基于龙芯处理器的自主可信计算机研究

赵 斌[1],杨明华[2],柳 伟[3],冯 磊[1],路永轲[1]
(1. 山东超越数控电子有限公司,山东 济南 250104;
2. 第二炮兵装备研究院,北京 100094;
3. 北京理工大学 计算机学院,北京 100081)

摘 要:“斯诺登”事件再一次证明,采用国外关键软硬件的计算机具有不可控的漏洞和后门,信息系统采用非自主的计算机给国家、企业、军队带来安全威胁。文中设计并实现了一种安全可信计算机,采用国产龙芯处理器,减少了后门安全隐患,通过设计板载可信密码模块、端口控制电路和身份认证装置,实现了 BIOS 主动度量恢复,硬件级的端口控制和身份认证功能,同时实现了对硬件、MBR、操作系统的完整性保护功能。通过实验测试表明,文中设计实现的安全可信计算机原理样机具备身份认证、主动度量 BIOS、端口控制、完整信任链保护等安全可信功能,大大提高了计算机的安全性。

关键词:可信计算;主动度量;龙芯处理器;端口控制;可信引导
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2015)03-0126-05
doi:10.3969/j.issn.1673-629X.2015.03.029

Research on Security & Trust Computer Based on Loongson CPU

ZHAO Bin[1], YANG Ming-hua[2], LIU Wei[3], FENG Lei[1], LU Yong-ke[1]
(1. Shandong Chaoyue Electronics Co., Ltd., Jinan 250104, China;
2. The Second Artillery Equipment Academy, Beijing 100094, China;
3. School of Computer, Beijing Institute of Technology, Beijing 100081, China)

Abstract: The event of "Snowden" once again proved that using foreign computers has not controllable bug and backdoor, information system using foreign computer poses a security threat to the state, enterprises and troops. In this paper, design and implement a trust & security computer, using Native Loongson CPU, reducing the security risks of back door, through the design of on-board trusted cryptographic module, port control circuit and authentication devices to achieve the initiative measurement of BIOS, BIOS restoring, hardware levels port control and authentication functions. Moreover, implement the integrity protection of the hardware, MBR and OS. The experiments indicated that the security trusted computer principle prototype designed and implemented in this paper has implemented the identity authentication, active measurement of BIOS, port control, complete chain of trust protection, which can greatly enhance the security of computer.

Key words: trusted computing; initiative measurement; Loongson CPU; port control; trusted boot

0 引 言

近年来,信息系统安全事件频发,计算机安全越来越受到企业、政府和国家的重视。多种泄密事件表明,采用国外核心硬件的计算机具有不可控的漏洞和后门,具备更大的安全隐患,采用自主可控的核心硬件对信息安全具有重要的意义。随着国产处理器、国产固件、国产操作系统的发展和成熟,自主可控国产化计算机是大势所趋。以国产 CPU 为例,近几年,我国在自主处理器芯片上加大研发投入,已经研发出多款处理器芯片,如龙芯系列处理器、飞腾系列处理器、UniCore 系列处理器、国芯系列处理器、申威系列处理器等[1-2]。国内自主处理器的现状如图 1 所示。

我国自主操作系统也已取得较大发展[3],推出了中标麒麟服务器操作系统、中标麒麟桌面操作系统、ReWorks 嵌入式实时操作系统、天熠实时操作系统等产品。在自主数据库方面,国内主要包括达梦、神舟 OSCAR、金仓等通用数据库,以及天熠等嵌入式实时数据库产品。在计算机外围部件(如内存、外存、显示

收稿日期:2014-04-30 **修回日期**:2014-07-30 **网络出版时间**:2015-01-20
基金项目:国家自然科学基金资助项目(61063042);中国博士后科学基金项目(201104753);北京市自然科学基金项目(4132025)
作者简介:赵 斌(1981-),男,硕士,研究方向为可信计算、信息安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20150120.2202.033.html

屏、电源、安全控制芯片)、办公软件、服务中间件等方面,我国也有了相应的自主技术和产品。

但是,由于计算机本身的体系架构的缺陷,采用自主核心硬件不等于完全安全,仍然存在着 BIOS 被恶意篡改、信息泄漏、非授权访问、缺乏系统完整性保护等安全缺陷。

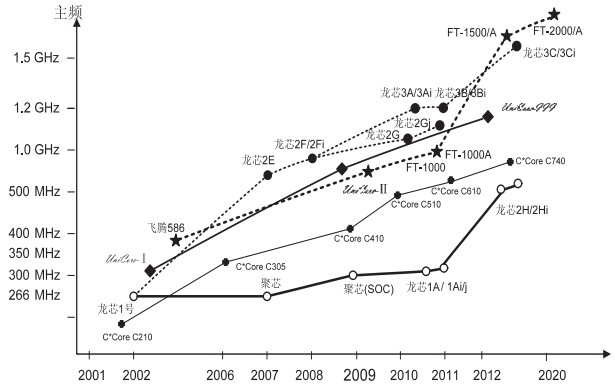

图 1　自主处理器芯片发展现状和趋势示意图

可信计算技术[4]通过在计算机平台中植入可信密码芯片作为可信根,对计算机体系结构进行改造,使用户拥有安全性、完整性和可靠性全面提高的可信赖计算环境成为可能[5-6]。国际上,可信计算技术已经得到了长足发展[7],按照 TCG 组织规范[8]的 TPM 芯片已经广泛应用,可信计算产品已经覆盖了计算机、服务器、移动终端和网络等众多领域[9-10]。我国更是提出了自己的可信计算标准,文献[11]以国产可信密码芯片为基础,提出了一种可信平台控制模块(Trusted Platform Control Modules,TPCM),对 TPM 架构进行了改进,具备密码运算器和受保护的存储器,内嵌自主知识产权密码算法,具有主动控制功能、模块固件支持扩展安全功能,为实现更加安全的可信计算平台构建了硬件基础。

文中基于国产龙芯处理器,将可信密码芯片与自主主板进行一体化设计,实现主动度量恢复 BIOS 功能、硬件级端口控制功能和强制身份认证功能,集成国产可信固件和国产操作系统,实现了一种自主可控安全可信计算机。

1　基于龙芯处理器的自主可信计算机架构设计

文中实现的可信计算机采用标准 ATX 主板形式,选用龙芯 3A 处理器,支持两个 DDR3 内存,工作频率可达 1 GHz。龙芯 3A 处理器[12]通过 HT 总线与北桥连接,北桥芯片集成显示核心,支持 VGA、DVI 输出,具有 PCI-E 链路扩展以太网接口,同时提供 1 路 PCIEx1 与可信密码模块进行可信数据通信。南桥芯片实现 SATA 接口、USB 接口和 PCI 插槽等丰富 I/O 接口,主板还集成端口控制芯片用来与可信密码模块交互完成可信端口控制。

可信密码模块作为信任根集成到自主主板上,通过自定义 PCIE 接口与主板衔接。其中,为了实现主动度量 BIOS 控制,设计主动度量切换电路进行 CPU 复位控制,同时 BIOS 芯片 LPC 信号通过自定义 PCIE 接口与可信密码模块衔接,提供开机时主动读取 BIOS 进行完整性度量的通路。自定义 PCIE 接口设计端口控制信号线分别与主板网络芯片、串口芯片和 USB 端口控制芯片衔接,实现硬件端口的可信控制,自定义 PCIE 接口通过一路 PCIEx1 接口与北桥衔接,实现可信密码服务数据通路。可信计算机前面板进行了安全状态和智能卡读卡器设计,分别与可信密码模块衔接完成开机身份认证和可信状态的指示。

基于龙芯处理器的安全可信计算机原理框图如图 2 所示。

2　关键设计

2.1　信任根设计

可信密码模块作为安全可信计算机的信任根,是整个平台的安全基础,为平台提供可信度量、可信存储和可信报告的功能。国外可信计算标准芯片 TPM 采用 LPC 接口,只作为从设备提供密码运算,处理速度有限,不能满足度量 BIOS、操作系统内核等较大数据量可信计算的需求。同时 TCG 标准规定 BIOS 的 CRTM 作为可信度量根的起点,可信度量根不存在于可信芯片中,给安全性带来隐患[13]。

文中设计实现的安全可信计算机采用我国 TPCM 架构设计可信密码模块作为信任根,以可信密码模块为度量根起点,通过在自主主板上集成设计可信密码模块电路单元,确保信任根硬件上不可移除,做到度量根、存储根和报告根的统一。可信密码模块以可信密码芯片为核心单元,可信密码芯片为一块专用 32 位高性能安全 SOC 芯片,芯片采用软硬件协同的方式实现 ECC 公钥算法、对称加密算法以及可信杂凑算法,给平台提供可信度量、可信存储和可信报告服务。

可信密码模块设计实现自定义 PCIE 接口,在标准 PCIE 接口的基础上增加 CPU 复位控制、主动度量控制、LPC 和端口控制信号定义,通过 PCIEx1 总线可提供高速数据通信,模块扩展了一块 2 GB Nand Flash 存储器用来存放 BIOS 备份数据、操作系统备份数据以及用户自定义备份文件。

可信密码模块通过开发固件程序实现可信安全功能,固件程序主要包括智能卡认证模块、状态指示模块、安全控制模块,安全控制模块完成开机上电时序控制和主动度量控制功能,智能卡认证模块实现 7816 信

号控制完成登录认证逻辑,状态指示模块通过状态信号控制前面板指示灯显示度量、认证和引导过程中的安全状态。图 3 描述了板载可信密码模块设计和主板接口关系的原理框图。

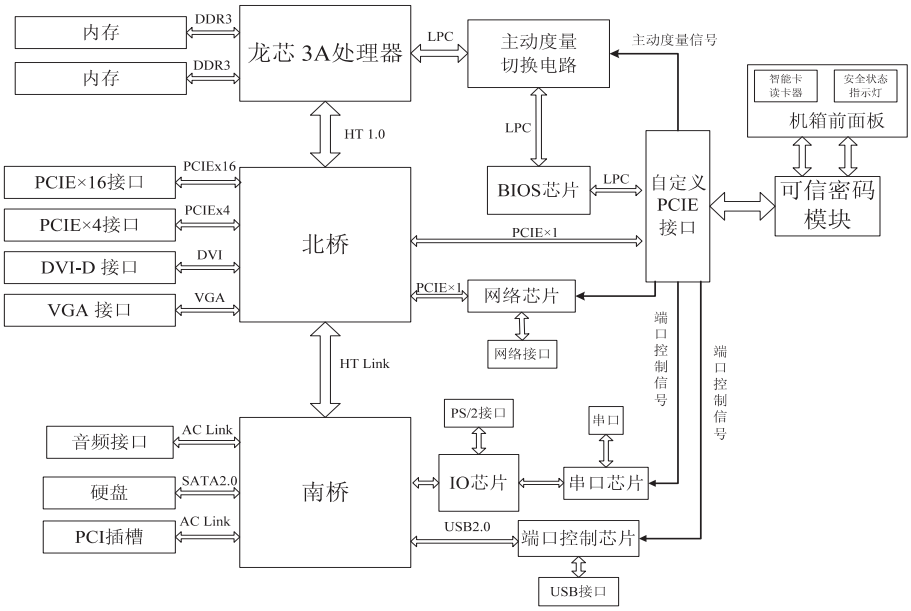

图 2 基于龙芯处理器的安全可信计算机原理框图

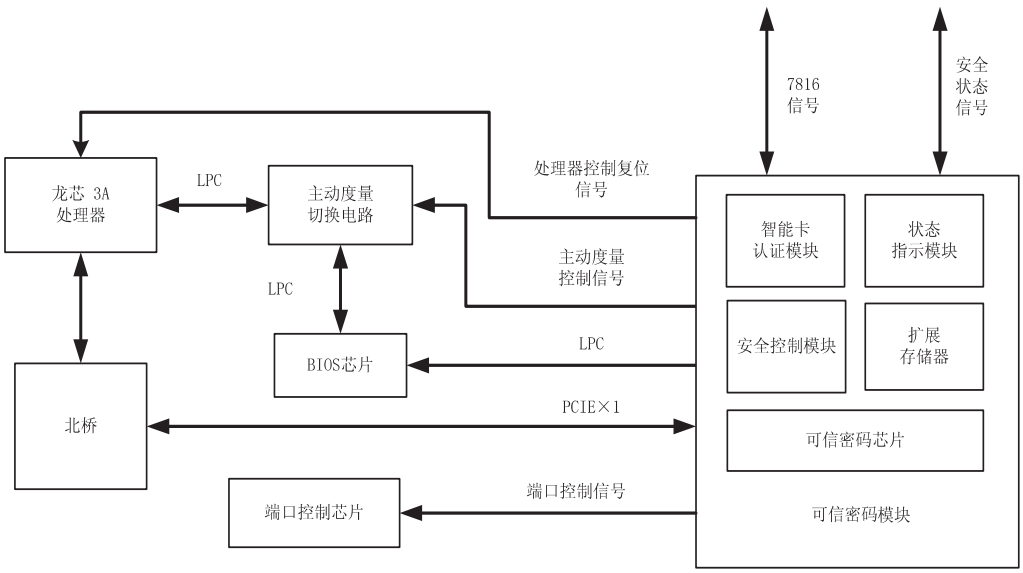

图 3 板载可信密码模块及接口原理框图

2.2 主动度量与可信恢复

文中设计实现的安全可信计算机以可信密码模块为信任根起点,开机加电由可信密码模块首先对 BIOS 进行完整性度量。根据龙芯 3A 处理器的特点,计算机上电后,时钟电路开始工作,时钟稳定后,系统会发出 CPU 及外设的复位信号,从而完成后续硬件启动过程,之后 BIOS 开始启动,龙芯 3A 处理器与 BIOS 之间通过 LPC 总线连接。

可信密码模块设计 LPC 接口与 BIOS 芯片连接实现 BIOS 度量和恢复通路,模块与 CPU 竞争访问 BIOS 由可信密码模块内部固件进行逻辑控制。在 BIOS 启动之前的这一阶段,通过模块上的固件编程实现安全控制模块代码完成对 BIOS 的主动读取,通过复位控制信号输出主动度量切换电路控制在度量开始一直到度量结束的这段时间内一直将 CPU 的复位信号置为有效,即在度量过程中,CPU 一直处于复位状态,在度量完成之后复位 CPU,主动度量切换电路导通 CPU 到 BIOS 的通路,完成正常启动流程。度量过程为安全控制模块调用可信密码芯片杂凑算法对 BIOS 数据杂凑计算的过程,当计算结果与可信密码芯片内预存的基准值不符合时,安全控制模块中的恢复引擎代码从扩展存储器中读取备份 BIOS 写入 BIOS 芯片完成恢复。此外,扩展存储器中还备份有 MBR、操作系统内核等其他计算机部件的可恢复数据,在后续 BIOS 启动过程中对硬件 ROM、MBR、操作系统内核、用户关键文件的度量和恢复同样采取以上方法。

2.3　信任链设计

信任根作为安全可信计算机的安全硬件基础提供可信密码学服务,信任链是以信任根为起点的一条系统保护链条。信任链的建立过程就是对计算机从底层到上层的安全保护过程,在计算机启动各阶段调用可信密码模块的可信密码功能服务,根据处理器计算平台工作原理、硬件组成、系统启动、引导和加载等机制,从底层到上层逐级建立安全可信计算机的信任链。

文中所设计信任链以可信密码模块为根节点,调用可信密码算法依次实现对可信 BIOS、各启动硬件及 OptionROM、OSLoader 及 MBR、操作系统、应用软件等软硬件内容的完整性验证度量,系统启动以后通过软件服务提供接入可信网络的接口,将信任链继续传递到可信网络。

信任链建立过程中可信密码模块 PCR(平台寄存器)中存储度量结果,并记录事件日志,同时通过扩展存储器中预存各个度量部件的原始数据,设计各阶段度量失败时的恢复机制,在度量失败时能够恢复相应数据,保持信任链的完整传递,设计用户身份认证机制、平台硬件端口控制策略保证信任链的访问安全和端口安全,启动操作系统以后,由应用软件提供文件加密、用户管理、端口控制管理、可信完整性保护、信任链更新和可信网络连接功能。信任链模型如图 4 所示。

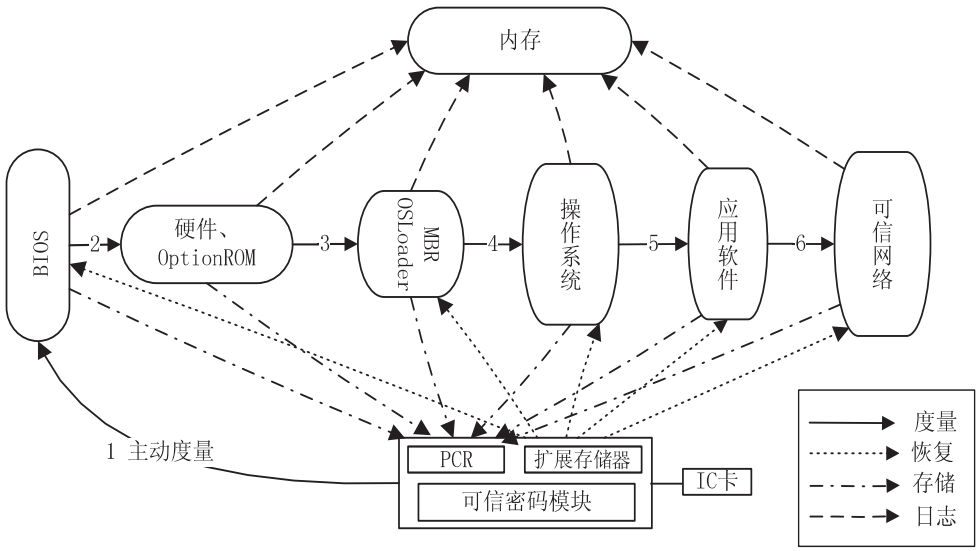

图 4　信任链模型

3　安全可信引导过程

植入可信根的计算机平台通过加入可信服务保证平台的安全可信引导[14],文中基于龙芯处理器的安全可信计算机通过可信硬件设计提供了可信控制的基础功能接口。文中计算机采用了国产可信 BIOS 和国产操作系统,国产可信 BIOS 通过加入可信控制代理实现对硬件、国产操作系统内核的引导和完整性保护,整个安全可信引导过程为:

Step1:可信密码模块首先上电,通过 7816 信号与机箱前面板的读卡器进行通信,根据用户插入的 IC 卡进行认证判断,认证过程在前面板状态指示灯进行显示,认证成功后进行主动度量控制;

Step2:可信密码模块下发主动度量控制信号给主动度量切换电路进行复位控制,可信密码模块通过 LPC 接口读取 BIOS 内容进行主动度量,度量成功后处理器复位,继续执行 Step4;否则执行 Step3;

Step3:主动度量失败后通过可信密码模块扩展存储器中的备份 BIOS 恢复主板上的 BIOS 数据;主动度量和恢复的过程在前面板状态指示灯分别显示;

Step4:可信密码模块读取用户 IC 卡中的端口控制策略,通过相应的端口控制信号下发给主板上端口控制芯片执行串口、网口、USB 口的端口开闭控制;

Step5:完成可信安全控制后继续启动 BIOS,启动过程中调用可信密码模块度量接口分别对主板上的硬件 ROM、MBR、操作系统内核和用户关键文件进行度量验证,完成整个系统引导过程的完整性保护。

4　设计成果

通过自主可信主板设计,适配国产可信 BIOS,国产操作系统,实现了基于龙芯 3A 处理器的安全可信计算机原理样机。图 5 所示为板载可信密码模块的自主可信主板和原理样机。

5　测试实验

文中对基于龙芯处理器的安全可信计算机样机功能进行了测试。主要测试了安全可信计算机的身份认证、BIOS 主动度量、各部件度量和可信恢复、端口控制

等相关功能。功能测试项目如表 1 所示。测试结果显示,安全可信计算机中基于 IC 卡身份认证、BIOS 主动度量和恢复、计算机各启动部件的完整性度量和可信恢复、端口控制功能符合预期设计。

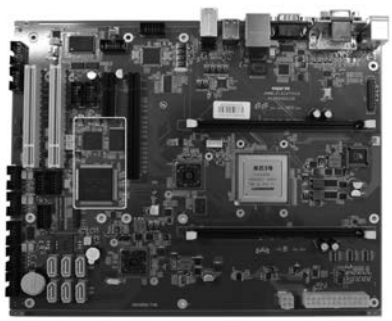

图 5 自主可信主板和基于龙芯处理器的安全可信计算机原理样机

表 1 基于龙芯处理器的安全可信计算机测试结果

测试功能	测试用例	测试结果
身份认证	插入 IC 卡输入用户密码验证	无 IC 卡无法启动,插入 IC 卡输入正确密码启动计算机
BIOS 主动度量	度量验证 BIOS 完整性	能够度量验证
BIOS 恢复	破坏 BIOS 数据后验证 BIOS 是否可以恢复	能够恢复
安全状态指示	主动度量状态灯动态显示 身份认证状态动态显示	度量成功和失败具有状态灯指示 认证成功失败具有状态灯指示
硬件度量	硬盘特征值度量 PCI 设备特征值度量 网卡特征值度量 显卡特征值度量	能够度量验证 能够度量验证 能够度量验证 能够度量验证
OSLoader 度量恢复	OSLoader 度量验证,破坏数据后验证是否可以恢复	能够度量验证和恢复
MBR 度量恢复	MBR 度量验证,破坏数据口验证是否可以恢复	能够度量验证和恢复
操作系统度量恢复	操作系统内核、关键文件度量,破坏数据后验证是否可以恢复	能够度量验证和恢复
应用软件度量	指定应用程序度量验证及数据恢复	能够度量验证和恢复
信任链管理	BIOS 层信任链更新 系统层信任链更新	能够更新 BIOS、硬件预期值 能够更新指定应用和文件预期值
端口控制	网口、USB 口、串口开启关闭验证	能够开启关闭指定端口

6 结束语

文中设计实现了一种基于龙芯处理器的安全可信计算机,通过采用国产龙芯处理器等核心硬件,减少了采用国外核心硬件的后门隐患。主板集成可信密码模块作为信任根,对计算机体系结构进行可信改造,能够主动对 BIOS、计算机主要硬件进行完整性保护,通过在主板增加控制电路,对硬件端口进行开启关闭控制,提高了端口使用安全性,提供基于可信密码模块的身份认证功能,增强了计算机访问控制的安全性。下一步工作中,将基于安全可信平台提供的可信接口对系统启动以后的软件运行环境进行动态度量研究和设计。

参考文献:

[1] Hu Weiwu, Zhang Fuxin, Li Zusong. Microarchitecture of the Godson-2 processor[J]. Journal of Computer Science and Technology, 2005, 20(2): 243-249.

[2] 胡伟武,张福新,李祖松. 龙芯 2 号处理器设计和性能分析[J]. 计算机研究与发展,2006,43(6):959-966.

[3] 吴玲达,吕雅帅,杨 超,等. 国产基础软硬件集成应用攻关关键技术研究[J]. 装备学院学报,2013,24(5):1-6.

[4] Marshall D A, Michael V J. Trusted computing update[J]. Computer & Security, 1995, 14(1): 57-68.

[5] Challener D. 可信计算[M]. 赵 波,译. 北京:机械工业出版社,2009.

[6] 刘 宁. 基于 TPM 的可信计算的研究[J]. 北京机械工业学院学报,2008,23(4):50-52.

[7] Pearson S. Trustedcomputing platform, the next security solutin[R]. Bristol: HP Laboratories, 2002.

[8] TCG. TCG specification architecture overview[EB/OL]. 2008-01-12. http://www.trustedcomputinggroup.org/groups/TCG_1_1_Architecture_Overview.pdf.

[9] 陈建勋,侯方勇,李 磊. 可信计算研究[J]. 计算机技术与发展,2010,20(9):1-4.

[10] 张 颖,周长胜. EFI 下基于便携式 TPM 的可信计算平台研究[J]. 计算机技术与发展,2010,20(1):167-171.

[11] 张 兴,沈昌祥. 一种新的可信平台控制模块设计方案[J]. 武汉大学学报:信息科学版,2008,33(10):1011-1014.

[12] 龙芯 3A 处理器数据手册[S]. 北京:北京龙芯中科技术服务中心有限公司,2009.

[13] 张海明. EFI 下可信链建立关键技术研究与实现[D]. 北京:北京交通大学,2008.

[14] 谭 良,周明天. 基于可信计算平台的可信引导过程研究[J]. 计算机应用研究,2008,25(1):232-234.

基于龙芯处理器的自主可信计算机研究

作者： 赵斌， 杨明华， 柳伟， 冯磊， 路永轲， ZHAO Bin， YANG Ming-hua， LIU Wei， FENG Lei， LU Yong-ke

作者单位： 赵斌,冯磊,路永轲,ZHAO Bin,FENG Lei,LU Yong-ke(山东超越数控电子有限公司,山东 济南,250104)， 杨明华,YANG Ming-hua(第二炮兵装备研究院,北京,100094)， 柳伟,LIU Wei(北京理工大学 计算机学院,北京,100081)

刊名： 计算机技术与发展 ISTIC

英文刊名： Computer Technology and Development

年，卷(期)： 2015(3)