
基于 SM2 国密算法的签名验签在 FPGA 上设计与实现

基于SM2国密算法的签名验签在FPGA上设计与实现

摘 要

随着互联网技术的飞速发展,以及智能手机、平板电脑等智能移动终端设备的普及,各种信息可以通过网络飞速传播,工业、商业、农业等各行各业无时无刻不在产生数据,传递数据,社会信息化程度越来越高,人们对网络的依赖性越来越强,而通过网络传递的信息具有匿名特性,因此需要有一种可以识别信息来源的方法,SM2 椭圆曲线签名验签算法很好的解决了信息的归属问题。

信息发送者通过对信息进行签名运算生成数字签名,然后将数字签名和信息一同发送给信息接收方,接收方收到信息后使用发送方的公钥等参数即可验证消息是否属于信息发送者所发送,同时还可以检查出信息发送过程中是否被修改。在公钥密码体制中,基于椭圆曲线离散对数问题的签名算法凭借它对宽带要求低、密钥短、安全性高、破解难度高等特点被广泛应用于政治、军事、计算机、通信等行业。我国于 2010 年正式颁布了《SM2 椭圆曲线公钥密码算法》标准,标志着我国椭圆曲线签名验签算法有了公开标准。但目前的数字签名及验签的实现大多数是通过纯软件的方式实现,运算速度慢,不适合高并发的场景下应用,尤其是在即将到来的 5G 时代,万物互联,这种低速的签名验签可能会极大的增加智能设备的计算负担。因此本文将椭圆曲线加密算法中最基础的模运算和点运算算法通过硬件描述语言在 FPGA 硬件实现,而签名验签步骤的调度则由嵌入式 CPU 负责,极大的缓解了 CPU 在签名验签过程中的计算负担,并且具有非常好的拓展性,通过修改调度程序即可实现其他椭圆曲线加密算法。同时为了验证硬件模块设计的正确性,使用 Miracl 大数运算库搭建验证平台,为硬件模块的测试产生参考数据,并设计签名和网络发送程序。在 FPGA 上开发嵌入式 SoC 平台,实现网络接收和签名验证功能。

第 1 章本文介绍了课题背景,阐述数字签名算法的现状和发展趋势,并明确本文的研究目的和意义。第 2 章为相关技术于开发环境的介绍,包括椭圆曲线加密算法的基础运算规则、SM2 签名算法的签名验签流程、Miracl 大数库介绍和 Quartus II 系列开发工具的介绍。第 3 章介绍了基于 FPGA 的 SM2 签名验签系统的总体设计和系统结构。第 4 章介绍了软件、硬件的详细开发步骤和设计细节。第 5 章详细展示了系统系统的运行状况,并展示实验结果。最后第 6 章是本文对所设计系统的总结。

关键词: 椭圆曲线, SM2, FPGA, SoC

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：

<https://d.book118.com/808032104006007007>