



(12) 发明专利申请

(10) 申请公布号 CN 102521166 A

(43) 申请公布日 2012. 06. 27

(21) 申请号 201110398177. 8

(22) 申请日 2011. 12. 05

(71) 申请人 苏州希图视鼎微电子有限公司

地址 215021 江苏省苏州市工业园区星湖街
328 号创意产业园 2-B702 单元

(72) 发明人 妙维 袁宏骏 余红斌 李张丰

(74) 专利代理机构 南京苏科专利代理有限责任
公司 32102

代理人 陆明耀 姚姣阳

(51) Int. Cl.

G06F 12/14 (2006. 01)

G06F 13/28 (2006. 01)

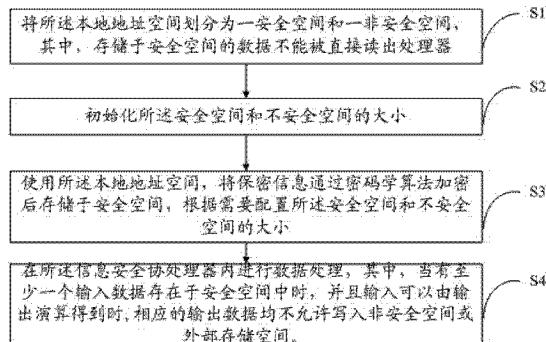
权利要求书 1 页 说明书 5 页 附图 2 页

(54) 发明名称

信息安全协处理器及其内部存储空间的管理
方法

(57) 摘要

本发明提供一种信息安全协处理器中内部存
储空间的管理方法，包括如下步骤：将所述本地
地址空间划分为一安全空间和一非安全空间，其
中，所述安全空间用于存储保密信息；初始化所
述安全空间和非安全空间的大小；使用所述本地
地址空间，将保密信息存储于安全空间，根据需要
配置所述安全空间和非安全空间的大小；在所述
信息安全协处理器内进行数据处理，其中，当有至
少一个输入数据存在于安全空间中，并且输入可
以由输出演算得到时，相应的输出数据均不允许
写入非安全空间或外部存储空间。本发明在保护
了重要数据的同时，也方便了对协处理器的使用。
同时，本发明中安全空间的大小可以根据需要进
行更改，从而方便了不同的应用需求和系统开发。



1. 一种信息安全协处理器，其特征在于，其包括如下单元：

本地地址空间单元：包括一安全空间和一非安全空间，两者均可配置，存储于安全空间的数据不能被直接读出处理器；

控制单元：用于通过一定的控制逻辑进行流程控制；

数学运算单元：用于实现数学运算；

密码算法引擎：用于执行密码学算法，以实现加密或解密功能。

2. 根据权利要求 1 所述的信息安全协处理器，其特征在于，所述信息安全协处理器还包括一用于负责 AHB 总线和本地地址空间单元之间数据传输的 DMA 引擎。

3. 根据权利要求 1 所述的信息安全协处理器，其特征在于，所述信息安全协处理器还包括一寄存器堆。

4. 根据权利要求 3 所述的信息安全协处理器，其特征在于，所述寄存器堆包括控制寄存器和状态寄存器。

5. 根据权利要求 1 所述的信息安全协处理器，其特征在于，所述数学运算包括复制、或者异或运算、或者以上两者的组合。

6. 一种信息安全协处理器中内部存储空间的管理方法，其特征在于，所述信息安全协处理器具有一外部可见的本地地址空间，所述方法包括如下步骤：

S1、将所述本地地址空间划分为一安全空间和一非安全空间，其中，存储于安全空间的数据不能被直接读出处理器；

S2、初始化所述安全空间和非安全空间的大小；

S3、使用所述本地地址空间，将保密信息存储于安全空间，根据需要配置所述安全空间和非安全空间的大小；

S4、在所述信息安全协处理器内进行数据处理，其中，当有至少一个输入数据存在于安全空间中时，并且输入可以由输出演算得到时，相应的输出数据均不允许写入非安全空间或外部存储空间。

7. 根据权利要求 6 所述的方法，其特征在于，所述数据处理的方式包括数学运算，其中，所述数学运算包括复制、或者异或运算、或者以上两者的组合。

8. 根据权利要求 6 所述的方法，其特征在于，所述步骤 S3 中“根据需要配置所述安全空间和非安全空间的大小”的步骤具体为：

所述安全空间和非安全空间的划分可以更改，其中，安全空间的大小只能增加，且原来属于安全空间的区域不能被更改为非安全空间。

9. 根据权利要求 6 所述的方法，其特征在于，该方法还包括通过 DMA 引擎在 AHB 总线和本地地址空间之间传输数据。

信息安全协处理器及其内部存储空间的管理方法

技术领域

[0001] 本发明涉及信息安全处理领域，尤其涉及使用密码学算法的信息安全协处理器及其内部存储空间的管理方法。

背景技术

[0002] 随着网络技术的迅猛发展，信息安全技术在当前变得尤为重要。对于日益增长的网络流量，单纯利用软件方式对数据流进行加密或者解密运算已经不能满足需求，因此构建由硬件实现的专用密码芯片的方法称为了一种新趋势。当前的信息安全芯片包括单功能型(比如 DES、3DES、AES、RSA 等)、多功能型、高端芯片、SOC、ASIC 等等。在嵌入式系统(Embedded System)应用中，提供信息安全解决方案的芯片被广泛采用。而在一个 SOC 系统中，信息安全处理器将以协处理器的形式出现。

[0003] 然而，一个提供信息安全防护功能的协处理器，可以简单的只是进行一些密码学算法，而不提供其它的保护；也可以是一个复杂的子系统，提供完整的方案和安全的执行环境。第一种类型的协处理器比较容易嵌入到不同系统中，但系统层面的安全保护困难且复杂。第二种类型的协处理器提供很好的安全防护方案，但是限制了使用它的系统的设计灵活性。

[0004] 区别于上述两种类型，非常有必要提供一种新的具备安全防护措施的协处理器，以实现在保持系统设计的灵活性的同时，可以减少系统层面信息保护的负担。

发明内容

[0005] 为解决上述技术问题，本发明的目的在于提供一种信息安全协处理器，其通过提供了一个外部可见的、包含大小可配置的安全和不安全两个区域的本地存储空间来进行信息的存储，其中存储在安全区域的信息不会被处理器外部得到。在实现信息保密的同时，该信息安全处理器可方便不同的应用需求和系统开发。

[0006] 相应地，本发明的目的还在于提供一种上述信息安全协处理器中内部存储空间的管理方法。

[0007] 为实现上述发明目的之一，本发明的一种信息安全协处理器，包括如下单元：

本地地址空间单元：包括一安全空间和一非安全空间，两者均可配置，存储于安全空间的数据不能被直接读出处理器；

控制单元：用于通过一定的控制逻辑进行流程控制；

数学运算单元：用于实现数学运算；

密码算法引擎：用于执行密码学算法，以实现加密或解密功能。

[0008] 作为本发明的进一步改进，所述信息安全协处理器还包括一用于负责 AHB 总线和本地地址空间单元之间数据传输的 DMA 引擎。

[0009] 作为本发明的进一步改进，所述信息安全协处理器还包括一寄存器堆。

[0010] 作为本发明的进一步改进，所述寄存器堆包括控制寄存器和状态寄存器。

[0011] 作为本发明的进一步改进，所述数学运算包括复制、或者异或运算、或者以上两者的组合。

[0012] 为实现本发明的另一发明目的，一种信息安全协处理器中内部存储空间的管理方法，所述信息安全协处理器具有一外部可见的本地地址空间，所述方法包括如下步骤：

S1、将所述本地地址空间划分为一安全空间和一非安全空间，其中，存储于安全空间的数据不能被直接读出处理器；

S2、初始化所述安全空间和非安全空间的大小；

S3、使用所述本地地址空间，将保密信息存储于安全空间，根据需要配置所述安全空间和非安全空间的大小；

S4、在所述信息安全协处理器内进行数据处理，其中，当有至少一个输入数据存在于安全空间中时，并且输入可以由输出演算得到时，相应的输出数据均不允许写入非安全空间或外部存储空间。

[0013] 作为本发明的进一步改进，所述数据处理的方式包括数学运算，其中，所述数学运算包括复制、或者异或运算、或者以上两者的组合。

[0014] 作为本发明的进一步改进，所述步骤 S3 中“根据需要配置所述安全空间和非安全空间的大小”的步骤具体为：

所述安全空间和非安全空间的划分可以更改，其中，安全空间的大小只能增加，且原来属于安全空间的区域不能被更改为非安全空间。

[0015] 作为本发明的进一步改进，该方法还包括通过 DMA 引擎在 AHB 总线和本地地址空间之间传输数据。

[0016] 与现有技术相比，本发明通过提供了一个可配置的、外部可见的安全空间来进行保密信息的存储，在保护了重要数据的同时，也方便了对协处理器的使用。同时，本发明中安全空间的大小可以根据需要进行更改，从而方便了不同的应用需求和系统开发。

附图说明

[0017] 图 1 是本发明一实施方式中信息安全协处理器的工作原理图；

图 2 是本发明一实施方式中信息安全处理器的安全空间的使用流程示意图；

图 3 示出的是本发明一实施方式中信息安全处理器的安全空间与非安全空间的四种配置；

图 4 是本发明一实施方式中信息安全协处理器内部存储空间的管理方法的工作流程图。

具体实施方式

[0018] 以下将结合附图所示的具体实施方式对本发明进行详细描述。但这些实施方式并不限制本发明，本领域的普通技术人员根据这些实施方式所做出的结构、方法、或功能上的变换均包含在本发明的保护范围内。

[0019] 请参照图 1 所示，在本发明一具体实施方式中，一种信息安全协处理器，包括如下单元：本地地址空间单元 10、控制单元 20、数学运算单元、密码算法引擎 40、DMA（Direct Memory Access，直接内存存取）引擎 50 以及寄存器堆 60。一个协处理器往往需要一定的

内部存储空间,而存放在其中的重要安全相关数据需要严格的保护。另一方面,协处理器的存储空间也要求一定的外部可见性以方便使用。本发明提出了一套协处理器内部存储空间的管理方案,在保护了重要数据的同时,也方便了对协处理器的使用。

[0020] 其中,在本实施方式中,DMA (Direct Memory Access,直接内存存取)引擎50用于负责 AHB 总线和本地地址空间单元之间数据传输,在其他实施方式中,DMA 引擎可替换为其他能实现类似功能的部件。其中,本发明采用两种总线进行数据传输 :AHB(Advanced High performance Bus) 系统总线和 APB(Advanced Peripheral Bus) 外围总线,AHB 主要用于高性能模块(如 CPU、DMA 和 DSP 等)之间的连接;APB 主要用于低带宽的周边外设之间的连接,例如 UART、1284 等。

[0021] 寄存器堆 60 包括用于控制和确定处理器的操作模式以及当前执行任务的特性的控制寄存器、用于体现当前指令执行结果的各种状态信息状态寄存器等等。寄存器堆 60 可于 APB 总线之间进行数据传输。

[0022] 本地地址空间单元 10 包括一安全空间和一非安全空间,两者均可配置的,存储于安全空间的数据不能被直接读出处理器;协处理器本地地址空间外部可见,被划分为安全和不安全两块。为了防止存储在安全区域的信息被泄漏,对于以下两个路径:(一)由本地地址空间经 DMA 引擎到 AHB 总线、(二)由本地地址空间经数学运算单元中的“=”(复制)或者“xor”(异或)运算后到本地地址空间,当有输入数据存在于安全地址空间中时,不允许输出数据写入非安全地址空间或外部存储空间,经密码算法引擎的数据的存放规则由硬件固化。

[0023] 关于外部可见性和安全区域中数据的外部不可得性,这两个并不矛盾。整个本地存储器是外部可见的,但安全区域的数据是禁止被读出的。同一个地址,当被划分为安全区域时,该地址可见但不能被读取。当被划分为非安全区域时,该地址可见并能够被读取。

[0024] 控制单元 20 用于通过一定的控制逻辑进行流程控制;

数学运算单元 30 用于实现数学运算,其中,在本实施方式中,数学运算可包括复制、或者异或运算、或者以上两者的组合。

[0025] 密码算法引擎 40 用于执行密码学算法,以实现加密或解密功能。密码算法是用于加密和解密的数学函数,密码算法是密码协议的基础。

[0026] 于本发明中,由于协处理器的外部可见(直接或间接)地址空间被划分为安全和不安全两种。如果将协处理器内部的数据处理用 $(y_1, \dots, y_M) = f(x_1, \dots, x_N)$, $M > 0, N > 0$, 表示,当函数的输入参数可以由结果反推出来时,只要函数的输入参数 x_i , $i=1, \dots, N$, 中有至少一个全部或部分来自安全地址空间,所有函数结果都不能全部或部分存在于非安全地址空间或外部地址空间中。

[0027] 参图 2 所示,当系统硬复位后,开始安全启动过程,在执行安全启动过程中,初始化安全空间大小,安全启动结束后,可以调整安全空间和非安全空间的比例(安全空间只能增加),开始使用协处理器。过程中可以根据需要再次增加安全空间比例。在一次硬复位后,协处理器的安全地址空间和非安全地址空间的划分可以更改,但是安全地址空间的大小只能增加,并且原来属于安全地址空间的区域不能被更改为非安全地址空间。

[0028] 参图 3 所示,在本实施方式中,本地地址空间为 4KB 的存储空间,对于此处 4KB 的本地地址空间,安全区和非安全区允许如图所示的四种配置,分别对应四个配置编号:0、1、

2、3。在一次硬复位后,配置 0 被采用。寄存器堆中存在一个标记,当它被置为 1,则变更为当前编号的下一个编号所对应的配置,并将该标记清 0。

[0029] 如图 4 所示,在本发明的一具体实施方式中,一种信息安全协处理器中内部存储空间的管理方法,该方法使用上述提及的信息安全协处理器来实现,所述信息安全协处理器具有一外部可见的本地地址空间,该方法包括如下步骤:

S1、将所述本地地址空间划分为一安全空间和一非安全空间,其中,存储于安全空间的数据不能被直接读出处理器;安全空间和非安全空间均为外部可见的,所以比较方便使用,且两者也是可配置的,这样也方便于根据需求作相应的更改。

[0030] 关于外部可见性和安全区域中数据的外部不可得性,这两个并不矛盾。整个本地存储器是外部可见的,但安全区域的数据是禁止被读出的。同一个地址,当被划分为安全区域时,该地址可见但不能被读取。当被划分为非安全区域时,该地址可见并能够被读取。

[0031] S2、初始化所述安全空间和非安全空间的大小;优选地,通过硬复位来初始化,初始化后的安全空间为 [0KB, 0KB), 非安全空间 [0KB, 4KB), 对应于配置编号 0。

[0032] S3、使用所述本地地址空间,将保密信息通过密码学算法加密后存储于安全空间,根据需要配置所述安全空间和非安全空间的大小;这里说指的是,安全空间的可适当增加空间以适应需求。

[0033] S4、在所述信息安全协处理器内进行数据处理,其中,当有至少一个输入数据存在于安全空间中时,并且输入可以由输出演算得到时,相应的输出数据均不允许写入非安全空间或外部存储空间。由于协处理器的外部可见(直接或间接)地址空间被划分为安全和不安全两种。如果将协处理器内部的数据处理用 $(y_1, \dots, y_M) = f(x_1, \dots, x_N)$, $M > 0$, $N > 0$, 表示,当函数的输入参数可以由结果反推出来时,只要函数的输入参数 x_i , $i=1, \dots, N$, 中有至少一个全部或部分来自安全地址空间,所有函数结果都不能全部或部分存在于非安全地址空间或外部地址空间中。

[0034] 其中,优选地,所述数据处理的方式包括数学运算,其中,所述数学运算包括复制、或者异或运算、或者以上两者的组合。

[0035] 其中,优选地,所述步骤 S3 中“根据需要配置所述安全空间和非安全空间的大小”的步骤具体为:

所述安全空间和非安全空间的划分可以更改,其中,安全空间的大小只能增加,且原来属于安全空间的区域不能被更改为非安全空间。

[0036] 其中,优选地,该方法还包括通过 DMA 引擎在 AHB 总线和本地地址空间之间传输数据。

[0037] 与现有技术相比,本发明通过提供了一个可配置的、外部可见的安全空间来进行保密信息的存储,在保护了重要数据的同时,也方便了对协处理器的使用。同时,本发明中安全空间的大小可以根据需要进行更改,从而方便了不同的应用需求和系统开发。

[0038] 以上所描述的装置实施方式仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施方式方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0039] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和 / 或硬件中实现。

[0040] 以上所描述的装置实施方式仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施方式方案的目的。本领域普通技术人员在不付出创造性劳动的情况下,即可以理解并实施。

[0041] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述,例如程序模块。一般地,程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请,在这些分布式计算环境中,由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中,程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0042] 应当理解,虽然本说明书按照实施方式加以描述,但并非每个实施方式仅包含一个独立的技术方案,说明书的这种叙述方式仅仅是为清楚起见,本领域技术人员应当将说明书作为一个整体,各实施方式中的技术方案也可以经适当组合,形成本领域技术人员可以理解的其他实施方式。

[0043] 上文所列出的一系列的详细说明仅仅是针对本发明的可行性实施方式的具体说明,它们并非用以限制本发明的保护范围,凡未脱离本发明技艺精神所作的等效实施方式或变更均应包含在本发明的保护范围之内。

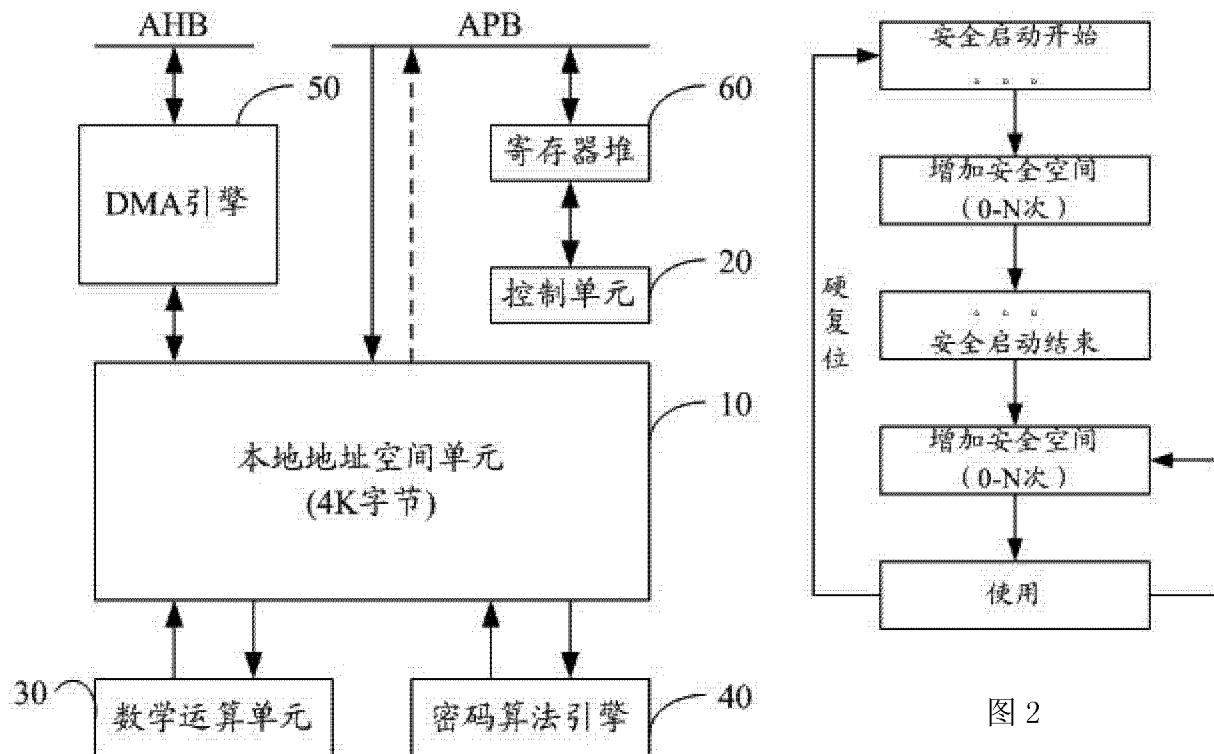


图 1

图 2

配置编号	安全区域	非安全区域
0#	[0KB, 0KB)	[0KB, 4KB)
1#	[0KB, 1KB)	[1KB, 4KB)
2#	[0KB, 2KB)	[2KB, 4KB)
3#	[0KB, 3KB)	[3KB, 4KB)

图 3

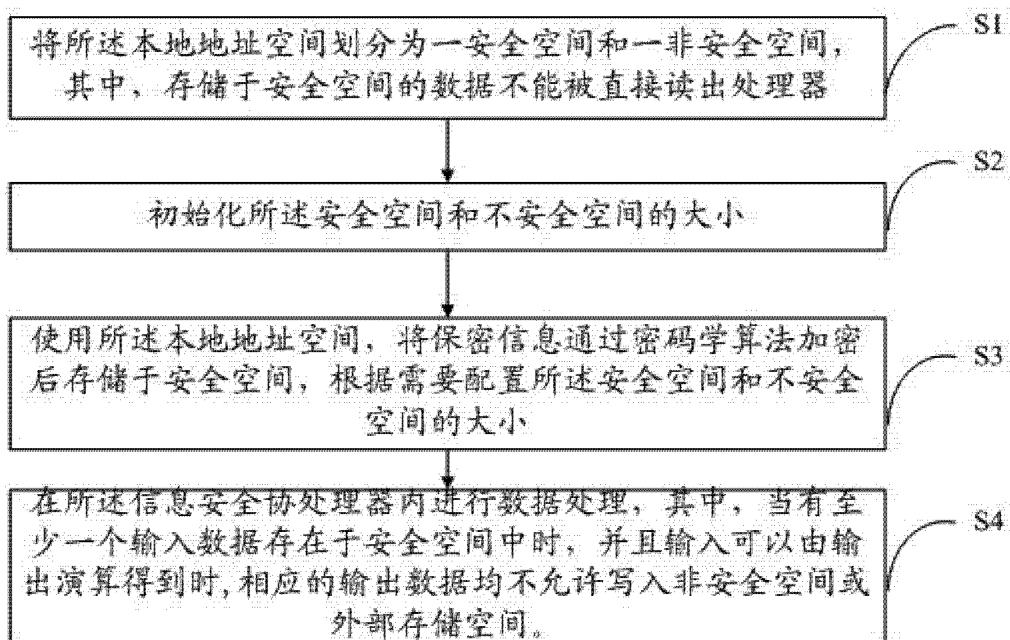


图 4