



[12] 发明专利申请公开说明书

[21] 申请号 02811384.5

[43] 公开日 2004 年 12 月 1 日

[11] 公开号 CN 1552013A

[22] 申请日 2002. 6. 6 [21] 申请号 02811384. 5

[30] 优先权

[32] 2001. 6. 6 [33] DE [31] 10127423. 8

[86] 国际申请 PCT/EP2002/006233 2002. 6. 6

[87] 国际公布 WO2002/099554 德 2002. 12. 12

[85] 进入国家阶段日期 2003. 12. 5

[71] 申请人 因芬尼昂技术股份公司

地址 德国慕尼黑

[72] 发明人 A·埃贝 N·詹森 H·塞德拉克

[74] 专利代理机构 中国专利代理(香港)有限公司

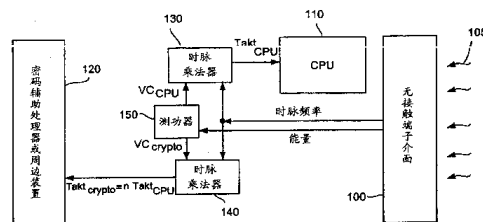
代理人 程天正 王 勇

权利要求书 3 页 说明书 12 页 附图 4 页

[54] 发明名称 具能量控制之电子电路

[57] 摘要

本案系指一种电子电路包括一控制器以及一能量决定装置，其中控制器系用以处理一处理器工作，能量决定装置系用以决定控制器之可使用能量，亦指一种电子电路的控制装置，藉由控制器可使用之能量以控制控制器，借着这种能量控制能够达成可使用能量的最大利用，以及因最大能量利用所产生的计算速度的最佳化。



1. 一种电子电路，包括：

一控制器(110, 120)，用以处理一处理器工作；

5 一能量决定装置(150)，用以决定该控制器(110, 120)可使用之能量；以及

一控制装置(130, 140, 150)，藉由该控制器(110, 120)可使用之能量以控制该控制器(110, 120)。

2. 如权利要求第1项所述之电子电路，其中该控制装置(130, 140, 150)系用以控制该控制器(110, 120)，使得该控制器(110, 120)
10 用于该处理器工作所需之能量实质上等于该控制器(110, 120)可使用之能量。

3. 如权利要求第1或2项所述之电子电路，更包括一能量供应装置(100)，用以自外部供应之电磁能量(105)产生该控制器(110, 120)可使用之能量。

15 4. 如权利要求第1至3任一项所述之电子电路，系设计成适用于无接触端子(310)之一应用的一集成电路。

5. 如权利要求第1至4任一项所述之电子电路，其中该控制装置(130, 140, 150)包括一装置(130, 140)，用以设定该控制器(110, 120)赖以运作的控制器时脉，当可使用之能量较多时控制器时脉的一
20 时脉比率增加，当可使用之能量较少时该时脉比率减少。

6. 如权利要求第1至5任一项所述之电子电路，其中该该控制器(110, 120)系以CMOS技术制作。

7. 如权利要求第1至6任一项所述之电子电路，其中该控制器(110, 120)包括：

25 复数个周边装置(120)，用以执行相关工作；以及

一中央处理单元(110)，用以驱动该复数个周边装置(120)；

其中该控制装置(130, 140, 150)系藉由该处理器工作、该相关工作以及该控制器(110, 120)可使用之能量以控制该复数个周边装置(120)。

30 8. 如权利要求第7项所述之电子电路，其中该控制装置(130, 140, 150)系用以控制该复数个周边装置(120)，使得该控制器(110, 120)执行该处理器工作所需之计算时间能最小化。

9. 如权利要求第 7 或 8 项所述之电子电路, 其中该控制器(110, 120)系为一密码处理器, 该复数个周边装置(120)系为执行计算工作的密码辅助处理器(120), 该处理器工作系根据 DES 标准、AES 方法、RSA 算法则以及椭圆曲线方法而选自于一加密、一解密、一鉴定以及一签署其中之一, 该复数个密码辅助处理器(120)的该计算工作系选自一模块化或非模块化加法、乘法、取幂以及倒置、一杂凑值计算以及一随机数决定。

10. 如权利要求第 7 至 9 任一项所述之电子电路, 其中该控制装置(130, 140, 150)更包括:

10 用以设定该复数个周边装置(120)赖以运作的周边装置时脉之一装置; 以及

用以关闭该复数个周边装置中的单一周边装置(120)之一装置。

11. 如权利要求第 10 项所述之电子电路, 其中用以设定该周边装置时脉(120)的该装置(140)包括一振荡器, 该振荡器系连接于该复数个周边装置之一, 且藉由一输出时脉频率以产生一时脉信号, 该相关周边装置(120)系藉由该输出时脉频率以计算时脉。

12. 如权利要求第 10 项所述之电子电路, 其中用以设定该周边装置时脉(120)的该装置(140)包括一时脉乘法器, 该时脉乘法器系连接于该复数个周边装置之一, 且藉由一输出时脉频率以产生一时脉信号, 该相关周边装置(120)系藉由该输出时脉频率以计算时脉。

13. 如权利要求第 1 至 12 任一项所述之电子电路, 其中该控制器(110, 120)包括一周边装置(120)以及一中央处理单元(110), 该周边装置(120)系用以执行一相关工作, 该中央处理单元(110)系用以驱动该周边装置(120), 并且该控制装置(130, 140, 150)包括一第一装置(130)以及一第二装置(140), 该第一装置(130)系用以设定该中央处理单元(110)赖以运作的一第一时脉, 该第二装置(140)系用以设定该周边装置(120)赖以运作的一第二时脉, 被设定的该第一及第二时脉使得可使用之能量足够处理该处理器工作, 同时使得该周边装置(120)分配到能够执行该相关工作的一最大能量。

14. 一种控制一电子电路的方法, 该电子电路包括用以处理一处理器工作的一控制器(110, 120), 该方法包括下列步骤:

决定(10)该控制器(110, 120)之可使用能量; 以及

藉由该控制器 (110, 120) 之可使用能量以控制 (20) 该控制器 (110, 120)。

具能量控制之电子电路

本案系指具有一控制器之电子电路，特别是在此电子电路中控制
5 该控制器。

随着非现款支付交易、经由公共网络的电子数据传输、以及经由
公共网络的信用卡号码的交换之使用的日渐普及，密码算法则之需要
性亦日渐增加，以便能执行数字签署、鉴定、或加密工作，已知的密
码算法则包括非对称加密算法则(例如：RSA 算法则)、或椭圆曲线建
10 构之方法、或对称加密算法则(例如：根据 DES 或是 AES 标准之加密
方法)。

为了能在日常生活中以一可接受的速度实施密码算法则的规定
计算，需使用特别提供之密码控制器，这种密码控制器可用于芯片卡
片中，例如 SIM 卡或签名卡，用于例如家用银行交易或受法律约束之
15 电子签署、并以行动电话进行支付的方面，另一方面，密码控制器亦
可用于计算机或作为安全集成电路的服务器以实行鉴定、或能够执行
加密工作，其系包括例如经由网际网络安全传输信用卡号码、传输秘
密内容和安全非现款支付交易的电子邮件。

随着密码控制器的需求日增，也满足了使用者的高期待与建立它
20 们在市场上的地位，为了确保算法则防止外界攻击的安全性，密码控
制器必须提供相当的计算能力，原因是密码算法则的安全性(例如已
知的 RSA 算法则)一般来说关键地建立在使用金钥的位长度、以及因
此实施对应密码算法则的那些密码控制器必须能够尽可能地处理位
长度的计算，例如在 RSA 算法则中，1024 或甚至达到 2048 的金钥位
25 长度会鉴于目前一般用途的处理器而工作于 8 位、32 位、或最大到 64
位的计算。

此外，密码控制器必须具有高度计算能力以便能够实行密码算法
则在每段适当时间长度中所需之计算，举例来说，要求任何使用者对
于鉴定或支付交易等上数分钟是极为不智的，为了达到这些高度计算
30 能力，已知的密码控制器需实行很多计算运作的平行处理以增加计算
速度。

当在如 SIM 卡或签名卡等芯片卡片中使用密码控制器时，一额外

的问题会产生，也就是须达到低成本的大量生产，即使它们必须尽可能地在一段短时间内实施，需要大量计算工夫的算法则的电子电路却也在另一方面不能够太过复杂及昂贵。

另一个在设计密码控制器时会发生的问题是太多相同密码算法
5 则的共同存在，例如在一芯片卡片中，其能够执行最多标准密码算法
则并因此能够显示出较宽广服务范围 and 赢得使用者青睐，亦将会主宰
市场，这种”多功能”密码控制器可以避免使用者携带数个芯片卡片在
身上，而其中每个芯片卡片却仅是为了达到特定应用或是特定密码程
序，在多用途功能加入之后，这样一个多功能密码控制器必须能够执
10 行很多的密码算法则所使用的大量计算运作，而这会导致复杂度的增
加以及电子电路速度的减少。

一个密码控制器的可能设计，一方面要能显示多功能性、另一方
面又须具备高速处理速度，包括一中央处理单元和一个或数个平行工
作的辅助处理器，例如现代的计算机、现代绘图卡，系经由一总线系
15 统而互相连接，这些辅助处理器会接手复杂的计算工作，并于特定的
密码算法则或特定的计算运作联合(例如：一模块或倍数化计算)操
作。

必须面对密码控制器另一额外的问题是仅能使用一有限的能
量，例如芯片卡片的接触端子最大仅提供数毫安的电流，然而在如行
20 动电话所使用的 SIM 卡等无接触应用与行动应用中，电流量可能被限
制于小于 10 毫安，因此，辅助处理器的计算速度会受限于可使用之
能量，CPU 之时脉频率以及时脉的密码辅助处理器系受到可使用之能
量的管制，由于控制器芯片卡片系以 CMOS 技术制作，消耗之电流量
系决定于时脉频率或是 MOSFET 的切换频率。

和可使用之低能量以及在不接触应用与行动应用中改变或减少
可使用能量有关的问题，在传统的密码控制器当中，仅与相同的某一
最小能量供应有关，对于 CPU 和辅助处理器、也就是整个密码控制器
来说，其系计算时脉于固定的时脉频率，使得时脉频率之需求能量符
合最小能量，因此，只有当可使用之能量足够，也就是等于或大于最
30 小能量时，电路方能运作，由于辅助处理器的固定时脉，密码处理器
运作所需的能量与密码处理器的工作无关，以致于建立在椭圆曲线的
计算越不复杂，RSA 密码应用所需之能量便越多，而当可使用之能量

超过密码控制器运作所需，额外的能量会散失而无法运用。

对于芯片卡片和安全-IC 生产者来说，具有较佳能量使用功能的密码控制器系更为重要，原因是一方面计算速度和因此所造成终端的等待时间以及使用者信赖度会增加，而另一方面电路复杂度和因此所造成控制器之成本在同样的计算速度上会减少，而这是有利于大量生产的。

本案之目的为提供一种电子电路及其控制方法，藉由控制此电子电路达到在可用能量相同的情况下，增加计算能力的目的。

本案之目的可藉由权利要求第 1 项所述之电子电路以及权利要求第 14 项所述之方法而达到。

本案之电子电路包括执行处理器工作的一控制器以及决定控制器可使用能量的一能量决定装置，电子电路的一控制装置可将控制器以其本身可使用能量的函数之方式控制。

本案之方法系控制一电子电路，其包括执行处理器工作的一控制器以及决定控制器可使用能量的一能量决定装置，以及将控制器以其本身可使用能量的函数之方式控制。

本案是基于若欲决定控制器可使用之能量，例如一密码控制器，运作之计算时间的最佳化系在被决定之能量以理想化的方式分配给作决定的辅助处理器的情况下达成，所谓作决定的辅助处理器是指对于目前处理器工作有需求的、其它的周边装置或是控制器的 CPU。即使能量决定装置或测功计为了达成这种目的而被加至电子电路中（当然这会增加电路的复杂度），一方面在同一电路复杂度的情况下计算能力的增进，另一方面电路复杂度的减少，皆会因为能量之理想化的使用而被达成。

根据本案一实施例，实行控制此控制器须以该控制器之可用能量的函数而运作，该控制器时脉系藉由可用之能量使得该控制器保持运作，若较多能量可供使用则函数增加，若较少能量可供使用则函数减少，换句话说，该控制器时脉系根据被决定之可使用能量而被追踪，以达成可使用能量的理想化使用，其中较佳者，特别是使用具有无接触端子芯片卡片之电子电路，由于在此情形下，可使用之能量决定于芯片卡片和无接触端子之间的距离，因此而产生较大之变化，在使用芯片卡片的情形中，由于理想化的能量使用造成端子的等候时间减

少，这会使得使用者对于芯片卡片之信赖度增加。

根据本案另一实施例，该控制器系包括用以执行相关工作的复数个周边装置(例如用于端子资料交换的一 UART 模块，其中 UART 系指通用异步接收器-发送器)、用以根据安全性而检查参数的侦测组件、
5 一随机数产生器、用以执行计算工作的一滤波器或辅助处理器(例如一 DES、RSA 或杂凑模块(HASH MODULE))、以及用以起动该复数个周边装置的 CPU，其中该控制器系以处理器工作函数、相关工作、以及该控制器之可用能量而受到控制，这种控制的实行一方面使得执行处理器工作所需的计算时间最小化，亦会额外使得可用之能量足够，这是因为被决定之可用能量主要被使用在周边装置、或是需要最大能量的辅助处理器、或是在应用方面或在处理器工作方面的计算能力(例如加密、解密、鉴定或是根据 DES 标准、AES 方法、RSA 算法则或是椭圆曲线方法的签署)，其次亦被使用于数据传输方面，换句话说，控制该控制器使得一方面处理该控制器之处理器工作之可使用能量
10 足够，另一方面使得一最小能量被分配给每个周边装置或是每个辅助处理器用以执行计算工作。

在一实施例之中，可用之能量系藉由低速、缓慢地对 CPU 计算时脉、和对该周边装置计算时脉，以分配给一周边装置和该控制器的一 CPU，也就是说，由于在一 RSA 加密过程中由 CPU 执行的小量工作造成辅助处理器须对倍数化模块负责，在另一实施例之中，可用之能量系依序地藉由于一椭圆曲线加密期间对主要的辅助处理器高速计算时脉和藉由低速对用于辅助计算的一辅助处理器计算时脉而分配至两个周边装置之间，总计在理想化能量使用或利用所须的计算时间因此而降低。

25 更进一不之较佳实施例以及本案之诸般变化方式可由后述之权利要求而得出。

以下所述，皆为将本案之较佳实施例以一更为详细之方式陈述、并佐以图标之论述，其中：

- 图 1：本案电子电路之能量控制流程图；
30 图 2：根据本案一较佳实施例绘制之电子电路方块图；
图 3：于图 2 之电子电路中使用一 PLL 用以时脉控制之方块图；以及

图 4：决定时脉频率之方块图，藉由此时脉频率功能，关于目前处理器工作的一周边装置可以一种与无接触端子保持一距离的方式计算时脉，该电子电路系以该无接触端子的方式设置于一芯片卡片上。

5 首先，本案能量控制以及其优点皆陈述于图 1 中，请参阅第二及图 3，陈述的是本案电子电路一较佳实施例，而图 4 则是本案之能量控制使用于无接触应用之情形。

即使本案可以应用于所有包括处理一处理器工作的一控制器之电子电路中，下面之陈述仍系仅关于密码之场合，下述之控制器有时
10 系指密码处理器或是密码控制器，然而，若欲转换至其它场合如笔记型计算机之绘图卡的应用，应是毫无困难的。

如图 1 之流程图所示，本案能量控制开始于步骤 10 的决定该电子电路的可使用能量 E，可使用能量 E 会因此不同原因而变化，如果该电子电路被使用于接触端子的芯片卡片上，可使用能量便可能从一
15 端变化至另一端、或是可能由于该接触端子和该电子电路之间的接触品质之改变而变化，而在无接触的应用方面，可使用能量 E 决定于该芯片卡片之一无接触端子与该无接触端子之间的距离，如图 4 所示，在行动通讯之应用方面，例如行动电话、笔记型计算机或其它类似的场合，可使用能量会由于电池放电增加而随之减少，决定的本身会受
20 到不同方式或不同装置的影响，其中不同之参数会被用于测量可使用能量，例如一输入电压或是一耦合电流。

在步骤 20 中，电子电路的控制器系以可使用能量 E 的函数之方式被控制，其中可使用能量 E 系在步骤 10 被决定，正如图 1 之支持，控制器可以由能量 E 的函数以不同之方式进行控制，图 1 所述之三种
25 可能性 20a、20b 以及 20c 仅系举例说明之用，控制该控制器的第一种可能性 20a 系以可使用能量 E 的函数设定该控制器的时脉频率，藉由改变时脉频率，形成该控制器的切换组件的切换频率将改变，使得以 CMOS 制程制作的控制器在电流消耗以及功率消耗方面产生改变，因此，如果可使用之能量较少，时脉频率必须设定的较低，相反的若
30 可使用之能量较多，时脉频率和计算速度便会增加，在包含数个组件的该控制器当中，时脉频率必须如图 2 所示地针对如一 CPU 或是如一辅助处理器的一周边装置的每一组件单独设定，藉由设定不同组件的

时脉频率，可使用能量 E 可以用于一理想化方式或是被完全分配给用于目前处理器工作的所有组件，藉由设定不同的时脉频率造成的可使用能量对于不同组件的分配亦会为了最佳化处理器工作的计算时间而受到影响，其中由于可使用能量之最大使用以及每个组件之同步最佳能量分配，计算时间便会被最小化。

控制该控制器的第二种可能性 20b 系关闭和目前处理器工作无关的控制器组件，这些无关的控制器组件系藉由额外的切换组件而与供应电压间形成断路，例如具有极低漏电流且处于休眠模式的 FET。

控制该控制器的第三种可能性 20c 系设定整个控制器或是该控制器的每个组件的供应电压，在可使用能量降至低于一特定门槛值的情形下，供应电压必须被设定于一较低值，例如在该较低值上该控制器之运作可靠度虽低，但仍然足够，再者，供应电压亦可改变以用于电子电路之模拟组件，例如该电子电路之一无接触端子接口的模拟部份。

和传统上设计用于一特定之最小供应能量之电子电路比较起来，图 1 中本案之能量控制方法之主要优点在于，可使用能量 E 系先被决定然后完全用尽于控制器的运作，在这种方法中，超过最小供应能量的可使用能量的部份会被用于加速进行处理器工作，因此相反地，在传统的电子电路中，决定系统整体表现的特定周边装置系仅运作于一 CPU 时脉的特殊固定的倍数中，然而这种情形却是只有在可使用能量足够的情形下才会发生，在本案能量控制之下，藉由多余之可使用能量可以使得每个周边装置以更快的速度计算时脉，使得可使用能量整体性地以一最佳化的方式被利用。

考虑目前处理器工作，例如实行一特定之密码算法则，被决定成可以使用之能量亦会以理想化计算时间为目的以一理想化方式被分配给作决定之辅助处理器，使得可使用能量不仅被完成用尽，还以一理想化之方式被利用，其中该控制器的计算速度会增加至一恒定能量，而该端之使用者等候时间亦会因此减少。

请参阅图 2，其为根据本案一较佳实施例绘制之电子电路方块图，根据此实施例，该电子电路系包含一密码处理器，并设置于用于无接触端子之应用方面的一芯片卡片之上。

如图 2 所示，该电子电路系包括一无接触端子接口 100 和一密码

处理器，该密码处理器系包括一 CPU10 和一周边装置 120，其中周边装置 120 可为一密码处理器、一 RNS 产生器或是一 UART 模块，为了叙述方便，该周边装置系作为如下所述之一密码处理器，CPU110 和密码处理器 120 二者分别具有一时脉乘法器 130 和 140，时脉乘法器 130 和 140 亦分别输出一时脉信号、clockCPU 和时脉密码，并且皆传送至 CPU110 和密码处理器 120，其中亦可能使用时脉产生器取代时脉乘法器，无接触端子接口 100 系用于自一无接触端子(图中未显示)将电磁能量 105 转换成电能以供应电子电路之用，并且包括一天线、一整流器以及一低通滤波器亦提供能量供应给时脉乘法器 130 和 140、以及一测功器或是一能量决定装置 150，测功器 150 输出控制信号 VCCPU 和 VCcrypto 给时脉乘法器 130 和 140 以作为供应能量或是无接触端子接口 100 之可使用能量之函数，以控制时脉乘法器 130 和 140 之时脉信号的时脉频率，其中时脉信号系被输出至 CPU110 和辅助处理器 120。

包含 CPU110 和密码辅助处理器 120 的密码处理器系适合用于处理特定之处理器工作，例如加密、解密、鉴定或是根据 DES 标准、AES 方法、RSA 算法则或是椭圆曲线方法的签署，密码辅助处理器 120 系依序地执行一特定的计算工作，例如一模块或是计算方面的加法、乘法、取幂或是倒置，一杂凑值之计算，而在周边装置 120 方面，同样可为一 RNS 产生器、UART 或是侦检器，一般来说，密码辅助处理器 120 的计算工作与 CPU110 的控制工作相比需要更多的计算工夫，其中 CPU110 的控制工作包括驱动密码辅助处理器 120，而 CPU 尚经由一总线(图中未显示)对密码辅助处理器 120 输出命令或是其它信息。

为了增加该密码辅助处理器的整体计算速度，无接触端子接口 100 自电磁能量 105 所获得的电能系由测功器 150 决定并且藉由时脉乘法器 130 和 140 而被分配给 CPU110 和密码辅助处理器 120，使得 CPU 之能量供应尽可能地减小，而密码辅助处理器 120 之能量供应尽可能地增大，在分配可使用能量给 CPU110 和密码辅助处理器 120 方面，改变这些组件的时脉信号 clockCPU 和 clockcrypto 的时脉频率之事实更进一步地决定了这些组件的能量消耗可自本案发明而受益，如果密码处理器系以 CMOS 技术制作，则能量消耗即无关于每个 MOSFET 的切换频率，因此，可使用能量之全面利用即可藉由尽可能快

速地对密码辅助处理器 120 计算时脉而达成，其中高速计算亦是被允许的。

在图 2 的实施例当中，时脉乘法器 130 和 140 的设计是为了在相同的控制信号下，它们可输出时脉信号 clockCPU 和 clockcrypto，其中的时脉频率系具有一固定倍数 n 的彼此不同，测功器 150 将能量供应自无接触端子接口 100 转换成相同强度的控制信号 VCCPU 和 VCcrypto，使得 $\text{clockcrypto} = n * \text{clockCPU}$ ，然而测功器 150 亦可能输出不同的时脉信号 VCCPU 和 VCcrypto 给时脉乘法器 130 和 140，测功器 150 不是形成将来自于无接触端子接口 100 的接收到之供应能量转换成由电路设计方式(例如一线性调节器)决定的适当之电压信号的调节器，就是形成一 A/D 转换器将供应能量转换成数字控制信号 VCCPU 和 VCcrypto，而在数字控制信号方面，提供控制信号 VCCPU 和 VCcrypto 储存于特定能量供应区域的检索表，其中控制信号 VCCPU 和 VCcrypto 可确保每一能量供应区域之密码处理器之最佳化计算时间。

图 2 之时脉乘法器 130 和 140 形成相锁回路(PLL)的形式，其中 PLL 使得一输入频率具有一时脉频率倍数 n/m ，举例来说，该输入频率可藉由无接触端子接口 100 所产生的一时脉信号而重新设定，时脉乘法器 130 和 140 可因此将该输入频率 f_{in} 的一时脉信号转换成该输出频率 $f_{out} = (n/m) * f_0$ 的一时脉信号，时脉乘法器 130 和 140 的方块图如图 3 所示，图中可看出，每个时脉乘法器包括一输入端 IN200、输入端 Inn 和 INm 以及一输出端 OUT，其中该输入频率 f_{in} 之时脉信号系应用于该输入端 IN200，且计数器 n 之值和有理倍数的分母 m 系于输入频率 f_{in} 与输出频率 f_{out} 之间应用于输入端 Inn 和 INm，而具有该时脉频率 f_{out} 的一时脉信号系输出于该输出端 OUT，除了一频率除法器 220，该电路尚包括由一电压控制振荡器 VC0230、一频率除法器 240、一 XOR 电路 250 以及一调节器 260 所构成的一 PLL，频率除法器 220 的一输入端系连接于该输入端 IN200，并且另一的输入端系连接于该输入端 INm210，在一输出端方面，频率除法器 220 输出频率 f_{in}/m 的一输出信号，其中该输出端系连接于该 XOR 电路 250 之一输入端，该 XOR 电路 250 之另一输入端系连接于该频率除法器 240 之一输出端，其中该频率除法器 240 的两个输入端系分别连接于该输入端

INn205 以及该 VC0230 之一输出端, 该 VC0230 之一输入端系经由该调节器 260 连接于该 XOR 电路 250 之一输出端, 该 VC0230 之该输出端更连接于该输出端 OUT215。

图 3 之电路的运作模式系陈述如下, 受到控制信号 VCCPU 和 VCcrypto(请参阅图 2)控制的该控制输入端 Inn 和 INm 亦可用于设定倍数 n 和 m(n, m 系为自然数), 其中藉由该倍数 n 和 m, 该频率除法器 220 和 240 可将该输入端 200 的该输入时脉信号的频率与该振荡器 230 的该输入时脉信号相除, 只有当该 VC0230 的该输出信号具有该输出频率 $f_{out} = (n/m) * f_0$, 具有相同时脉频率 f_{in}/m 和相位的单一信号才能被应用于该 XOR 电路 250 的两个输入端, 然而如果不是这种情形的话, 电压控制振荡器 230 即会被该 XOR 电路 250 以及该调节器 260 进行联合调整以达到该输入时脉信号与该输出时脉信号之间所需的比率倍数, 因此, 应用于该输出端 OUT 的该时脉信号即具有所需的频率 f_{out} 。

以上所述皆为图 2 之电子电路的电路配置及运作方式, 以下所述则为该电子电路用于无接触端子之芯片卡片的较佳应用例。

图 4 所绘制的是其上具有图 2 之电子电路的一芯片卡片, 其中该电子电路系设置于一无接触端子 310 的 300a、300b 以及 300c 等三个位置上, 而该无接触端子 310 会发射具某一频率的电磁幅射 320, 如图 4 的双箭号所示, 不同位置 300a 至 300c 与无接触端子 310 之间系分别相隔不同之距离 10cm、7cm 以及 5cm, 由于自该电子电路之该无接触端子接口(请参阅图 2)之电磁幅射 320 所得到的可使用之能量 E 系无关于该芯片卡片与该电子电路之该无接触端子 310 之间的距离 d, 因此该电子电路的该控制器之一时脉频率 f_1 、 f_2 以及 f_3 会被分别设定于不同的位置 300a、300b 以及 300c 上, 其中时脉频率可能较高亦可能较低, 须视该无接触端子 310 与该芯片卡片之间的距离而定, 如果芯片卡片距离端子 310 较远, 则该电子电路之可使用能量便较少, 时脉频率必定较低, 如果芯片卡片较为靠近端子 310, 则该电子电路之可使用能量便较多, 而该控制器也会以一较高的频率进行计算时脉, 以这种方式, 总是藉由调整时脉频率来配合可使用能量, 使得如果可使用能量较多, 便可能只需要较短之计算时间, 相比较之下, 使得传统的密码芯片卡片之解决方法, 则会具有一固定的能量消

耗(例如一固定之时脉频率),会为了配合端子 310 与该芯片卡片之间的一特定距离而被预先设定,以及成为最大计算功率以及最大距离范围二者之间的折衷,因此,密码处理器的运作便可能仅局限在该范围之内,而在此较小的范围之内任何多余的能量皆不会被转换。

5 为了简化描述,仅具如上所陈述之第二及图 4 之应用,其中一密码处理器系包括一 CPU 和一周边装置或一密码辅助处理器,然而在目前为止多数的习知情形中,一密码处理器将包括数个周边装置和密码辅助处理器,在这种情形下,可使用能量将会被分配给辅助处理器,使得在一最大能量使用之情形下达到一最小计算时间,这是因为在分配由测功器所决定的可使用能量给辅助处理器及 CPU 时,已经将目前的处理器工作和/或辅助处理器的不同的计算工作、以及其余的周边装置的相关工作皆考虑进去,可使用能量接着便总是会被用于在应用和处理器工作方面最常被使用的辅助处理器当中,在实施鉴定的情形中,密码辅助处理器可能分配到最多能量,相反地 CPU 和其余的辅助处理器则仅能分配到可使用能量的最小部份,相似的是,在一加密工作和杂凑值之计算之中,可使用能量会以如时脉速度一样快地被分别分配给 DES 模块和杂凑模块,和目前处理器工作无关的辅助处理器会藉由与供应电压间形成断路而被完全关闭或处于一休眠模式以避免漏电流的发生。

20 藉由每个辅助处理器分配到一时脉乘法器可以达到将可使用能量理想化地分配给数个辅助处理器,如图 2 中密码辅助处理器 120 分配到时脉乘法器 140 所示,在最简单的情形下,辅助处理器依序被 CPU 驱动或使用以执行处理器工作, CPU 会运作于时脉频率 f_{CPU} ,然而目前无须用于处理器工作的辅助处理器会被关闭或是运作于频率 f_{CPU} ,同时只有目前有需要使用的密码辅助处理器会被设定以一较高之时脉频率进行计算时脉,使得可使用能量能尽可能被用尽,换句话说,只有目前主要使用于处理器工作的辅助处理器的时脉频率增加或减少使得其于可能之最大时脉频率进行计算时脉,且只有剩余之可使用能量足够运作剩余之必须组件的情形之下,计算速度和最大能量使用的理想化才能达到。

在密码辅助处理器之平行运作的情形中,可使用能量之分配于密码辅助处理器可藉由查询一检索表而实行,其中密码辅助处理器之时

脉频率之最佳化设定系分类式地储存于该检索表，其系分别用于可使用能量之某些区域或是需要密码处理器之某些应用，每套时脉频率皆会将相关之可使用能量分配给相关计算工作所需之密码辅助处理器，此外，每套时脉频率皆系以在该套时脉频率中将可使用能量完全用尽为目标而被决定，通常由于数个密码辅助处理器会用于相同应用之中，或是执行相同应用所需之计算工作，因此这些密码辅助处理器会藉由相同之时脉或同一 PLL 进行计算时脉，或是彼此以一时脉频率树中的固定时脉频率比率进行计算时脉，其中将时脉频率的数字控制于减少的方向。

- 10 即使以上已陈述藉由仅允许有理倍数比率的时脉乘法器或 PLL 以设定 CPU 和辅助处理器的时脉信号，然而若欲藉由彼此独立之振荡器的使用使得控制器组件之时脉频率之间具有相关之主要比率仍是可能的，和前述之时脉乘法器比较起来其优点在于，可使用能量可以一更为最佳化的方式被利用，这是因为时脉频率不仅被完全设定成有理倍数，彼此间还被设定成具有相对质数性质，这种能量的最大利用是非常吸引人的，特别是在可使用能量极为有限的应用场合之中，例如无接触和行动通讯之应用当中，然而，用于全体或是部份的密码辅助处理器的特殊振荡器需要同步于使用中的密码辅助处理器，这是因为其亦系以同步于 CPU 的方式进行计算时脉，使用中的密码辅助处理器
- 15 之间接口上的所有输入和输出必须经由适当的同步装置被同步化，该同步装置包括彼此串联的两个同步触发器。

- 20 最后需要指出的是，对于任何形式的控制器来说，不管其是否具有辅助处理器，即使如图 2 之实施样态，该电子电路包括一 CPU 以及一辅助处理器仍是可能的，仅将能量控制应用于整个控制器会产生如上所述之本案的优点。

请参阅图 2，应该进一步指出的是，该电子电路可设置于一电路板或是积体化于一芯片之上，相似地，该控制器亦可包括设置于一电路板或是积体化于一芯片之上的个别组件。

- 30 即使本案已如上所陈述关于无接触应用之第二及图 4，本案仍可应用于接触端子或是行动通讯之应用，在这种情形中，图 2 的接触端子接口可由一单一接点所取代。

必须进一步指出的是，即使本案已如上所陈述该时脉乘法器系以

硬件布线的方式设于该电子电路之中，它们仍可经由有线或无线连接的方式连接于该电子电路，时脉乘法器或振荡器可在该电子电路于端子处使用芯片卡片的情形之下连接于每个端子或接口。

5

图标符号说明：

100 无接触端子接口

105 电磁能量

110 CPU

10 120 密码辅助处理器或周边装置

130 时脉乘法器

140 时脉乘法器

150 测功器

200 输入端

15 205 输入端

210 输入端

215 输出端

220 频率除法器

230 VCO

20 240 频率除法器

250 XOR 电路

260 调节器

300a 位置

300b 位置

25 300c 位置

310 无接触端子

320 电磁幅射

10 决定可使用能量 E

20 依照 E 控制处理器

30 20a 设定时脉频率

20b 关闭无关之组件

20c 设定供应电压

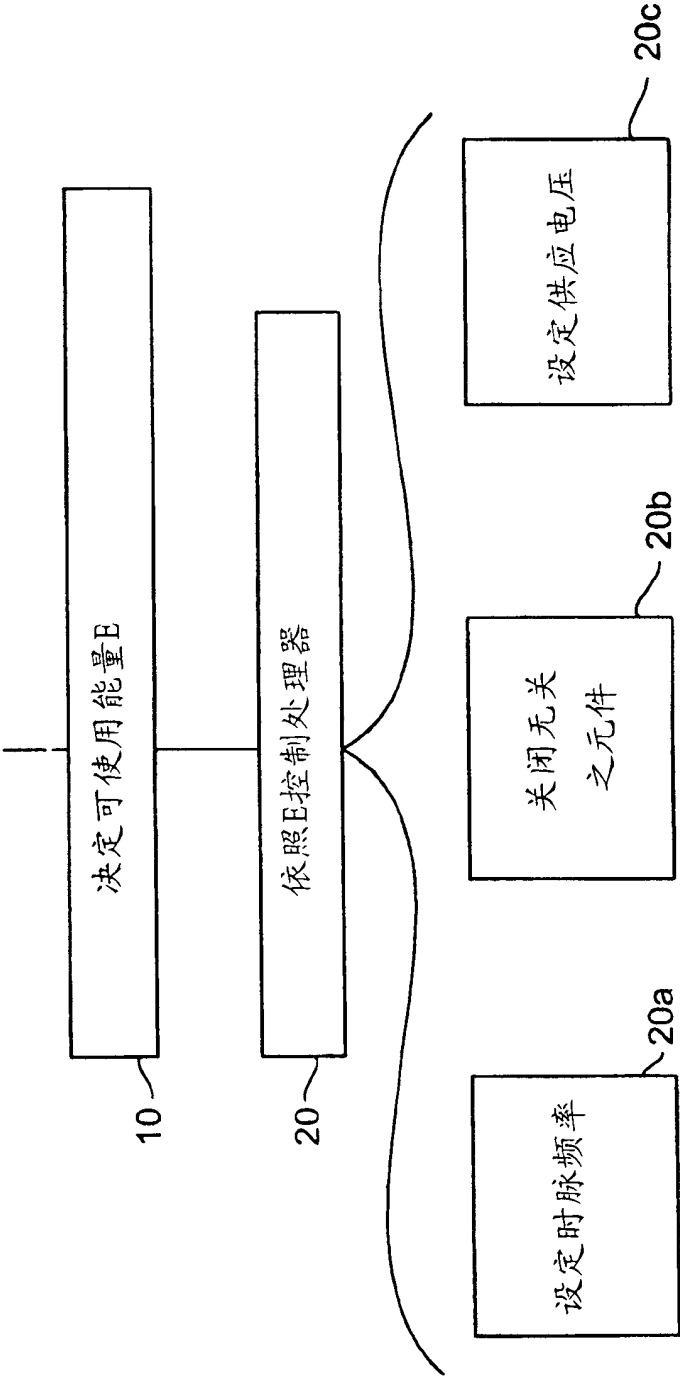


图 1

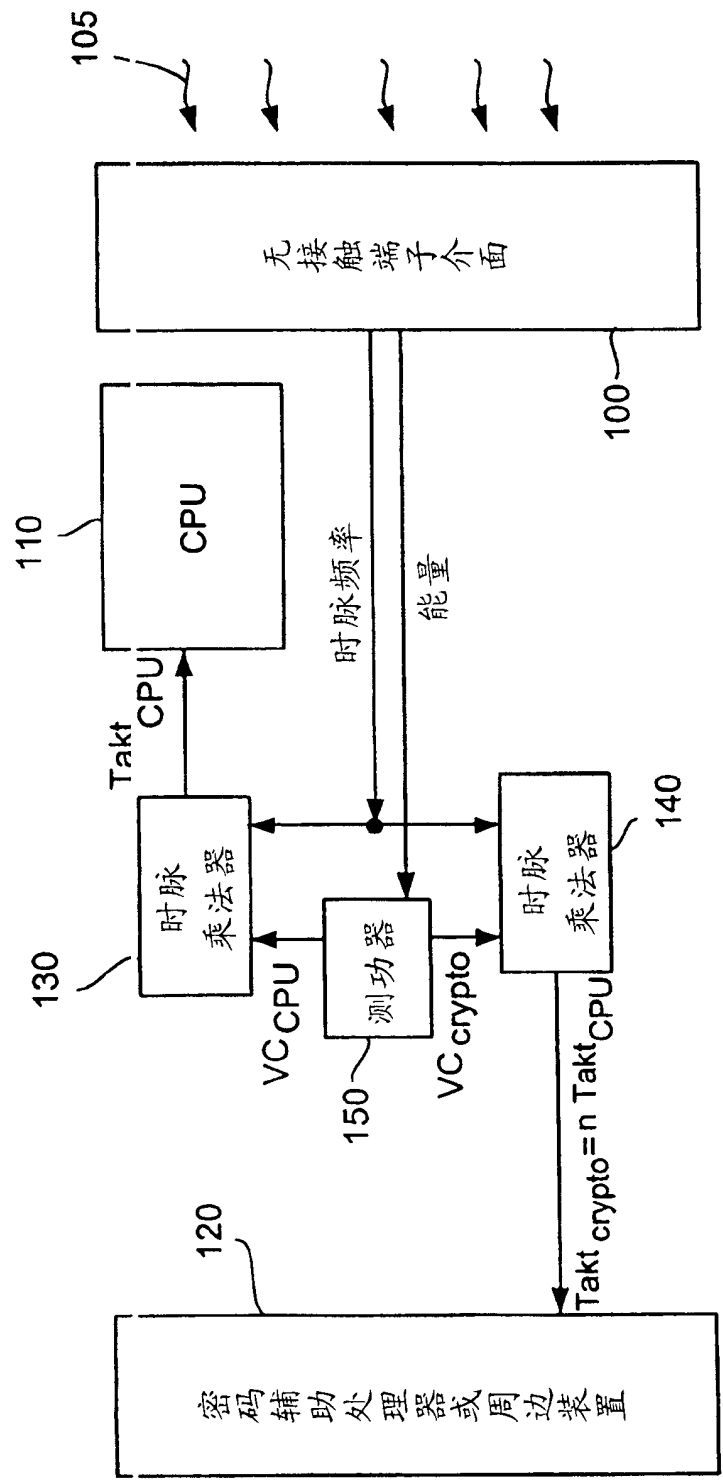


图 2

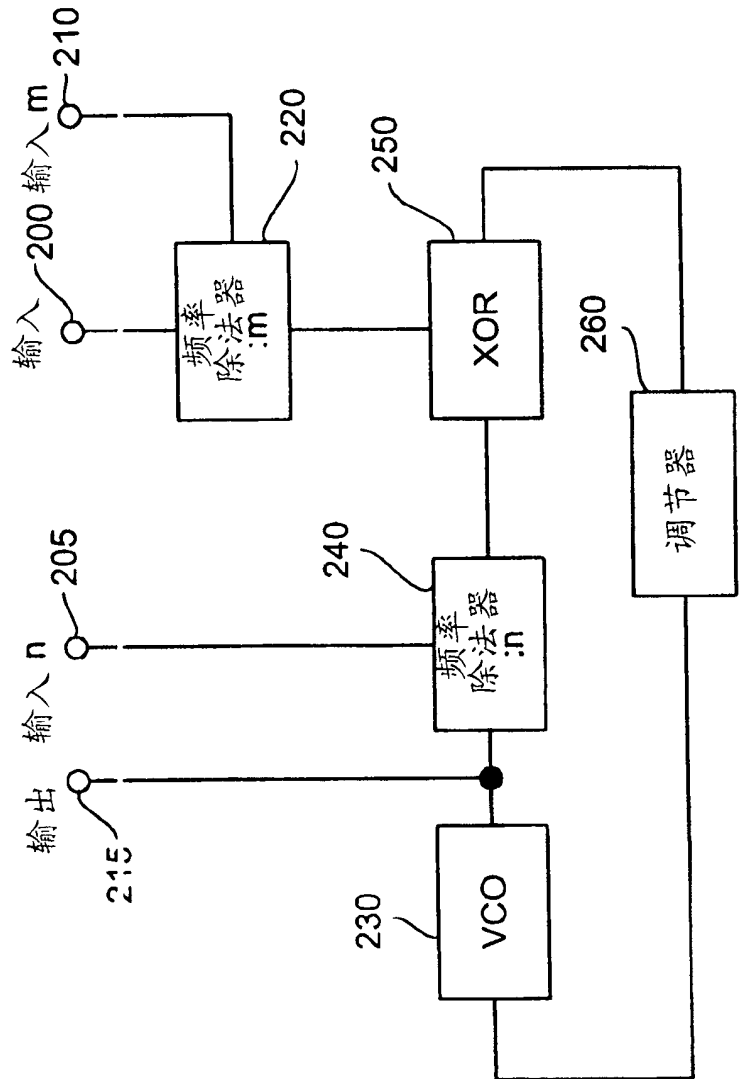


图 3

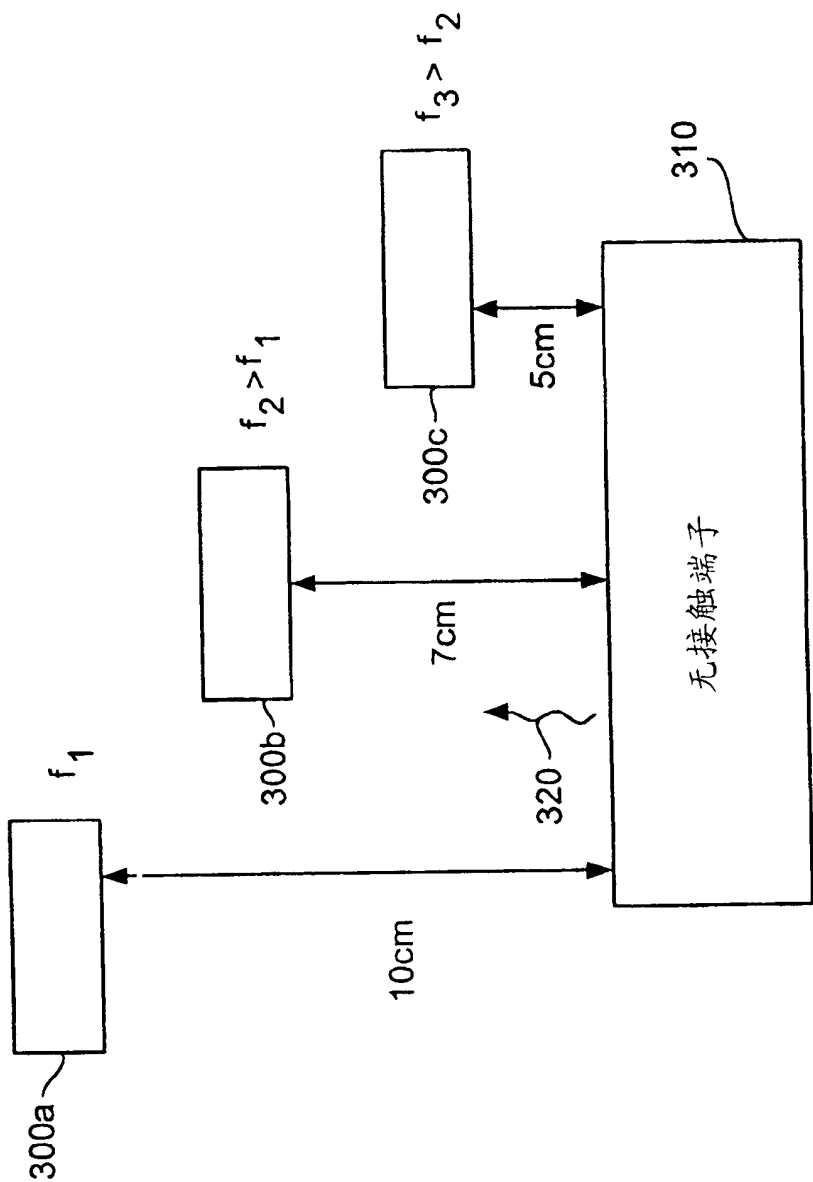


图 4