

一种加速器、加速方法和电子设备

5 本申请要求于 2022 年 02 月 25 日提交中国专利局、申请号为 202210179799.X、申请名称为“一种加速器、加速方法和电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术，具体涉及一种加速器、加速方法和电子设备。

背景技术

10 ECC（Elliptic Curves Cryptography，椭圆曲线加密）是一种主流的非对称密码算法，被广泛应用在很多安全领域，比如安全传输、密钥交换、数字签名、隐私计算、安全多方计算等。ECC 算法包括点乘，模加，模乘，模减等运算。其中点乘运算可以由若干次的模加，模乘，模减等实现。目前通过加速器实现 ECC 算法。

15 相关技术一，通过状态机严格控制加速器的各个计算环节，实现特定的计算流程以实现特定的功能，由于状态机的控制和修改比较繁琐，导致这些加速器只能实现特定的功能，使用不够灵活。

相关技术二，通过不同的指令调用加速器中不同的计算单元分别实现点乘、模乘、模加等运算，如此导致硬件资源的浪费。

发明内容

20 有鉴于此，本申请至少公开一种加速器。所述加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算；所述加速器还包括：获取单元，获取根据待实现的目标类型运算，生成的与所述目标类型运算对应的目标微码指令；所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标
25 输入数据；解析单元，解析所述目标微码指令，得到与所述目标输入数据对应的解析结果；控制单元，响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

30 在一些实施例中，所述加速器与处理器 CPU 通信连接；所述加速器或所述 CPU，用于：获取针对操作数执行目标类型运算的操作程序；根据所述目标类型运算，基于所述操作程序包括的操作数，生成与所述目标类型运算对应的所述目标微码指令。

在一些实施例中，所述加速器还包括预设的数据存储空间；所述数据存储空间存储了用于生成微码指令的预设操作数；所述加速器或所述 CPU 还用于：将解析得到的所述操作数存储至所述数据存储空间；根据所述目标类型运算，基于所述操作数和/或所述预设操作数在所述数据存储空间的存储地址，生成所述目标微码指令。

- 5 在一些实施例中，所述解析结果包括所述目标输入数据的存储地址；所述控制单元，根据所述存储地址，控制所述计算单元从所述数据存储空间读取所述目标输入数据并基于所述目标输入数据执行所述目标类型的运算。

所述基础运算包括模加运算和模乘运算，所述通用运算逻辑为对两次模加运算的计算结果进行模乘。

- 10 在一些实施例中，所述通用运算逻辑所需的输入包括第一输入，第二输入，第三输入与第四输入；所述通用运算逻辑运算过程包括：对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；对所述第三输入与所述第四输入进行模加运算，得到第二模加结果；对所述第一模加结果与所述第二模加结果进行模乘运算，得到最终计算结果。

- 15 在一些实施例中，所述操作数包括第一操作数与第二操作数；所述加速器或所述 CPU，进一步：响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数，将所述第三输入置为 1，将所述第四输入置为 0；响应于所述目标类型运算为对所述第一操作数与第二操作数进行模减运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数并将所述第二输入对应的符号调整为负号，将所述第三输入置为 1，将所述第四输入置为 0；响应于所述目标类型运算为对所述第一操作数与第二操作数进行模乘运算，将所述第三输入置为所述第二操作数，将所述第二输入和所述第四输入置为 0；响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加的平方运算，将所述第一输入和所述第三输入置为所述第一操作数，将所述第二输入和所述第四输入置为所述第二操作数；根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

- 20 在一些实施例中，所述操作程序还包括点乘标量；所述目标类型运算为对所述点乘标量和所述操作数进行点乘运算；所述加速器或所述 CPU，进一步：根据所述操作程序包括的所述点乘标量和操作数，生成用于实现所述点乘运算的多条目标微码指令；所述加速器，进一步：控制所述计算单元执行所述多条目标微码指令中的每一目标微码指令，以完成所述点乘运算。

- 25 在一些实施例中，所述模乘运算包含第一类型的模乘运算与第二类型的模乘运算；所述加速器还包括预设的数据存储空间；所述数据存储空间存储了预设常数；所述预设常数用于第一数据域和第二数据域之间的相互转变；所述第一数据域用于所述第一类型的模乘运算；所述第二数据域用于所述第二类型的模乘运算；所述计算单元，响应于所述模乘运算由所述第一类型转变为所述第二类型，获取所述预设常数，并根据所述预设常数，将所

述第一数据域转换为所述第二数据域以实现所述第二类型的模乘运算；响应于所述模乘运算由所述第二类型转变为所述第一类型，获取所述预设常数，并根据所述预设常数，将所述第二数据域转换为所述第一数据域以实现所述第一类型的模乘运算。

5 在一些实施例中，所述控制单元包括断点子单元；所述断点子单元，响应于接收到中断指令，中断所述计算单元执行后续微码指令，以使与所述加速器对应的调试单元获取所述计算单元的计算结果，并输出所述计算结果与预设计算结果的比较结果。

在一些实施例中，所述加速器为基于 FPGA 或 ASIC 实现的用于椭圆曲线算法加速的协处理器；或，基于 CPU 实现的用于针对所述椭圆曲线算法进行算法加速的辅助加速模块。

本申请还提出一种加速方法，应用于加速器。所述加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算；所述方法包括：获取根据待实现的目标类型运算，生成的与所述目标类型运算对应的目标微码指令；所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据；解析所述目标微码指令，得到与所述目标输入数据对应的解析结果；响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

本申请还提出一种电子设备，所述电子设备包括如前述任一实施例示出的加速器。

前述方法中，第一，可以通过根据待实现的目标类型运算，生成目标微码指令，并根据目标微码指令没完成对计算单元内通用运算逻辑实现目标类型运算所需的输入的相关配置，以使加速器完成所述目标类型运算，与相关技术一相比，可以通过变更微码指令的方式可以使加速器实现不同类型运算，简化了对加速器的配置操作，降低了对加速器的配置难度，从而可以更灵活地使用加速器。

第二，在计算单元中部署了由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算，以相关技术二相比，可以通过一个计算单元可以实现至少两种类型的运算，节省了硬件资源。

应当理解的是，以上所述的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

30 为了更清楚地说明本申请一个或多个实施例或相关技术中的技术方案，下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请一个或多个实施例中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本申请实施例示出的一种加速器的结构示意图；

图 2 为本申请实施例示出的一种加速器的结构示意图；

图 3 本申请实施例示出的一种加速器的结构示意图；

图 4 为本申请实施例示出的一种加速方法的方法流程示意图。

具体实施方式

下面将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本申请相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本申请的一些方面相一致的设备和方法的例子。

在本申请使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在可以包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。还应当理解，本文中所使用的词语“如果”，取决于语境，可以被解释成为“在……时”或“当……时”或“响应于确定”。

基于此，本申请提出一种加速器。所述加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算；所述加速器还包括：获取单元，获取根据待实现的目标类型运算，生成的与目标类型运算对应的目标微码指令；所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据；解析单元，解析所述目标微码指令，得到与目标输入数据对应的解析结果；控制单元，响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

前述方法中，第一，可以通过根据待实现的目标类型运算，生成目标微码指令，并根据目标微码指令未完成对计算单元内通用运算逻辑实现目标类型运算所需的输入的相关配置，以使加速器完成所述目标类型运算，与相关技术一相比，可以通过变更微码指令的方式可以使加速器实现不同类型运算，简化了对加速器的配置操作，降低了对加速器的配置难度，从而可以更灵活地使用加速器。

第二，在计算单元中部署了由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算，以相关技术二相比，可以通过一个计算单元可以实现至少两种类型的运算，节省了硬件资源。

请参见图 1，图 1 为本申请实施例示出的一种加速器的结构示意图。

如图 1 所示，加速器 10 可以包括依次连接的获取单元 11，解析单元 12，控制单元 13，计算单元 14。其中，所述计算单元 14 包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算。

所述加速器可以基于硬件与软件相结合实现 ECC 加速。所述加速器包括的各种功能单元可以是硬件单元、软件装置单元、或者软件装置和硬件相结合的单元。

在一些实施例中,所述加速器基于协处理器或CPU实现;其中所述加速器为基于FPGA或ASIC实现的用于椭圆曲线算法加速的协处理器;或,基于CPU实现的用于针对所述椭圆曲线算法进行算法加速的辅助加速模块。

所述获取单元11,可以获取根据待实现的目标类型运算,生成的与目标类型运算对应的目标微码指令;所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据。

所述目标类型运算可以是与椭圆曲线算法相关的运算。在一些实施例中,所述目标类型运算可以包括以下至少一种:

模加;模减;模乘;模加的平方;模减的平方;模加乘模减;模加乘模加;模减乘模减。

所述目标微码指令用于触发加速器10完成所述目标类型运算。由于微码指令具备逻辑简单,编写方便等性质,从而可以简化开发人员的研发难度。

所述目标微码指令可以通过以下至少两种方式指示所述目标输入数据。其一,目标微码指令直接携带目标输入数据;其二,目标微码指令携带目标输入数据的存储地址。

在一些方式中,所述目标微码指令可以是根据需求人工编写得到的程序指令。这些目标微码指令可以在通过编码器进行编码之后经过配置总线发送至所述获取单元11。所述加速器可以通过所述获取单元11获取所述目标微码指令。

在一些方式中,所述目标微码指令可以通过非人工方式,对操作程序进行转换操作之后得到的指令。所述操作程序为根据需求编写的代码程序。所述转换操作可以在所述加速器10或与所述加速器通信连接的CPU中执行。完成所述转换操作之后,可以将所述目标微码指令发送至所述获取单元11。

所述加速器或所述CPU,可以用于:获取针对操作数执行目标类型运算的操作程序;根据所述目标类型运算,基于所述操作程序包括的操作数,生成与目标类型运算对应的所述目标微码指令。由此可以采用非人工方式对操作程序进行转换操作生成可以使加速器执行目标类型运算的目标运算操作,对于研发人员无需了解加速器内部的运算逻辑,简化了开发代码的难度,从而提升了加速器的实用性。

在一些方式中,可以预先维护所述计算单元实现每一种类型的运算时所需的输入数据配置规则。在进行所述转换操作时,可以根据所述目标类型运算,确定对应的目标配置规则,然后根据所述目标配置规则以及所述操作数,为目标微码指令配置输入数据,以生成目标微码指令。

所述解析单元12,可以解析所述目标微码指令,得到与目标输入数据对应的解析结果。

在一些实施例中,获取单元11可以将获取的目标微码指令存储在预设的指令存储空间中。所述解析单元12可以从所述指令存储空间中获取未执行过的所述目标微码指令,并进行相关解析,得到解析结果。

如果所述目标微码指令直接携带目标输入数据，则所述解析结果包括所述目标输入数据。

如果所述目标微码指令携带的是所述目标输入数据的存储地址，则所述解析结果包括所述存储地址。

5 在一些实施例中，所述解析单元 12 也可以解析出目标微码指令的指令类型，以辅助控制单元执行微码指令。例如，有些微码指令可能是数据搬移（MOV）指令，此时控制单元仅执行数据搬移操作即可，无需控制计算单元进行运算。再例如，有些微码指令可能涉及到减法运算（比如模减，模加乘模减，模减的平方等），控制单元可以控制计算单元将获取的输入数据的符号调整为负号。

10 所述控制单元 13，可以响应于所述解析结果控制所述计算单元 14，以使所述计算单元 14 获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

其中，如果所述解析结果包括所述目标输入数据，则计算单元可以从所述解析结果获取所述目标输入数据。

15 如果所述解析结果包括所述目标输入数据的存储地址，则计算单元可以根据所述存储地址，从预设的数据存储空间中读取所述目标输入数据。

在一些实施例中，所述基础运算包括模加运算和模乘运算，所述通用运算逻辑为对两次模加运算的计算结果进行模乘。由此可以通过一种通用运算逻辑实现至少两种运算。

例如，所述通用运算逻辑用公式表示为 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p)$ 。如果令 C 为 0，D 为 1，则该通用运算逻辑可以变为 $(A+B) \bmod (p)$ ，相当于实现了 A 和 B 的模加运算。如果令 B 和 D 为 0，则该通用运算逻辑可以变为 $(A*C) \bmod (p)$ ，相当于实现了 A 和 C 的模乘运算。

在一些实施例中，所述基础运算包括模加运算和模乘运算，所述通用运算逻辑所需的输入包括第一输入，第二输入，第三输入与第四输入：

25 所述通用运算逻辑运算过程包括：
 对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；
 对所述第三输入与所述第四输入进行模加运算，得到第二模加结果；
 对所述第一模加结果与所述第二模加结果进行模乘运算，得到最终计算结果。

30 通过对计算单元的前述设计，可以使所述计算单元可以响应于不同的微码指令指示的输入数据，通过运行通用运算逻辑实现以下至少两种类型的运算：模加；模减；模乘；模加的平方；模减的平方；模加乘模减；模加乘模加；模减乘模减。由此可以使一个计算单元实现多种类型的运算，提升硬件利用率，节省了硬件资源。

需要说明的是，对前述通用运算逻辑进行简单变形得到的方案也在本申请保护的范围内。

35 以下对计算单元实现不同类型的所述运算的过程进行进一步说明。假设每次运算对应

的操作数包括第一操作数与第二操作数，并且所述目标微码指令基于 CPU 或加速器生成。

为了简化说明，利用公式 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p)$ 表示计算单元的前述通用运算逻辑。

其中，A、B、C、D 分别指示第一输入至第四输入。p 为数据域，表示 ABCD 均处于 0 至 p 的范围内。mod (p) 指示对 p 取模。 $(A+B) \bmod (p)$ 指示对 A 和 B 进行模加运算，即 A 与 B 的对 p 取模。 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p)$ 可以指示：对 A 和 B 进行模加，对 C 和 D 进行模加，再对两个模加的结果进行模乘。

第一种运算情形，所述目标类型运算为对所述第一操作数与第二操作数进行模加运算。

所述加速器或所述 CPU，进一步：

10 响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数，将所述第三输入置为 1，将所述第四输入置为 0；

根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。可以理解的是，所述目标微码指令可以包括以上四个输入（包括第一输入，第二输入，第三输入与第四输入），或者以上四个输入的存储地址。

所述计算单元 14 可以进一步：

获取所述第一输入，第二输入，第三输入与第四输入；

对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；

对所述第三输入与所述第四输入进行模加运算，得到 1；

20 对所述第一模加结果与 1 进行模乘运算，得到所述第一模加结果以完成针对所述操作数的模加运算。

以前述公式为例，其中 A 为第一操作数，B 为第二操作数，C=1，D=0。则 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p) = (A+B) \bmod (p)$ ，相当于计算单元实现了对第一操作数和第二操作数的模加运算。

25 第二种运算情形，所述目标类型运算为对所述第一操作数与第二操作数进行模减运算。

所述加速器或所述 CPU，进一步：

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模减运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数并将所述第二输入对应的符号调整为负号，将所述第三输入置为 1，将所述第四输入置为 0；

30 根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

所述计算单元 14，进一步：

获取所述第一输入，第二输入，第三输入与第四输入；

响应于所述目标类型运算为模减运算，将所述第二输入对应的符号调整为负号；

对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；

35 对所述第三输入与所述第四输入进行模加运算，得到 1；

对所述第一模加结果与 1 进行模乘运算，得到所述第一模加结果以完成针对所述操作数的模减运算。

以前述公式为例，其中 A 为第一操作数，B 为第二操作数，C=1，D=0，B 的符号为“-”。则 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p) = (A-B) \bmod (p)$ ，相当于
5 计算单元实现了对第一操作数和第二操作数的模减运算。

第三种运算情形，所述目标类型运算为对所述第一操作数与第二操作数进行模乘运算。

所述加速器或所述 CPU，进一步：

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模乘运算，将所述第一输入置为所述第一五操作数，将所述第三输入置为所述第二操作数，将所述第二输入和
10 所述第四输入置为 0；

根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

所述计算单元 14，可以进一步：

获取所述第一输入，第二输入，第三输入与第四输入；

对所述第一输入与所述第二输入进行模加运算，得到所述第一输入；

15 对所述第三输入与所述第四输入进行模加运算，得到所述第三输入；

对所述第一输入与所述第三输入进行模乘运算，得到计算结果以完成针对所述操作数的模乘运算。

以前述公式为例，其中 A 为第一操作数，C 为第二操作数，B=D=0。则 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p) = (A*C) \bmod (p)$ ，相当于计算单元实现了对第一操作数和第二操作数的模乘运算。
20

第四种运算情形，所述目标类型运算为对所述第一操作数与第二操作数进行模加的平方运算。

所述加速器或所述 CPU，进一步：

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加的平方运算，将
25 所述第一输入和所述第三输入置为所述第一操作数，将所述第二输入和所述第四输入置为所述第二操作数；

根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

所述计算单元 14，进一步：

获取所述第一输入，第二输入，第三输入与第四输入；

30 对所述第一输入与第二输入进行模加运算，得到第一模加结果；

对所述第三输入与第四输入进行模加运算，得到所述第一模加结果；

对所述第一模加结果与所述第一模加结果进行模乘运算，得到计算结果以完成针对所述操作数的模加的平方运算。

以前述公式为例，其中 A=C=第一操作数，B=D=第二操作数。则 $((A+B) \bmod (p) * (C+D) \bmod (p)) \bmod (p) = ((A+B) \bmod (p))^2 \bmod (p)$ ，相当于计算单元实现了
35

对第七操作数和第八操作数的模加的平方运算。

参照前述第一至第四种运算情形对计算单元实现四种运算的说明可以得出，通过调整通用运算逻辑所需的以上四个输入，计算单元也可以实现模减的平方，模加乘模减，模加乘模加，模减乘模减。在此不进行详细说明。

- 5 在一些实施例中，所述基础运算包括的模乘运算包含第一类型的模乘运算与第二类型的模乘运算。所述加速器还包括预设的数据存储空间；所述数据存储空间存储了预设常数；所述预设常数用于第一数据域和第二数据域之间的相互转变；所述第一数据域用于所述第一类型的模乘运算；所述第二数据域用于所述第二类型的模乘运算。

- 10 所述计算单元 14，响应于所述模乘运算由所述第一类型转变为所述第二类型，获取所述预设常数，并根据所述预设常数，将所述第一数据域转换为所述第二数据域以实现所述第二类型的模乘运算；响应于所述模乘运算由所述第二类型转变为所述第一类型，获取所述预设常数，并根据所述预设常数，将所述第二数据域转换为所述第一数据域以实现所述第一类型的模乘运算。

- 15 本申请不限定所述第一类型与所述第二类型，比如所述第一类型可以为常规类型，第二类型为蒙哥马利类型。

两种不同类型的模乘的区别之一在于数据域不同。通过预设常数可以进行数据域的转换。例如，预设常数为 a ，第一数据域为 0 至 p ，将 $p+a$ 则得到第二数据域 0 至 $(p+a)$ 。通过将预设常数存储在数据存储空间内，可以在模乘类型发生变化的时候通过该预设常数调整对应的数据域，从而在计算单元中兼容多种模乘类型。

- 20 以第一类型为常规类型，第二类型为蒙哥马利类型为例。通过配置总线可以预先将用于蒙哥马利数据域与常规数据域之间转换的预设常数存储在数据存储空间。计算单元可以通过获取所述预设常数实现数据域的转换，以实现兼容常规类型的模乘和蒙哥马利类型的模乘。

在一些实施例中，可以通过与加速器对应的调试单元对加速器进行调试。

- 25 加速器中的所述控制单元可以包括断点子单元。

所述断点子单元，用于响应于接收到中断指令，中断所述计算单元执行后续微码指令，以使与所述加速器对应的调试单元获取所述计算单元的计算结果，并输出所述计算结果与预设计算结果的比较结果。由此可以通过对计算单元计算过程的监测，实现对加速器的调试。

- 30 假设加速器在执行连续的多条目标微码指令，这些目标微码指令中包括中断指令。当断点子单元接收到该中断指令后，可以向解析单元发起中断解析的请求，以中断加速器继续执行微码指令。断点子单元还可以向调试单元发送请求，使得调试单元可以通过配置总线从数据存储空间中读取计算单元的计算结果，并与预设的计算结果比较，如果二者一致通过连接器发出绿灯，如果二者不一致，通过连接器发出红灯，使得开发人员可以获知加速器的运行情况，便于进行调试。
- 35

请参见图 2，图 2 为本申请实施例示出的一种加速器的结构示意图。

如图 2 所示，加速器 20 可以包括依次连接的获取单元 21，解析单元 22，控制单元 23，计算单元 24 和数据存储空间 25。

其中，所述加速器 20 与前述加速器 10 中相同的功能单元可以实现相同的用途，在此
5 不做详述。

图 2 示意的配置总线可以将所述加速器 20 与其他器件连通。比如通过所述配置总线
可以将所述加速器 20 与处理器 CPU 或图形处理器 GPU 连通。通过配置总线进行数据与指
令的传输可以提升传输的稳定性。

通过所述配置总线可以为所述加速器 20 输入目标微码指令，以及可以使计算单元完
10 成目标类型运算的目标输入数据等等。所述微码指令可以存储在预设的指令存储空间中，
所述目标输入数据可以存储在预设的数据存储空间 25 中。

在一些方式中，目标微码指令由加速器或 CPU 对操作程序进行转换得到。其中，所述
加速器或所述 CPU 还用于：

将解析得到的所述操作数存储至所述数据存储空间；

15 根据所述目标类型运算，基于所述操作数和/或所述预设操作数在所述数据存储空间的
存储地址，生成所述目标微码指令。

所述操作数即为从操作程序中解析出来的用于执行目标类型运算的操作数。

通过配置总线可以将所述操作数发送至所述数据存储空间进行存储，所述数据存储空间
可以返回所述操作数对应的存储地址。通过配置总线还可以预先将用于生成微码指令的
20 预设操作数存储至所述数据存储空间。

所述预设操作数可以辅助计算单元实现目标类型运算。所述预设操作数可以根据需求
进行设定，比如可以包括 0 和 1。举例来说，所述计算单元包括前述公式示出的通用运算
逻辑。如果所述计算单元需要实现模加运算，则可以将 A 和 B 设置为从操作程序中解析出
的操作数，将 C 设置为预设操作数 0，将 D 设置为预设操作数 1。

25 完成操作数存储之后，可以根据所述目标类型运算，确定用于对所述目标微码指令包
括的每一输入进行配置的目标配置规则，然后根据所述目标配置规则，对每一所述输入进
行配置，生成所述目标微码指令。具体地可以根据所述操作数和/或所述预设操作数在所述
数据存储空间的存储地址，对每一所述输入进行配置，生成所述目标微码指令。

由此得到的目标微码指令可以包括这些目标输入数据在数据存储空间的存储地址。在
30 此情形下，对所述目标微码指令进行解析得到的解析结果也可以包括所述目标输入数据的
存储地址。所述控制单元，根据所述存储地址，控制所述计算单元从所述数据存储空间读
取所述目标输入数据并基于所述目标输入数据执行所述目标类型的运算。

在一些实施例中，数据存储空间 25 可以包括数据缓冲区与数据寄存器。数据缓冲区
可以包括输入缓冲区与输出缓冲区。配置总线传输的输入数据，以及计算单元 24 得到的
35 计算结果可以按需存储在数据缓冲区与数据寄存器，本申请不进行特别限定。当然，如果

计算单元 24 连续执行多次计算，其中间计算结果可以存储在数据寄存器中，从而提升计算效率。

在一些实施例中，所述操作程序还包括点乘标量；所述目标类型运算为对所述点乘标量和所述操作数进行点乘运算；所述加速器或所述 CPU，进一步：

5 根据所述操作程序包括的所述点乘标量和操作数，生成用于实现所述点乘运算的多条目标微码指令；

所述加速器，进一步：

控制所述计算单元执行所述多条目标微码指令中的每一目标微码指令，以完成所述点乘运算。

10 由此通过对操作程序进行解析，得到多条目标微码指令，并根据多条目标微码指令控制计算单元实现点乘运算。

请参见图 3，图 3 为本申请实施例示出的一种加速器的结构示意图。

如图 3 所示，所述加速器 30 可以包括依次连接的获取单元 31，解析单元 32，控制单元 33，计算单元 34 和数据存储空间 35；以及与控制单元 33 和计算单元 34 连接的缓存单元 36。其中，单元 31 至 35 的相关说明可以参照前述实施例，在此不做详述。

缓存单元 36 存储了用于点乘的点乘标量。所述点乘标量可以是具有预设比特位数的预设进制数，比如 256 比特位的二进制数。在一些方式中可以通过配置总线将点乘标量存储在所述缓存单元 36。

可以理解的是，点乘的运算过程实际是结合点乘标量每一位上的比特数进行若干次简单运算。所述简单运算可以包括模加，模减，模乘，模加的平方，模减的平方，模加乘模减，模加乘模加，模减乘模减。因此为了实现点乘运算，可以人工编写或者由加速器或 CPU 对操作程序进行转换得到多条与这些简单运算分别对应的目标微码指令，以控制计算单元完成前述多种简单运算以完成点乘。

以下以通过 ECC 实现非对称加密为例进行说明。

25 已知椭圆上的基点 G，可以选取该椭圆上的两个点 d 和 Q，其中 $Q=dG$ ，分别作为私钥和公钥。

利用公钥 Q 对明文 M 加密时，可以获取随机数 r，通过公式 $M+rQ$ ，得到密文 C。

在利用私钥 d 对密文 C 解密时，可以通过公式 $C-d(rG)=M+r(dG)-d(rG)=M$ ，即可解密得到明文 M。

30 在前述加解密过程中，需要频繁进行点乘运算（例如 Rq ， Dg 等）。通过前述实施例示出的加速器进行 ECC 计算，一方面可以，可以通过变更微码指令的方式可以使加速器实现不同类型运算，简化了对加速器的配置操作，降低了对加速器的配置难度，从而可以更灵活地使用加速器；另一方面，通过一个计算单元可以实现至少两种类型的 ECC 运算，节省了硬件资源。

35 本申请一种加速方法。所述加速方法可以应用于前述任一实施例示出的加速器，所述

加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算。

请参见图 4，图 4 为本申请实施例示出的一种加速方法的方法流程示意图。如图 4 所示，所述方法可以包括 S402-S406。除特别说明外，本申请不限定这些步骤的执行顺序。

S402，获取根据待实现的目标类型运算，生成的与所述目标类型运算对应的目标微码指令；所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据。

S404，解析所述目标微码指令，得到与所述目标输入数据对应的解析结果。

10 S406，响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

前述方案中，第一，可以通过根据待实现的目标类型运算，生成目标微码指令，并根据目标微码指令未完成对计算单元内通用运算逻辑实现目标类型运算所需的输入的相关配置，以使加速器完成所述目标类型运算，与相关技术一相比，可以通过变更微码指令的方式可以使加速器实现不同类型运算，简化了对加速器的配置操作，降低了对加速器的配置难度，从而可以更灵活地使用加速器。

第二，在计算单元中部署了由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算，以相关技术二相比，可以通过一个计算单元可以实现至少两种类型的运算，节省了硬件资源。

20 以下介绍一些与加速方法相关的实施例。这些实施例的实施过程可以参照前面关于加速器的实施例，在此不做详述。

在一些实施例中，所述加速器与处理器 CPU 通信连接；所述方法还包括：

获取针对操作数执行目标类型运算的操作程序；

25 根据所述目标类型运算，基于所述操作程序包括的操作数，生成与所述目标类型运算对应的所述目标微码指令。

在一些实施例中，所述加速器还包括预设的数据存储空间；所述数据存储空间存储了用于生成微码指令的预设操作数；

所述根据所述目标类型运算，基于所述操作程序包括的操作数，生成与所述目标类型运算对应的所述目标微码指令，包括：

30 将解析得到的所述操作数存储至所述数据存储空间；

根据所述目标类型运算，基于所述操作数和/或所述预设操作数在所述数据存储空间的存储地址，生成所述目标微码指令。

在一些实施例中，所述解析结果包括所述目标输入数据的存储地址；

35 所述响应于所述解析结果，控制所述计算单元获取所述目标输入数据，以使所述计算单元基于所述目标输入数据执行所述目标类型的运算，包括：

根据所述存储地址，控制所述计算单元从所述数据存储空间读取所述目标输入数据并基于所述目标输入数据执行所述目标类型的运算。

在一些实施例中，所述基础运算包括模加运算和模乘运算，所述通用运算逻辑为对两次模加运算的计算结果进行模乘。

- 5 在一些实施例中，所述通用运算逻辑所需的输入包括第一输入，第二输入，第三输入与第四输入；

所述通用运算逻辑运算过程包括：

对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；

对所述第三输入与所述第四输入进行模加运算，得到第二模加结果；

- 10 对所述第一模加结果与所述第二模加结果进行模乘运算，得到最终计算结果。

在一些实施例中，所述操作数包括第一操作数与第二操作数；

所述加速器或所述 CPU，进一步：

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数，将所述第三输入置为 1，将所述第四输入置为 0；

- 15

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模减运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数并将所述第二输入对应的符号调整为负号，将所述第三输入置为 1，将所述第四输入置为 0；

- 20 响应于所述目标类型运算为对所述第一操作数与第二操作数进行模乘运算，将所述第一输入置为所述第一操作数，将所述第三输入置为所述第二操作数，将所述第二输入和所述第四输入置为 0；

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加的平方运算，将所述第一输入和所述第三输入置为所述第一操作数，将所述第二输入和所述第四输入置为所述第二操作数；

- 25 根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

在一些实施例中，所述操作程序还包括点乘标量；所述目标类型运算为对所述点乘标量和所述操作数进行点乘运算；

所述根据所述目标类型运算，基于所述操作程序包括的操作数，生成与所述目标类型运算对应的所述目标微码指令，包括：

- 30 根据所述操作程序包括的所述点乘标量和操作数，生成用于实现所述点乘运算的多条目标微码指令；

所述方法还包括：

控制所述计算单元执行所述多条目标微码指令中的每一目标微码指令，以完成所述点乘运算。

- 35 在一些实施例中，所述模乘运算包含第一类型的模乘运算与第二类型的模乘运算；所

述加速器还包括预设的数据存储空间；所述数据存储空间存储了预设常数；所述预设常数用于第一数据域和第二数据域之间的相互转变；所述第一数据域用于所述第一类型的模乘运算；所述第二数据域用于所述第二类型的模乘运算；

所述方法还包括：

- 5 所述计算单元响应于所述模乘运算由所述第一类型转变为所述第二类型，获取所述预设常数，并根据所述预设常数，将所述第一数据域转换为所述第二数据域以实现所述第二类型的模乘运算；

- 10 响应于所述模乘运算由所述第二类型转变为所述第一类型，获取所述预设常数，并根据所述预设常数，将所述第二数据域转换为所述第一数据域以实现所述第一类型的模乘运算。

在一些实施例中，所述方法还包括：

响应于接收到中断指令，中断所述计算单元执行后续微码指令，以使与所述加速器对应的调试单元获取所述计算单元的计算结果，并输出所述计算结果与预设计算结果的比较结果。

- 15 在一些实施例中，所述加速器为基于 FPGA 或 ASIC 实现的用于椭圆曲线算法加速的协处理器；或，基于 CPU 实现的用于针对所述椭圆曲线算法进行算法加速的辅助加速模块。

- 20 本申请还提出一种电子设备。所述电子设备包括如前述任一实施例示出的加速器。通过所述电子设备进行 ECC 加速，一方面由于可以通过变更微码指令的方式可以使加速器实现不同类型运算，简化了对加速器的配置操作，降低了对加速器的配置难度，从而降低对电子设备的操作难度，从而可以更灵活地使用电子设备；另一方面，加速器中的一个计算单元可以实现至少两种类型的 ECC 运算，节省了硬件资源。

本申请提出一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序用于使所述计算机中的加速器可以执行如前述任一实施例示出的加速方法。

- 25 本领域技术人员应明白，本申请一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本申请一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请一个或多个实施例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（可以包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

- 30 本申请中的“和/或”表示至少具有两者中的其中一个，例如，“A 和/或 B”可以包括三种方案：A、B、以及“A 和 B”。

本申请中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于数据处理设备实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

- 35 以上对本申请特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一

些情况下，在权利要求书中记载的行为或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

5 本申请中描述的主题及功能操作的实施例可以在以下中实现：数字电子电路、有形体现的计算机软件或固件、可以包括本申请中公开的结构及其结构性等同物的计算机硬件、或者它们中的一个或多个的组合。本申请中描述的主题的实施例可以实现为一个或多个计算机程序，即编码在有形非暂时性程序载体上以被数据处理装置执行或控制数据处理装置的操作的计算机程序指令中的一个或多个模块。可替代地或附加地，程序指令可以被编码
10 在人工生成的传播信号上，例如机器生成的电、光或电磁信号，该信号被生成以将信息编码并传输到合适的接收机装置以由数据处理装置执行。计算机存储介质可以是机器可读存储设备、机器可读存储基板、随机或串行存取存储器设备、或它们中的一个或多个的组合。

 本申请中描述的处理及逻辑流程可以由执行一个或多个计算机程序的一个或多个可编程计算机执行，以通过根据输入数据进行操作并生成输出来执行相应的功能。所述处理
15 及逻辑流程还可以由专用逻辑电路—例如 FPGA（现场可编程门阵列）或 ASIC（专用集成电路）来执行，并且装置也可以实现为专用逻辑电路。

 适合用于执行计算机程序的计算机可以包括，例如通用和/或专用微处理器，或任何其他类型的处理单元。通常，处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的基本组件可以包括用于实施或执行指令的处理单元以及用于存储指令和数据的一个或多个存储器设备。通常，计算机还将可以包括用于存储数据的一个或多个大容量存储设备，例如磁盘、磁光盘或光盘等，或者计算机将可操作地与此大容量存储设备耦接以
20 从其接收数据或向其传送数据，抑或两种情况兼而有之。然而，计算机不是必须具有这样的设备。此外，计算机可以嵌入在另一设备中，例如移动电话、个人数字助理（PDA）、移动音频或视频播放器、游戏操纵台、全球定位系统（GPS）接收机、或例如通用串行总线（USB）闪存驱动器的便携式存储设备，仅举几例。

 适合于存储计算机程序指令和数据的计算机可读介质可以包括所有形式的非易失性存储器、媒介和存储器设备，例如可以包括半导体存储器设备（例如 EPROM、EEPROM 和闪存设备）、磁盘（例如内部硬盘或可移动盘）、磁光盘以及 CD ROM 和 DVD-ROM 盘。处理器和存储器可由专用逻辑电路补充或并入专用逻辑电路中。

30 虽然本申请包含许多具体实施细节，但是这些不应被解释为限制任何公开的范围或所要求保护的公开的范围，而是主要用于描述特定公开的具体实施例的特征。本申请内在多个实施例中描述的某些特征也可以在单个实施例中组合实施。另一方面，在单个实施例中描述的各种特征也可以在多个实施例中分开实施或以任何合适的子组合来实施。此外，虽然特征可以如所述在某些组合中起作用并且甚至最初如此要求保护，但是来自所要求保护的组
35 合中的一个或多个特征在一些情况下可以从该组合中去除，并且所要求保护的组合可以指

向子组合或子组合的变型。

- 类似地，虽然在附图中以特定顺序描绘了操作，但是这不应被理解为要求这些操作以所示的特定顺序执行或顺次执行、或者要求所有例示的操作被执行，以实现期望的结果。在某些情况下，多任务和并行处理可能是有利的。此外，所述实施例中的各种系统模块和
- 5 组件的分离不应被理解为在所有实施例中均需要这样的分离，并且应当理解，所描述的程序组件和系统通常可以一起集成在单个软件产品中，或者封装成多个软件产品。

- 由此，主题的特定实施例已被描述。其他实施例在所附权利要求书的范围以内。在某些情况下，权利要求书中记载的动作可以以不同的顺序执行并且仍实现期望的结果。此外，附图中描绘的处理并非必需所示的特定顺序或顺次顺序，以实现期望的结果。在某些实现
- 10 中，多任务和并行处理可能是有利的。

以上仅为本申请一个或多个实施例的较佳实施例而已，并不用以限制本申请一个或多个实施例，凡在本申请一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本申请一个或多个实施例保护的范围之内。

权 利 要 求 书

1.一种加速器，其特征在于，所述加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算；所述加速器还包括：

5 获取单元，获取根据待实现的目标类型运算，生成的目标微码指令；所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据；解析单元，解析所述目标微码指令，得到与所述目标输入数据对应的解析结果；

控制单元，响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

10

2.根据权利要求 1 所述的加速器，其特征在于，所述加速器与处理器 CPU 通信连接；所述加速器或所述 CPU，用于：

获取针对操作数执行目标类型运算的操作程序；

根据所述目标类型运算，基于所述操作程序包括的操作数，生成与所述目标类型运算
15 对应的所述目标微码指令。

3.根据权利要求 2 所述的加速器，其特征在于，所述加速器还包括预设的数据存储空间；所述数据存储空间存储了用于生成微码指令的预设操作数；

所述加速器或所述 CPU 还用于：

20 将解析得到的所述操作数存储至所述数据存储空间；

根据所述目标类型运算，基于所述操作数和/或所述预设操作数在所述数据存储空间的存储地址，生成所述目标微码指令。

4.根据权利要求 3 所述的加速器，其特征在于，所述解析结果包括所述目标输入数据
25 的存储地址；

所述控制单元，根据所述存储地址，控制所述计算单元从所述数据存储空间读取所述目标输入数据并基于所述目标输入数据执行所述目标类型的运算。

5.根据权利要求 1-4 任一所述的加速器，其特征在于，所述基础运算包括模加运算和
30 模乘运算，所述通用运算逻辑为对两次模加运算的计算结果进行模乘。

6.根据权利要求 5 所述的加速器，其特征在于，所述通用运算逻辑所需的输入包括第一输入，第二输入，第三输入与第四输入；

所述通用运算逻辑运算过程包括：

35 对所述第一输入与所述第二输入进行模加运算，得到第一模加结果；

对所述第三输入与所述第四输入进行模加运算，得到第二模加结果；
对所述第一模加结果与所述第二模加结果进行模乘运算，得到最终计算结果。

7.根据权利要求 6 所述的加速器，其特征在于，所述操作数包括第一操作数与第二操作数；

所述加速器或所述 CPU，进一步：

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数，将所述第三输入置为 1，将所述第四输入置为 0；

10 响应于所述目标类型运算为对所述第一操作数与第二操作数进行模减运算，将所述第一输入置为所述第一操作数，将所述第二输入置为所述第二操作数并将所述第二输入对应的符号调整为负号，将所述第三输入置为 1，将所述第四输入置为 0；

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模乘运算，将所述第一输入置为所述第一操作数，将所述第三输入置为所述第二操作数，将所述第二输入和
15 所述第四输入置为 0；

响应于所述目标类型运算为对所述第一操作数与第二操作数进行模加的平方运算，将所述第一输入和所述第三输入置为所述第一操作数，将所述第二输入和所述第四输入置为所述第二操作数；

根据所述第一输入，第二输入，第三输入与第四输入，生成所述目标微码指令。

20

8.根据权利要求 6 所述的加速器，其特征在于，所述操作程序还包括点乘标量；所述目标类型运算为对所述点乘标量和所述操作数进行点乘运算；

所述加速器或所述 CPU，进一步：

根据所述操作程序包括的所述点乘标量和操作数，生成用于实现所述点乘运算的多条
25 目标微码指令；

所述加速器，进一步：

控制所述计算单元执行所述多条目标微码指令中的每一目标微码指令，以完成所述点乘运算。

30 9.根据权利要求 6 所述的加速器，其特征在于，所述模乘运算包含第一类型的模乘运算与第二类型的模乘运算；所述加速器还包括预设的数据存储空间；所述数据存储空间存储了预设常数；所述预设常数用于第一数据域和第二数据域之间的相互转变；所述第一数据域用于所述第一类型的模乘运算；所述第二数据域用于所述第二类型的模乘运算；

所述计算单元，响应于所述模乘运算由所述第一类型转变为所述第二类型，获取所述
35 预设常数，并根据所述预设常数，将所述第一数据域转换为所述第二数据域以实现所述第

二类型的模乘运算；

响应于所述模乘运算由所述第二类型转变为所述第一类型，获取所述预设常数，并根据所述预设常数，将所述第二数据域转换为所述第一数据域以实现所述第一类型的模乘运算。

5

10. 根据权利要求 1 所述的加速器，其特征在于，所述控制单元包括断点子单元；

所述断点子单元，响应于接收到中断指令，中断所述计算单元执行后续微码指令，以使与所述加速器对应的调试单元获取所述计算单元的计算结果，并输出所述计算结果与预设计算结果的比较结果。

10

11. 根据权利要求 1 所述的加速器，其特征在于，所述加速器为基于 FPGA 或 ASIC 实现的用于椭圆曲线算法加速的协处理器；或，基于 CPU 实现的用于针对所述椭圆曲线算法进行算法加速的辅助加速模块。

15

12. 一种加速方法，应用于加速器，其特征在于，所述加速器包括用于实现与椭圆曲线算法相关的运算的计算单元；其中，所述计算单元包括由基础运算逻辑构成的通用运算逻辑；所述通用运算逻辑响应于不同的输入，实现不同运算类型的所述运算；

所述方法包括：

获取根据待实现的目标类型运算，生成的与所述目标类型运算对应的目标微码指令；

20

所述目标微码指令用于指示使所述通用运算逻辑实现所述目标类型运算所需的目标输入数据；

解析所述目标微码指令，得到与所述目标输入数据对应的解析结果；

响应于所述解析结果，响应于所述解析结果控制所述计算单元，以使所述计算单元获取所述目标输入数据并基于所述目标输入数据运行所述通用运算逻辑，完成所述目标类型运算。

25

13. 一种电子设备，其特征在于，所述电子设备包括如权利要求 1-11 任一所述的加速器。