文章编号:1005-0523(2018)05-0111-06

基于FPGA的SMS4算法实现及在线验证

张利华[1],吴 松[2],蒋腾飞[2],姜攀攀[2]

(华东交通大学 1. 软件学院;2. 电气与自动化工程学院,江西 南昌 330013)

摘要:针对软件实现加解密算法占用主机系统资源较多、数据处理复杂、加密速度较慢的不足,提出一种硬件实现算法加密的方法。硬件加密具有成本低、加密速度快等优势,可以减轻CPU的负担以及提高服务性能。利用Vivado 2016.3开发工具和Verilog HDL硬件描述语言完成对SMS4算法的设计输入、功能测试、时序仿真,并封装为独立的IP核。在ZYNQ芯片上设计测试系统,通过ARM处理器调用自定义IP,完成算法在实际应用中的验证。结果表明:软件仿真验证,设计的算法功能正确,性能良好。在硬件实际测试过程中,算法运行正确,其工作最大频率为200 MHz,数据吞吐率达到800 Mbps。

关键词:SMS4;硬件加密;ZYNQ;FPGA

中图分类号:TP307 **文献标志码**:A

分组密码算法是对称密码算法中的一种,效率高、易于实现是其显著的优点,在各个领域应用非常广泛。SMS4算法在2016年8月正式发布成为国家标准,它是国内首个用于无线局域网产品的商用密码算法[1]。伴随着物联网的快速发展,分组密码算法在智能终端、无线传感网络以及射频识别等资源有限的设备中应用日益明显。因而对以SMS4算法为代表的轻量级算法的实现的研究具有重要的实际意义[2]。

当前实现算法主要是通过硬件和软件两种方式实现,软件实现的运行方式是顺序执行,它不仅限制了算法运行速度的提升空间,而且功耗和安全性也制约了它的应用领域;而使用硬件FPGA(可编程逻辑器件)实现采用并行处理的方式,既能够提高加密的速度,也便于设备小型化和提高安全性[3-5]。为了加快算法的执行速度,很多学者在算法的实现结构以及执行方式上做了很多研究。文献[6]提出一种单轮循环结构的SMS4方案,减少了硬件资源的利用,提高了算法的加解密速度。文献[7]通过对硬件实现SMS4算法加快运行速度,但仅限于软件仿真,在硬件平台上验证不明确。文献[8]提出利用FPGA实现SMS4加解密算法,实现最大工作频率139 MHz时,数据吞吐率达到539 Mbps。文献[9]提出利用迭代体系结构以及加密和密钥扩展的相似性来缩小面积,但以牺牲吞吐量缩小占用面积。文献[10]中在实现SMS4算法时,采用每轮加密前都需要先计算子密钥的方式进行工作,线性变换的单元没有实现复用,增加了硬件的开销。

为了实现SMS4算法更快的加解密速度和更高的数据吞吐率,同时能够在实际硬件平台上验证算法的正确性。提出一种在FPGA中采用循环结构完成密钥扩展以及加解密算法的硬件实现方法,提高算法的运算速度。通过软件仿真验证了算法的正确性,并将完成的SMS4算法IP核封装,通过软件调用在实际硬件ZYNQ器件上测试了算法的正确性,数据吞吐率以及最大工作频率有较好的提高。

1 SMS4算法

SMS4分组算法是一种对称密码,属于典型的Feistel结构,分组长度和密钥长度均为128 bit,密钥算法和密钥扩展算法采用32轮非线性迭代结构。

收稿日期:2018-04-10

作者简介:张利华(1972—),男,副教授,博士,主要研究方向为无线与移动通信网络安全,工业控制网络安全。

1.1 相关参量表示

字与字节：用 Z^e 表示 e 比特的元素集合，Z^{32} 中元素为字，Z^8 中元素为字节。运算：⊕表示32位异或运算；<<<i 表示循环左移 i 位。S盒是一个8比特输入8比特输出的置换，记作 sbox(·)。

SMS4密码算法加密密钥长度为128 bit，表示为 $MK=(MK_0,MK_1,MK_2,MK_3)$，其中 $MK_i(i=0,1,\cdots,31)$ 为32 bit。轮密钥表示为 $(rk_0,rk_1,\cdots,rk_{31})$，其中 $rk_i(i=0,1,\cdots,31)$ 为32bit。轮密钥由加密密钥生成。FK 为系统参数。$CK=(CK_0,CK_1,\cdots,CK_{31})$ 为固定参数，用于密钥扩展算法，其中 $FK_i(i=0,1,\cdots,31)$，$CK_i(i=0,1,\cdots,31)$ 均为32 bit。

1.2 SMS4加解密算法

SMS4加密过程经过32次迭代运算和1次反序变换R组成。明文 X 和密文 Y 各分为4组，明文 $X=(X_0,X_1,X_2,X_3)$，密文 $Y=(Y_0,Y_1,Y_2,Y_3)$。加密算法变换公式如式(1)所示，其中 $i=0,1,\cdots,31$。

$$X_{i+4}=X_i\oplus T(X_{i+1}\oplus X_{i+2}\oplus X_{i+3}\oplus rk_i)\qquad (Y_0,Y_1,Y_2,Y_3)=(X_{35},X_{34},X_{33},X_{32}) \tag{1}$$

其中 $T(\cdot)=L(\tau(\cdot))$。τ 由4个并行的 S 盒构成，输入明文 $A=(a_0,a_1,a_2,a_3)$，输出密文 $B=(b_0,b_1,b_2,b_3)$，则 B 计算如式(2)所示

$$B=\tau(A)=(\text{sbox}(a_0),\text{sbox}(a_1),\text{sbox}(a_2),\text{sbox}(a_3)) \tag{2}$$

线性变换 $L(B)$，如式(3)所示

$$L(B)=B\oplus(B<<<2)\oplus(B<<<10)\oplus(B<<<18)\oplus(B<<<24) \tag{3}$$

1.3 密钥扩展算法

轮密钥由加密密钥通过密钥扩展算法生成。对应的计算公式如式(4)，式(5)所示

$$rk_i=K_{i+4}=K_i\oplus T'(K_{i+1}\oplus K_{i+2}\oplus K_{i+3}\oplus K_i) \tag{4}$$

$$K_0=MK_0\oplus FK_0;K_1=MK_1\oplus FK_1;K_2=MK_2\oplus FK_2;K_3=MK_3\oplus FK_3 \tag{5}$$

其中：T' 表示合成置换 T 的线性变换 L 替换成 L'：$L'(B)=B\oplus(B<<<13)\oplus(B<<<23)$；$K_i$ 为轮密钥生成过程中的中间变量；固定参数 CK，系统参数 CK 根据《无线局域网产品使用的SMS4密码算法》来取值[11]。

2 SMS4算法硬件实现及IP封装

算法SMS4中固定参数 CK、FK 存储空间为32×32 bit，在使用硬件描述语言设计的时候，将参数固定存储在FPGA的RAM中，不占用逻辑资源，采用LUT方式求值增加运算速度。在FPGA中采用循环结构实现SMS4算法。扩展密钥电路以及轮函数电路循环使用计算得到加解密的数据。SMS4算法在文中采用循环结构实现密钥扩展以及加解密算法，结构如图1所示。

2.1 密钥扩展

密钥扩展运算在设计过程中，采用状态机方式进行运算，包括4个状态Idle，Setkey1，Setkey2，Ready。空闲状态为Idle，当检查到新数据信号时候，跳转到Setkey1状态，进行公式(5)运算，计算 $K_i(i=1,2,3,4)$，然后转移到Setkey2状态按照公式(4)计算每一轮的轮密钥 rk_i，直到计算32次跳转到Ready状态，此时轮密钥准备完成，密钥扩展进入Idle状态。密钥扩展状态转移图如图2所示。其中，new_key表示密钥更新状态信号、key_cnt表示计算轮密钥计数信号、data_ready表示允许修改密钥信号。

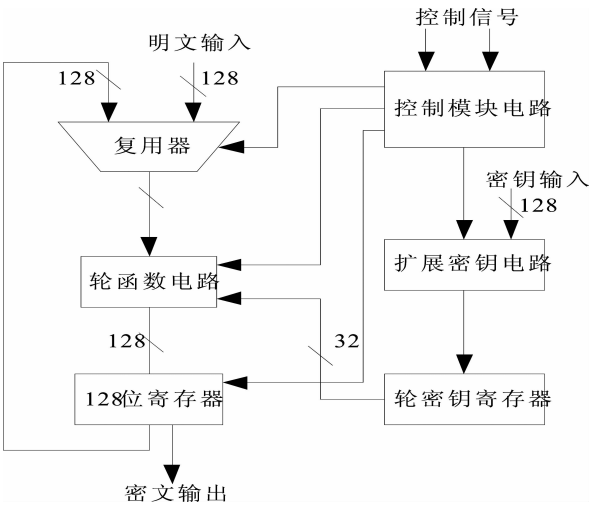

图1 SMS4在FPGA中的循环结构

Fig.1 The circular structure of SMS4 in FPGA

2.2 加密

在加密过程中，同样采用状态机方法设计，

包括 4 个状态 Idle,ECB1,ECB2,READY 状态。当检查到新的数据状态状态进入 ECB1 状态,对输入的 128 位数据进行分组。当扩展密钥 rk_i 准备就绪,进入状态 ECB2,按照式(1)~式(4)进行每一轮轮函数值的计算。直到计算 32 次之后,进入 Ready 状态。最后通过在 Ready 状态进行一次逆序变换 R,得到加密后的数据。加密流程状态转移图如图 3 所示, 其中,new_data 表示待操作数据更新信号,key_ready 表示轮密钥准备就绪信号,ECB_cnt 表示加密轮数计数信号。解密过程类似加密。

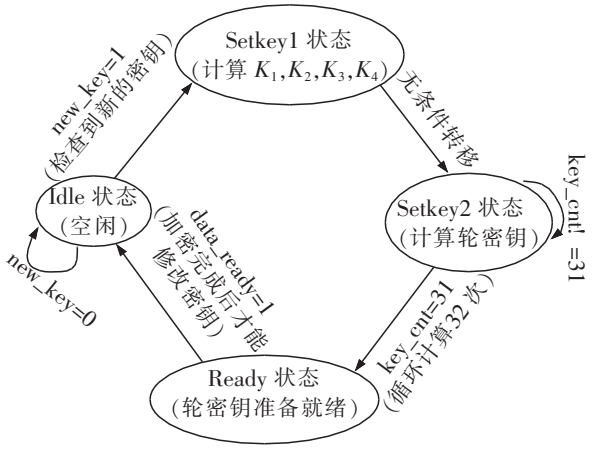

图 2　密钥扩展状态转移图

Fig.2　Transfer diagram of key extended state

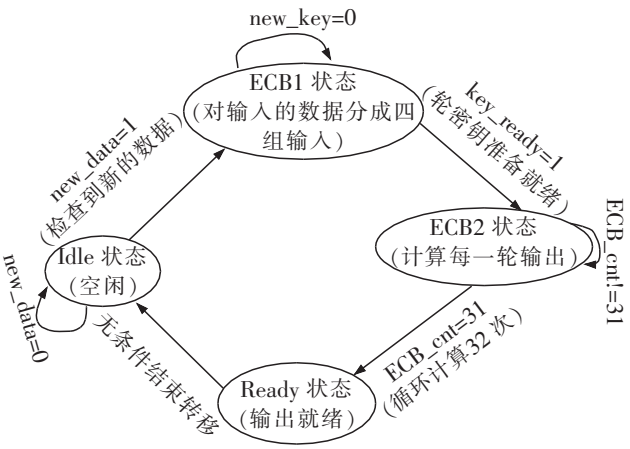

图 3　加密流程状态转移图

Fig.3　State transfer diagram of encryption process

2.3　软件仿真验证

采用 Verilog HDL 硬件描述语言编写测试程序 Testbench 文件,并在仿真软件 modelsim 10.0c 集成环境中进行功能仿真。加密运算仿真波形如图 4 所示。初始密钥为:AD92EF2191AE2C4D23DA8167FA45C593;待加密的明文序列为:ABEF12EDAFC2B3163719AD23AE346712;

经过 32 轮加密运算得到的密文为:C8D464FB462B65047D713C9756B10EA7。

在加密运算过程中,输入待加密数据 data_i、密钥 key,通过密钥扩展函数生成轮密钥,当 key_ready_o 变为高电平后,进行 32 次迭代运算和 1 次反序变换得到输出数据,并且操作完成后信号 data_ready_o 变为高电平,此时加密完成。同理,解密运算和加密操作运算结构相同,只是轮密钥使用顺序相反,可以软件验证解密算法正确。

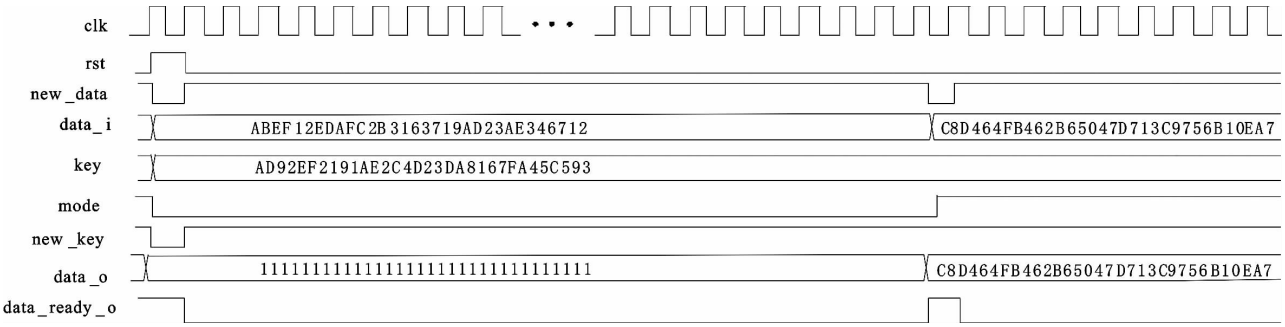

图 4　SMS4 加密运算仿真波形

Fig.4　Simulation waveform of SMS4 encryption operation

2.4　IP 核封装

生成 SMS4 算法 IP 核如图 5 所示。生成的 SMS4 算法集成 IP 核,各引脚功能如表 1 所示。

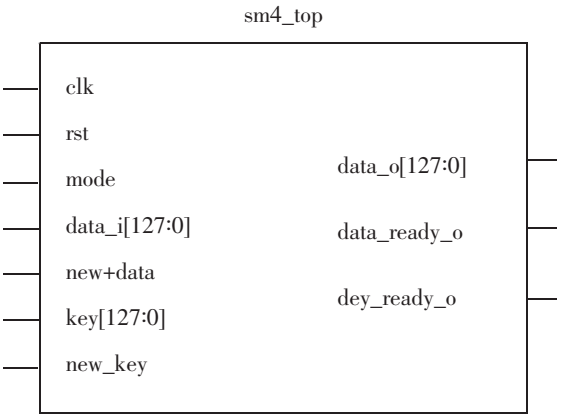

图5 SMS4算法IP核
Fig.5 SMS4 algorithm IP kernel

表1 SMS4算法引脚功能图
Tab.1 SMS4 algorithm pin function diagram

引脚	功能
rst,mode	rst:高电平复位
mode	0:加密;1:解密
new_key	检测是否有新的密钥,上升沿
new_data	检测是否有新的数据,上升沿
data_o	输出数据(128位)
data_ready_o	输出数据准备好时,输出高电平
key_ready_o	扩展密钥准备好,输出高电平

3 SMS4算法在线平台验证

SMS4算法在可扩展处理平台ZYNQ的可编程逻辑PL实现,与PS(processing system)通过AXI总线进行数据交互[12]。SMS4算法在PL上实现,达到硬件加速算法处理的目的。PS部分为处理器系统,内部包含两个Cortex A9的ARM和总线接口。PS和PL通过AXI总线进行数据的交互。用户通过ARM控制器将需要加密或解密的数据写入内存,DMA控制器将内存中的数据以AXI Stream的方式发送给SMS4算法IP。经算法IP处理后,将数据存储到内存中。搭建的系统工程,系统工程主要包括3个模块:PS模块(processing_system_0)、DMA控制器(axi_sms4_in_0(输入缓冲)和axi_sms4_out_0(输出缓冲))及sms4算法模块。系统结构图如图6所示。

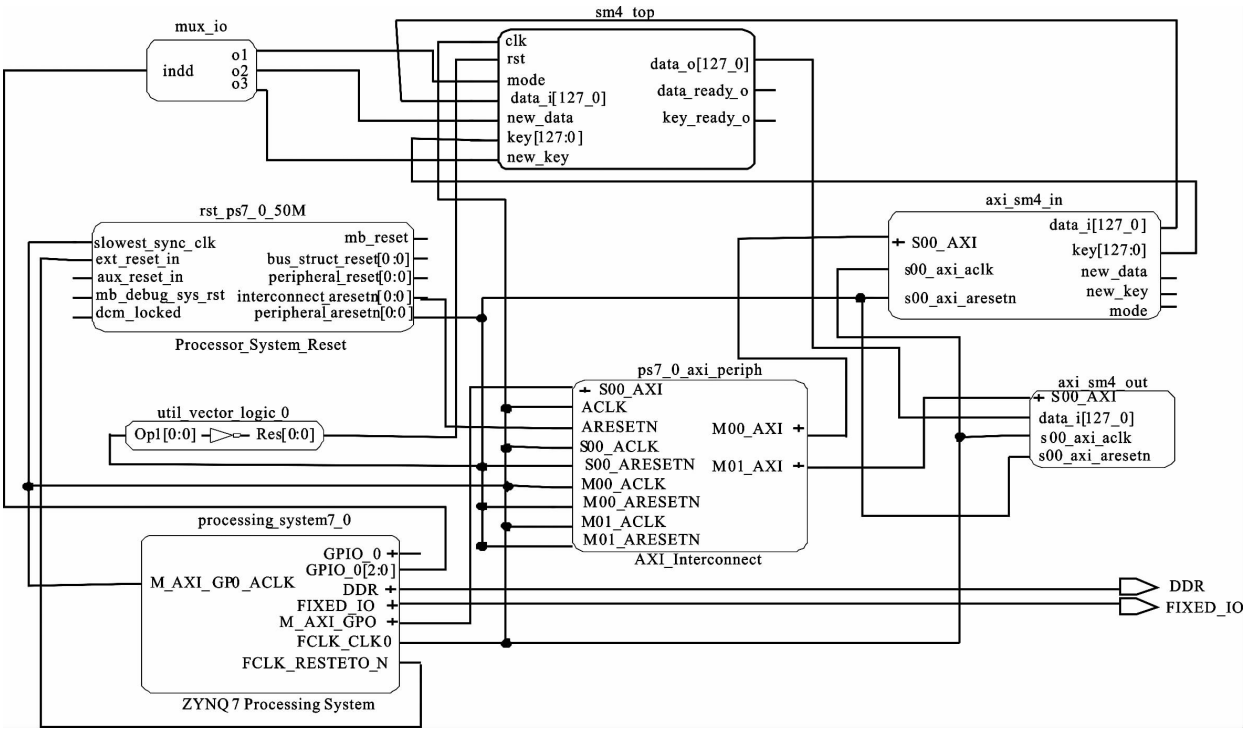

图6 系统工程图
Fig.6 System engineering drawings

硬件系统工作流程包括主要包括硬件平台的初始化、SMS4 算法加解密模式选择、写入密钥以及待处理数据、加密\解密、等待加\解密完成以及加\解密后数据存储显示等部分组成。通过软件完成相关操作程序设计，并将系统工程编译并下载到硬件平台上中，通过串口观察处理结果。为了能够在硬件平台正确测试 SMS4 算法实现的正确可靠，采用和仿真程序测试不一样的测试数据。串口反馈结果如表 2 所示。从表 2 可以看出，通过 ARM 核向 SMS4 算法 IP 核写入数据，能够正确得到加密和解密的结果。

表 2　串口反馈测试结果

Tab.2　Test results of serial port feedback

指标	数据 1(加密)	数据 2(解密)
待处理数据	ABEF12EDAFC2B3163719AD23AE346712	C8D464FB462B65047D713C9756B10EA7
密钥	AD92EF2191AE2C4D23DA8167FA45C593	AD92EF2191AE2C4D23DA8167FA45C593
处理结果	C8D464FB462B65047D713C9756B10EA7	ABEF12EDAFC2B3163719AD23AE346712

4　算法性能分析

在 ZYNQ 7020 型号 FPGA 中实现了 SMS4 算法，综合、布线资源消耗情况如表 3 所示。在 ZYNQ 7020 型号可编程逻辑器件中资源使用情况：查找表使用 3 703 个，触发器使用 4 520 个以及 1 个缓存器，使用率都低于 5%。SMS4 算法性能指标对比如表 4 所示。

表 2　综合后器件资源消耗使用情况

Tab.2　Utilization of device resource consumption

资源	使用个数/个	使用率/%
查找表(LUT)	3 703	2.77
触发器(FF)	4 520	1.69
缓存器	1	3.13

表 3　SMS4 算法性能对比

Tab.3　SMS4 algorithm performance comparison

指标	文献[7]	文献[8]	本文
最大工作频率/MHz	189	139	200
数据吞吐率/Mbps	721	539	800

文献[7]实现的 SMS4 算法最大工作频率 189 MHz，数据吞吐率达到 721 Mbps，而文献[8]中实现算法的数据吞吐率为 539 Mbps，最大工作频率为 139 MHz。在本文中，器件工作的最大工作频率为 200 MHz，数据吞吐率可达到 800 Mbps。结果表明，占用的硬件资源较少。设计的算法运算速度整体提高，数据吞吐量增加。

5　结论

通过分析 SMS4 密码算法加密和解密的流程，本文提出了一种在 FPGA 中采用循环结构完成密钥扩展以及加解密算法的硬件实现方法，并利用 XINLINX 公司的集成开发工具 Vivado 及 VHDL 语言完成 SMS4 算法硬件描述，并将其封装成 IP 核供给软件调用测试。设计了密码算法在线验证平台，算法模块封装成独立模块，通过改变算法 IP 可以验证其他算法的正确性。结果表明：通过软件仿真验证，设计的算法功能正确，性能良好。在硬件实际测试过程中，算法运行正确，其工作最大频率达到 200 MHz，数据吞吐率达到 800 Mbps，该算法在 ZYNQ 7020 芯片上占用的资源使用率低于 5%。

参考文献：

[1] 吕述望，苏波展，王鹏，等. SM4 分组密码算法综述[J]. 信息安全研究，2016，2(11)：995-1007.

[2] 张利华，沈友进. 基于 ECC 和指纹 USBKey 的身份认证协议[J]. 华东交通大学学报，2014，31(2)：95-98.

[3] LEI C，BING SUN. Revised cryptanalysis for SMS4[J]. Science China Information Sciences，2017，60(12)：122101.

[4] 程海，丁群，杜辉，等. 基于 FPGA 实现的 SMS4 算法研究[J]. 仪器仪表学报，2011，32(12)：2845-2850.

[5] 朱坤崧,戴紫彬,张立朝,等. 面向物联网的SM4算法轻量级实现[J]. 电子技术应用,2016,42(12):27-30.
[6] 蔡玉莹,曲英杰. 基于单轮循环结构的SMS4加密芯片的研究与设计[J]. 电子设计工程,2016,24(22):39-42.
[7] 王艳红. 硬件实现SMS4密码算法的研究[J]. 自动化与仪器仪表,2015(6):46-47.
[8] GAO X,LU E,XIAN L,et al. FPGA implementation of the SMS4 block cipher in the chinese WAPI standard[C]//International Conference on Embedded Software and Systems Symposia,2008. Icess Symposia. IEEE,2008:104-106.
[9] WANG HUSEN. High performance FPGA Implementation for SMS4(A) Intelligent information technology application association. high performance networking. computing and communication systems(ICHCC-ICTMF2011CCIS0163)[C]//Intelligent Information Technology Application Association,2011:7.
[10] 王晨光,乔树山,黑勇. 分组密码算法SM4的低复杂度实现[J]. 计算机工程,2013,39(7):177-180.
[11] 国家密码管理局.无线局域网产品用的SMS4密码算法[EB/OL]. [2018-03-10]. http://www.oscca.gov.cn/sca/c100061/201611/1002423/files/330480f731f64e1ea75138211ea0dc27.pdf.
[12] 钟汉华,陈剑云,周欢. 基于Zynq的RTU遥测量计算与误差补偿实现[J]. 华东交通大学学报,2017,34(4):91-96.

Implementation and Online Verification of SMS4 Algorithm Based on FPGA

Zhang Lihua[1], Wu Song[2], Jiang Tengfei[2] , Jiang Panpan[2]

(1. School of Software, East China Jiaotong University, Nanchang 330013, China;
2. School of Electrical and Automation Engineering, East China Jiaotong University, Nanchang 330000, China)

Abstract: Aiming at the problems of software encryption including the excessive use of host system resources, complex data processing, and slow encryption speed, a method of hardware encryption was proposed. Hardware encryption has the advantages of low cost and fast encryption speed, which can reduce the burden of CPU and improve service performance. By using Vivado 2016.3 development tools and Verilog HDL hardware description language, this paper completed the SMS4 algorithm design input, functional testing and timing simulation, and encapsulated them into independent IP core. The testing system was designed on ZYNQ chip, the user-defined IP was called through ARM processor and the verification of the algorithm in actual application was finished. The research results show that the designed algorithm has the correct function and good performance. In the actual hardware test process, the algorithm is running correctly with the maximum working frequency of 200 MHz and the data throughput rate of 800 Mbps.

Key words: SMS4; hardware encryption; ZYNQ; FPGA