第 8 卷 第 3 期
2019 年 5 月
集 成 技 术
JOURNAL OF INTEGRATION TECHNOLOGY
Vol. 8 No. 3
May 2019

引文格式：
苏振宇. 密码卡虚拟化技术研究与实现［J］. 集成技术, 2019, 8(3): 31-41.
Su ZY. On the virtualization of cryptographic card［J］. Journal of Integration Technology, 2019, 8(3): 31-41.

密码卡虚拟化技术研究与实现

苏振宇

（浪潮集团高效能服务器和存储技术国家重点实验室 济南 250101）

摘 要 密码卡是一种密码设备，位于网络安全平台的物理层，通过各种密码算法为上层应用系统提供加解密、数字签名等密码运算服务。从云计算安全方面考虑，密码卡需要具备高速运算的特点，并且需要通过虚拟化技术实现高并发性。密码卡作为输入/输出(Input/Output，I/O)设备面临的挑战是，如何在虚拟化的情况下获得良好的 I/O 性能并有效地共享 I/O 设备。目前 I/O 虚拟化技术的发展相对滞后，影响了虚拟机的整体性能。基于此，该文提出了 3 种密码卡虚拟化设计方案，实现了基于现场可编程门阵列(FPGA)的软件虚拟化密码卡和基于单根 I/O 虚拟化技术的硬件虚拟化密码卡。在实际应用中，虚拟化密码卡通过高速外设部件互连标准(PCI-E)总线内置于服务器中，具备高性能并且通过软件调度可以被多用户共享。结果表明，该技术可应用于金融、电信等信息安全领域，具备广阔的应用前景。

关键词 密码卡；虚拟化；现场可编程门阵列；单根 I/O 虚拟化；高速外设部件互连标准
中图分类号 TP 309 **文献标志码** A doi: 10.12146/j.issn.2095-3135.20181113001

On the Virtualization of Cryptographic Card

SU Zhenyu

(*National Key Laboratory for High-efficient and Storage Technology*, *Inspur*, *Jinan* 250101, *China*)

Abstract Cryptographic card is a kind of encryption device located in the physical layer of the network security platform. It provides several encryption and decryption algorithms, digital signature, and other cryptographic operation services for application systems. Considering the security of cloud computing, the cryptographic card needs to be high speed and achieve high concurrency through virtualization technology. The challenge for the cards as input/output (I/O) devices is how to achieve high I/O performance and share I/O devices in the case of virtualization effectively. At present, the development of I/O virtualization technology is lagging behind, which affects the overall performance of the virtual machine. Based on this, this paper realizes the software virtualization cryptographic card by using field-programmable gate array and the single root I/O virtualization technology. In practical applications, a virtualized cryptographic card is built into the server through the peripheral component interconnect express bus, which has high performance and can be shared by many users. The results show that this technology has broad applications in the field of information security.

Keywords cryptographic card; virtualization; field-programmable gate array (FPGA); single root I/O virtualization; peripheral component interconnect express

收稿日期：2018-11-13 **修回日期**：2019-03-31

作者简介：苏振宇，硕士，高级工程师，研究方向为信息安全、嵌入式系统，E-mail：suzhenyu2006@aliyun.com。

1 引 言

随着云计算技术的普及，云应用需要底层硬件设备的技术支撑。由于在云环境中不同的用户会分享同一组硬件资源，因此服务器端的设备需具备高性能和虚拟化的特性来支撑云环境的应用。密码卡作为一种硬件设备，为适应云时代发展的要求，需要支持虚拟化环境的调用。

密码卡应用于信息安全领域，位于网络安全平台的硬件加密层。用户可以根据需要灵活地选择密码算法来为上层应用系统提供密码运算服务[1]。密码卡虚拟化，即基于物理上单一的密码卡硬件设备，虚拟出多个功能相同的“逻辑密码卡”，供多个虚拟机终端使用。尽管各终端通过虚拟机共享相同的物理密码卡，但被虚拟出的“逻辑密码卡”在功能上是独立的，因此用户使用过程中相互之间不会影响。

在计算机系统架构中，密码卡属于输入输出(Input/Output，I/O)设备。I/O 虚拟化的性能对系统整体性能的提高起到至关重要的作用。然而，在密码卡的虚拟化方面，目前国内外的研究仍较少：一方面是由于设备的多样性，使得作为 I/O 设备的密码卡虚拟化缺少统一的标准；另一方面是由于作为安全设备的特殊性，在技术实现方面很复杂，其中面临的一个重大挑战是如何在虚拟化的情况下，获得良好的 I/O 性能并且有效地共享 I/O 设备。

刘涛[2]提出了一种适合动态迁移的加密卡设备虚拟化方案，给出了动态迁移的具体协议和分析证明，并对虚拟机动态迁移的性能影响因素进行测试，但没有给出具体加密卡的实现。张嘉夫[3]为了解决虚拟桌面下的隐私保护问题，提出一种基于密码卡虚拟化的隐私保护方法，即通过软件模拟的方式实现了一种安全模型，但并没有给出硬件实现方案。李玉玲[4]对云计算环境下密码算法模型进行了研究，通过冗余技术对密码运算的容错进行了设计和实现，但通过 OpenSSL 算法库以软件方式实现的密码算法性能有限。Berger 等[5]提出了可信平台模块(TPM)的虚拟化，对安全设备的虚拟化有一定的指导意义，但缺少高速外设部件互连标准(Peripheral Component Interconnect-Express，PCI-E)总线设备的实现。马龙宇[6]设计并实现了基于单根 I/O 虚拟化技术(Single Root I/O Virtualization，SR-IOV)的虚拟化密码卡，但密码算法仅支持 160 位安全哈希算法(Secure Hash Algorithm，SHA1)，应用范围受限。杨永娇等[7]进行了基于直接 I/O 虚拟化技术(Virtualization Technology for directed I/O，VT-d)的虚拟化安全隔离框架研究，同样缺少实现。

综上所述，密码卡虚拟化技术发展相对滞后，大多数仍停留在理论研究层面，缺乏实际应用，影响了虚拟机的整体性能。基于此，本文分析了密码卡的虚拟化技术和密码卡虚拟化的模型，提出 3 种密码卡虚拟化技术方案，最终设计实现了基于软件虚拟化方式的密码卡和基于 SR-IOV 技术的硬件虚拟化密码卡。本文提出的技术能够解决虚拟化的数据安全保密问题，使得用户在虚拟环境中有效地共享物理密码卡资源，利用虚拟化密码卡获得良好的数据加解密性能。

2 密码卡虚拟化技术分析

密码卡虚拟化的整体架构如图 1 所示。其中，虚拟机监控程序(Virtual Machine Monitor，VMM)介于密码卡和客户操作系统的虚拟机之间，运行在特权模式，为每个虚拟机虚拟出一套独立于物理密码卡的虚拟硬件环境，隔离并管理上层运行的多个虚拟机。从应用程序的角度来看，程序运行在虚拟机上与运行在实际物理密码卡上是相同的。

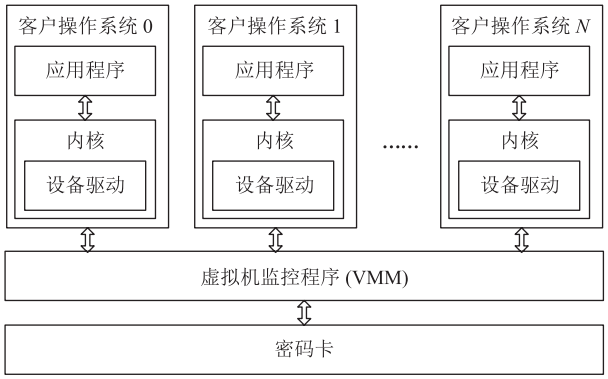


图 1　密码卡虚拟化的整体架构

Fig. 1　Architecture of cryptographic card virtualization

在密码卡虚拟化方面，存在性能损失的问题。密码卡作为 I/O 设备，其利用率成为了虚拟机性能的瓶颈。这是因为当采用虚拟技术后，由于虚拟机中都是模拟的逻辑密码卡，逻辑设备对物理设备又要经过一次 I/O 访问过程，导致虚拟机中的密码卡性能与直接使用物理密码卡的性能相比存在 50%～90% 的损失[8]。因此，密码卡虚拟化技术需要考虑功能、性能、共享、安全和隔离等技术问题。

(1) 功能：密码卡虚拟化需要实现与物理密码卡一致的密码运算、密钥管理等功能，并实现对资源的合理分配。

(2) 性能：需要对采用虚拟化后的密码卡的性能进行提升，以接近物理密码卡的性能。

(3) 共享：密码卡需要为多个虚拟机提供服务，需要提高密码卡的共享能力。

(4) 安全：采用虚拟化技术会引入新的入侵方式，存在安全风险，因此在设计虚拟化密码卡时需要考虑安全性与隔离性。

(5) 透明：虚拟机需要自动保存密码卡设备的状态，提供密码卡的驱动，支持硬件升级等。

3　密码卡虚拟化模型

提高虚拟机中的 I/O 设备性能需要在设备共享和使用效率之间进行折中。这是因为：如果 $N(N>1)$ 个虚拟机共享一个设备，由于设备频繁地在虚拟机之间进行切换，从而导致设备的使用效率很低；如果设备只提供给一个虚拟机使用，虽然使用效率很高，但设备的共享性却没有得到体现。以下对 3 种常用的密码卡虚拟化模型进行分析。

3.1　基于软件的 I/O 模型

该模型是将密码卡硬件的逻辑部分移入到虚拟机中，模拟层位于客户机与底层密码卡之间。主流的软件模拟 I/O 虚拟化技术有 Split I/O、Direct I/O 等。这些技术在不同程度上实现了 I/O 设备的虚拟化功能，并通过硬件级的支持提高了 I/O 设备虚拟化的性能。但由于体系结构硬件的限制，软件 I/O 虚拟化技术在性能方面仍然存在差距。

3.2　硬件辅助的模型

基于软件的虚拟化 I/O 模型增加了 CPU 的负担，因此需要硬件辅助技术完成一部分 I/O 虚拟化的功能。Passthrough I/O 是一种硬件辅助模型，支持客户域直接访问物理 I/O 设备，具有最高的性能，但其只能将 I/O 设备分配给一个客户独占使用，无法实现在多个客户之间的共享[9]。Intel 和 AMD 公司都在处理器架构中提供了对 Passthrough I/O 的支持。其中，Intel 将这种支持称为直接 I/O 虚拟化技术(VT-d)[10]，AMD 称之为 I/O 存储管理单元(I/O Memory Management Unit，IOMMU)[11]。这种支持虚拟化技术的 CPU 能够将 PCI-E 设备物理地址映射到客户机中，硬件负责访问和保护，客户机像宿主系统一样可以直接使用 PCI-E 设备。除了将客户机映射到物理内存外，还提供隔离机制以阻止其他客户机访问该区域。

3.3　基于 SR-IOV 的模型

基于软件和硬件辅助的 I/O 虚拟化方式虽然能够提高虚拟化 I/O 的能力，但无法同时实现 I/O 设备的高性能和共享性能。因此，Intel 公

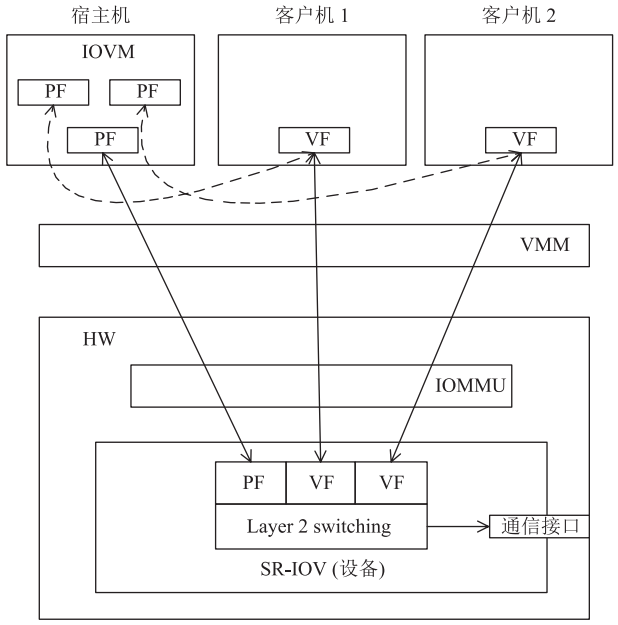
司提出了解决虚拟化 I/O 的单根 I/O 虚拟化技术（Single Root I/O Virtualization，SR-IOV）。其中，SR-IOV 是 PCI-SIG 组织公布的规范[12]，旨在消除 VMM 对虚拟化 I/O 操作的干预，提高数据传输的性能。该技术不仅能够继承 Passthrough I/O 虚拟化方式的高性能优势，同时还支持 I/O 设备的跨域共享[13]。

具有 SR-IOV 功能的 I/O 设备符合 PCI-E 规范[14]，能够管理并创建 *N* 个虚拟功能（Virtual Function，VF）。物理功能（Physical Function，PF）在 PCI-E 总线上是主要实体。其中，PCI-E 作为 SR-IOV 设备可以有一个以上物理功能，每个物理功能都是标准的 PCI-E 功能，并且关联多个虚拟功能。每个虚拟功能都有与性能相关的资源，专门用于软件实体在运行时的性能数据运转，同时这些虚拟功能共享物理设备资源。因此，虚拟功能可以视为由物理功能进行配置和管理的“轻量级”PCI-E 功能。与传统的 PCI-E 设备相比，在有限的芯片设计预算里，SR-IOV 设备可以最多包含 256 个虚拟功能[8]，具备更好的可扩展性。

SR-IOV 的实现模型如图 2 所示，包括 VF 驱动、PF 驱动和 SR-IOV 管理器（IOVM）。其中，VF 驱动运行在客户机上；PF 驱动部署在宿主机上对 VF 进行管理；宿主机中的 IOVM 管理 PCI-E 的控制点以及每个 VF 的配置空间。为了使该模型独立于底层的 VMM，每部分都不能使用特定的 VMM 接口。例如，PF 驱动和 VF 驱动的通信可以直接使用 SR-IOV 设备，但其接口不会依赖于特定的 VMM 接口。

4 密码卡虚拟化技术方案

密码卡虚拟化的开发步骤是基于物理密码卡，在虚拟机监控程序 VMM 中实现密码卡的逻辑功能与硬件接口，即 VMM 作为中间层，其中



IOVM：单根 I/O 虚拟化技术管理器；PF：物理功能；VF：虚拟功能；VMM：虚拟机监控程序；HW：硬件；IOMMU：I/O 存储管理单元；Layer 2 switching：二层交换机功能；SR-IOV：单根 I/O 虚拟化技术

图 2 SR-IOV 技术实现模型

Fig. 2 Implementation model of SR-IOV technology

的硬件接口实现与底层物理密码卡之间的通信，逻辑功能需要实现物理密码卡的所有功能，以便客户端进行调用。根据密码卡的虚拟化模型，以下给出 3 种密码卡虚拟化的实现技术方案。

4.1 基于软件虚拟化的密码卡（方案 1）

该方案在传统功能的硬件 PCI-E 密码卡的基础上通过软件模拟的方式实现虚拟化的功能。硬件架构如图 3 所示，以 Altera 具有 PCI-E 硬核[15]的 Cyclone IV 系列的现场可编程门阵列（Field-Programmable Gate Array，FPGA）为控制核心，与 PCI-E 物理总线进行连接；利用硬件描述语言 VHDL/Verilog HDL 在 FPGA 中设计状态机实现对密码算法芯片 SM1、SM2、SM3 和 SM4 的控制，或通过设计 IP 核的方式在 FPGA 内部实现 SM3 和 SM4 算法。另外，电可擦除可编程只读存储器（EEPROM）用于存储密码卡密钥等关键参数；Flash 作为非易失存储器用于存储需要长期保

存的数据；同步动态随机存取内存(SDRAM)芯片作为缓存；物理噪声源用于生成真随机数。该密码卡具备数据加解密、数字签名、验证签名等功能。

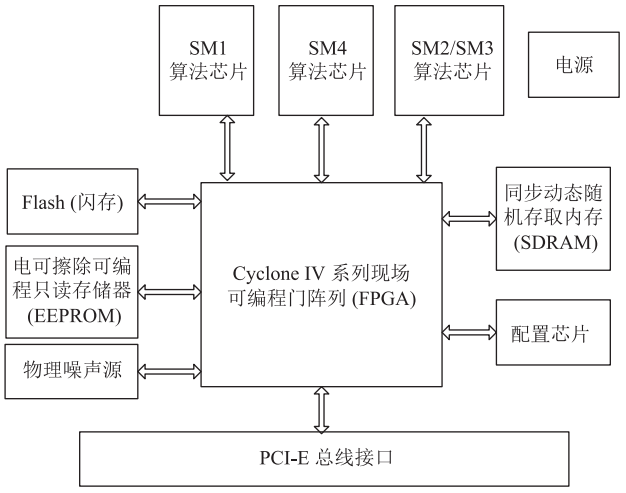


图 3　基于软件虚拟化的密码卡硬件架构

Fig. 3　Hardware architecture of cryptographic card based on software virtualization

软件虚拟化的设计流程如图 4 所示，具体是把物理密码卡的驱动程序分别移植到宿主机(Host)和客户机(Guest)的操作系统中，之后在 VMM 中设计密码卡模拟器软件，分别实现与宿主机中密码卡驱动程序和客户机中密码卡驱动程序的通信，使客户端通过 API 接口分时访问宿主机中的密码卡 API 接口，从而实现对密码资源的调用。基于 Linux 操作系统的虚拟机(KVM)采用的是宿主操作系统(hosted VMM)结构，即 VMM 实际上运行于一个传统操作系统之上。这类 VMM 无法获得对硬件资源的完全控制，因此采用软件模拟的方法来虚拟密码卡。软件层面的具体实现方法是：以调用 SM4 算法加密功能为例进行说明，客户操作系统的密码卡调用 SM4 加密函数接口的操作会被 VMM 捕获，并转交给宿主操作系统的一个用户态进程，该进程通过对宿主操作系统的系统调用来模拟密码卡的调用物理算法芯片行为，从而实现 SM4 算法的加密功能。模拟密码卡的方法对客户操作系统是透明的，并且设计 VMM 不复杂，兼容性好，但软件模拟最大的开销在于切换处理器模式，采用虚拟化后密码卡的性能最差时能够降低为物理密码卡性能的 20%[8]。

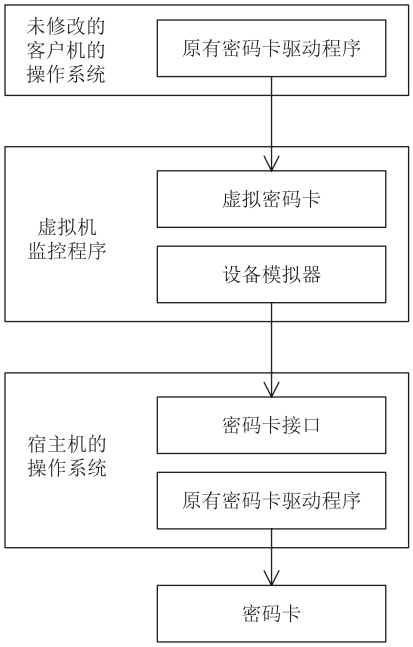


图 4　密码卡软件虚拟化方式

Fig. 4　Software virtualization method of cryptographic card

4.2　基于 SR-IOV 的硬件虚拟化密码卡(方案 2)

该方案是采用 SR-IOV 技术的硬件虚拟化密码卡，硬件系统架构如图 5 所示。该方案采用 Intel 82576EB Gigabit 以太网控制器芯片[16]，其中该芯片支持 PCI-E 总线 v2.0 协议并支持 SR-IOV 虚拟化功能。通过 Intel 82576 实现与 PCI-E 物理总线的连接和千兆网口功能，并且实现 SR-IOV 功能。采用 Altera Cyclone III 系列的 FPGA 作为密码卡的协处理器[17]，控制密码算法芯片工作。EEPROM、Flash、SDRAM 和物理噪声源等模块的功能与方案 1 中所述一致。

硬件虚拟化的设计流程是：将密码卡作为 SR-IOV 设备，在宿主机中实现 PF 驱动程序和 IOVM 程序，而在客户机中实现 VF 驱动程序。其中，PF 实现对 VF 的管理，IOVM 实现对作为

PCI-E 物理节点的密码卡和 VF 配置空间的管理，从而使宿主机和客户机实现对密码资源的调用。

以下结合图 5 和图 2 的 SR-IOV 模型，介绍密码卡在硬件环境下作为 SR-IOV 的使用说明。SR-IOV 协议将物理密码卡抽象为物理功能(PF)和虚拟功能(VF)。密码卡作为 SR-IOV 设备可以具有一个以上的 PF，PF 即标准的 PCI-E 设备，每个 PF 又可以创建 $N(N>1)$ 个 VF，VF 属于轻量级的 PCI-E 设备，拥有处理数据包的关键资源。图 2 中的通信接口实现密码卡与宿主机的通信，PF 和 VF 都具备 SM2、SM3 等密码算法功能，PF 中的设备管理程序负责对 VF 进行配置和管理，PF 功能接口负责将待加密/解密的数据包进行转发。密码卡虚拟化功能的启动过程为：首先，物理密码卡硬件初始化和特权域的启动，宿主机 PF 中的驱动程序对 VF 进行设置，把密码卡抽象为 VF 设备；然后，客户机的 VF 驱动程序进行初始化，其中每个客户机的 VF 都代表一个密码卡；最终，客户端通过调用 VF 中的各类密码算法接口实现对密码资源的使用。

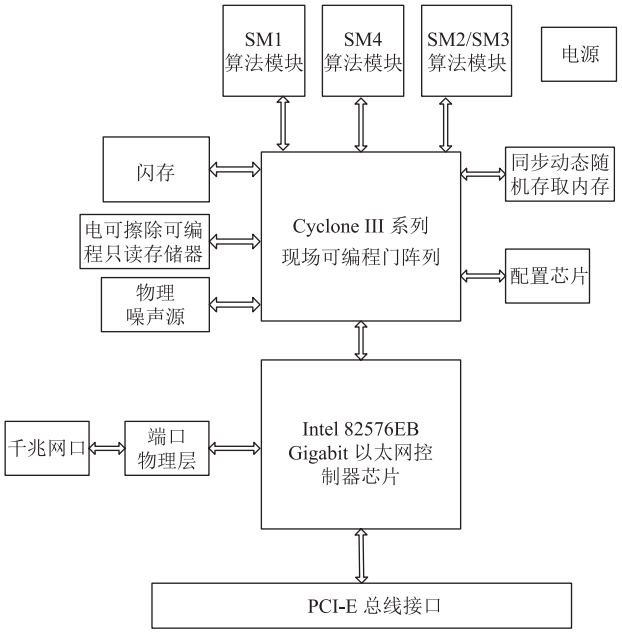


图 5 基于 SR-IOV 技术的硬件虚拟化密码卡架构

Fig. 5 Hardware virtualization cryptographic card architecture based on SR-IOV technology

4.3 基于 SR-IOV 软核的硬件虚拟化密码卡(方案 3)

该方案与方案 2 类似，采用了高性能的 Altera FPGA 代替 Intel 82576EB 芯片实现 SR-IOV 协议，系统架构如图 6 所示。方案 3 采用 FPGA 与 PCI-E 物理总线进行连接，但需要在 FPGA 中通过硬件逻辑设计实现 SR-IOV 协议，因此需要采用 Altera 中端 Arria 系列或高端 Stratix 系列的 FPGA 才能满足设计需求。其中，为深入了解 SR-IOV 协议并实现协议的每一个细节，开发 SR-IOV 硬件逻辑的周期为 6 个月以上。因此，为缩短开发周期，通常需要购买 Altera 或其他厂商的自主知识产权的 SR-IOV 协议 IP 软核，嵌入到 FPGA 中进行开发。

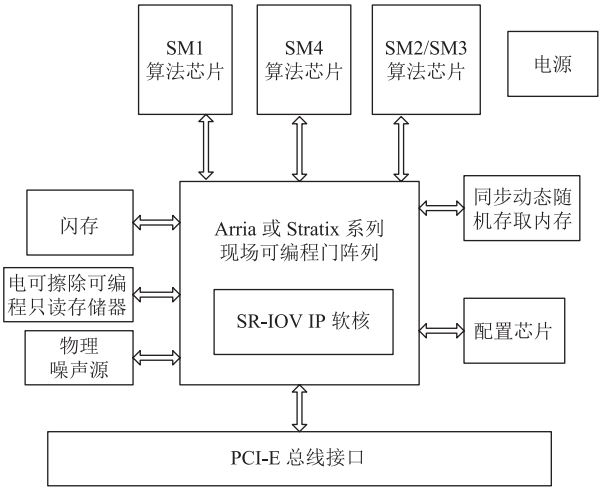


图 6 基于 SR-IOV IP 软核的硬件虚拟化密码卡架构

Fig. 6 Hardware virtualization cryptographic card architecture based on SR-IOV soft IP core

5 设计实现与应用

5.1 设计实现

通过上述方案 1～3 比较可知，方案 3 不仅需要购买 IP 软核(费用为 1 万美金)，而且根据以往的开发经验，基于软核的开发、调试难度也

大。因此，与方案 1、方案 2 相比，方案 3 存在开发周期长、开发成本高的风险。可见，采用方案 1 和方案 2 是切实可行的办法。目前已完成针对方案 1 和方案 2 的密码卡虚拟化技术的设计开发。其中，图 7 是方案 1 部署密码卡软件虚拟化作为计算节点的虚拟化应用系统图；图 8 是方案 2 基于 SR-IOV 技术的硬件虚拟化密码卡实物图。

图 7　密码卡软件虚拟化系统界面

Fig. 7　System interface of cryptographic card software virtualization

以下对方案 1 和方案 2 的密码算法性能进行测试与对比分析。测试环境为浪潮 Romley 服务器，服务器配置为：Intel Xeon E5-2600 处理器，DDR3 内存，160 GB SATA 硬盘，Red Hat 6.5 操作系统。测试过程中逐渐增加虚拟机的数量，并在开启不同虚拟机数量时对方案 1 和方案 2 的各种密码算法性能进行测试，具体测试结果如图 9～12 所示。其中，图 9 为 SM1 算法的性能对比，图中标注了物理密码卡的 SM1 性能作为参照结果显示，在只开启 2 个虚拟机(Virtual Machine，VM)的情况下，方案 1 的软件实现方法与方案 2 的硬件实现方法性能相当，都接近物理密码卡的性能 1 000 Mb/s；当逐渐增加 VM 数量时，方案 1 比方案 2 的 SM1 算法性能衰减明显；当 VM＝10 时，方案 1 的性能衰减为 200 Mb/s，仅为物理密码卡性能的 20%，而方案 2 尽管有 50% 的性能损失，但 500 Mb/s 的加密性能足以满足用户的需求。同理，图 10 为 SM4 对称密码算法的性能对比，在 VM＝10 时，方案 1 的 SM4 加密性能为 500 Mb/s，而方案 2 能够达到 1 000 Mb/s；

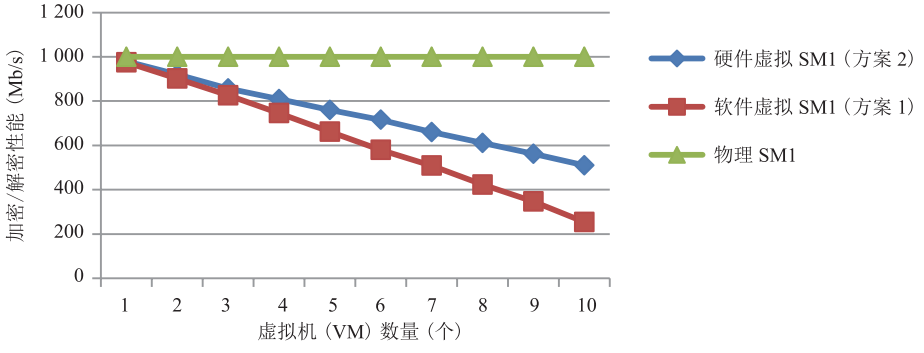


图 9　SM1 算法性能对比

Fig. 9　Performance comparison of SM1 algorithm

图 8　基于 SR-IOV 技术的虚拟化密码卡实物图

Fig. 8　Physical chart of virtualized cryptographic card based on SR-IOV technology

图 11 为 SM3 密码杂凑算法的性能对比，同样在 VM＝10 时，方案 2 的性能接近 1 Gb/s，是方案 1 性能的 2 倍；图 12 为公钥算法 SM2 签名的性能对比，在 VM＝10 时，方案 2 的 SM2 签名值速度为 330 次/s，而方案 1 仅有 153 次/s。由以上对比实验可知，随着虚拟机数量的增加，软件虚拟化方式性能衰减明显，其中在虚拟机数量为 10 个时，软件实现方案的性能仅为物理密码卡性能的 20%，而硬件虚拟化方案的性能超过了物理性能的 50%，能够满足用户加解密的性能需求。

我国《商用密码管理条例》第十四条规定，任何单位只能使用经国家密码管理机构认可的商

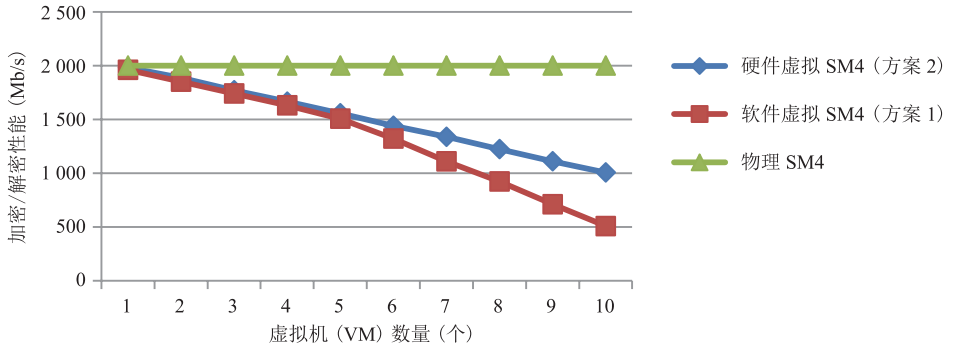


图 10　SM4 算法性能对比

Fig. 10　Performance comparison of SM4 algorithm

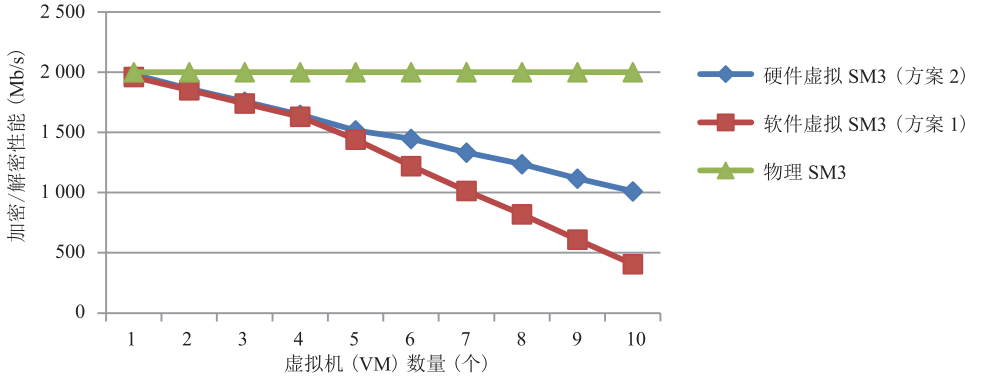


图 11　SM3 算法性能对比

Fig. 11　Performance comparison of SM3 algorithm

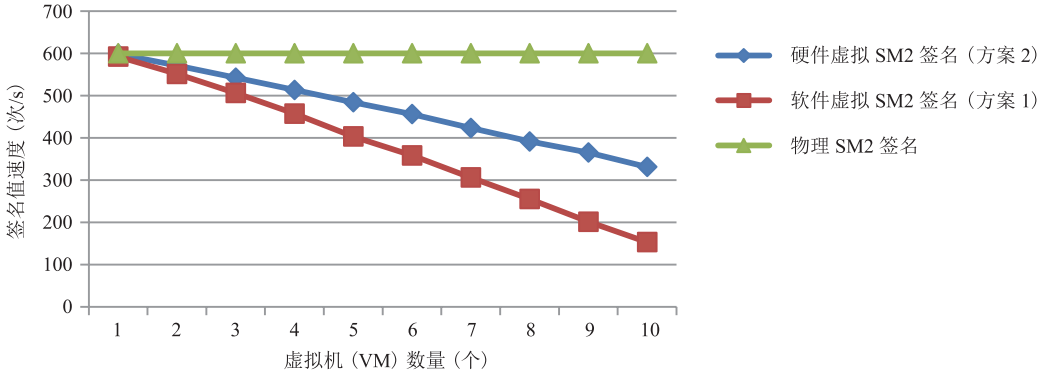


图 12　SM2 签名算法性能对比

Fig. 12　Performance comparison of SM2 signature algorithm

用密码产品，不得使用境外生产的密码产品[18]。由于密码卡作为特殊的商用密码产品，国家是严格管控的，不允许使用国外的密码产品，因此在同类产品的对比分析方面，本文只与国内的同类产品进行对比。

经过调研，国内大多数密码卡产品是功能单一的物理硬件板卡，如基于 PCI、PCI-E 接口设计实现，并提供国产密码算法功能[19]。在虚拟化密码卡产品研发和实现方面，国内大多数公司尚处于研究和实验阶段，还未形成产品化。在业界较为知名的公司中，北京三未信安公司提出基于 SR-IOV 技术密码卡硬件虚拟化解决方案[20]，该密码卡能够在 KVM、XEN 等虚拟机环境下应用，但并未公布具体的密码算法虚拟化性能数据。江南天安[21]、得安科技[22]公司分别在产品手册和宣传材料中说明了密码设备支持虚拟化功能，但未公布具体的性能指标。天融信[23]、山东渔翁[24]等作为行业中优秀的信息安全公司，也未推出虚拟化密码卡。在国内研究成果中，马龙宇[6]在 3 个 VF 同时进行 SHA1 运算的条件下，每个客户机系统调用 SHA1 算法的性能为 160 MB/s，但 SHA1 算法本身已被破解，安全性差，只能应用于安全性较低的场合。杨维永等[25]设计的密码卡虚拟化可信平台，实现的 SM4 算法经虚拟化后的性能只有 100 Mb/s，远低于本文实现的虚拟 SM4 算法性能(1 000 Mb/s)。由此可知，本文实现的虚拟化密码卡在国内同类产品中具有较高的性能优势。

5.2　应用场景

设计实现的方案 1 和方案 2 虚拟化密码卡的产品形态是以硬件板卡的形式内置于安全服务器、可信服务器中。其中，物理接口为 PCI-E，符合 PCI Express 接口规范 V2.0 及以上；板卡具备国内对称密码算法 SM1 和 SM4、非对称椭圆曲线密码算法 SM2 和密码杂凑算法 SM3，提供高速的数据加解密、数字签名、验证签名、杂凑运算等功能。板卡提供虚拟化的功能，支持 XEN 和 KVM 等虚拟机，同时具备千兆网口，实现网络通信的功能。

目标客户为金融、电信、政府、电子商务等领域，具体应用场景见表 1。本文设计的虚拟化密码卡集成到浪潮服务器 NF8480、i48 等产品型号中，已应用于国家电网试点、北京科委可信计算池等项目，用于解决虚拟环境中的数据安全问题，应用前景广阔。

6　结　语

针对密码卡虚拟化技术实际应用不足的现状，本文详细分析了密码卡虚拟化的技术架构，在密码卡虚拟化模型的基础上提出了 3 种设计方案并给出了软硬件设计流程，最终设计并实现了软件和硬件两种方式的虚拟化密码卡：(1) 软件虚拟化是基于 FPGA 的物理密码卡，通过设计驱动软件和虚拟化中间件的方式实现了虚拟化功能；(2) 硬件虚拟化是基于 Intel 的专用控制芯

表 1　密码卡虚拟化应用场景

Table 1　Application scenarios for cryptographic card virtualization

应用场景	典型应用系统
公钥（PKI）基础设施	数字证书管理系统、密钥管理系统
安全产品	签名验证服务器、安全认证网关、虚拟专用网络（VPN）、可信服务器、安全主机
安全应用系统	文件加密系统、身份管理系统
云服务	云存储、身份认证
企业核心应用系统	企业资源计划系统（ERP）、安全数据交换系统

片和 FPGA，通过 SR-IOV 技术设计实现了硬件虚拟化加密卡。与传统 I/O 设备的虚拟化方案相比，本文技术方案的创新性在于采用了 SR-IOV 技术，使各虚拟终端对密码卡的操作不会受到虚拟机相互之间的影响，并且通过 FPGA 对密码芯片的调度使得每个虚拟机调用密码算法的性能能够接近真实物理密码卡的算法性能。因此，本文设计的虚拟化密码卡能够解决现有虚拟化技术密码算法性能较低的问题，同时利用国产密码算法能够有效提升产品的安全性。该技术已应用于浪潮高端服务器、安全服务器等产品中，具有较好的应用前景，有效地填补了市场的空白。后续工作可通过将物理 PCI-E 总线接口由目前的 ×4 扩展为 ×16 规格，以便进一步提升密码算法的运算性能。

参 考 文 献

[1] 王玉净, 杜君, 李延, 等. 一种支持国密算法的 miniPCI-E 密码卡设计 [J]. 单片机与嵌入式系统应用, 2018, 18(1): 34-37.

[2] 刘涛. 支持动态迁移的加密卡设备虚拟化 [D]. 武汉: 华中科技大学, 2016.

[3] 张嘉夫. 基于密码卡虚拟化的虚拟桌面隐私保护研究 [D]. 武汉: 华中科技大学, 2017.

[4] 李玉玲. 云计算环境下密码算法模型的研究与实现 [D]. 济南: 山东大学, 2016.

[5] Berger S, Cáceres R, Goldman KA, et al. vTPM: virtualization the trusted platform module [C] // Proceedings of the 15th Conference on USENIX Security Symposium, 2006: 305-320.

[6] 马龙宇. 基于 SR-IOV 虚拟化技术高速密码卡的设计与实现 [D]. 上海: 上海交通大学, 2016.

[7] 杨永娇, 严飞, 于钊, 等. 一种基于 VT-d 技术的虚拟化安全隔离框架研究 [J]. 信息网络安全, 2015(11): 7-14.

[8] 金海. 计算系统虚拟化——原理与应用 [M]. 北京: 清华大学出版社, 2010.

[9] 李超. SR-IOV 虚拟化技术的研究与优化 [D]. 长沙: 国防科学技术大学研究生院, 2010.

[10] Intel Corporation. Intel® virtualization technology for directed I/O [EB/OL]. 2018[2018-11-13]. https://software.intel.com/sites/default/files/managed/c5/15/vt-directed-io-spec.pdf?wapkw=intel.

[11] AMD. AMD I/O virtualization technology (IOMMU) specification [EB/OL]. 2009[2018-11-13]. http://developer.amd.com/wordpress/media/2012/10/34434-IOMMU-Rev_1.26_2-11-09.pdf.

[12] PCI-SIG. Single root I/O virtualization and sharing specification revision 1.1 [EB/OL]. 2010[2018-11-13]. https://members.pcisig.com/wg/PCI-SIG/document/download/8238.

[13] 刘明达, 马龙宇. 一种基于 SR-IOV 技术的虚拟环境安全隔离模型 [J]. 信息网络安全, 2016(9): 84-89.

[14] PCI-SIG. PCI express base specification revision 3.0 [EB/OL]. 2010[2018-11-13]. https://members.pcisig.com/site/login?return=%2Fwg%2FPCI-SIG%2Fdocument%2Fdownload%2F8265.

[15] Altera Corporation. IP compiler for PCI express user guide [EB/OL]. 2014[2018-11-13]. https://www.intel.com/content/dam/www/programmable/us/en/pdfs/literature/ug/ug_pci_express.pdf?wapkw=ip+compiler+for+pci+express+user+guide.

[16] Intel Corporation. Intel® 82576EB gigabit ethernet controller [EB/OL]. 2018[2018-11-13]. https://ark.intel.com/content/www/us/en/ark/products/37166/intel-82576eb-gigabit-ethernet-controller.html.

[17] Altera Corporation. Cyclone III device handbook [EB/OL]. 2012[2018-11-13]. http://www.altera.com.https://www.intel.com/content/dam/www/programmable/us/en/

pdfs/literature/hb/cyc3/cyclone3_handbook.pdf?wapkw=cyclone+iii+handbook.

[18] 国家密码管理局. 商用密码管理条例 [EB/OL]. 1999.10[2018-11-13]. http://www.oscca.gov.cn/sca/xxgk/1999-10/07/content_1002578.shtml.

[19] 国家密码管理局. 商用密码产品目录(共 1963 项)[EB/OL]. 2018[2018-11-13]. http://www.oscca.gov.cn/app-zxfw/cpxx/symmcp2.jsp?manuscript_id=1000038.

[20] 三未信安. 虚拟化高速密码卡方案 [EB/OL]. 2018[2018-11-13]. http://www.sansec.com.cn/html/jjfa/mmcpyjhfa/106.html.

[21] 江南天安. 产品&服务手册 [EB/OL]. 2018[2018-11-13]. http://www.tass.com.cn/upload/file/5f49ad7a-84f4-4424-8839-26519ed3b4b4.pdf.

[22] 崔传桢, 田霞. 得安, 密码创新护航网络安全 20 年——基于网络强国背景下的得安集团信息安全及战略 [J]. 信息安全研究, 2017, 3(10): 866-878.

[23] 崔传桢. 天融信, 自主创新助力网络强国战略 [J]. 信息安全研究, 2018, 4(9): 774-782.

[24] 山东渔翁信息技术有限公司. PCI-E 加密卡产品详情 [EB/OL]. 2018[2018-11-13]. https://www.fisec.cn/202.html.

[25] 杨维永, 刘金锁, 屠正伟, 等. 基于密码卡的虚拟化可信平台设计 [J]. 信息技术, 2016(1): 171-176.