

通用高性能密码服务系统模型

寇文龙, 陈莉君

(西安邮电大学 计算机学院, 陕西 西安 710121)

摘 要: 互联网行业的飞速发展, 使安全传输成为关注的焦点, 单一密码机的性能已经不能满足日益增长的安全服务需求. 提出了一种通用的高性能密码服务系统模型, 通过统一的服务接口设计和相应的密码服务资源调度算法, 实现不同密码机密码服务资源的统一管理. 经测试, 基于该模型实现的密码服务系统能够很好地满足互联网应用安全传输的安全服务需求.

关键词: 密码机; 密码服务; 资源虚拟化

中图分类号: TP311

文献标识码: A

文章编号: 1000-7180(2016)10-0087-04

General High-Performance Cryptographic Service System Model

KOU Wen-long, CHEN Li-jun

(School of Computer Science, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: With the rapid development of Internet industry, secure transmission has become the focus of attention, the performance of single cryptographic machine cannot meet the demand of the growing security services. Aiming at this problem put forward a general high-performance cryptographic service system model, implement unified management of different types of cryptographic machine, through designing a unified service interface and cryptographic service resources scheduling algorithm. After the test, the cryptographic service system can meet the demand of the secure service.

Key words: cryptographic machine; cryptographic service; resource virtualization

1 引言

随着各种互联网应用的蓬勃发展, 如何保证数据在传输过程中的安全问题已经成为关注的热门话题. 为解决这个问题, 互联网应用提供商普遍使用密码机来保证数据的安全传输. 随着互联网应用规模的逐渐增大, 对密码机的工作性能要求也逐渐提高, 如系统响应时间, 能够支持的加解密算法以及加解密速率, 系统所能承受的负载等, 单一密码机的性能已经远远不能满足大型系统的需求.

针对单一密码机的性能问题, 文献[1-10]对密码机和密码服务的特点以及安全需求进行了分析, 并提出了一些密码服务解决方案. 文献[6]将密码运行与密钥管理下移至硬件设备, 提出了一个多任务的密码服务系统, 该方案仅对单一密码机进行优化,

无法满足大型系统的需求; 文献[1, 2, 9]从面向服务的角度出发, 归类组合传统密码服务, 提出抽象服务的观点, 提高了密码机的性能, 但是单靠软件来实现无法有效地保证密码服务的安全性; 文献[4, 7, 8]提出密码服务器的概念, 用线性扩充密码机数量的方法构建密码机集群, 并用并行数据处理的思路提高密码服务的性能, 该方案没有解决通用性, 密码机不同接口也就不完全相同, 密码机的更换就需要对密码服务系统做一定的修改, 降低了系统的可移植性, 增加了系统的维护成本且使系统的安全风险加大.

在总结已有方案的基础上, 本文提出了一种通用的高性能密码服务系统模型, 该模型利用资源虚拟化技术, 能够兼容不同厂商的密码机设备, 动态分配和管理密码机的加解密资源, 有效地提高了密码服务系统加解密性能和资源利用率.

2 密码服务系统模型

2.1 模型概述

本文提出的通用密码服务模型采用分层架构,主要由密码机设备层、资源虚拟化层、密码设备接口层、密码服务接口层四层组成.其架构模型如图 1 所示.该模型架构中,每一层都代表了密码服务的一个业务逻辑,每一层都有特定的角色和功能.通过分层架构将密码服务和具体的密码算法运算分隔到不同的层中,每一层保持在同一抽象级别上的高内聚性,限制各层之间的依赖关系,使密码服务系统以更松散的方式耦合.

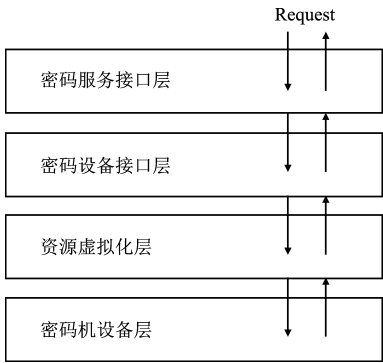


图 1 通用密码服务模型架构

在本文提出的密码服务模型中,密码服务接口层能够将应用层海量的密码服务请求经过简单和必要的处理之后传递给密码设备接口层,然后通过资源虚拟化层的调度后交给某个密码机进行密码运算,最后将运算的结果逐层返回给用户.密码服务接口层通过提供统一的密码服务接口使得用户不需要关心使用的密码机的厂商和设备型号,也不需要知道底层密码机的状态,只需要根据自己的需求,调用相应的服务接口函数.在密码设备接口层和密码机设备层之间形成的资源虚拟化层将符合规范的密码机提供的加解密资源进行抽象和管理,在内部实现调度和协调资源,让各个密码机能够高效均衡的使用.

2.2 模块设计

密码机设备层:由各种型号的密码机组成.密码机是根据密码学原理,利用物理噪声源来生成随机数,采用常用的各种加解密算法,是一种采用硬件加密方式的物理设备.相对于软件加密,采用硬件加密有更高的安全性和更好的性能.密码机内置两块加密卡,其中一块加密卡为工作卡,另一块为备份卡,用于对通过密码机的网络信息进行加密和解密,当

工作卡发生故障时,备份卡自动接管,继续工作.除此之外,密码机还包含两块高速以太网卡,用于隔断内外网络,保证进出内部网络的数据必须经过密码机的处理.

资源虚拟化层:该层负责把密码机设备层中不同型号密码机所能提供的数据加解密、数字签名、随机数生成、密钥管理等密码服务功能进行抽象整合,该层利用资源虚拟化技术,屏蔽了底层密码机设备之间性能和密码服务种类的差异性,并采用适当的资源调度算法,动态分配和管理底层的密码机硬件资源,实现系统加解密性能和资源利用率的提高.

密码设备接口层:该层将底层抽象的密码服务资源进行分类整理,把调用规则复杂的接口转化为统一的、易于理解的、简洁的服务接口.主要有以下几个部分:设备管理类,负责与设备相关的操作,如打开设备、获取设备信息等;密钥管理类,负责密钥的生成、存储、分配、使用、销毁等操作;密码算法运算类,主要包括常用的对称和非对称加解密算法运算;文件操作类,如打开文件、读取文件等操作.

密码服务接口层:该层将上层应用发来的密码服务请求转化为具体操作.主要分为以下几类:环境类,负责创建和管理密码服务所需的各种资源、信号,并确保在运行期间不会被非法访问,造成信息泄漏;证书类,提供各种证书的相关操作,如证书获取、证书验证、证书生成等;运算类,负责具体的密码算法运算,并将运算结果返回给上层应用,实现数据保密性、完整性和不可抵赖性;消息类,主要将数据按照一定的格式进行封装,实现数据格式与应用系统无关性,并保证系统互联互通,实现消息共享.

3 密码服务系统实现

3.1 密码服务系统框图

为了验证本文所提的密码服务系统模型的可用性,设计了一套密码服务系统方案.如图 2 所示.

该密码服务系统方案图中,通用密码服务接口层通过统一的密码服务接口,向典型密码服务层和应用层提供证书解析,证书获取,证书验证,信息的机密性、完整性和不可否认性等通用密码服务,将上层应用的密码服务请求转化为具体的基础密码操作请求.通用密码服务层可以接受多进程或者多线程的调用,通过多线程技术能够迅速处理应用程序发来的海量密码服务请求并交给密码设备应用接口层去处理.该过程速度很快,能够保证在高并发环境下快速响应应用程序的服务请求.

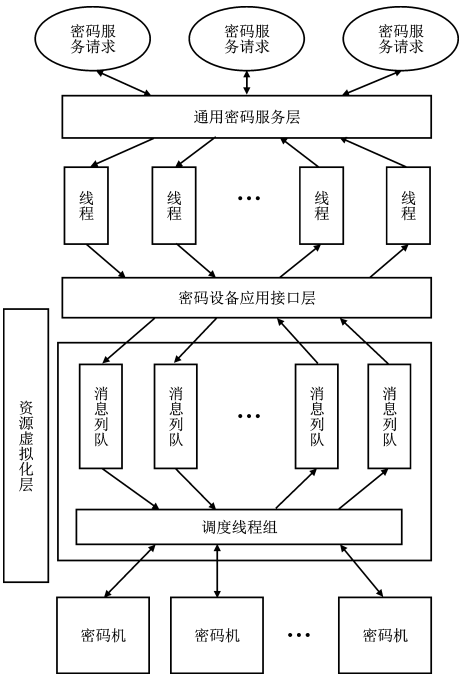


图2 密码服务系统方案图

密码设备应用接口层通过下行消息队列将接收的密码服务请求以作业包的形式发送给调度线程组,调度线程组中的线程从消息队列中取出作业包,读取密码服务请求,根据各个密码机的服务状态值决定该请求需交给哪个密码机去处理,同时更新该密码机的服务状态.其中,下行消息队列的数目根据配置文件配置一个固定值.密码机将处理完成的密码服务请求通过上行消息队列发送给相对应的线程,然后返回给密码服务请求发送方.上行消息队列的数目和系统中所有的进程或者线程是一一对应的,各进程或者线程的PID就是上行消息队列的key值,在将密码机的处理结果返回给服务请求方时起到重要作用.

3.2 系统处理流程

本文所实现的密码服务系统的密码服务请求处理流程如图3所示.

- 图3所示的密码服务请求执行流程描述如下.
- (1)应用程序发起密码服务请求,请求指定的密码服务.
 - (2)通用密码服务层接受并处理密码服务请求.
 - ①调度线程接收服务请求.
 - ②生成作业包,并记录线程与作业包的对应关系等信息.
 - (3)密码设备层接受密码作业并处理.
 - ①接收作业包,并加入相应的消息队列.
 - ②调度线程从消息队列取出作业包,然后解析

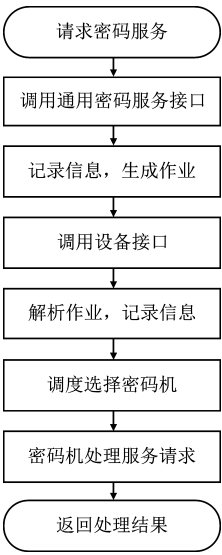


图3 系统处理流程

- 作业包,并提取服务请求.
- ③根据调度算法选择密码机,分配连接,并更新该密码机的服务状态值.
 - (4)密码机处理服务请求.
 - ①密码机执行相应的运算.
 - ②生成运算结果.
 - (5)处理结果返回给应用程序.
 - ①将服务请求处理结果通过对应的上行消息队列返回密码设备层.
 - ②密码设备层将服务请求处理结果根据作业包对应的线程返回给应用程序.

3.3 密码资源调度算法

本文提出的密码服务系统采用单服务器模式,通过与密码机设备建立SSL(Secure Socket Layer)的方式进行密码服务请求的传递.因此需要根据每个密码机建立的SSL连接数来衡量各个密码机的负载情况.目前服务器负载均衡算法有很多,针对本文提出的密码服务模型的特点,采用加权最小连接调度算法(Weighted Least-Connection Scheduling)作为资源虚拟化层的负载均衡调度算法.加权最小连接调度算法是最小连接调度算法的超集,各个服务器用相应的权值表示其处理性能,管理员可以动态地设置服务器的权值.加权最小连接调度在新连接到来时尽可能使服务器已建立的连接数和其权值成一定的比例.一般情况下,加权最小连接调度是一个非常公平的调度方案,已建立的连接数和服务器权重比最低的服务器自动接收下一个服务请求.

加权最小连接调度算法在本文的密码服务系统

中应用如下:假设有一组密码机 $S = \{S_0, S_1, \dots, S_{n-1}\}$, $W(S_i)$ 表示密码机 S_i 的权值, $C(S_i)$ 表示密码机 S_i 当前的连接数. 所有服务器当前连接数的总和 $C_{sum} = \sum C(S_i) (i=0, 1, \dots, n-1)$, 当前的新连接请求会发送给密码机 S_m . 密码机 S_m 要接收该连接需满足以下条件:

$$(C(S_m)/C_{sum})/W(S_m) = \min((C(S_i)/C_{sum})/W(S_i)) (i=0, i, \dots, n-1, W(S_i) \neq 0)$$

本文所提出的密码服务系统方案中应用的加权最小连接调度算法的算法流程图如图 4 所示.

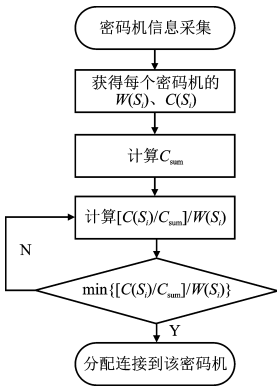


图 4 加权最小连接调度算法流程图

4 性能测试与分析

4.1 测试环境

为了验证本文所提的通用高性能密码服务框架的可用性,构造如图 5 所示的测试环境. 用户层用来模拟密码服务请求,调度服务器加载本文提出的通用密码服务方案和密码服务资源调度机制,密码机集群采用联想 SJW44,天融信 SJW11-A,得安 SJY05 来做模拟.

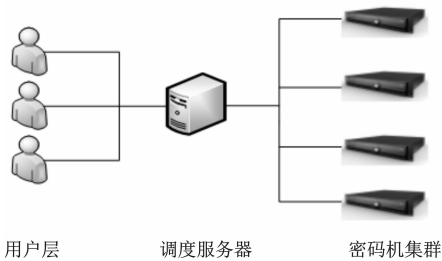


图 5 测试环境图

4.2 测试结果与分析

为了测试系统的性能笔者用三台性能相近的密码机进行测试和分析. 图 6 和图 7 分别给出了随着密码服务请求数的增加,三种不同型号的密码机单独工作和三台密码机同时工作的情况下系统加解密

速率、系统吞吐率的变化规律.

(1)加解密速率

从图 6 可以看出,在相同密码服务请求数的情 况下,三台密码机同时工作时的加解密速率明显高 于单台密码机单独工作时的加解密速率,优势明显.

(2)系统吞吐率

如图 7 所示,在并发数较低时,三台密码机同时 工作的效果并不明显,随着密码服务请求数的增加, 系统吞吐率会逐步提高,本文所提出的密码服务系 统的优势才逐渐显露出来,在密码服务请求数为 500 000 次左右时达到最大值. 在高并发环境下,该 系统能有效地解决海量密码服务请求带来的系统 压力.

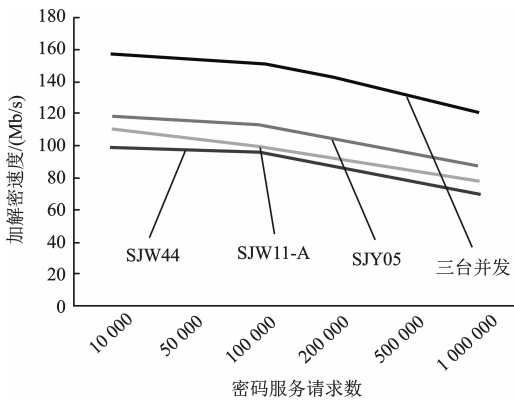


图 6 加解密速率变化曲线

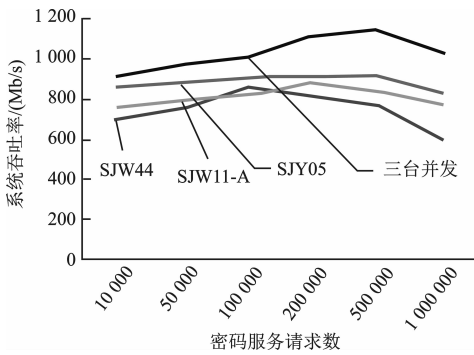


图 7 系统吞吐率变化曲线

5 结束语

通过对密码服务系统的关键性能指标:系统加 解密速率和系统吞吐率的测试,本文所提出的通用 的高性能密码服务模型能够在解决密码机兼容问题 的基础上很好地实现资源的动态分配和管理,并实 现密码服务性能和利用率的提升. 基于这个方案可 以很好地解决互联网在线应用对密码机性能的需求

路面积。

通过电路及版图后仿真,有效位数达到 7.6 bit,在满足胎压监测系统较低速采样(2 kHz)的要求下,功耗仅为 $0.9 \mu\text{W}$ 。MATLAB 频谱分析结果显示,在 $-40 \sim 125^\circ\text{C}$ 范围内,ADC 可以实现稳定的精度,并已加入到胎压监测 SoC 中提交流片。为完成低功耗高可靠性的胎压监测系统级集成做好了准备。对于胎压监测标准中的 ESD 静电防护 $\pm 2 \text{ kV}$ 的要求,需要与胎压监测系统的其他模块综合设计防护方案,这部分内容将在后续流片中加入。

参考文献:

- [1] Weibo Hu, Donald Y C Lie, Yen-Ting Liu, 8-bit Single-Ended Ultra-Low-Power SAR ADC with a novel DAC switching method", Circuits and Systems[C]// 2012 IEEE International Symposium on ISCAS. [s. l.]:IEEE,2012:2349-2352.
- [2] Scott M D, Boser B E, Pister K S J. An ultralow-energy ADC for smart dust[J]. IEEE J Solid-State Circuits, 2003,8(7):1123-1129.
- [3] Chao Yuan, Yvonne Y H Lam. A novel Low-Voltage SAR ADC for biomedical applications[J]. IEEE New Circuits and Systems Conference(NEWCAS), 2011,36(2):26-29.
- [4] van Elzakker M, van Tuijl E, Geraedts P, et al. A 1.9-uW 4.4fJ/Conversion-step 10b 1MS/s Charge redis-

tribution ADC[J]. ISSCC Dig Tech Papers, 2008, 27(5): 244-245.

- [5] You-Kuang Chang, Chao-Shiun Wang, Chorng-Kuang Wang. 8-bit 500-KS/s low power SAR ADC for biomedical applications[J]. IEEE Solid-State Circuits, [s. l.]:IEEE,2007:228-231.
- [6] 许嘉林,卢燕娥,丁子明. ADC 信噪比的分析及高速高分辨率 ADC 的实现[J]. 电子技术应用. 2004,39(4):65-69.
- [7] 孙彤. 低功耗逐次逼近模数转换器的研究与设计[D]. 北京:清华大学. 2007.
- [8] 李勇. 无电池胎压监测系统关键模块的研究与设计[D]. 北京:清华大学. 2007.

作者简介:

王 义 男,(1990-),硕士研究生. 研究方向为无电池胎压监测系统关键 IP 设计。

乌力吉(通讯作者) 男,(1965-),博士,博士生导师. 研究方向为汽车电子与信息安全。

E-mail:lijiwu@mail. tsinghua. edu. cn.

张向民 男,(1966-),硕士,助理研究员. 研究方向为汽车电子与信息安全。

方华军 男,(1972-),博士,副研究员. 研究方向为微电子机械系统。

吴行军 男,(1969-),博士,副研究员. 研究方向为汽车电子与信息安全集成电路。

(上接第 90 页)

问题,能够有效地提高系统的可移植性,有效地节约系统的维护成本,有效降低系统安全可能存在的风险。

参考文献:

- [1] 李建军,郁滨,陈武平. 基于抽象服务的密码服务组合模型设计与实现[J]. 计算机工程与设计,2012,33(8): 2920-2925.
- [2] 容晓峰,李增欣,郭晓雷. 密码服务系统研究综述[J]. 计算机安全,2010,10(3):62-66.
- [3] 刘刚. 密码服务中间件设计与实现研究[D]. 郑州:解放军信息工程大学,2008.
- [4] 容晓峰,李增欣,刘平,等. 高性能密码服务系统体系结构设计[J]. 吉林大学学报(信息科学版),2005,23(4): 408-415.
- [5] 谢小斌,姚春华. 基于 SOA 的密码服务系统研究[J]. 信息安全与通信保密,2011,9(7):95-97.
- [6] 章文嵩,吴婷婷,金士尧,等. 一个虚拟 Internet 服务器的设计与实现[J]. 软件学报,2000,11(1):122-125.

[7] 刘敏,房至一,王红斌,等. 一种新的处理能力优先的权值分配调度算法[J]. 吉林大学学报(理学版),2011,37(6):1105-1109.

[8] 燕彩蓉,彭勤科,沈钧毅. 一种基于内容分发请求的 Web 集群服务器研究[J]. 西安交通大学学报,2005,55(4):380-383.

[9] Chen J C, Chen K H, Wu J J, et al. A study of the flexible job shop scheduling problem with parallel machines and reentrant process[J]. The International Journal of Advanced Manufacturing Technology, 2008, 39(3-4): 344-354.

[10] Law L, Menezes A, Qu M, et al. An efficient protocol for authenticated key agreement[J]. Designs, Codes and Cryptography, 2003, 28(2): 119-134.

作者简介:

寇文龙 男,(1990-),硕士研究生. 研究方向为云计算与大数据. E-mail:15829350768@163. com

陈莉君 女,(1964-),硕士,教授. 研究方向为 Linux 操作系统,云计算与大数据研究。