

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 10 月 19 日 (19.10.2017)



(10) 国际公布号
WO 2017/177686 A1

(51) 国际专利分类号:
H04L 9/30 (2006.01)

(21) 国际申请号: PCT/CN2016/107549

(22) 国际申请日: 2016 年 11 月 28 日 (28.11.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201610230897.6 2016 年 4 月 14 日 (14.04.2016) CN

(71) 申请人: 深圳市中兴微电子有限公司 (SANE-CHIPS TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市南山区西丽街道留仙大道中兴工业园, Guangdong 518055 (CN)。

(72) 发明人: 林先萌 (LIN, Xianmeng); 中国广东省深圳市南山区西丽街道留仙大道中兴工业园, Guangdong 518055 (CN)。王永 (WANG, Yong); 中国广东省深圳市南山区西丽街道留仙大道中兴工业园, Guangdong 518055 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OF-

FICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: DEVICE FOR SIMULTANEOUSLY ACHIEVING RSA/ECC ENCRYPTION AND DECRYPTION ALGORITHMS

(54) 发明名称: 同时实现 RSA/ECC 加解密算法的装置

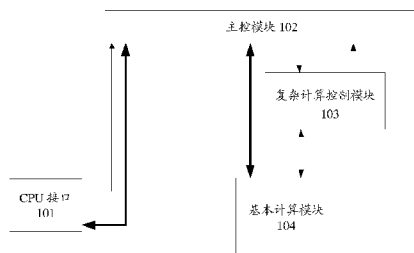


图 1

101 CPU interface
102 Main control module
103 Complex computation control module
104 Basic computation module

(57) Abstract: Embodiments of the present invention provide a device for simultaneously achieving RSA/ECC encryption and decryption algorithms, comprising: a CPU interface module configured to receive a configuration parameter and send the configuration parameter to a main control module, and to return a state parameter; the main control module configured to receive and store the configuration parameter, to send, according to the configuration parameter, a computation command to a complex computation control module, to send the state parameter to the CPU interface module, and to receive a read command and send a computation parameter to a basic computation module; the complex computation control module configured to receive the computation command, to generate an operation command according to the computation command and send the operation command to the basic computation module, and to receive a completion signal of the basic computation module; the basic computation module configured to receive the operation command, to send the read command to the main control module to obtain the computation parameter, to complete computation according to the operation command and the computation parameter, to send the completion signal to the complex computation control module, and to send the computation result to the main control module.

(57) 摘要:

[见续页]



WO 2017/177686 A1



本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

本发明实施例提供一种同时实现 RSA/ECC 加解密算法的装置, 包括: CPU 接口模块, 配置为接收配置参数并发送给主控模块, 返回状态参数; 主控模块, 配置为接收并存储配置参数, 根据所述配置参数向复杂计算控制模块发送计算命令; 将状态参数发送给所述 CPU 接口模块; 接收读取命令并向基本计算模块发送计算参数; 复杂计算控制模块, 配置为接收计算命令, 根据所述计算命令, 生成运算命令发送给基本计算模块; 接收基本计算模块的完成信号; 基本计算模块, 配置为接收运算命令, 并向主控模块发送读取命令以获取计算参数, 根据运算命令以及计算参数完成计算, 向复杂计算控制模块发送完成信号, 同时将计算结果发送给主控模块。

同时实现 RSA/ECC 加解密算法的装置

技术领域

本发明涉及公钥加解密技术，尤其涉及一种同时实现 RSA (Ron Rivest, Adi Shamir, Leonard Adleman, 罗纳德·李维斯特、阿迪·萨莫尔和伦纳德·阿德曼) /ECC (Elliptic curve cryptography, 椭圆曲线密码学) 加解密算法的装置。

背景技术

RSA 公钥加密算法是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被国际标准化组织 (International Organization for Standardization, ISO) 推荐为公钥数据加密标准。

RSA 公钥加密算法的安全性是基于大素数因式分解的困难性，随着计算机处理速度与分布式计算等理论的飞速发展，较短的 RSA 密钥已不再安全。目前 1024 位长度的密钥也可以在较短的时间内被破解，因此，为了提高 RSA 加密的安全强度，需要采用更高位宽的密钥。但是，随着密钥长度的增加，RSA 加解密的速度将大幅降低，严重影响使用效率。

椭圆曲线密码学 (Elliptic Curve Cryptography, ECC) 加密算法的安全性是基于解决椭圆曲线离散对数问题的困难性，目前已知的公钥加密体制中，ECC 加密算法是对每比特所提供加密强度最高的一种体制，即在位宽相同的情况下，ECC 加密算法具有最高的安全强度。因此，在对位宽，功耗，安全性等方面有更高要求的应用场景下，ECC 加密算法具有极大的优势。

公钥加密算法中密钥对的生成需要若干个随机的大素数，以及一系列复杂的计算；目前绝大部分的密钥对生成是通过软件实现的；但通过软件

生成公钥密钥对耗时较长，且会有被第三方窃取素数或随机因子的风险。

RSA 加密算法的核心为大数模幂运算，ECC 加密算法的核心为椭圆点乘运算；由于计算步骤非常复杂，目前大部分加解密装置只是单一实现其中一种加密算法，而可以同时实现两种加密算法的装置，又很难平衡运算速度、面积和功耗，不能适配于分别对速度或面积有较高要求的不同场景。

发明内容

有鉴于此，本发明实施例期望提供一种同时实现 RSA/ECC 加解密算法的装置，以在一个装置中同时实现 RSA/ECC 两种加解密算法。

本发明实施例的技术方案是这样实现的：

10 本发明实施例提供一种同时实现 RSA/ECC 加解密算法的装置，所述装置包括：

中央处理器 CPU 接口模块、主控模块、复杂计算控制模块和基本计算模块；

15 其中，所述 CPU 接口模块，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；

所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模块发送计算参数；

20 所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，根据所述计算命令，生成运算命令发送给所述基本计算模块；接收所述基本计算模块的完成信号；

所述基本计算模块，配置为接收所述运算命令，并向所述主控模块发送读取命令以获取所述计算参数，根据所述运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送完成信号，同时将计算结果

发送给所述主控模块。

如上所述的装置，其中，所述计算命令中包含 RSA/ECC 计算；

所述复杂计算控制模块配置为，将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算，并生成与各模乘运算对应的运算命令发送给所述基本计算模块。

如上所述的装置，其中，所述装置还包括：

从机接口和主机接口；

所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，并将所述配置参数发送给所述主控模块；

所述主机接口，配置为接收所述主控模块发送的所述配置参数，并进行存储。

如上所述的装置，其中，所述装置还包括：

存储模块，配置为存储明文参数、密文参数、密钥参数和所述基本计算模块的计算中间结果。

如上所述的装置，其中，所述配置参数用于配置所述装置运行的算法为 RSA 算法或 ECC 算法、密钥位宽以及工作模式，所述工作模式包括加密模式和解密模式。

如上所述的装置，其中，所述 CPU 接口模块、所述从机接口和所述主机接口均支持外围总线 APB 协议、系统总线 AHB 协议、片内总线 AXI 协议和 ACE_Lite 总线协议。

一种同时实现 RSA/ECC 加解密算法的装置，所述装置包括：

中央处理器 CPU 接口模块、主控模块、复杂计算控制模块、基本计算模块、直接内存存取 DMA 控制器、密钥生成模块、真随机数发生模块和大数乘法处理模块；

其中，所述 CPU 接口模块，配置为接收配置参数并发送给所述主控模

块，返回所述主控模块中的状态参数；

所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述密钥生成模块发送密钥生成命令；向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模块发送计算参数；

所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，根据所述计算命令，生成加减法运算命令发送给所述基本计算模块，生成模乘运算命令发送给所述大数乘法处理模块；接收所述基本计算模块和所述大数乘法处理模块的完成信号；

10 所述基本计算模块，配置为接收所述加减法运算命令，并向所述主控模块发送读取命令以获取所述计算参数，根据所述加减法运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送所述完成信号，同时将计算结果发送给所述主控模块；

15 所述密钥生成模块，配置为接收所述密钥生成命令，并调用所述真随机数发生模块生成随机数生成密钥对，并发送给所述主控模块进行存储；

所述真随机数发生模块，配置为产生真随机数并发送给所述密钥生成模块；

所述 DMA 控制器，配置为接收并存储数据；

20 所述大数乘法处理模块，配置为接收所述模乘运算命令，并向所述 DMA 控制器发送读取命令以获取所述计算参数，根据所述模乘运算命令以及获取的所述计算参数完成计算，将计算的中间结果存储至存储器，向所述复杂计算控制模块发送所述完成信号。

如上所述的装置，其中，所述计算命令中包含 RSA/ECC 计算；

25 所述复杂计算控制模块配置为，将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算和加减运算，并生成所述加减法运算

命令发送给所述基本计算模块，生成所述模乘运算命令发送给所述大数乘法处理模块。

如上所述的装置，其中，所述装置还包括：

从机接口和主机接口；

- 5 所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，并将所述配置参数发送给所述主控模块；

所述主机接口，配置为接收所述主控模块发送的所述配置参数，并进行存储。

- 如上所述的装置，其中，所述 CPU 接口模块、所述主机接口和所述从机接口均支持外围总线 APB 协议、系统总线 AHB 协议、片内总线 AXI 协议和 ACE_Lite 总线协议。
- 10

如上所述的装置，其中，所述配置参数用于配置所述装置运行的算法为 RSA 算法或 ECC 算法、密钥位宽以及工作模式，所述工作模式包括加密模式和解密模式。

- 15 如上所述的装置，其中，所述装置还包括：

存储模块，配置为存储明文参数、密文参数、密钥参数、所述基本计算模块的计算中间结果和所述大数乘法处理模块的计算中间结果。

如上所述的装置，其中，所述存储模块采用双口随机存取存储器 RAM。

- 如上所述的装置，其中，所述大数乘法处理模块，配置为调用可伸缩的循环脉动阵列完成任意位宽的大数模乘运算。
- 20

- 本发明实施例提供的同时实现 RSA/ECC 加解密算法的装置，包括：所述 CPU 接口模块，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接口模块；接收所述基本计算模块发送的读取命令，向所
- 25

述基本计算模块发送计算参数；所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，根据所述计算命令，生成运算命令发送给所述基本计算模块；接收所述基本计算模块的完成信号；所述基本计算模块，配置为接收所述运算命令，并向所述主控模块发送读取命令以获取所述计算参数，根据所述运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送完成信号，同时将计算结果发送给所述主控模块。能够同时实现 RSA/ECC 两种公钥加解密算法，用户可以根据速度优先或面积优先的场景进行相应的配置，大幅提高本发明在不同应用场景下的适配性。

附图说明

图 1 为本发明实施例提供的同时实现 RSA/ECC 加解密算法的装置的结构示意图；

图 2 为使用本实施例提供的同时实现 RSA/ECC 加解密算法的装置完成公钥加密运算的配置示意图一；

图 3 为本发明实施例提供的同时实现 RSA/ECC 加解密算法的装置的结构示意图；

图 4 为使用本实施例提供的同时实现 RSA/ECC 加解密算法的装置完成公钥加密运算的配置示意图二。

具体实施方式

在本发明的各实施例中，本发明提出了一种 RSA/ECC 公钥加解密装置，可以同时实现 RSA/ECC 两种公钥加解密算法。用户可以根据速度优先或面积优先的场景进行相应的配置，大幅提高本发明在不同应用场景下的适配性。该装置支持外围总线（Advanced Peripheral Bus, APB）协议、系统总线（Advanced High performance Bus, AHB）协议、片内总线（Advanced eXtensible Interface, AXI）协议和 ACE_Lite 等多种总线协议，支持 RSA/ECC

密钥生成功能，根据存储空间大小，可支持任意长度的密钥。

图 1 为本发明实施例提供的同时实现 RSA/ECC 加解密算法的装置的结构示意图。如图 1 所示，本实施例提供的装置包括：

中央处理器（Central Processing Unit，CPU）接口模块 101、主控模块
5 102、复杂计算控制模块 103 和基本计算模块 104；

其中，所述 CPU 接口模块 101，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；

所述主控模块 102，配置为接收并存储配置参数，根据所述配置参数向
所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接
10 口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模块发送计算参数；

所述复杂计算控制模块 103，配置为接收所述主控模块发送的计算命令，根据所述计算命令，生成运算命令发送给所述基本计算模块；接收所述基本计算模块的完成信号；

15 所述基本计算模块 104，配置为接收所述运算命令，并向所述主控模块发送读取命令以获取所述计算参数，根据所述运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送完成信号，同时将计算结果发送给所述主控模块。

所述计算命令中包含 RSA/ECC 计算；所述复杂计算控制模块 103，配
20 置为将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算，并生成与各模乘运算对应的运算命令发送给所述基本计算模块。

需要说明的是，所述复杂计算控制模块主要实现 ECC 算法中的椭圆点乘、椭圆点加运算，RSA 算法中的大数模幂运算，以及通用的模除和 Montgomery 预计算等运算控制；所述基本计算模块主要实现大数的加法、
25 减法、乘法、模约减和模乘等基本运算。

在本发明的其他实施例中，所述装置还包括：从机接口和主机接口；所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，并将所述配置参数发送给所述主控模块；所述主机接口，配置为接收所述主控模块发送的所述配置参数，并进行存储。

5 在本发明的其他实施例中，所述装置还包括：存储模块，配置为存储明文参数、密文参数、密钥参数和所述基本计算模块的计算中间结果。

需要说明的是，所述配置参数用于配置所述装置运行的算法为 RSA 算法或 ECC 算法、密钥位宽以及工作模式，所述工作模式包括加密模式和解密模式；所述 CPU 接口模块、所述从机接口和所述主机接口均支持 APB
10 协议、AHB 协议、AXI 协议和 ACE_Lite 总线协议。

参照图 2，对使用本实施例提供的同时实现 RSA/ECC 加解密算法的装置完成公钥加密运算的过程进行详细说明。图 2 所示的应用场景为在面积优先或功耗优先场景，工作流程如下：

装置初始化。处理器通过总线访问装置 CPU 接口，发送配置参数。首先配置装置的算法为 RSA 或 ECC 算法，其次配置密钥位宽，最后配置工作
15 模式为加密模式。

接收并存储数据。总线主机发送明文、密钥等数据到装置的从机接口，从机接口将数据传递给主控模块，主控模块将从机接口数据传递给主机接口由主机接口控制完成存储。

20 RSA/ECC 加密复杂计算控制。主控模块发送 RSA/ECC 加密命令到复杂计算控制模块，复杂计算控制模块根据命令将 RSA 模幂运算分解成一系列的模乘运算，将 ECC 点乘运算分解成一系列的椭圆点加运算，并将椭圆点加运算分解成大数模乘和加法运算。所有的运算命令均发送至基本计算模块。

25 完成基本计算。基本计算模块收到复杂计算控制模块发出的模乘、加

法、模约减等命令后，发送读取命令至主控模块，通过主控模块从存储器中读取计算参数，调用模块内部的面积较小的加法器、乘法器等基本运算单元实现大数乘法、加法与模约减运算。计算完成后通过主控模块将结果存入存储器中，发送完成信号至复杂计算控制模块，并等待下一次基本运算命令。

加密完成，发送密文。主控模块控制主机接口读取存储器中的密文数据，通过从机接口发送给总线主机。

本实施例的技术方案，可以同时实现 RSA 加解密运算和 ECC 加解密运算，通过 CPU 对装置控制寄存器配置实现 RSA 与 ECC 的切换；实现 RSA 签名/验证、ECDSA 签名/验证以及 ECDH 密钥交换功能；减少软件预计算等操作，降低预计算的复杂度，提高了运算效率。同时可以根据存储空间的大小，可支持任意长度的密钥。

图 3 为本发明实施例提供的同时实现 RSA/ECC 加解密算法的装置的结构示意图，如图 3 所示，本实施例提供的同时实现 RSA/ECC 加解密算法的装置包括：

CPU 接口模块、主控模块、复杂计算控制模块、基本计算模块、直接内存存取 DMA 控制器、密钥生成模块、真随机数发生模块和大数乘法处理模块；

其中，所述 CPU 接口模块，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；

所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述密钥生成模块发送密钥生成命令；向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模块发送计算参数；

所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，

根据所述计算命令，生成加减法运算命令发送给所述基本计算模块，生成模乘运算命令发送给所述大数乘法处理模块；接收所述基本计算模块和所述大数乘法处理模块的完成信号；

所述基本计算模块，配置为接收所述加减法运算命令，并向所述主控
5 模块发送读取命令以获取所述计算参数，根据所述加减法运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送所述完成信号，同时将计算结果发送给所述主控模块；

所述密钥生成模块，配置为接收所述密钥生成命令，并调用所述真随机数发生模块生成随机数生成密钥对，并发送给所述主控模块进行存储；

10 所述真随机数发生模块，配置为产生真随机数并发送给所述密钥生成模块；

所述 DMA 控制器，配置为接收并存储数据；

所述大数乘法处理模块，配置为接收所述模乘运算命令，并向所述 DMA 控制器发送读取命令以获取所述计算参数，根据所述模乘运算命令以及
15 及获取的所述计算参数完成计算，将计算的中间结果存储至存储器，向所述复杂计算控制模块发送所述完成信号。

在本发明的其他实施例中，所述大数乘法处理模块，配置为调用可伸缩的循环脉动阵列完成任意位宽的大数模乘运算。

在本发明的其他实施例中，所述计算命令中包含 RSA/ECC 计算；所述
20 复杂计算控制模块配置为，将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算和加减运算，并生成所述加减法运算命令发送给所述基本计算模块，生成所述模乘运算命令发送给所述大数乘法处理模块。

进一步地，所述装置还包括：从机接口和主机接口；所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，并将所述配置参数发
25 送给所述主控模块；所述主机接口，配置为接收所述主控模块发送的所述

配置参数，并进行存储。

需要说明的是，所述 CPU 接口模块、所述主机接口和所述从机接口均支持 APB 协议、AHB 协议、AXI 协议和 ACE_Lite 总线协议；所述配置参数配置为配置所述装置运行的算法为 RSA 算法或 ECC 算法、密钥位宽以及
5 工作模式，所述工作模式包括加密模式和解密模式。

进一步地，所述装置还包括：存储模块，配置为存储明文参数、密文参数、密钥参数、所述基本计算模块的计算中间结果和所述大数乘法处理模块的计算中间结果；实际应用中，所述存储模块采用双口随机存取存储器 RAM。

10 参照图 4，对使用本实施例提供的同时实现 RSA/ECC 加解密算法的装置完成公钥加密运算的过程进行详细说明。图 4 所示的应用场景为在速度优先场景，工作流程如下：

装置初始化。处理器通过总线访问装置 CPU 接口，发送配置参数。首先配置装置的算法为 RSA 或 ECC 算法，其次配置密钥位宽以及调用大数乘法处理器，再次配置使能密钥生成功能，最后配置工作模式为加密模式。
15

接收并存储数据。总线主机发送数据到装置的从机接口，从机接口将数据传递给 DMA 控制器，DMA 控制器将从机接口数据传递给主机接口，由主机接口控制完成存储。

生成密钥对。主控模块发送密钥生成命令至密钥生成模块，密钥生成
20 模块调用真随机数产生模块生成随机数，完成筛选质数因子，生成密钥，删除质数因子等操作实现密钥对生成。密钥对通过主控模块控制存储在存储器中，并根据需求将公钥发出。

RSA/ECC 加密复杂计算控制。主控模块发送 RSA/ECC 加密命令到复杂计算控制模块，复杂计算控制模块根据命令将 RSA 模幂运算分解成一系列的模乘运算，将 ECC 点乘运算分解成一系列的椭圆点加运算，并将椭圆
25

点加运算分解成大数模乘和加法运算。根据 CPU 配置，模乘运算命令发送至大数乘法处理模块，加法运算命令发送至基本计算模块。

模乘与加法计算。大数乘法处理模块根据复杂计算控制模块发出的命令开始一次模乘运算。从存储器中读取计算参数后，经过模块内部的循环脉动阵列完成模乘计算，中间结果存储到为该模块专门开辟的存储空间中。模乘计算完成后，大数乘法处理模块发送完成信号至复杂计算控制模块，并等待下一次模乘运算命令。基本计算模块收到复杂计算控制模块发出的加法命令后，发送读取命令至主控模块，通过主控模块从存储器中读取计算参数，调用模块内部的加法器实现大数加法与模约减运算。计算完成后通过主控模块将结果存入存储器中，发送完成信号至复杂计算控制模块，并等待下一次基本运算命令。

加密完成，发送密文。DMA 控制器控制主机接口读取存储器中的密文数据，通过从机接口发送给总线主机。

本实施例的技术方案，可以同时实现 RSA 加解密运算和 ECC 加解密运算，通过 CPU 对装置控制寄存器配置实现 RSA 与 ECC 的切换；实现 RSA 签名/验证、ECDSA 签名/验证以及 ECDH 密钥交换功能；装置中包含了真随机数发生器与密钥生成模块，可以在装置中实现密钥生成功能。与通常的软件生成密钥相比，安全性更强，密钥生成速度更快，用户操作更便捷；复杂计算控制模块能够实现 ECC 点乘，RSA 模幂，通用的模除以及 Montgomery 预计算等多种复杂运算；减少了软件预计算等操作，降低了预计算的复杂度，提高了运算效率。同时可以根据存储空间的大小，可支持任意长度的密钥。可以适用于速度优先、面积优先、功耗优先等各种不同应用场景。装置中包含了大数运算处理模块，可以快速完成模乘运算，大幅提高加解密运算速度。同时，装置中的复杂计算控制模块可以根据不同的应用场景需求，选择是否调用大数运算处理模块，从而匹配各种需求。

本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用硬件实施例、软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘
5 存储器和光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、
10 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个
15 流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机
20 实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

以上所述，仅为本发明的较佳实施例而已，并非用于限定本发明的保护范围。

工业实用性

本实施例中，可以同时实现 RSA 加解密运算和 ECC 加解密运算，通过 CPU 对装置控制寄存器配置实现 RSA 与 ECC 的切换；实现 RSA 签名/验证、ECDSA 签名/验证以及 ECDH 密钥交换功能；减少软件预计算等操作，降低预计算的复杂度，提高了运算效率。同时可以根据存储空间的大小，可支持任意长度的密钥。

5

权利要求书

1、一种同时实现 RSA/ECC 加解密算法的装置，所述装置包括：

中央处理器 CPU 接口模块、主控模块、复杂计算控制模块和基本计算模块；

5 其中，所述 CPU 接口模块，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；

所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述 CPU 接口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模
10 块发送计算参数；

所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，根据所述计算命令，生成运算命令发送给所述基本计算模块；接收所述基本计算模块的完成信号；

所述基本计算模块，配置为接收所述运算命令，并向所述主控模块
15 发送读取命令以获取所述计算参数，根据所述运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送完成信号，同时将计算结果发送给所述主控模块。

2、根据权利要求 1 所述的装置，其中，所述计算命令中包含 RSA/ECC 计算；

20 所述复杂计算控制模块配置为，将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算，并生成与各模乘运算对应的运算命令发送给所述基本计算模块。

3、根据权利要求 2 所述的装置，其中，所述装置还包括：

从机接口和主机接口；

25 所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，

并将所述配置参数发送给所述主控模块；

所述主机接口，配置为接收所述主控模块发送的所述配置参数，并进行存储。

4、根据权利要求3所述的装置，其中，所述装置还包括：

5 存储模块，配置为存储明文参数、密文参数、密钥参数和所述基本计算模块的计算中间结果。

5、根据权利要求4所述的装置，其中，所述配置参数用于配置所述装置运行的算法为RSA算法或ECC算法、密钥位宽以及工作模式，所述工作模式包括加密模式和解密模式。

10 6、根据权利要求5所述的装置，其中，所述CPU接口模块、所述从机接口和所述主机接口均支持外围总线APB协议、系统总线AHB协议、片内总线AXI协议和ACE_Lite总线协议。

7、一种同时实现RSA/ECC加解密算法的装置，其中，所述装置包括：

15 中央处理器CPU接口模块、主控模块、复杂计算控制模块、基本计算模块、直接内存存取DMA控制器、密钥生成模块、真随机数发生模块和大数乘法处理模块；

其中，所述CPU接口模块，配置为接收配置参数并发送给所述主控模块，返回所述主控模块中的状态参数；

20 所述主控模块，配置为接收并存储配置参数，根据所述配置参数向所述密钥生成模块发送密钥生成命令；向所述复杂计算控制模块发送计算命令；将所述状态参数发送给所述CPU接口模块；接收所述基本计算模块发送的读取命令，向所述基本计算模块发送计算参数；

所述复杂计算控制模块，配置为接收所述主控模块发送的计算命令，
25 根据所述计算命令，生成加减法运算命令发送给所述基本计算模块，生

成模乘运算命令发送给所述大数乘法处理模块；接收所述基本计算模块和所述大数乘法处理模块的完成信号；

所述基本计算模块，配置为接收所述加减法运算命令，并向所述主控模块发送读取命令以获取所述计算参数，根据所述加减法运算命令以及获取的所述计算参数完成计算，向所述复杂计算控制模块发送所述完成信号，同时将计算结果发送给所述主控模块；

所述密钥生成模块，配置为接收所述密钥生成命令，并调用所述真随机数发生模块生成随机数生成密钥对，并发送给所述主控模块进行存储；

10 所述真随机数发生模块，配置为产生真随机数并发送给所述密钥生成模块；

所述 DMA 控制器，配置为接收并存储数据；

所述大数乘法处理模块，配置为接收所述模乘运算命令，并向所述 DMA 控制器发送读取命令以获取所述计算参数，根据所述模乘运算命令以及获取的所述计算参数完成计算，将计算的中间结果存储至存储器，向所述复杂计算控制模块发送所述完成信号。

8、根据权利要求 7 所述的装置，其中，所述计算命令中包含 RSA/ECC 计算；

20 所述复杂计算控制模块配置为，将接收到的所述计算命令中的 RSA/ECC 计算分解成一系列模乘运算和加减运算，并生成所述加减法运算命令发送给所述基本计算模块，生成所述模乘运算命令发送给所述大数乘法处理模块。

9、根据权利要求 8 所述的装置，其中，所述装置还包括：

从机接口和主机接口；

25 所述从机接口，配置为接收所述 CPU 接口模块发送的所述配置参数，

并将所述配置参数发送给所述主控模块;

所述主机接口, 配置为接收所述主控模块发送的所述配置参数, 并进行存储。

10、根据权利要求 9 所述的装置, 其中, 所述 CPU 接口模块、所述
5 主机接口和所述从机接口均支持外围总线 APB 协议、系统总线 AHB 协议、片内总线 AXI 协议和 ACE_Lite 总线协议。

11、根据权利要求 9 所述的装置, 其中, 所述配置参数用于配置所述装置运行的算法为 RSA 算法或 ECC 算法、密钥位宽以及工作模式, 所述工作模式包括加密模式和解密模式。

10 12、根据权利要求 7 所述的装置, 其中, 所述装置还包括:

存储模块, 配置为存储明文参数、密文参数、密钥参数、所述基本计算模块的计算中间结果和所述大数乘法处理模块的计算中间结果。

13、根据权利要求 12 所述的装置, 其中, 所述存储模块采用双口随机存取存储器 RAM。

15 14、根据权利要求 8 所述的装置, 其中, 所述大数乘法处理模块, 配置为调用可伸缩的循环脉动阵列完成任意位宽的大数模乘运算。

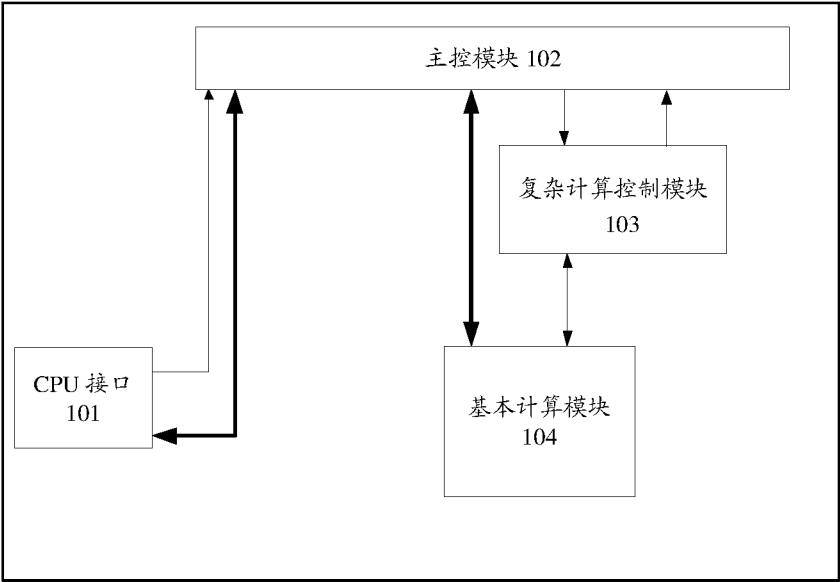


图 1

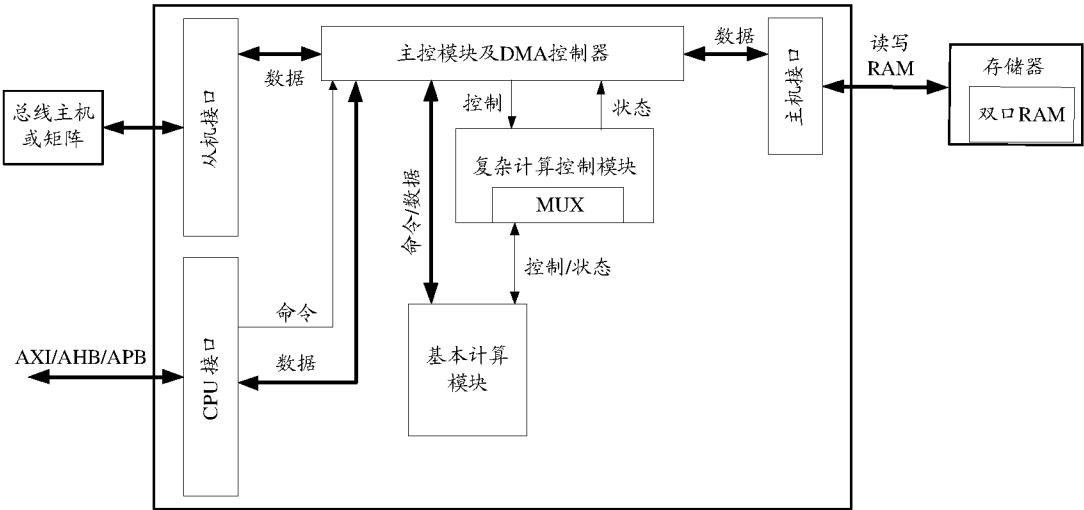


图 2

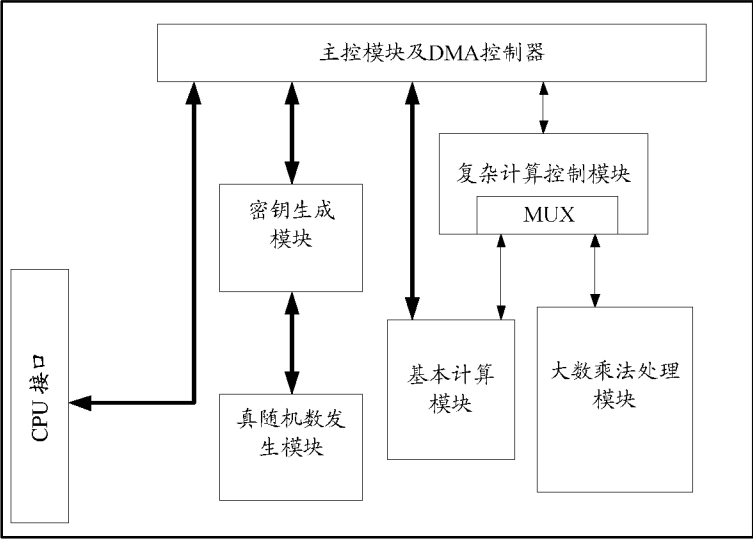


图 3

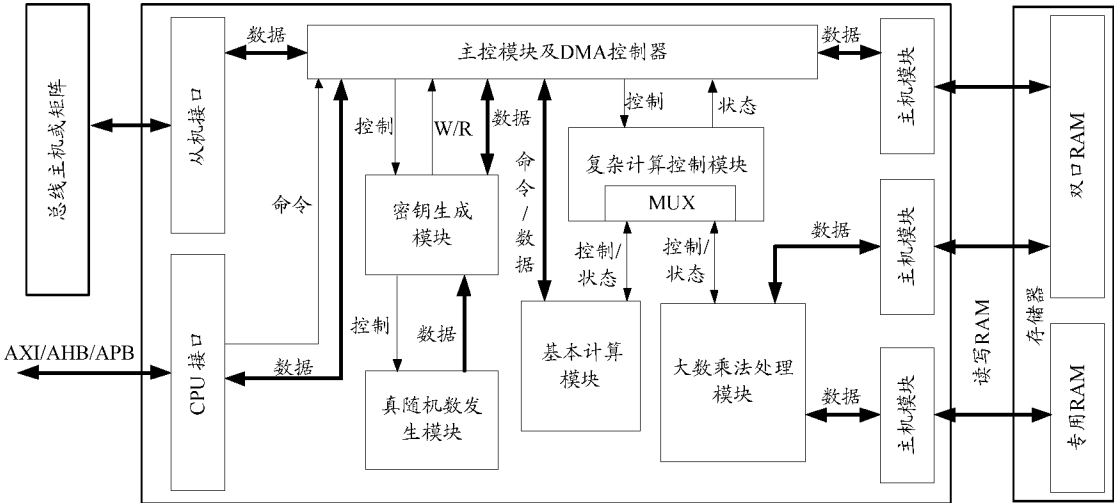


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/107549

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/30 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC: encrypt, decrypt, encryption and decryption, RSA, ECC, encipher, decipher, Ron Rivest, Adi Shamir, Leonard Adleman, elliptic curve cryptography, at the same time, speed, area, parameter, configuration

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101212292 A (AISINO CORPORATION INC.), 02 July 2008 (02.07.2008), description, pages 3-5	1-14
A	CN 105095739 A (NATIONZ TECHNOLOGIES INC.), 25 November 2015 (25.11.2015), the whole document	1-14
A	CN 102279725 A (BEIJING HUADA INFOSEC TECHNOLOGY CO., LTD.), 14 December 2011 (14.12.2011), the whole document	1-14
A	US 2014108798 A1 (SONY CORPORATION), 17 April 2014 (17.04.2014), the whole document	1-14

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 24 January 2017 (24.01.2017)	Date of mailing of the international search report 21 February 2017 (21.02.2017)
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer ZHANG, Qi Telephone No.: (86-10) 62413262

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2016/107549

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101212292 A	02 July 2008	None	
CN 105095739 A	25 November 2015	None	
CN 102279725 A	14 December 2011	CN 102609239 A	25 July 2012
US 2014108798 A1	17 April 2014	CN 103731408 A	16 April 2014
		JP 2014081787 A	08 May 2014

国际检索报告

国际申请号

PCT/CN2016/107549

A. 主题的分类

H04L 9/30(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CNPAT, CNKI, WPI, EPDOC: 加密, 解密, 加解密, RSA, ECC, 同时, 速度, 面积, 参数, 配置, encipher, decipher, Ron Rivest, Adi Shamir, Leonard Adleman, elliptic curve cryptography, at the same time, speed, area, parameter, configuration

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	CN 101212292 A (航天信息股份有限公司) 2008年 7月 2日 (2008 - 07 - 02) 说明书第3-5页	1-14
A	CN 105095739 A (国民技术股份有限公司) 2015年 11月 25日 (2015 - 11 - 25) 全文	1-14
A	CN 102279725 A (北京华大信安科技有限公司) 2011年 12月 14日 (2011 - 12 - 14) 全文	1-14
A	US 2014108798 A1 (SONY CORPORATION) 2014年 4月 17日 (2014 - 04 - 17) 全文	1-14

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2017年 1月 24日

国际检索报告邮寄日期

2017年 2月 21日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

传真号 (86-10)62019451

受权官员

张琦

电话号码 (86-10)62413262

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/107549

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101212292	A	2008年 7月 2日	无			
CN	105095739	A	2015年 11月 25日	无			
CN	102279725	A	2011年 12月 14日	CN	102609239	A	2012年 7月 25日
US	2014108798	A1	2014年 4月 17日	CN	103731408	A	2014年 4月 16日
				JP	2014081787	A	2014年 5月 8日

表 PCT/ISA/210 (同族专利附件) (2009年7月)