SM3 算法硬件实现研究与应用

周 威 王 博 张卫东
(西安电子科技大学 西安 710071)

摘 要：伴随现阶段运用 SM3 密码杂凑算法的应用不断增加，执行速度和实用效率越来越无法满足用户大数据量实时处理的需求。为了进一步满足大数据时代的安全需求以及提高该算法的硬件效率，本文结合 SM3 算法特性利用硬件描述语言 Verilog 对其进行高效的 FPGA 硬件设计，并利用 Xilinx 公司软件开发套件进行综合仿真验证，设计相应的接口与驱动软件。最后在 ARM 和 FPGA 联合处理平台利用我们设计的 SM3 完整性认证 IP 模块，完成对实时视频完整性验证的实际测试。与纯软件实现相同功能相比，时钟仅为 100 MHz 的情况下，吞吐量提升了 2 倍以上，大大提升了 SM3 算法的执行效率，解决了现阶段实时视频认证的难题。

关键词：SM3 ；FPGA；Verilog；认证；视频
中图分类号：TP309.7 **文献标识码**：A **国家标准学科分类代码**：520.1060

Research and application of SM3 hardware implementation

Zhou Wei Wang Bo Zhang Weidong
(Xidian University, Xi'an 710071, China)

Abstract: With the increasing of SM3 password hash algorithm used at present stage, the execution speed and practical efficiency increasingly unable to meet the needs of processing large amount of data real-time of users. In order to further meet security needs of the era of big data, and improve the hardware efficiency of the SM3 algorithm, considering the feature of SM3 algorithm for efficient, we use hardware description language Verilog design FPGA hardware and integrated simulation using Xilinx software which test the design. Finally, we use the SM3 module in video data authentication on ARM and FPGA platform. Compared with the pure software which realize the same function, when clock is 100 MHz, throughput is increased more than 2 times, the execution efficiency of SM3 algorithm is greatly improved and the problem of real-time video authentication at the present stage is solved.

Keywords: SM3; FPGA; Verilog; Authentication; Video

1 引 言

SM3 杂凑算法由我国自主研制，已成为我国商业密码的行业标准之一[1]。此杂凑算法可以用于数字签名、消息认证码的生成与校验，以及随机数的产生，适用各种应用与产品的安全需求，在我国商业中有着广泛的应用。但现阶段针对 SM3 算法的实现多为软件，但由于 SM3 迭代轮数多，逻辑运算多，软件的处理速度已经越来越无法满足现阶段大数据实时处理的需求。效率和速度急需进一步提高。而且现阶段相关研究只是对 SM3 算法本身进行了简单的优化实现，应用性不强，工作十分有限。文献[2]仅将压缩函数部分进行了并行优化，效率提升不足；文献[3]虽然仔细分析了硬件实现该算法的延迟特点进行了优化，但受器件的局限性，实现复杂，应用价值不大。并且现阶段有关杂凑算法实现的相关文献中，均未考虑对应的总线与接口的设计，使其应用范围和最终执行效率大打折扣。所以本文在深入分析 SM3 算法和其他杂凑算法的基础[4-6]上，结合 FPGA 高速并行等特点，利用 Verilog 硬件描述语言对其进行高效硬件设计实现，对结果进行验证与性能分析，结果表明，该方法在芯片资源占用仅为 1743 个 Slice 的主频 167 Hz 情况下达到了 1.35 Gbps的吞吐量，与目前已知最优实现方法在相同时钟频率相比[3]，芯片资源占用较少，单位面积吞吐量提高 12%左右，可以在减少芯片硬件资源占用的同时快速高效地实现 SM3 算法。并且参考国内 CPU 与 FPGA 接口设计后，设计了高效的专用总结接口模块与参考驱动设计，与现有设计相比大大提高了接口

收稿日期：2015-03

CPU 的工作效率与读写效率，保证了 SM3 模块在实际应用中的高吞吐率。最后为了实际验证我们设计的 SM3 算法 IP 模块与相应接口的效率，我们将此设计实际运用于实时视频的认证中，1 秒可认证 30 帧以上的视频数据。可以很好地解决现阶段无压缩编码实时视频认证的难题。满足了实时视频加认证的需求。同时解决了大数据无法实时认证只能后期验证的缺陷，有着良好的应用前景与市场空间。

2　SM3 算法流程简述

SM3 密码杂凑算法是一种基于分组迭代的杂凑算法，该算法采用双字结合的消息字处理方式，运用不同的群运算混合，实现了消息在局部范围内快速扩散和混乱，防止了比特追踪和其他已知分析方法的攻击。SM3 杂凑算法可以通过填充和迭代压缩对任何小于 2^{64} bit 的数据，生成长度为 256 bit 的杂凑值。算法流程主要包括对消息的预处理与压缩计算 Hash 值，下做简要介绍。

假设消息 m 的长度为 l 比特。第一步将比特“1”添加到消息的末尾，再添加 k 个“0”，使其满足 $l+1+k\equiv 448 \bmod 512$ 。再添加一个 64 位二进制比特串，使填充后的消息 m' 的比特长度为 512 的倍数。再将填充后的消息 m' 按 512 比特进行分组将每个消息分组扩展生成 132 个字 W0，W1，…，W67，W0′，W1′，…，W63′，用于压缩函数。

压缩函数包含 64 轮，每轮包括 12 步运算，64 轮循环计算结束后，再将计算结果与输入到本轮计算的初始数据进行异或运算，得到本次 Hash 值输出 H_{i+1}。迭代 64 轮后输出最终的杂凑值。

3　硬件优化设计介绍

3.1　算法流程设计

本文采用硬件描述语言 Verilog 对 SM3 算法进行实现，借助自上至下的模块化设计方法[7]完成算法 IP 核的整体设计。首先进行模块化设计，包括迭代模块、消息扩展模块、压缩模块和顶层设计模块。在顶层设计模块中，通过调用各子模块来实现 SM3 算法的杂凑值计算。顶层调用模块设计成时序逻辑电路，利用状态机对子模块进行调用，可以很好地控制算法的执行。

执行工作过程为：算法启动，开始依次读入初始化参数和消息 m，进行消息填充，迭代，扩展、压缩，最后输出杂凑值，并给出工作完成标志位。这一过程可以用图 1 描述。

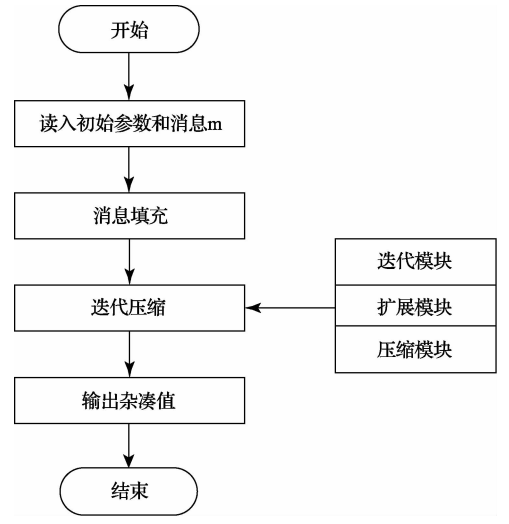

图 1　SM3 算法顶层模块设计流程图

3.2　硬件优化设计

本文设计的 SM3_IP 核的硬件结构主要包括消息扩展、压缩函数以及控制电路。

本文结合多种已知的最优杂凑硬件实现方法，在尽可能提高吞吐量的同时减少硬件资源的使用。首先，由于 SM3 算法消息填充部分的软硬件实现的效率差别不大，本文将其利用上层软件控制的实现，从而节省硬件开销。其次在实现过程中，为了提高执行效率，首先将使用频率较高的常量 T 和 IV 的用 ROM 结构实现。然后主要分析和优化了 SM3 在迭代过程中计算的硬件优化实现。

1）结合比较多种 FPGA 实现迭代的方法[8]考虑利用循环展开的结构进行实现，因为 SM3 每轮压缩函数和消息扩展运算中都要消耗一个时钟周期，而且在消息扩展过程中，由于每组 W_j 和 W'_j 两个字的计算量较小。为了进一步提高硬件效率，我能考虑如果在一个时钟周期里进行两组 W_j 和 W'_j 的计算，同时把一个时钟压缩函数的运算也增加到两轮[7]，如图 2 所示的压缩结构不仅可以充分地利用硬件资源提高计算速度，而且使整个 SM3 算法核心运算时钟消耗缩短了将近 1 倍，从而大大提高了吞吐量。

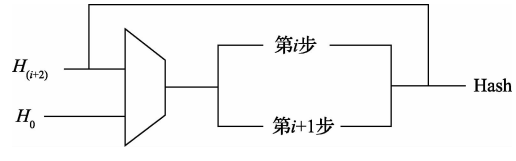

图 2　压缩结构

2)在迭代过程中的移位和逻辑运算只是简单的逻辑门电路,它们占用 FPGA 关键路径的时间延迟很小。运算电路中主要的时间延迟产生于 32 位的加法运算[8]。因此本文主要对加法电路进行了优化设计。通过 2 个进位加法器和 3 个超前进位加法器,将移位加法运算和直接加法运算分开。使延迟相似的逻辑单元首先进行运算,这样在利用很少量的硬件资源下,使加法电路的路径延迟较之前的进位加法电路缩小很多。

4　功能验证与性能分析

4.1　验证平台

为了验证 FPGA 硬件设计的正确性同时为了软件方便调用与测试的需要:我们选用 Xilinx 公司的微处理器和 FPGA 联合处理芯片 ZYNQ-7020 为目标器件进行测试,主要测试框图如图 3 所示。

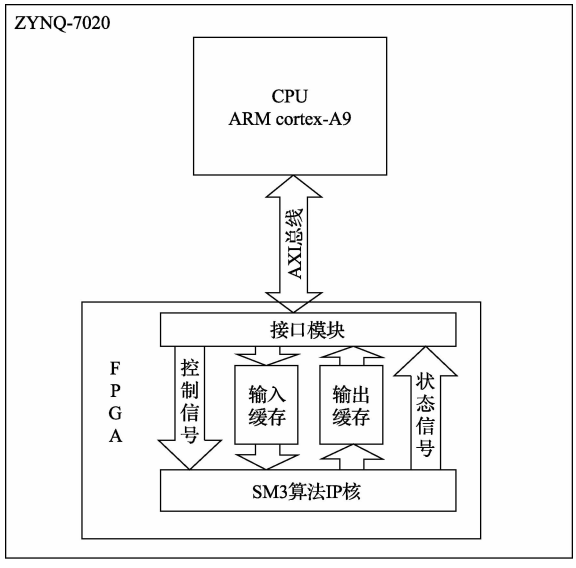

图 3　硬件验证平台

4.2　测试方案

本文这里为了充分验证设计的 SM3 算法的高效性和实际应用的需要,将本文设计的 SM3 模块封装成 IP 核,并参考多种 FPGA 与 CPU 互联方法[9-10],设计了一种高效的总结接口设计和接口驱动,方便 IP 核的拓展与应用。最后在 Xilinx 公司的 ZYNQ-7020 目标器件 ARM 和 FPGA 上进行设计验证。本文这里 ZYNQ 的处理器为主频 667 MHz ARM Cortex-A9 处理器,通过 AXI 总线与 FPGA 互联,其他处理器设计类似。下面分部分简述验证方案。

4.2.1　SM3 IP 核总线接口设计

使用硬件实现密码算法的主要目的是利用 FPGA 的高速及高效处理能力。提高硬件处理速度的方法是通过空间换时间,使用更多的硬件资源获得更快的处理速度。本设计将 SM3 算法作为硬核 IP 挂接到系统总线,系统与 SM3_IP 的传输使用 ARM 控制方式实现。根据 ARM 硬核嵌入式系统的工作要求和 SM3 算法的特性,SM3_IP 的设计分为四个模块:系统接口模块、输入缓冲区模块、输出缓冲区模块、密码算法模块,如图 3 硬件验证平台所示。

4.2.2　接口驱动软件设计

当完成 SM3 算法的 IP 核后,需要 ARM 主控程序对 SM3 算法的 IP 核进行调用以及实现数据的传输和控制,并最终输出结果。驱动程序设计的流程如图 4 所示。

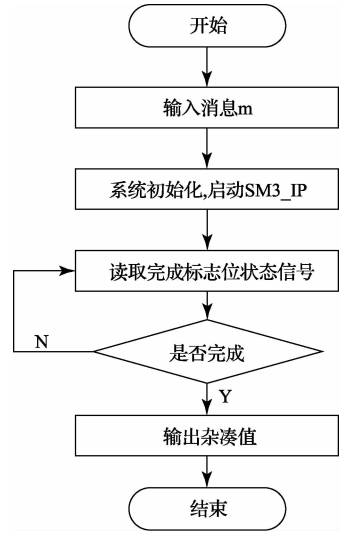

图 4　SM3 软件程序流程图

4.3　结果分析

4.3.1　结果验证

首先测试验证 SM3_IP 及总线连接正确性,将 ARM 处理器获得的前三组密钥流输出到串口进行验证。采用国家密码管理局公布 SM3 密码杂凑算法运算示例进行测试验证,输入消息为“abc”,其 ASCII 码表示为 616263,填充后的消息为 61626380 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000018,输出杂凑值为 66c7f0f4 62eeedd9 d1f2d46b dc10e4e2 4167c487 5cf2f7a2 297da02b 8f4ba8e0。测试结果如图 5 所示:

```
Running SM3_IP_SelfTests() for SM3_encrypt...
Read data1:0x0
Read data1:0x1
Read data1:0x66C7F0F4
Read data2:0x62EEEDD9
Read data3:0xD1F2D46B
Read data4:0xDC10E4E2
Read data5:0x4167C487
Read data6:0x5CF2F7A2
Read data7:0x297DA02B
Read data8:0x8F4BA8E0
SM3_IP_encrypt PASSED.
```

图 5　SM3 IP 接口测试图

结论:测试数据与官方数据一致,证明 SM3_IP 驱动软件设计正确,系统总线通信正常。

4.3.2　硬件资源分析

使用 Xilinx 公司的 ISE 工具对我们的 SM3 IP 核代码进行综合，目标器件为 Zynq-7020，综合后的资源占用情况如表 1 所示。

表 1　FPGA 资源统计

硬件占用资源 (ALUTs)	寄存器数 (total registers)	存储单元利用率	工作主频 /MHz
1743 3%	1323 1%	1%	167.8

结论：本文设计的 SM3 IP 核硬件占用资源较少。

4.3.3　吞吐量分析

由 ISE 工具综合后给出时钟分析报告如表 1，可知 SM3 模块在本文测试的 Xilinx 公司的 ZYNQ-7020 平台时钟频率可达到 167 MHz，64 个时钟完成 512 比特数据的处理。吞吐量可达 167.785×512/64＝1342.28 Mbps 。

结论：可见本文用 FPGA 设计的 SM3 算法模块使其吞吐量大大提升。

5　实际视频应用

5.1　硬件测试平台

为了进一步验证我们设计的 SM3 模块的性能，并且尝试解决实时视频认证的难题[11]，参考结合其他视频认证方法[12]，将此设计具体应用在实时视频数据杂凑认证上，最后进行性能分析。

为了保证应用与上述硬件验证的一致，我们这里仍然选用 Xilinx 公司的微处理器和 FPGA 联合处理芯片 ZYNQ-7020 为核心的 zedboard 板卡为目标器件进行实验，主要实验平台如图 6 所示。

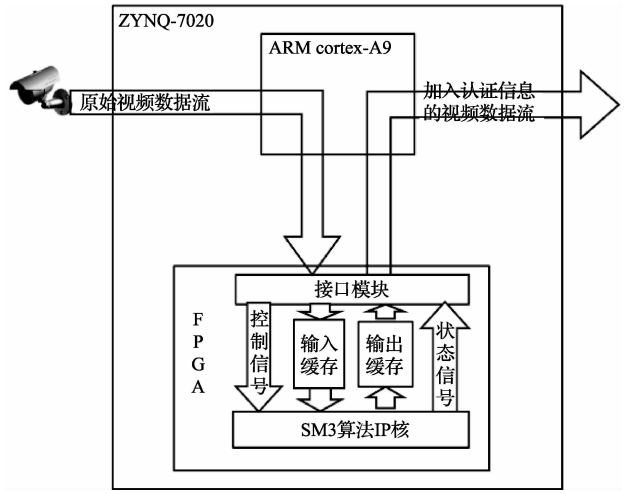

图 6　视频认证测试框图

5.2　应用流程

根据上述硬件框图，首先将摄像头采集的原始视频送入内存，然后将数据送入板卡的 FPGA 部分，可以对每一帧或者每几帧视频数据也可以对完整视频数据进行认证，认证完成后向 ARM 发出信号，通过 AXI 总线传输认证码原始视频数据。调用驱动读取认证码，后续可以认证码和视频数据一起写入存储器保存，或者直接送入网卡进行有线或者无线传输，方便实用。可以满足实时视频认证的需求。

5.3　测试结果

5.3.1　认证效果

如图 7 所示，上图是板卡输出的数据认证码，下图是 PC 对原始视频再次取 SM3 杂凑值，可以看出两次的认证码相同，证明原始视频没有被篡改过。验证了我们设计模块的正确性。

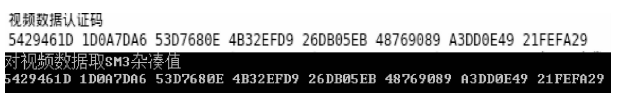

图 7　视频认证验证图

5.3.2　软硬件速度对比

我们利用 ISE 工具综合得到在测试的目标器件上时钟频率可达到 167 MHz，在 64 个时钟完成 512 比特数据的处理。这里为了系统的稳定性选用时钟频率 100 Hz 的总线进行测试，吞吐量可达 100×512/64＝800 Mbps

我们这里首先用板卡认证约 70 MB 视频数据测试时间结果如图 8，由于 ARM 需要驱动调用总线所以用时比理论速率稍慢。

图 8　板卡认证时间

本文在主频 2.5 GHz 内存 12 G 64 位操作系统的 PC 机上同样完成对 70 M 视频数据的 SM3 完整性认证用时如图 9 所示。

图 9　PC 认证时间

可以看出对相同大小的视频数据去 SM3 杂凑值，使用我们设计的硬件 SM3 芯片可以比高端 PC 机处理速度还要提高 2 倍以上。

5.3.3　鲁棒性分析

为了进一步验证设计的 SM3 完整性认证模块的有效性和鲁棒性，随意更改上述测试的视频数据的 1 个 bit 信息，再次进行杂凑验证，认证码如图 10，可以看到虽然只有一个 bit 信息的更改但和前面的认证码发生了很大的改变，可以很容易的得知原始数据发生了篡改。很好的证明了我们设计模块的具有高灵敏性和抗攻击性。

图 10　篡改后数据认证码

6　应用前景

本文设计 FPGA 高效 SM3 完整性验证模块，可以设计成固定的杂凑认证芯片，也可以作为 FPGA 中可编

辑软核,用于杂凑认证处理。方便实用,占用硬件资源少,认证速度快,可以运用于实时视频,语音等大数据的完整性认证,解决了一些大数据无法实时认证只能后期验证的缺陷。也满足了视频认证的需求,同时也可运用于现阶段物联网云存储[13]等的完整性认证,及时的防止对原始数据的恶意篡改,有效的保护了数据的完整性,有着广泛的应用前景。

7 结　论

本文利用 FPGA 的并行高速处理的特点,并对硬件设计进行优化设计,高效的实现了 SM3 算法,并进行了软件仿真和在实际硬件测试,最后封装成 IP 核并给出了相应的总线和接口软件设计方便推广和使用。实验结果说明本文设计的 SM3 模块吞吐量可达 1.3 G 以上速度远远大于 PC 软件处理,并且方便实用,对 SM3 算法的推广和使用有着重要作用,有着广阔的市场前景。

参考文献

[1] 国家密码管理局. SM3 密码杂凑算法[EB/OL]. 2010.

[2] 丁冬平,高献伟. SM3 算法的 FPGA 设计与实现[J]. 微型机与应用, 2012, 31(5): 26-28.

[3] 王晓燕,杨先文. 基于 FPGA 的 SM3 算法优化设计与实现[J]. 计算机工程, 2011,37(19):1-3.

[4] JEON J C, SEO K J, KIM K W. Hardware complexity of SHA-1 and SHA-256 based on area and time analysis [C]//2012 International Conference on Information Networking (ICOIN). IEEE, 2012: 557-561.

[5] XUE Y, HU A Q. Optimized SHA-1 hash function implemented on FPGA [J]. Journal of Southeast University, 2014(1):13-16.

[6] SHA-3 杂凑算法硬件实现研究[D]. 北京:清华大学,2011.

[7] 张松,李筠. FPGA 的模块化设计方法[J]. 电子测量与仪器学报, 2014,28(5):560-565.

[8] 韩春,蔡俊. 基于 FPGA 的高速伪随机序列发生器设计[J]. 电子测量技术,2013,36(7):55-57.

[9] 胡亚平. FPGA 与 CPU 高速接口的实现[J]. 国外电子测量技术, 2013,32(4):66 -68.

[10] 张京晶, 万旻, 程甘霖,等. 基于 FPGA 嵌入式的 PROM 接口实现[J]. 电子测量技术, 2013, 36(1): 75-78.

[11] 陈学涛, 郑力明. 实时视频传输系统[J]. 计算机系统应用, 2013, 22(10): 60-64.

[12] 庄景晖. 数字视频篡改被动认证研究的若干进展[J]. 漳州职业技术学院学报, 2014, 16(4): 1-6.

[13] 王浩,李玉,秘明睿,等. 一种基于监督机制的工业物联网安全数据融合方法[J]. 仪器仪表学报, 2013, 34(4): 817-823.

作者简介

周威,1993 年出生,现本科就读于西安电子科技大学信息安全专业,主要研究方向为安全芯片设计,系统安全,图像处理与信息隐藏技术。

E-mail: chunwei123hu@163.com

张卫东,1964 年出生,西安电子科技大学计算机系统结构专业工学硕士学位,曾担任国家级实验教学示范中心副主任,西安电子科技大学计算机基础教学实验中心副主任。主要研究方向为数字签名认证系统,网络安全体系架构,网络 P2P 安全技术实现等。

E-mail: wdzhang@xidian.edu.cn