(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 111435396 A
(43)申请公布日 2020.07.21

(21)申请号 201910034048.7

(22)申请日 2019.01.15

(71)申请人 量子芯云(北京)微电子科技有限公司
地址 100164 北京市丰台区方庄南路58号院5-4-602

(72)发明人 许丰

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/72(2013.01)

权利要求书2页 说明书3页

(54)发明名称

智能安全主控

(57)摘要

本发明公开了一种智能安全主控,由一个或多个大核处理器组成的主控模块、电源管理模块、多个能够并发协作的小核处理器组成的硬件加速模块和具备抗攻击单向计数器的硬件加密模块组成;所述智能安全主控具备FLASH控制器和DRAM控制器功能,主接口支持PCI Express系列标准,经过版图重构和加扰数据线设计,具备时钟探测电路,具备符合国际及国密标准的高性能加密引擎以及抗攻击单向计数器的硬件电路。所述智能安全主控芯片具备高安全与高性能,适于安全存储控制器,服务器加速卡,物联网安全主控模块,边缘计算节点设备和人工智能安全主控模块,是覆盖万亿元人民币市场规模的存储器、物联网和人工智能行业必备的关键部件。

CN 111435396 A

1.一种智能安全主控,其特征在于,由一个或多个大核处理器组成的主控模块、电源管理模块、多个能够并发协作的小核处理器组成的硬件加速模块和具备抗攻击单向计数器的硬件加密模块组成;所述智能安全主控具备FLASH控制器和DRAM控制器功能,主接口支持PCI Express系列标准;所述硬件加速模块具备缓冲加速和特定运算加速功能;所述硬件加密模块经过版图重构和加扰数据线设计,具备时钟探测电路,具备符合国际及国密标准的高性能加密引擎以及抗攻击单向计数器的硬件电路,所述抗攻击单向计数器采用双路互补校验计数器;所述双路互补校验计数器的设计是每路计数器由一个符合特定规律的数字转盘组成,且只能够单方向运转,但两个计数器的当前数值经过运算后满足特定规律,这样能够保护总体计数器的合法性,当试图通过破坏性攻击修改任一路计数器时,由于无法精确修改另一路计数器对应的匹配值,导致计数器校验不通过。

2.根据权利要求1中所述的智能安全主控,其特征在于,所述主控模块至少包括一个安全SPU,所述安全SPU即安全CPU,是基于独立的安全内核架构,包括唯一编号、独立的内存、存储器、加密运算组件和控制其它处理器及总线的加密接口,所述安全SPU内部的启动程序根据加密逻辑和认证公钥,调用加密运算组件,能够有效控制所有处理器及SPU的操作系统及安全应用的执行和安全更新,操作系统和安全应用的程序代码通过特定私钥签名,才能用安全SPU的认证公钥认证通过,所有处理器及SPU的操作系统和应用程序经过特定的安全编译器编译后,也需要安全SPU进行协助处理才能正确执行,通过安全SPU的唯一编号或数字签名方的唯一编号对应的认证公钥,验证数字签名,实现更安全的多应用。

3.根据权利要求2中所述的智能安全主控,其特征在于,安全SPU能够控制点到点的数据加解密处理,使得所述安全应用能够实现数据信号加密传输,不被传输通道窃听,具备指定接收方才能解密的特点。

4.根据权利要求3中所述的智能安全主控,其特征在于,所述安全内核的工作流程包括:(1)在安全内核中设置并启动安全SPU;(2)由安全SPU验证当前底层固件的完整性,如正确则完成正常的系统初始化后执行步骤(3),否则停止启动;(3)由底层固件验证当前操作系统的完整性,如正确则正常运行操作系统,否则停止装入操作系统;SPU是通过在启动过程中对监控程序或BIOS、底层固件、操作系统依次进行完整性验证,从而保证安全启动之后,再利用安全SPU内置的加密运算组件调用并管理系统中各种密钥,对安全应用进行加解密,以保证安全应用的安全。

5.根据权利要求4中所述的智能安全主控,其特征在于,所述安全SPU具有多安全分区,通过对唯一编号运算实现可信认证功能,同时兼容现有应用系统规范,能够创建互联互通应用,具备电子钱包和电子存折功能;所述可信认证通过将密钥运算绑定安全SPU芯片唯一编号和/或用户唯一标识实现;所述可信认证互联互通应用上有多种应用目录,包括兼容现有应用系统规范的应用,以及带有可信认证功能的安全应用;带可信认证功能的安全应用名称和发行密钥是用户能够自定义的;在装载现有应用系统统一密钥的情况下能够在现有应用系统中运行;在装载配合可信认证的自定义密钥的情况下能够在装有可信认证的系统中运行;所述可信认证的具体实现方式为,根据外部云服务平台或终端中PSAM卡发出的随机数和认证申请,所述可信认证互联互通应用通过安全SPU内部安全指令方式获取唯一编号和认证密钥,然后用认证密钥对唯一编号和随机数进行运算,把运算结果返回给外部云服务平台或PSAM卡,由外部云服务平台或PSAM卡判断可信认证互联互通应用申请的合法

性;所述唯一编号的来源是所述可信认证互联互通应用写入安全SPU的用户唯一标识和/或安全SPU的芯片唯一编号;所述PSAM卡也能够由主控模块中额外的安全SPU实现。

6.根据权利要求5中所述的智能安全主控,其特征在于,所述随机数的一部分能够校验随机数另一部分的正确性,且校验运算还需要唯一编号、特定密钥、授权文件数据和时间数据中的一种或多种数据参与。

7.根据权利要求6中所述的智能安全主控,其特征在于,所述安全应用通过发出带校验数据的请求指令,使得安全SPU能够验证请求指令并生成正确的一次性认证数据,安全应用负责将安全SPU生成的一次性认证数据显示出来或播放出来;所述安全SPU内置加密算法以及与用户唯一编号对应的秘密种子,能够通过秘密种子与迭代参数进行加密运算生成一定时间内有效的一次性认证数据;所述迭代参数是当前时间、随机序列、计数器、用户唯一编号、与用户唯一编号对应的密钥、与云端服务系统同步的同步码、上次计算的一次性认证数据中的一个或多个;云端服务系统存储有与安全SPU一致的秘密种子,能够通过同样的加密运算验证一次性认证数据,所述云端服务系统还能够联网更新或销毁安全SPU及秘密种子;所述一次性认证数据能够通过纯数字、字符、条形码、二维码、图形码、链接地址的一种或多种进行显示。

8.根据权利要求7中所述的智能安全主控,其特征在于,所述安全SPU在加密运算中用到的特定硬件参数或相应的哈希值,在秘密种子生成或激活中,安全SPU也会将特定硬件参数或相应的哈希值传送给云端服务系统。

9.根据权利要求8中所述的智能安全主控,其特征在于,所述安全应用还包括在外部设备上运行的应用程序;所述安全应用根据用户输入的PIN码、指纹、虹膜、图像和音频中的一种或多种,与预先设定或存储的数据进行比对,正确后才能够发出带校验数据的请求指令,使得安全SPU能够验证请求指令并生成正确的一次性认证数据,输出给应用程序。

10.根据权利要求9中所述的智能安全主控,其特征在于,所述主控模块具备独立的安全输入接口,使得用户能够直接在安全接口的输入设备上输入用户的PIN码、指纹、虹膜、图像和音频中的一种或多种,避免在通用系统的开放输入环境里泄露用户隐私。

智能安全主控

技术领域

[0001] 本发明涉及一种具备大小核心、硬件加密引擎及单向计数器硬件电路的支持PCI Express接口的高性能安全主控芯片或模块，能够用于存储控制器、物联网安全主控模块及人工智能安全主控模块。

技术背景

[0002] 存储器、物联网和人工智能都是芯片需求达到万亿元人民币规模的行业市场，都需要高性能的主控芯片和模块，移动终端、云计算、物联网、大数据、人工智能等新兴产业的发展也都离不开存储芯片与信息安全，迫切需要智能安全主控芯片。普通的控制器芯片没有硬件加密引擎和高速总线，不能同时进行高速的存储器数据管理及安全计算功能，对于存储器颗粒及数据都缺乏有效的保护。智能安全主控芯片通过新的硬件安全电路和硬件加速架构，采用多核并行处理机制，既支持存储器高性能管理，同时能够针对特定运算及安全性能进行多通道并行加速，使得存储器访问性能成倍提高，有效提升了大数据处理及安全应用的效率，在做为服务器PCI Express加速卡使用时，能够比没有加速卡的通用服务器成倍提高数据处理性能。

发明内容

[0003] 本发明公开了一种智能安全主控，其特征在于，由一个或多个大核处理器组成的主控模块、电源管理模块、多个能够并发协作的小核处理器组成的硬件加速模块和具备抗攻击单向计数器的硬件加密模块组成；所述智能安全主控具备FLASH控制器和DRAM控制器功能，主接口支持PCI Express系列标准；所述硬件加速模块具备缓冲加速和特定运算加速功能；所述硬件加密模块经过版图重构和加扰数据线设计，具备时钟探测电路，具备符合国际及国密标准的高性能加密引擎以及抗攻击单向计数器的硬件电路，所述抗攻击单向计数器采用双路互补校验计数器；所述双路互补校验计数器的设计是每路计数器由一个符合特定规律的数字转盘组成，且只能够单方向运转，但两个计数器的当前数值经过运算后满足特定规律，这样能够保护总体计数器的合法性，当试图通过破坏性攻击修改任一路计数器时，由于无法精确修改另一路计数器对应的匹配值，导致计数器校验不通过。

[0004] 所述的智能安全主控，其特征在于，所述主控模块至少包括一个安全SPU，所述安全SPU即安全CPU，是基于独立的安全内核架构，包括唯一编号、独立的内存、存储器、加密运算组件和控制其它处理器及总线的加密接口，所述安全SPU内部的启动程序根据加密逻辑和认证公钥，调用加密运算组件，能够有效控制所有处理器及SPU的操作系统及安全应用的执行和安全更新，操作系统和安全应用的程序代码通过特定私钥签名，才能用安全SPU的认证公钥认证通过，所有处理器及SPU的操作系统和应用程序经过特定的安全编译器编译后，也需要安全SPU进行协助处理才能正确执行，通过安全SPU的唯一编号或数字签名方的唯一编号对应的认证公钥，验证数字签名，实现更安全的多应用。

[0005] 所述的智能安全主控，其特征在于，安全SPU能够控制点到点的数据加解密处理，

使得所述安全应用能够实现数据信号加密传输，不被传输通道窃听，具备指定接收方才能解密的特点。

[0006] 所述的智能安全主控，其特征在于，所述安全内核的工作流程包括：(1)在安全内核中设置并启动安全SPU；(2)由安全SPU验证当前底层固件的完整性，如正确则完成正常的系统初始化后执行步骤(3)，否则停止启动；(3)由底层固件验证当前操作系统的完整性，如正确则正常运行操作系统，否则停止装入操作系统；SPU是通过在启动过程中对监控程序或BIOS、底层固件、操作系统依次进行完整性验证，从而保证安全启动之后，再利用安全SPU内置的加密运算组件调用并管理系统中各种密钥，对安全应用进行加解密，以保证安全应用的安全。

[0007] 所述的智能安全主控，其特征在于，所述安全SPU具有多安全分区，通过对唯一编号运算实现可信认证功能，同时兼容现有应用系统规范，能够创建互联互通应用，具备电子钱包和电子存折功能；所述可信认证通过将密钥运算绑定安全SPU芯片唯一编号和/或用户唯一标识实现；所述可信认证互联互通应用上有多种应用目录，包括兼容现有应用系统规范的应用，以及带有可信认证功能的安全应用；带可信认证功能的安全应用名称和发行密钥是用户能够自定义的；在装载现有应用系统统一密钥的情况下能够在现有应用系统中运行；在装载配合可信认证的自定义密钥的情况下能够在装有可信认证的系统中运行；所述可信认证的具体实现方式为，根据外部云服务平台或终端中PSAM卡发出的随机数和认证申请，所述可信认证互联互通应用通过安全SPU内部安全指令方式获取唯一编号和认证密钥，然后用认证密钥对唯一编号和随机数进行运算，把运算结果返回给外部云服务平台或PSAM卡，由外部云服务平台或PSAM卡判断可信认证互联互通应用申请的合法性；所述唯一编号的来源是所述可信认证互联互通应用写入安全SPU的用户唯一标识和/或安全SPU的芯片唯一编号；所述PSAM卡也能够由主控模块中额外的安全SPU实现。

[0008] 所述的智能安全主控，其特征在于，所述随机数的一部分能够校验随机数另一部分的正确性，且校验运算还需要唯一编号、特定密钥、授权文件数据和时间数据中的一种或多种数据参与。

[0009] 所述的智能安全主控，其特征在于，所述安全应用通过发出带校验数据的请求指令，使得安全SPU能够验证请求指令并生成正确的一次性认证数据，安全应用负责将安全SPU生成的一次性认证数据显示出来或播放出来；所述安全SPU内置加密算法以及与用户唯一编号对应的秘密种子，能够通过秘密种子与迭代参数进行加密运算生成一定时间内有效的一次性认证数据；所述迭代参数是当前时间、随机序列、计数器、用户唯一编号、与用户唯一编号对应的密钥、与云端服务系统同步的同步码、上次计算的一次性认证数据中的一个或多个；云端服务系统存储有与安全SPU一致的秘密种子，能够通过同样的加密运算验证一次性认证数据，所述云端服务系统还能够联网更新或销毁安全SPU及秘密种子；所述一次性认证数据能够通过纯数字、字符、条形码、二维码、图形码、链接地址的一种或多种进行显示。

[0010] 所述的智能安全主控，其特征在于，所述安全SPU在加密运算中用到的特定硬件参数或相应的哈希值，在秘密种子生成或激活中，安全SPU也会将特定硬件参数或相应的哈希值传送给云端服务系统。

[0011] 所述的智能安全主控，其特征在于，所述安全应用还包括在外部设备上运行的应

用程序;所述安全应用根据用户输入的PIN码、指纹、虹膜、图像和音频中的一种或多种,与预先设定或存储的数据进行比对,正确后才能够发出带校验数据的请求指令,使得安全SPU能够验证请求指令并生成正确的一次性认证数据,输出给应用程序。

[0012] 所述的智能安全主控,其特征在于,所述主控模块具备独立的安全输入接口,使得用户能够直接在安全接口的输入设备上输入用户的PIN码、指纹、虹膜、图像和音频中的一种或多种,避免在通用系统的开放输入环境里泄露用户隐私。

具体实施方式

[0013] 本发明的智能安全主控,其具体实施方式为,主控模块采用优化的RISC-V双大核处理器,一个做安全SPU,一个做通用CPU,具有唯一芯片ID,配备有多块ROM,安全OTP,RAM,配备FLASH控制器、DRAM控制器、ECC校验模块以及PCI Express4.0接口模块,硬件加速模块采用32核简化的RISC-V小核处理器,由大核处理器负责调度,采用经过版图重构和加扰数据线设计的硬件加密模块,具备时钟探测电路,符合国际及国密标准的高性能加密引擎以及抗攻击用的单向计数器做全盘校验,用于防止历史存储镜像回写。