RSA 协处理器与 F2812 接口设计

章明朝[1,2]，于 晓[3]，李佩玥[1,2]，娄宏伟[1]，隋永新[1]，杨怀江[1]
(1. 中国科学院长春光学精密机械与物理研究所应用光学国家重点实验室，吉林 长春 130033；
2. 中国科学院研究生院，北京 100039；
3. 空军航空大学 训练部，吉林 长春 130022)

摘 要：采用 RSA 协处理器作为嵌入式 VPN 服务器中 RSA 运算核心部件，给出了其与主控制器 F2812 间的硬件接口设计、供电电源系统的设计，并进行了与硬件接口相关的软件模块设计与实现。经系统调试及测试，RSA 运算速度达到预期性能，可以满足嵌入式 VPN 服务器的要求。

关键词：RSA；RSA 协处理器；F2812；接口
中图分类号：TN23　　**文献标识码**：A

Design of interface between RSA coprocessor and F2812

ZHANG Ming Chao[1,2], YU Xiao[3], LI Pei Yue[1,2], LOU Hong Wei[1], SUI Yong Xin[1], YANG Huai Jiang[1]
(1.State Key Laboratory of Applied Optics, Changchun Institute of Optic, Fine Mechanics and Physics, the Chinese Academy of Science, Changchun 130033, China;
2. Graduate School of the Chinese Academy of Sciences, Beijing 100039, China;
3. Training Ministry, Aviation University of Air Force, Changchun 130022,China)

Abstract: To use RSA coprocessor as the kernel component of embedded VPN server on RSA operation, the power supply system and hardware interface F2812 between the co-processor and the main controller has been designed in this article. The software has been achieved which correlated with the hardware interface. By system debugging and testing, the arithmetic speed of RSA operation has reached the anticipated performance, and can satisfy the request of embedded VPN server.

Key words: RSA; RSA coprocessor; F2812; interface

随着互联网技术的日益普及，网络数据传输的安全问题日益显露出来，如何保障网络传送各种信息的安全是人们关注的热点。在此背景下产生的虚拟专用网(VPN)技术得到了重视，VPN 技术基于安全协议(IPSec 协议)，通过隧道加密技术，采用策略管理组建虚拟专用网，实现数据传输的完整性、机密性[1-2]。

在 IPSec VPN 设计实现时，需要采用身份认证及数字签名技术来保证信息的不可否认性。RSA 是公认的最优秀的公钥密码体制之一，是实现身份认证及数字签名核心技术之一，而 RSA 的核心算法是一种模指数函数运算，运算过程中需要进行大量的大数模幂乘运算，导致在每次运算都要消耗大量的时间[2]。因此，在进行嵌入式 IPSec VPN 产品设计、特别是嵌入式 VPN 服务器设计时，如何提高 RSA 算法运算速度是提高产品性能的关键技术。嵌入式 VPN 服务器设计采用 RSA 协处理器作为 RSA 运算核心部件及其与主处理器 F2812 接口的软硬件设计可以提高运算速度，满足服务器要求。

1 RSA 协处理器 SSX26 简介

SSX26 是由北京芯光天地集成电路设计有限公司自主设计开发的一款具有完全自主知识产权的专用集成电路，主要功能是实现大数模幂/模乘的加速运算，可作为 RSA、DSA、ECC 等公钥密码算法的协处理器[3]。其具有如下的特点：内核电压为1.8 V，I/O 电压为 3.3 V；外部时钟频率范围为 5~10 MHz，内核工作频率范围为 40~100 MHz；硬件支持模长最高为 1 024 bit 的模幂运算，对于模长和幂长均为 1 024 bit 的模幂运算速度大于 1 400 次；硬件支持模乘运算。其引脚定义如表 1 所示，内部寄存器定义如表 2 所示。

表 1 SSX26 引脚定义

管脚名称	管脚说明
READY	芯片状态指示,高电平有效
BUSY	芯片忙标志信号,高电平有效
PErr	输入参数错误,高电平有效
nFLG	数据状态指示信号,低电平有效
PLL_RESET	PLL 复位
nRESET	芯片异步复位信号,低电平有效
nCS	片选信号,低电平有效
RnW	读写选择信号
nAS	地址写入选通信号,低电平有效
nDS	数据读写选通信号,低电平有效
CLK_OUT	内部工作频率的 2 分频参考输出
CLK	片外时钟输入
PLL_M1~0	PLL 倍频选择
D0~D15	数据/地址复用双向总线
VDD_IO	芯片 I/O 电源(+3.3 V)
VSS_IO	芯片 I/O 地
VDD_CORE	芯片内核电源(+1.8 V)
VSS_CORE	芯片内核地
VDDA1.8V	芯片 PLL+1.8 V 模拟电源
VDDA3.3V	芯片 PLL+3.3 V 模拟电源
VSSA	芯片 PLL 地

注意:数据/地址复用总线没有高阻态。

表 2 SSX26 寄存器定义

名称	地址	宽度	读写
地址寄存器(AR)		3	只写
输入寄存器(DIR)	0	1 024	只写
输出寄存器(DOR)	1	1 024	只读
命令寄存器(CMR)	2	8	读写
模式寄存器(MDR)	3	1	读写
状态字寄存器(SWR)	4	8	只读

2 SSX26 与 F2812 硬件接口设计实现

2.1 接口时序分析

从表 1 可知,SSX26 与外部控制器是采用并行总线连接的方式,如果将 SSX26 直接接在 F2812 的外部总线上,则需要对 SSX26 的数据读写时序与 F2812 总线的读写时序进行分析比较。图 1 所示为 SSX26 的写时序图,图 2 所示为 F2812 的写时序图[4]。

从图 1 中可知,SSX26 的写信号 RnW、数据选通 nDS 及数据 D[0:15]需要在片选信号 nCS 之前至少需要一个内部时钟周期的建立时间。虽然 F2812 外部总线相对于写信号 nXWE 其前导时间、有效时间及保持时间可以通过软件配置,但从图 2 可知,其读写信号 XR/W#、地址信号 XA[0:18]及片选信号 nXZCS01 几乎同时在nXWE 信号之前输出有效,而数据信号 XD[0:15]在 nXWE 信号之

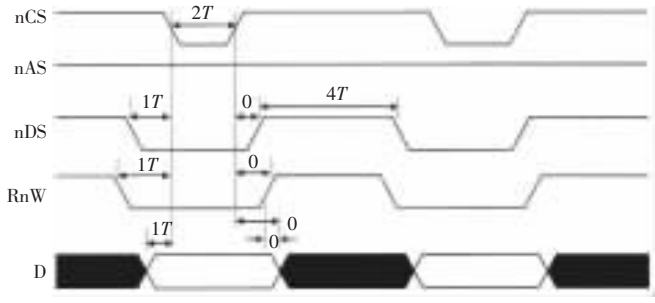

图 1 SSX26 写数据时序

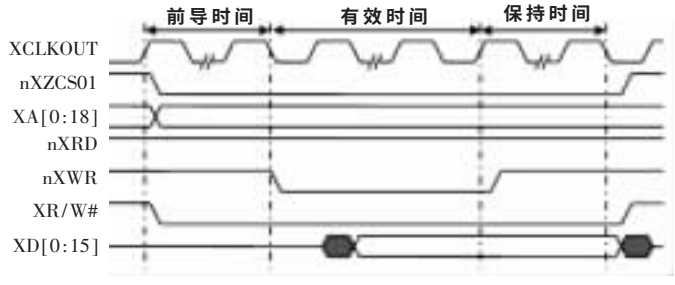

图 2 F2812 写数据时序图

后才有效。从上面时序分析可知,F2812 总线的时序关系显然不符合 SSX26 的时序要求,因此 SSX26 不能直接接在 F2812 的外部总线上。为解决其时序问题,一种方案是采用 FPGA 或 CPLD 进行时序转换,但这会导致硬件设计比较复杂,同时增加软件工作量;另一种方案是采用 F2812 的 I/O 口来进行连接,由于 F2812 具有多达 56 个通用 I/O 口,且输出频率可高达 20 MHz,因此采用此方案可以有效地解决时序问题[4]。

2.2 接口硬件设计

SSX26 与 F2812 接口连接及 SSX26 的外围电路示意图如图 3 所示,图中未给出 F2812 的外围电路。数据/地址复用双向总线 D[15:0]接在 F2812 的 GPB[15:0];芯片的控制引脚及状态引脚接到 F2812 的 GPF [3:0] 及 GPF [13:8]。外部输入时钟为 5 MHz,时钟的电源引脚通过一个磁珠 BLM21PG221 接到 V_{CC}3.3 V,另外接 1 个 0.1 μF 的陶瓷电容去藕;倍频选择引脚通过电阻接到 V_{CC} 3.3 V,设置的倍频关系为 20 倍频,因此内部工作时钟为 100 MHz。芯

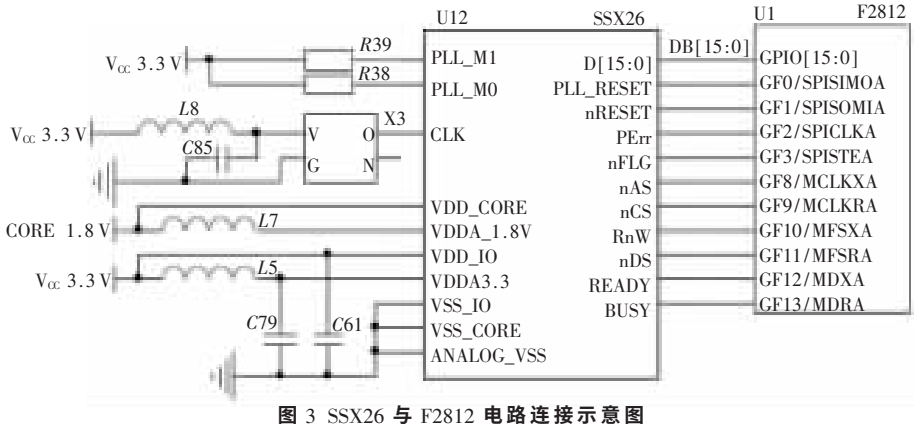

图 3 SSX26 与 F2812 电路连接示意图

片 PLL+1.8V 模拟电源及芯片 PLL+3.3 V 模拟电源分别通过磁珠接到内核电源 CORE1.8 V 及 I/O 电源 V_{CC} 3.3 V，另外接一个 0.1 μF 的陶瓷电容去藕，以达到更好的信号质量。

2.3 SSX26 的电源系统设计

F2812 的供电电压分为内核电压+1.8 V 和 I/O 电压+3.3V，且其上电有时序要求，因此采用的电源管理芯片为 TPS767HD301，内有两路输出，一路为+3.3 V，另一路通过外部电阻调节输出+1.8V，其输出的电流都为1 A。

SSX26 的供电电压也分为内核电压+1.8V 和 I/O 电压+3.3 V，I/O 电压+3.3 V 可以与 F2812 共用。由于 SSX26 在运算时具有较大的内核功耗，在 100 MHz 内核时钟时，1.8 V 峰值电流可达 1A，而 TPS767HD301 输出的电流为 1A，显然不能满足其要求，因此需要设计单独的内核供电电路，如图 4 所示。电源管理芯片采用 Micrel 公司 MIC29302BU，输出电流可高达 3 A，输出电压可以通过外部电阻进行设定，其输出电压计算公式为 $V_{OUT}=1.240(1+R13/R14)=1.240(1+14.7\ k\Omega/33\ k\Omega)=1.79$ V。

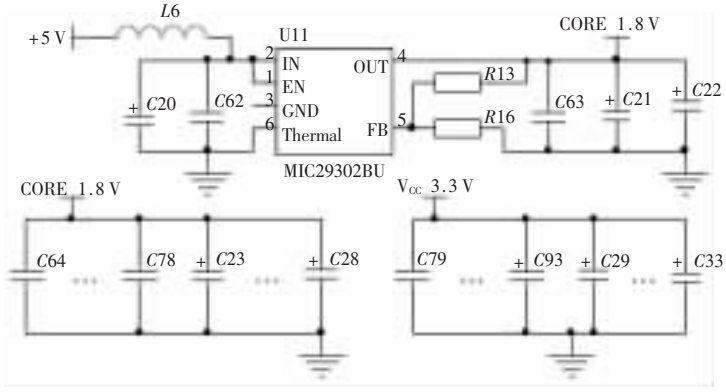

图 4 SSX26 内核供电电路及电源去藕

SSX26 内部工作时钟高达 100 MHz，且在运算时其峰值电流高达 1 A。为防止瞬间的大电流引起电压跌落，放置了 2 个 220 μF 的电解电容。为了保证电源系统的稳定，放置了较多的去藕电容，在进行 PCB 设计时，这些去藕电容都在靠近芯片电源引脚放置。

3 软件模块设计实现

软件开发在 TI 公司集成化 DSP 开发工具 CCS3.3 环境下完成，在 TI 公司提供的程序开发例程 spra958g.zip 下进行编程工作。软件设计采用分层化、模块化的设计思想，可分为硬件相关层 、功能模块层及应用层。硬件相关层包括 F2812 相关 I/O 设置、复位、SSX26 写地址操作、SSX26 写数据操作及 SSX26 读数据操作；功能模块层包括载入模幂对、启动模幂运算及启动模乘运算。

3.1 F2812 相关 I/O 设置

F2812 的 I/O 口具有多个功能，在本设计中所使用的 I/O 口都作为通用 I/O 口来使用，根据信号的要求设置 I/O 口的方向，GPF0~1、GPF8~11 设置为输出，其他设置为输入；GPB 口初始状态设置为输入，在需要输出时变更其方向。

3.2 总线操作子程序

由于 SSX26 数据、控制及状态总线通过通用 I/O 口与 F2812 进行连接，因此需要通过软件按照总线控制时序要求来完成总线的操作。总线操作分为写地址操作、写数据操作及读数据操作。下面按照图 1 的写时序给出参考代码。

```
void SSX26_WR_ONE_Data(Uint16 Data)
{
    SSX26_RnW_L();
    SSX26_nDS_L();
    GpioDataRegs.GPBDAT.all=Data;
    SSX26_nCS_L();
    asm(" RPT #3 || NOP");
    SSX26_BUS_H();
}
```

3.3 复位

SSX26 在进行操作前需要进行可靠的复位，其复位时序如图 5 所示。复位完成后，同时进行模式配置，SSX26 总线宽度可以通过模式寄存器配置成 8 bits 或 16 bit 方式，本设计中配置成 16 bit 方式。

```
void SSX26_Reset(void)
```

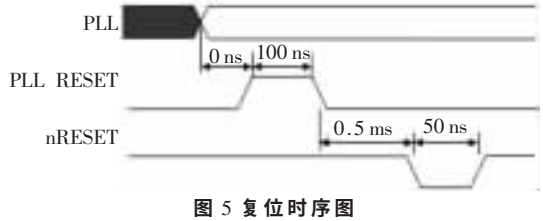

图 5 复位时序图

```
{
    GpioDataRegs.GPFSET.bit.GPIOF0=1;
    asm(" RPT #50 || NOP");
    GpioDataRegs.GPFCLEAR.bit.GPIOF0=1;
    DelayUs(2000);
    GpioDataRegs.GPFCLEAR.bit.GPIOF1=1;
    DelayUs(20000);
    GpioDataRegs.GPFSET.bit.GPIOF1=1;
    DelayUs(100);
    SSX26_WR_Addr(SSX26_MDR); X26_WR_ONE_Data
        (SSX26_MOD_16);
}
```

3.4 功能模块子程序设计

SSX26 可以完成模幂运算和模乘运算，如下所示。

$R1=A^E \bmod M$，$R2=A * B \bmod M$

执行一次完整的模幂运算或模乘运算，需要分 2 个步骤进行操作，载入模幂对和启动模幂运算(或启动模乘运算)，每个操作都要按照一定顺序进行，因此需要有

3 个功能模块与其相对应,分别为载入模幂对、启动模幂运算及启动模乘运算。载入模幂对的处理流程如图 6 所示。

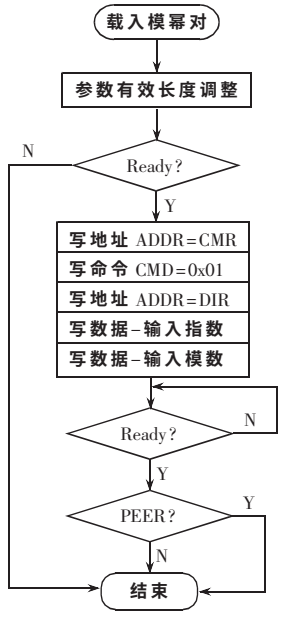

图 6 载入模幂对处理流程图

本文介绍的接口设计方法,经测试,符合实际的要求,能够实现预期的功能,其 RSA 运算速度可以达到 1100 次/s,可以满足高速 RSA 运算的需求。采用该芯片作为 RSA 协处理器所设计的接口系统,可以广泛应用于嵌入式 VPN 网关及嵌入式 VPN 服务器中。

参考文献

[1] 于晓,高安全 VPN 的嵌入式 PPPoE 接入研究[J].光学精密工程,2008,16(11):2252-2256.

[2] STALLINGS W 著.密码编码学与网络安全:原理与实践(第二版)[M].杨明等译.北京:电子工业出版社,2001.

[3] 北京芯光天地集成电路设计有限公司.SSX26 用户手册 v2.2[M],2005.

[4] Texas Instruments. TMS320F2812 digital signal processors data manual[M]. July 2007.

(收稿日期:2009-11-11)

作者简介:

章明朝,男,1982 年生,在读博士,主要研究方向:光电探测,信息安全,嵌入式 DSP 系统设计。