以一个字节（8 bit）为一个单位，将数据块和密钥视为4x4字节的矩阵。算法的核心前置步骤为密钥扩展（KeyExpansion），将128位原始密钥扩展为10组128位的轮密钥，为每一轮迭代的轮密钥加操作提供密钥支持。



图：密钥拓展核心逻辑