



(12) 发明专利

(10) 授权公告号 CN 115758397 B

(45) 授权公告日 2025. 07. 01

(21) 申请号 202211295201.X

G06F 21/72 (2013.01)

(22) 申请日 2022.10.21

G06F 21/45 (2013.01)

(65) 同一申请的已公布的文献号

申请公布号 CN 115758397 A

(56) 对比文件

WO 2016127422 A1, 2016.08.18

CN 113010264 A, 2021.06.22

(43) 申请公布日 2023.03.07

审查员 汪见晗

(73) 专利权人 北京计算机技术及应用研究所

地址 100854 北京市海淀区永定路51号

(72) 发明人 汪婧 曲新春 郭慧波 李凤祥

任艳慧 郑煦

(74) 专利代理机构 中国兵器工业集团公司专利

中心 11011

专利代理师 刘瑞东

(51) Int. Cl.

G06F 21/60 (2013.01)

G06F 21/62 (2013.01)

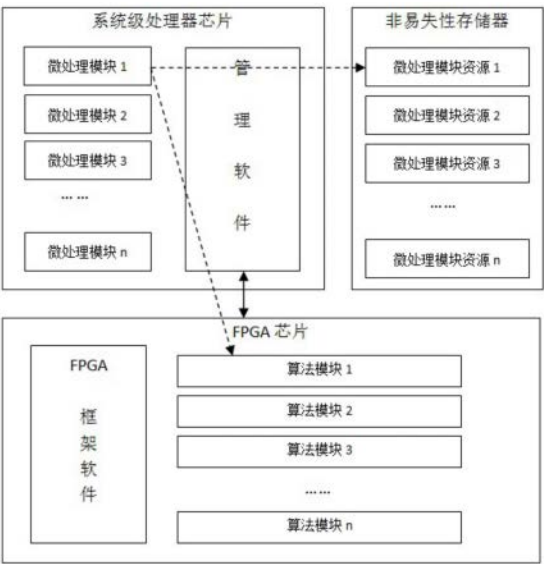
权利要求书2页 说明书6页 附图3页

(54) 发明名称

一种模块化的数据加解密系统和方法

(57) 摘要

本发明涉及一种模块化的数据加解密系统和方法,属于计算机密码领域。本发明采用所述模块化的加解密架构,分别在系统级芯片处理器和FPGA上运行,通过系统级芯片上管理软件和微处理模块软件的解耦设计和协同工作,实现密码处理与底层硬件的解耦,解决密码应用模块的重复设计和重复替换问题;FPGA架构采用多算法模块嵌入的方式,微处理模块与FPGA算法模块一一对应,解决一种密码应用模块可以运行多种硬件平台,一个硬件平台运行多种密码应用模块。管理软件通过采用系统内部标准socket的方式与微处理模块通信,采用总线的方式与FPGA通信,实现不同微处理模块与不同密码模块的标准化与平台化,完成密码微处理模块的调度和密码资源统一管理等功能。



1. 一种模块化的数据加解密系统,其特征在于,该系统包括系统级处理器芯片、FPGA芯片和非易失性存储器,系统级处理器芯片包括微处理模块和管理软件,FPGA芯片包括算法模块和FPGA框架软件;非易失性存储介质上存储微处理模块资源;

FPGA芯片上的软件包括FPGA框架软件和算法模块;FPGA框架软件负责提供所有对外接口、内部互联总线、外设调用、时钟复位资源、以及底层协议解析功能,为FPGA算法模块提供服务;算法模块实现具体的业务数据密码协议解析、密码算法实现;FPGA框架软件与算法模块通过FPGA模块接口协议进行交互;

处理器芯片上运行实时操作系统,处理器芯片上的软件包括管理软件和微处理模块;管理软件用于模块的加载、系统进程的整体调度、密码资源的管理,包括资源管理模块、系统控制模块和FPGA通信模块,FPGA通信模块用于接收微处理模块的数据通过总线接口发送给FPGA;微处理模块实现密钥的派生、资源的处理、算法模块的控制;

算法模块和微处理模块的二进制文件为一一对应关系,存储于FLASH中;

管理软件启动后,从FLASH中读取算法模块二进制文件,并通过总线接口将算法模块发送给FPGA框架软件,FPGA框架软件将其加载并运行;同时通过调用操作系统相应接口的方式启动执行微处理模块,微处理模块以进程的方式独立运行于系统中,管理软件根据实际应用需求对微处理模块进程优先级进行控制;管理软件与微处理模块和FPGA通信模块进行数据交互,微处理模块的端口号由管理软件统一分配,并在启动时将端口号转换为字符串传入main(int argc,char **argv)中,argc 指向传入参数的数量,argv[1]指向传入参数微处理模块端口号字符串。

2. 如权利要求1所述的模块化的数据加解密系统,其特征在于,算法模块以二进制bin文件方式存储。

3. 如权利要求1所述的模块化的数据加解密系统,其特征在于,微处理模块以elf可执行程序方式存储。

4. 如权利要求1所述的模块化的数据加解密系统,其特征在于,管理软件一次能加载多个微处理模块,并通过不同的端口号实现与不同微处理模块的socket通信。

5. 如权利要求1所述的模块化的数据加解密系统,其特征在于,FPGA算法模块软件与FPGA框架软件进行管理类资源数据的交互,管理类资源数据包括:密码算法参数、密钥、随机数和算法状态。

6. 如权利要求1所述的模块化的数据加解密系统,其特征在于,微处理模块还用于状态的上报、自检结果的上报。

7. 如权利要求1所述的模块化的数据加解密系统,其特征在于,FPGA框架软件接收外部数据送到算法模块中进行加解密运算。

8. 如权利要求1所述的模块化的数据加解密系统,其特征在于,管理软件通过AF-INET域UDP协议套接字与微处理模块和FPGA通信模块进行数据交互。

9. 一种基于权利要求1-8任一项所述的模块化的数据加解密系统的加解密方法,其特征在于,该方法包括如下步骤:

步骤一:FPGA框架软件启动,管理软件启动并从FLASH中读取算法模块二进制文件并通过总线接口发送给FPGA框架软件,FPGA框架软件接收并将算法模块加载起来;

步骤二:管理软件创建socket套接字,通过进程方式加载微处理模块,并传入端口号作

为加载参数,微处理模块单独运行等待接收配置信息;

步骤三:管理软件通过socket接口向微处理模块发送密码资源,微处理模块接收密码资源进行派生、封装处理,通过socket将处理后的数据发送给管理软件,管理软件将其通过FPGA通信模块发送给FPGA框架软件,FPGA框架软件接收后传入算法模块,算法模块进行算法自检;

步骤四:算法模块将算法自检数据传给FPGA框架软件,FPGA框架软件通过总线接口发送给管理软件,管理软件将自检数据传给微处理模块,微处理模块将自检数据进行比对,得出算法自检结果并上报给管理软件;

步骤五:管理软件向微处理模块发送算法模块启动指令,微处理模块将指令封装后发送给FPGA通信模块,FPGA通信模块将其转发给FPGA框架软件,FPGA框架软件收到启动指令后开始工作,接收外部加解密数据输入到FPGA算法模块中进行运算。

10. 如权利要求9所述的方法,其特征在于,所述步骤三中的密码资源包括:算法参数和密钥。

一种模块化的数据加解密系统和方法

技术领域

[0001] 本发明属于计算机密码领域,具体涉及一种模块化的数据加解密系统和方法。

背景技术

[0002] 随着密码系统装备的多样化发展,其硬件平台往往根据不同应用场景和特定功能采用定制化的设计思路,只有提高密码系统硬件平台的兼容性和通用性,才能使嵌入式密码设备具有较高处理性能和快速交互能力。实现这一需求的关键技术是采用模块化的设计思路,实现计算与管理分离,满足不同的应用需求。

[0003] 在实现标准化设计的嵌入式密码系统中,现在大都采用算法集成在FPGA架构中,管理软件进行密码资源和算法调度的统一管理,因此无法实现模块化更换,难以针对不同处理器、不同FPGA、不同算法实现通用性,限制开发效率与代码的可重用性。

发明内容

[0004] (一)要解决的技术问题

[0005] 本发明要解决的技术问题是如何提供一种模块化的数据加解密系统和方法,以解决现有的加解密系统无法实现模块化更换,难以针对不同处理器、不同FPGA、不同算法实现通用性,限制开发效率与代码的可重用性的问题。

[0006] (二)技术方案

[0007] 为了解决上述技术问题,本发明提出一种模块化的数据加解密系统,该系统架构包括系统级处理器芯片、FPGA芯片和非易失性存储器,系统级处理器芯片包括微处理模块和管理软件,FPGA芯片包括算法模块和FPGA框架软件;非易失性存储介质上存储微处理模块资源;

[0008] FPGA芯片上的软件包括FPGA框架软件和算法模块;FPGA框架软件负责提供所有对外接口、内部互联总线、外设调用、时钟复位资源、以及底层协议解析功能,为FPGA算法模块提供服务;算法模块实现具体的业务数据密码协议解析、密码算法实现;FPGA框架软件与算法模块通过FPGA模块接口协议进行交互;

[0009] 处理器芯片上运行实时操作系统,处理器芯片上的软件包括管理软件和微处理模块;管理软件用于模块的加载、系统进程的整体调度、密码资源的管理,包括资源管理模块、系统控制模块和FPGA通信模块,FPGA通信模块用于接收微处理模块的数据通过总线接口发送给FPGA;微处理模块实现密钥的派生、资源的处理、算法模块的控制;

[0010] 算法模块和微处理模块的二进制文件为一一对应关系,存储于FLASH中;

[0011] 管理软件启动后,从FLASH中读取算法模块二进制文件,并通过总线接口将算法模块发送给FPGA框架软件,FPGA框架软件将其加载并运行;同时通过调用操作系统相应接口的方式启动执行微处理模块,微处理模块以进程的方式独立运行于系统中,管理软件根据实际应用需求对微处理模块进程优先级进行控制;管理软件与微处理模块和FPGA通信模块进行数据交互,微处理模块的端口号由管理软件统一分配,并在启动时将端口号转换为字

字符串传入main(int argc,char **argv)中,argc 指向传入参数的数量,argv[1]指向传入参数微处理模块端口号字符串。

[0012] 进一步地,算法模块以二进制bin文件方式存储。

[0013] 进一步地,微处理模块以elf可执行程序方式存储。

[0014] 进一步地,管理软件一次能加载多个微处理模块,并通过不同的端口号实现与不同微处理模块的socket通信。

[0015] 进一步地,FPGA算法模块软件与FPGA框架软件进行管理类资源数据的交互,管理类资源数据包括:密码算法参数、密钥、随机数和算法状态。

[0016] 进一步地,微处理模块还用于状态的上报、自检结果的上报。

[0017] 进一步地,FPGA框架软件接收外部数据送到算法模块中进行加解密运算。

[0018] 进一步地,管理软件通过AF-INET域UDP协议套接字(socket)与微处理模块和FPGA通信模块进行数据交互。

[0019] 本发明还提供一种加解密方法,该方法包括如下步骤:

[0020] 步骤一:FPGA框架软件启动,管理软件启动并从FLASH中读取算法模块二进制文件并通过总线接口发送给FPGA框架软件,FPGA框架软件接收并将算法模块加载起来;

[0021] 步骤二:管理软件创建socket套接字,通过进程方式加载微处理模块,并传入端口号作为加载参数,微处理模块单独运行等待接收配置信息;

[0022] 步骤三:管理软件通过socket接口向微处理模块发送密码资源,微处理模块接收密码资源进行派生、封装处理,通过socket将处理后的数据发送给管理软件,管理软件将其通过FPGA通信模块发送给FPGA框架软件,FPGA框架软件接收后传入算法模块,算法模块进行算法自检;

[0023] 步骤四:算法模块将算法自检数据传给FPGA框架软件,FPGA框架软件通过总线接口发送给管理软件,管理软件将自检数据传给微处理模块,微处理模块将自检数据进行比对,得出算法自检结果并上报给管理软件;

[0024] 步骤五:管理软件向微处理模块发送算法模块启动指令,微处理模块将指令封装后发送给FPGA通信模块,FPGA通信模块将其转发给FPGA框架软件,FPGA框架软件收到启动指令后开始工作,接收外部加解密数据输入到FPGA算法模块中进行运算。

[0025] 进一步地,所述步骤三中的密码资源包括:算法参数和密钥。

[0026] (三)有益效果

[0027] 本发明提出一种模块化的数据加解密系统和方法,本发明提出一种模块化的数据加解密系统,实现采用多种算法完成多种类型数据的加解密。通过采用模块化的设计思路,实现计算与管理的分离,解决多重应用时的硬件重复设计和重复替换问题;通过微处理模块的跨平台编译和运行的特性,实现一种微处理模块可以运行在多种硬件平台,一个硬件平台运行多种微处理模块,解决传统模式带来的制约和瓶颈;通过采用标准socket接口API通信和高速总线通信,形成可扩展性强、标准化高的数据加解密系统。

附图说明

[0028] 图1为本发明数据加解密系统的逻辑架构;

[0029] 图2为系统内部数据流向图;

[0030] 图3为管理软件运行流程。

具体实施方式

[0031] 为使本发明的目的、内容和优点更加清楚,下面结合附图和实施例,对本发明的具体实施方式作进一步详细描述。

[0032] 本发明要解决的技术问题是如何提供一种模块化的数据加解密系统和方法,屏蔽操作系统与密码机硬件平台的差异性,实现管理与计算的分离,一种密码应用模块可以运行多种硬件平台,一个硬件平台运行多种密码应用模块。

[0033] 本发明涉及一种模块化的加解密密码机架构,属于计算机密码领域。本发明采用所述模块化的加解密架构,分别在系统级芯片处理器和FPGA上运行,通过系统级芯片上管理软件和微处理模块软件的解耦设计和协同工作,实现密码处理与底层硬件的解耦,解决密码应用模块的重复设计和重复替换问题;FPGA架构采用多算法模块嵌入的方式,微处理模块与FPGA算法模块一一对应,解决一种密码应用模块可以运行多种硬件平台,一个硬件平台运行多种密码应用模块。管理软件通过采用系统内部标准socket的方式与微处理模块通信,采用总线的方式与FPGA通信,实现不同微处理模块与不同密码模块的标准化与平台化,完成密码微处理模块的调度和密码资源统一管理等功能。

[0034] 为了解决上述技术问题,本发明提出一种模块化数据加解密系统,该系统包括系统级处理器芯片、FPGA芯片和非易失性存储器。系统级处理器芯片包括微处理模块和管理软件;FPGA芯片包括算法模块和FPGA框架软件;非易失性存储介质上存储微处理模块资源。

[0035] 密码应用模块以模块软件的方式安装在密码机硬件平台上,用以实现某一业务的加解密功能。模块软件一般划分为算法模块和微处理模块,二者为一一对应关系。通过模块化实现方式,实现一种密码应用模块可以运行多种硬件平台,一个硬件平台运行多种密码应用模块。

[0036] FPGA芯片上的软件包括FPGA框架软件和算法模块。FPGA框架软件负责提供所有对外接口、内部互联总线、外设调用、时钟复位资源、底层协议解析等功能,为FPGA算法模块提供服务。算法模块实现具体的业务数据密码协议解析、密码算法实现等功能。FPGA框架软件与算法模块通过FPGA模块接口协议进行交互。

[0037] 处理器芯片上运行实时操作系统,处理器芯片上的软件包括管理软件和微处理模块。管理软件主要用于模块的加载、系统进程的整体调度、密码资源的管理,包括资源管理模块、系统控制模块和FPGA通信模块。FPGA通信模块用于接收微处理模块的数据通过总线接口发送给FPGA。微处理模块实现密钥的派生、资源的处理、FPGA算法模块的控制。

[0038] 密码应用模块统一存储在FLASH中,算法模块以二进制bin文件方式存储,微处理模块以elf可执行程序方式存储。管理软件启动后,从FLASH中读取FPGA算法模块二进制文件,并通过总线接口将FPGA算法模块发送给FPGA框架软件,FPGA框架软件将其加载并运行。同时通过调用操作系统相应接口(如posix_spawn)的方式启动执行微处理模块,微处理模块以进程的方式独立运行于系统中,管理软件可根据实际应用需求对微处理模块进程优先级进行控制。管理软件通过AF_INET域UDP协议套接字(socket)与微处理模块和FPGA通信模块进行数据交互,微处理模块的端口号由管理软件统一分配,并在启动时将端口号转换为字符串传入main(int argc,char **argv)中,argc 指向传入参数的数量,argv[1]指向传

入参数微处理模块端口号字符串。

[0039] 进一步地,管理软件可一次加载多个微处理模块,并通过不同的端口号实现与不同微处理模块的socket通信;

[0040] 进一步地,FPGA算法模块软件与FPGA框架软件会进行密码算法参数、密钥、随机数、算法状态等管理类资源数据的交互;

[0041] 进一步地,微处理模块可实现状态的上报、自检结果的上报;

[0042] 进一步地,FPGA框架软件会接收外部数据送到算法模块中进行加解密运算。

[0043] 本发明还提供一种基于所述的系统的密码机加解密使用方法,该方法用于多种业务、算法的加解密,包括如下步骤:

[0044] 步骤一:FPGA框架软件启动,管理软件启动并从FLASH中读取算法模块二进制文件并通过总线接口发送给FPGA框架软件,FPGA框架软件接收并将算法模块加载起来;

[0045] 步骤二:管理软件创建socket套接字,通过进程方式加载微处理模块,并传入端口号作为加载参数,微处理模块单独运行等待接收配置信息;

[0046] 步骤三:管理软件通过socket接口向微处理模块发送算法参数、密钥等密码资源,微处理模块接收密码资源进行派生、封装等处理,通过socket将处理后的数据发送给管理软件,管理软件将其通过FPGA通信模块发送给FPGA框架软件,FPGA框架软件接收后传入算法模块,算法模块进行算法自检;

[0047] 步骤四:算法模块将算法自检数据传给FPGA框架软件,FPGA框架软件通过总线接口发送给管理软件,管理软件将自检数据传给微处理模块,微处理模块将自检数据进行比对,得出算法自检结果并上报给管理软件;

[0048] 步骤五:管理软件向微处理模块发送算法模块启动指令,微处理模块将指令封装后发送给FPGA通信模块,FPGA通信模块将其转发给FPGA框架软件,FPGA框架软件收到启动指令后开始工作,接收外部加解密数据输入到FPGA算法模块中进行运算。

实施例

[0049] 图1是本发明数据加解密系统的逻辑结构示意图。该系统包括微处理模块、算法模块、微处理模块资源管理、密码处理器芯片、管理软件、FPGA处理器芯片、FPGA软件、FLASH存储介质。

[0050] 微处理模块为可以运行在CPU对应操作系统上的可执行程序文件,软件源码具备源码跨平台编译和运行的特性,采用一组“与管理软件无关的接口API函数”,通过FPGA通信模块实现与FPGA算法模块的通信、以及与处理器上其他模块进行交互。微处理模块与管理软件解耦,屏蔽操作系统与密码机硬件平台的差异性。

[0051] 管理软件是整个系统的控制核心,系统上电后管理软件运行,根据实际应用场景通过创建进程的方式加载微处理模块,并通过接口向FPGA传输算法模块,以实现算法模块的动态重构。管理软件与微处理模块作为独立进程运行在处理器上,通过socket进行通信。

[0052] FLASH存储介质中存储多个模块的密码资源和二进制文件,借助非易失性RAM的防掉电丢失能力,保护关键数据不被丢失。

[0053] FPGA处理器芯片上运行框架软件,框架软件接收管理软件传输的算法模块,进行动态加载,并按照协议对传输数据进行解析,送入到算法模块中加解密。FPGA算法模块提供

统一的对外接口,支持动态可重构。

[0054] 图2是系统内部数据流向,图3是管理软件的运行流程。

[0055] 步骤一:FPGA框架软件启动,管理软件启动并从FLASH中读取算法模块并通过总线接口发送给FPGA框架软件,FPGA框架软件接收并将算法模块加载起来;

[0056] 步骤二:管理软件创建socket套接字,通过进程方式加载微处理模块,并传入端口号作为加载参数,微处理模块单独运行等待接收配置信息;

[0057] 步骤三:管理软件通过socket接口向微处理模块发送算法参数、密钥等密码资源,微处理模块接收密码资源进行派生、封装等处理,通过socket将处理后的数据发送给管理软件,管理软件将其通过FPGA通信模块发送给FPGA框架软件,FPGA框架软件接收后传入算法模块,算法模块进行算法自检。

[0058] 步骤四:算法模块将算法自检数据传给FPGA框架软件,FPGA框架软件通过总线接口发送给管理软件,管理软件将自检数据传给微处理模块,微处理模块将自检数据进行比对,得出算法自检结果并上报给管理软件。

[0059] 步骤五:管理软件向微处理模块发送算法模块启动指令,微处理模块将指令封装后发送给FPGA通信模块,FPGA通信模块将其转发给FPGA框架软件,FPGA框架软件收到启动指令后开始工作,接收外部加解密数据输入到FPGA算法模块中进行运算。

[0060] 采用本发明所述模块化的数据加解密系统,实现采用多种算法实现多种类型数据的加解密。通过采用模块化的设计思路,实现计算与管理的分离,解决多重应用时的硬件重复设计和重复替换问题;通过微处理模块的跨平台编译和运行的特性,实现一种微处理模块可以运行在多种硬件平台,一个硬件平台运行多种微处理模块,解决传统模式带来的制约和瓶颈;通过采用标准socket接口API通信和高速总线通信,形成可扩展性强、标准化高的数据加解密系统。

实施例

[0061] 一种软件定义的模块化数据加解密系统,该系统包括系统级芯片、FPGA芯片、非易失性存储器。系统级处理器芯片包括微处理模块和管理软件;FPGA芯片包括算法模块、FPGA框架软件;非易失性存储介质上存储微处理模块资源;

[0062] 密码应用模块以模块软件的方式安装在密码机硬件平台上,用以实现某一业务的加解密功能。模块软件一般划分为FPGA算法模块和处理器微处理模块。通过模块化实现方式,实现一种密码应用模块可以运行多种硬件平台,一个硬件平台运行多种密码应用模块;

[0063] FPGA软件包括FPGA框架软件和FPGA算法模块。FPGA框架软件负责提供所有对外接口、内部互联总线、外设调用、时钟复位资源、底层协议解析等功能,为FPGA算法模块提供服务。FPGA算法模块实现具体的业务数据密码协议解析、密码算法实现等功能。FPGA框架软件与FPGA算法模块通过FPGA模块接口协议进行交互;

[0064] CPU芯片上运行实时操作系统,CPU软件包括管理软件、处理器微处理模块软件。管理软件用于模块的加载、系统进程的整体调度,密码资源的管理,包括资源管理模块、系统控制模块、FPGA通信模块。FPGA通信模块用于接收微处理模块的数据通过总线接口发送给FPGA;微处理模块实现密钥的派生、资源的处理,FPGA算法模块的控制。

[0065] 进一步地,所述管理软件可一次加载多个微处理模块,并通过不同的端口号实现

与不同微处理模块的socket通信；

[0066] 进一步地,所述FPGA框架软件可动态重构多个算法模块,微处理模块与算法模块一一对应,微处理模块可实现算法模块状态的上报、自检结果的上报；

[0067] 进一步地,所述FPGA算法模块软件与FPGA框架软件会进行密码算法参数、密钥、随机数、算法状态等管理类资源数据的交互；

[0068] 进一步地,密码应用模块统一存储在FLASH中,管理软件启动后,分别从FLASH中读取FPGA算法模块和微处理模块,并通过总线接口将FPGA算法模块发送给FPGA框架软件,FPGA框架软件将其加载并运行。同时通过调用操作系统相应接口(如posix_spawn)的方式启动执行微处理模块,微处理模块以进程的方式独立运行于系统中,管理软件可根据实际应用需求对微处理模块进程优先级进行控制。管理软件通过AF_INET域UDP协议套接字(socket)与微处理模块和FPGA通信模块进行数据交互,微处理模块的端口号由管理软件统一分配,并在启动时将端口号转换为字符串传入main(int argc,char **argv)中,argv[1]指向微处理模块端口号字符串。

[0069] 进一步地,软件的启动与交互流程,包括如下步骤:

[0070] 步骤一:FPGA框架软件启动,管理软件启动并从FLASH中读取算法模块并通过总线接口发送给FPGA框架软件,FPGA框架软件接收并将算法模块加载起来；

[0071] 步骤二:管理软件创建socket套接字,通过进程方式加载微处理模块,并传入端口号作为加载参数,微处理模块单独运行等待接收配置信息；

[0072] 步骤三:管理软件通过socket接口向微处理模块发送算法参数、密钥等密码资源,微处理模块接收密码资源进行派生、封装等处理,通过socket将处理后的数据发送给管理软件,管理软件将其通过FPGA通信模块发送给FPGA框架软件,FPGA框架软件接收后传入算法模块,算法模块进行算法自检；

[0073] 步骤四:算法模块将算法自检数据传给FPGA框架软件,FPGA框架软件通过总线接口发送给管理软件,管理软件将自检数据传给微处理模块,微处理模块将自检数据进行比对,得出算法自检结果并上报给管理软件；

[0074] 步骤五:管理软件向微处理模块发送算法模块启动指令,微处理模块将指令封装后发送给FPGA通信模块,FPGA通信模块将其转发给FPGA框架软件,FPGA框架软件收到启动指令后开始工作,接收外部加解密数据输入到FPGA算法模块中进行运算。

[0075] 本发明提出一种模块化的数据加解密系统,实现采用多种算法完成多种类型数据的加解密。通过采用模块化的设计思路,实现计算与管理的分离,解决多重应用时的硬件重复设计和重复替换问题;通过微处理模块的跨平台编译和运行的特性,实现一种微处理模块可以运行在多种硬件平台,一个硬件平台运行多种微处理模块,解决传统模式带来的制约和瓶颈;通过采用标准socket接口API通信和高速总线通信,形成可扩展性强、标准化高的数据加解密系统。

[0076] 以上所述仅是本发明的优选实施方式,应当指出,对于本技术领域的普通技术人员来说,在不脱离本发明技术原理的前提下,还可以做出若干改进和变形,这些改进和变形也应视为本发明的保护范围。

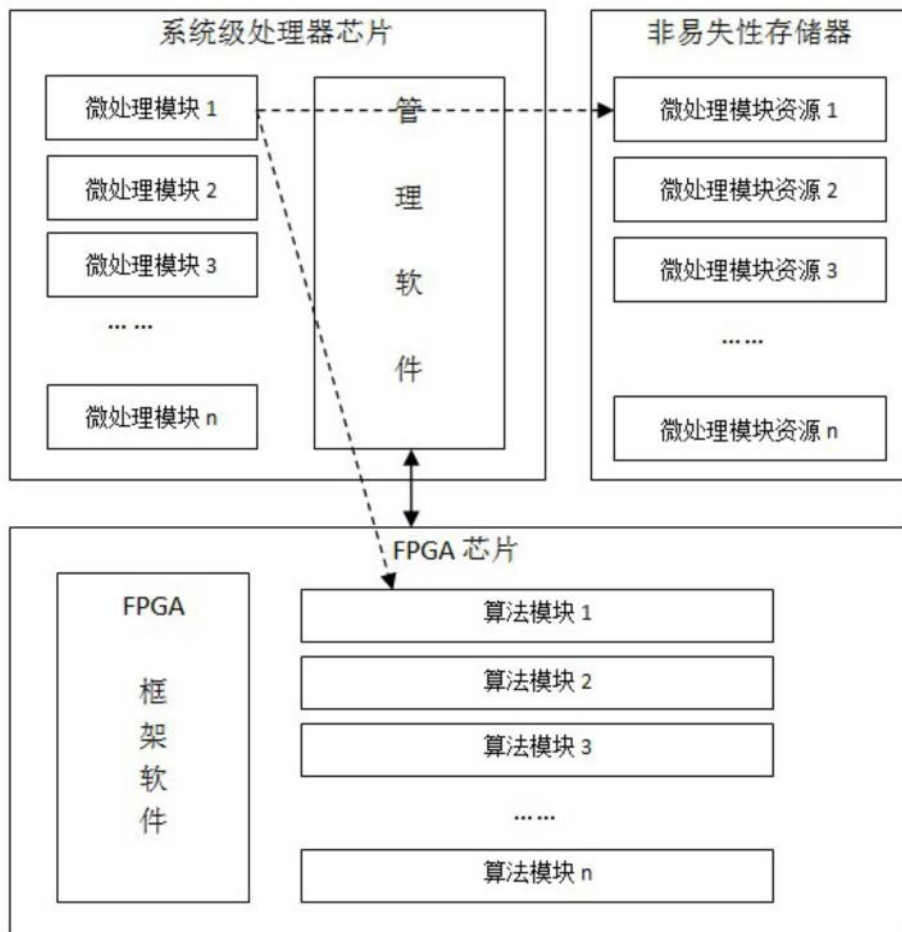


图1

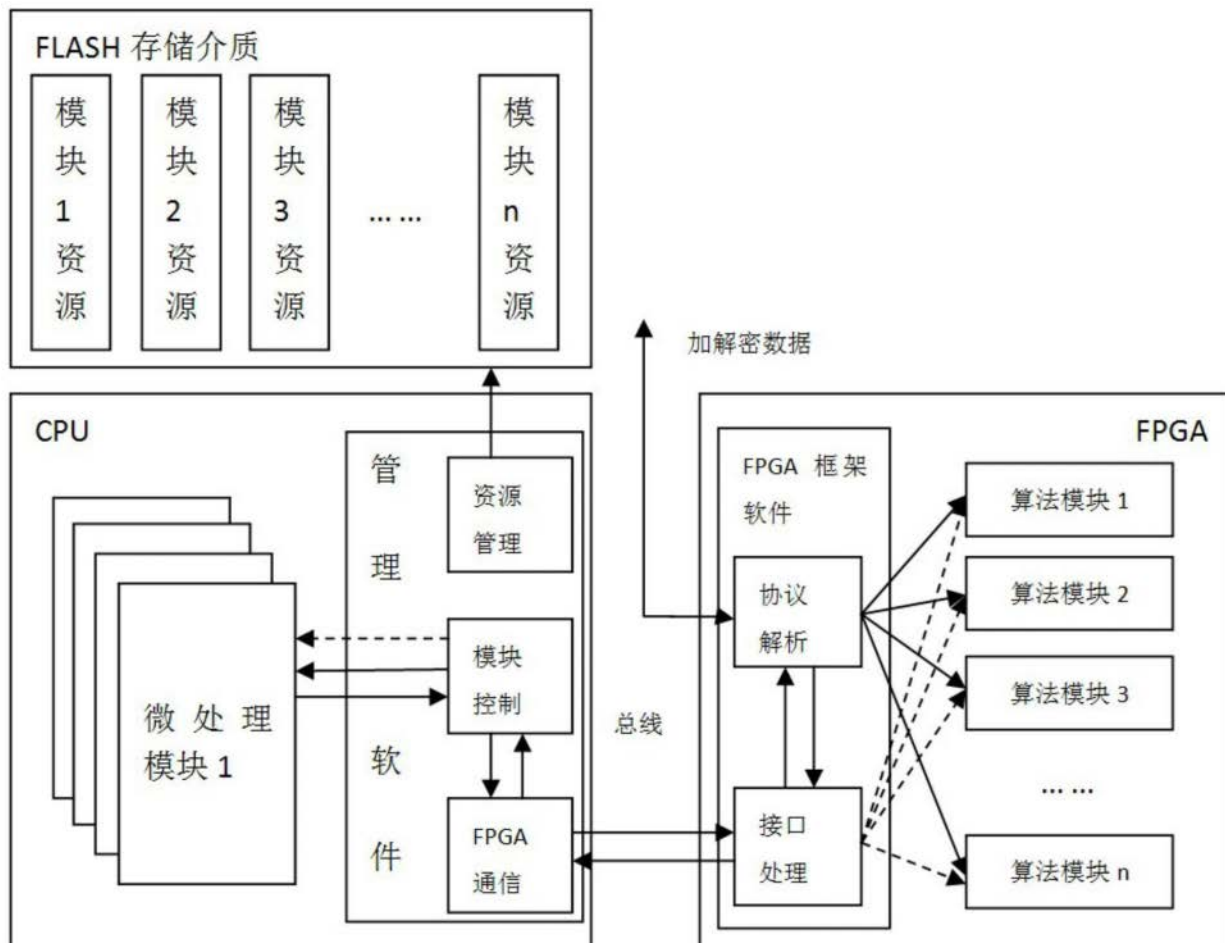


图2

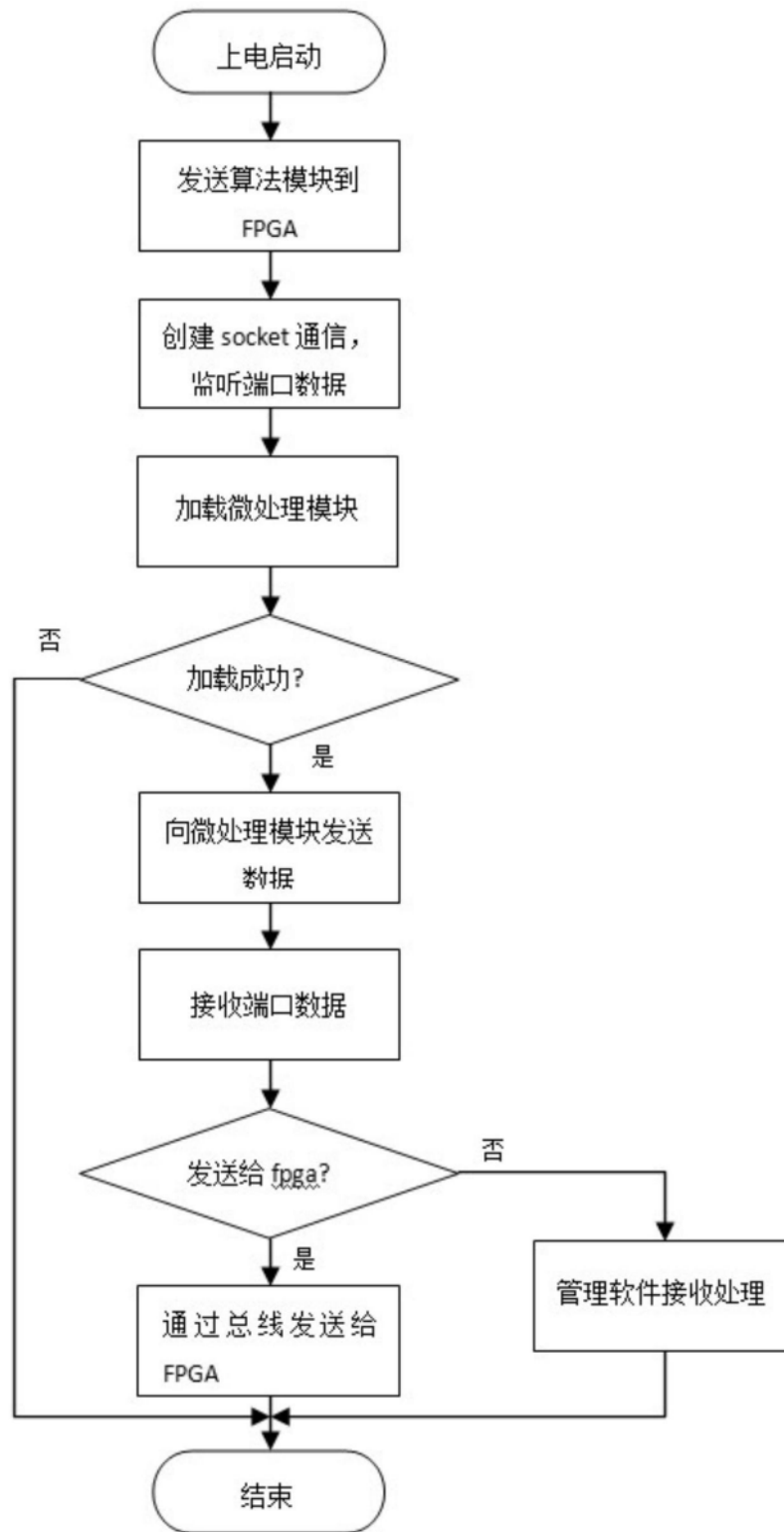


图3