



[12] 发明专利申请公开说明书

[21] 申请号 01811984.0

[43] 公开日 2003 年 9 月 17 日

[11] 公开号 CN 1443343A

[22] 申请日 2001.6.7 [21] 申请号 01811984.0

[30] 优先权

[32] 2000.6.27 [33] US [31] 09/604,682

[86] 国际申请 PCT/US01/18692 2001.6.7

[87] 国际公布 WO02/01328 英 2002.1.3

[85] 进入国家阶段日期 2002.12.27

[71] 申请人 英特尔公司

地址 美国加利福尼亚州

[72] 发明人 R·哈斯邦 J·沃格特

J·布里泽克

[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 王忠忠

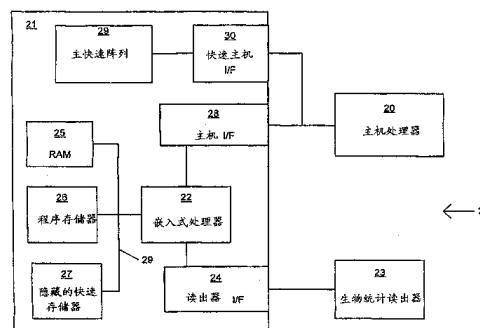
权利要求书 3 页 说明书 12 页 附图 4 页

[54] 发明名称 非易失性存储设备中基于生物统计的鉴权

存储器也可以在集成电路中提供而用于保存非安全数据。这个第二存储器有它自己的接口端口，并且与有关安全的功能和存储器分开，使得安全功能和非安全功能在物理上是互相隔离的，并且不能通过修改来克服这种隔离。

[57] 摘要

一种基于生物统计的安全电路，其中用户数据库、处理器和生物统计图生成功能都位于同一个集成电路中，它的安全内容不能从该集成电路外部来访问。像指纹、视网膜扫描和声纹的生物统计数据从请求访问受限的资源的用户处获得。该生物统计数据被发送到集成电路中，在那里它被变换成生物统计图，并与存储在集成电路中非易失性存储器里的生物统计图的数据库相比较。这个存储的图表示预先授权的用户，并且匹配会触发该安全电路发送一个信号给主机处理器，以授权主机处理器允许请求的到受限资源的用户访问。集成电路基本上充当于安全数据的只写存储器，因为集成电路中的安全数据和安全功能不能直接通过一个管脚或端口来访问，并且因而不能通过专门的安全攻击来读取或监控。可以从集成电路外部来访问的第二非易失性



1、一种装置，包括：

集成电路，它包括：

第一处理器；

5 与该第一处理器耦合以与该集成电路外部的第二处理器通信的第一接口；

与该第一接口分离并与第一处理器耦合以存储第一生物统计数据的第一非易失性存储器，该数据用来识别至少一个授权用户，并且该存储器具有不能从该集成电路外部读取的内容；以及

10 与该第一处理器耦合以从生物统计读出器输入第二生物统计数据的第二接口。

2、如权利要求 1 的装置，其中集成电路进一步包括与第三接口耦合并与第一处理器、第一接口、第二接口和第一非易失性存储器分离的第二非易失性存储器，并且该存储器具有不能通过该第三接口从该装置
15 外部来访问的内容。

3、如权利要求 1 的装置，其中第一非易失性存储器是快速存储器。

4、如权利要求 1 的装置，其中第二非易失性存储器是快速存储器。

5、如权利要求 1 的装置，其中生物统计读出器是指纹读出器。

6、如权利要求 1 的装置，其中：

20 第一生物统计数据包括第一生物统计图；以及

集成电路包含能使得第一处理器把第二生物统计数据变换成第二生物统计图的代码。

7、如权利要求 6 的装置，其中集成电路包含能使得第一处理器执行第二生物统计图和第一生物统计图之间的比较的代码。

25 8、如权利要求 7 的装置，其中：

集成电路包含代码，在比较中发现匹配的情况下，该代码能使得第一处理器通过第一接口发送一个验证信号；以及

集成电路包含代码，在比较中没有发现匹配的情况下，该代码能使第一处理器通过第一接口发送一个未验证信号。

30 9、如权利要求 1 的装置，其中集成电路包含能使得第一处理器授权下载到集成电路中的程序的代码。

10、一种系统，包括：

主机处理器；

生物统计读出器；

与生物统计读出器和主机处理器耦合的集成电路，并且该集成电路包括：

5 第一处理器；

与第一处理器和主机处理器耦合的第一接口；

与第一接口分离并与第一处理器耦合以存储第一生物统计数据的第一非易失性存储器，该数据用来识别至少一个授权用户，并且该存储器具有不能从该集成电路外部读取的内容；以及

10 与第一处理器和生物统计读出器耦合以输入第二生物统计数据的第二接口。

11、权利要求 10 的系统，其中集成电路进一步包括通过第三接口与主机处理器耦合并与第一处理器、第一接口、第二接口和第一非易失性存储器分离的第二非易失性存储器，并且该存储器具有不能通过该第 15 三接口从该装置外部访问的内容。

12、如权利要求 10 的系统，其中：

第一生物统计数据包括第一生物统计图；以及

集成电路包含能使得第一处理器把第二生物统计数据转换成第二生物统计图的代码。

20 13、如权利要求 12 的系统，其中集成电路包含能使得第一处理器执行第二生物统计图和第一生物统计图之间的比较的代码。

14、如权利要求 13 的系统，其中：

集成电路包含代码，在比较中发现匹配的情况下，该代码能使得第一处理器通过第一接口发送一个验证信号；以及

25 集成电路包含代码，在比较中没有发现匹配的情况下，该代码能使得第一处理器通过第一接口发送一个未验证信号。

15、如权利要求 10 的系统，其中该集成电路包含能使得第一处理器鉴权下载到该集成电路中的程序的代码。

16、一种方法，包括：

30 把用户的生物统计数据输入到集成电路中；

从该集成电路中的非易失性存储器读取先前存储的生物统计数据的数据库，其中不能从该集成电路外部读取该非易失性存储器的内容；

使用置于该集成电路中的处理器，把用户的生物统计数据与该数据库的至少一部分相比较；

如果比较产生一个匹配，则发送一个验证信号给一外部设备；以及如果比较没有产生匹配，则发送一个未验证信号给该外部设备。

5 17、如权利要求 16 的方法，其中：

存储的生物统计数据包括存储的生物统计图；以及

比较包括把该用户的生物统计数据转换成用户的生物统计图，以及把该用户的生物统计图与存储的生物统计图相比较。

18、如权利要求 16 的方法，其中非易失性存储器是快速存储器。

10 19、如权利要求 16 的方法，其中发送验证信号包括发送一个该用户被授权访问的资源的指示。

20、一种具有存储在其上的指令的机器可读媒体，在由至少一个处理器执行该指令时，它会使得所述至少一个处理器执行：

把用户的生物统计数据输入集成电路中；

15 从该集成电路中的非易失性存储器中读取先前存储的生物统计数据的数据库，其中不能从集成电路外部读取该非易失性存储器的内容；

使用置于该集成电路中的处理器，把用户的生物统计数据与该数据库的至少一部分相比较；

如果比较产生一个匹配，则发送一个验证信号给一外部设备；以及如果比较没有产生匹配，则发送一个未验证信号给该外部设备。

21、如权利要求 20 的媒体，其中：

存储的生物统计数据包括存储的生物统计图；以及

比较包括把该用户的生物统计数据转换成用户的生物统计图，以及把该用户的生物统计图与存储的生物统计图相比较。

25 22、如权利要求 20 的媒体，其中非易失性存储器是快速存储器。

非易失性存储设备中基于生物统计的鉴权

发明背景

5 1. 发明领域

本发明总体上属于安全系统。尤其是它属于基于用户的生物统计特征的改进型安全设备。

2. 有关技术描述

10 电路小型化、无线技术和电池电源的进步导致了便携式设备的广泛使用，该便携式设备能访问大量分布式系统的资源。蜂窝电话的使用就是一个实例，它允许订户用一种他们能够在个人身上携带的设备来访问国家和全球电话系统的资源。典型的蜂窝电话允许拥有该蜂窝电话的任何人访问这些资源。对于像处于安全域的台式机这样的较大设备，使安全性基于拥有权并不是问题。但是对于易于丢失或被盗的小型便携式设备，这种安全等级是不够的。

20 解决该问题的常规方法是使用密码。但是基于密码的安全是完全以保护密码为基础的。密码可以被未经授权的人以各种各样的方式非法获得，像通过观察某人输入密码、电子监控密码登录或者在新密码被发送给预定用户时截取它。由于该用户仍然拥有密码，所以只有在未经授权的人不正确地使用该密码若干时间之后，安全破坏才能够被检测到。另一个问题是有时候合法用户会忘记密码，这导致用户受挫并带来不便，而且要采取措施来以可能危及到密码安全的方式避免这一问题。

25 另一种方法是用户接口模块（SIM），它把密码与人工制品结合起来，比如既包含安全数据又包含处理能力的机器可读塑料卡。由于访问既需要卡又需要密码，所以与只有密码的方法相比，这提供了改良的安全等级，但是它仍然遭受许多同样的问题。

30 这些常规方法的问题是那些密码会被盗或遗忘，而人工制品也会丢失、被盗、被复制或被伪造。访问控制的改良方法是使用生物统计数据来识别特定用户，而不需要密码或人工制品。生物统计数据是描述用户唯一的物理特征的数据，并且它能够在请求访问时直接从用户个人读取。某些已知的生物统计方式是通过指纹、视网膜扫描以及声纹来识别用户。每种方法都有其优点和弱点，但是所有方法都是基于用户唯一的

物理特征的，这些特征很难复制并且不要求用户记住什么。但是基于生物统计的安全系统也有弱点。如果能够获得生物统计数据，那么指纹、视网膜图像及声音等就能被伪造或复制，并且会被非法使用以获得对系统的访问。

图 1 显示了常规的生物统计安全系统 1。主机系统 11 包括主机处理器 12、存储器 13、连到生物统计读出器 16 的读出器接口 14 以及连到系统其它部分的通用接口 18。存储器 13 包括各种类型的存储器，比如随机存取存储器 (RAM)、只读存储器 (ROM) 以及快速存储器。典型地，快速存储器被用来存储已核准用户的有效生物统计数据，并且能够在增加用户、删除用户或用户需要修改他们的数据时被更新。该生物统计数据可能是原始格式，像指纹的数字化图像，但更可能是简化格式，它表示以预先定义的数字格式定义该图像的相关点的图像编码图。在请求访问时，生物统计读出器 16 从用户处得到合适的生物统计输入。例如，读出器 16 可以是指纹读出器、视网膜扫描仪或声纹识别设备。生物读出器 16 把原始生物统计数据变成数字化图，并通过读出器接口 14 把该图发送给主机处理器 12，主机处理器 12 把它与快速存储器中的参考图比较。如果存在匹配，则处理器 12 将典型地通过通用接口 18 来启动对所请求资源的访问。该设计至少有三个主要的弱点。1) 读出器 16 和接口 14 之间的链路可使生物统计图面临监控和复制。非法复制的图以后可被直接提供给读出器接口 14，而不需要再复制实际的生物统计图像或数据，因而骗取系统 11 相信它正在从授权的用户处读取有效数据。2) 主机处理器 12 典型地处理非安全功能，比如蜂窝电话的操作功能。因此主机处理器 12 易遭受到黑客攻击以及其它入侵性的篡改。这可被错误地引导成通过通用接口 18 提供安全用户数据，或者把错误的用户数据存储到快速存储器中。任何一种行为都允许一个未经授权的人在以后通过读出器 16 以正常方式使用该系统。3) 快速存储器（以及因此是安全数据）可以从外部的系统 11 通过公共总线 15 并配合处理器 12、存储器 13 和接口 14、18 来访问。

这些弱点也使系统面临破坏性的篡改，而篡改的目的就是破坏正常的操作，而不是得到这些操作的未经授权的使用。

附图简述

图 1 显示了现有技术的设备。

图 2 显示了本发明的设备。

图 3 显示了图 2 设备的更详细的视图。

图 4 显示了本发明的系统。

发明详述

5 本发明提供一个自主式安全电路，它维护存储器中的安全数据，该数据不能从安全电路的外部来访问，但是它能够被用来核实从安全电路的外部提供的数据。图 2 显示了本发明系统 2 的一种实施方案。主机处理器 20 可以是非安全处理器，比如在蜂窝电话中控制整个蜂窝电话运行的处理器。安全电路 21 是一个在系统 2 中提供自主式安全环境的单个集成电路，并且没有它的允许就不能从外部访问它。电路 21 能控制传送给电路 21 的或从电路 21 传送出的任何数据。电路 21 包括它自己的嵌入式处理器 22，如此称谓是因为该处理器嵌入在安全电路 21 的周围内。处理器 22 也能控制连到主机处理器 20 的主机接口 28 以及连到生物统计读出器 23 的读出器接口 24。嵌入处理器 22 能够在内部总线 10 29 上与存储器 25、26 和 27 一起运行。程序存储器 26 可以是可编程的只读存储器 (PROM) 或其它包含运行处理器 22 的指令的非易失性存储器。在处理器运行过程中，RAM 25 可以用作工作区，但是不应用来存储永久数据，因为如果设备 2 的电池没电或被断开，RAM 25 将丢失它的内容。快速存储器 27 可以用于周期地变化但是必须在功率损耗之后还存在的数据。快速存储器 27 是可以存储用户特定数据的地方，比如每个被授权使用该系统的用户的参考生物统计数据。虽然 RAM 25、程序存储器 26 和快速存储器 27 被显示为三种单独的存储器类型，但是它们中的两种或两种以上能够被合并为单个存储器类型。例如快速存储器可以被用来代替 RAM 25 和/或程序存储器 26。虽然该公开内容始终描述的是快速存储器的使用，但是其它类型的可写非易失性存储器也能在不超出本发明的范围的情况下被使用。

20

25

主快速阵列 29 可以提供一个分开的用于非安全数据的可写非易失性存储器，并且主机处理器 20 能够通过快速主机接口 30 访问它。虽然主机接口 28 和快速主机接口 30 被显示成共享一条公共总线，但是它们也能够通过完全分开的连接来实现。在一种实施方案中，主快速阵列 29 可以在功能上与集成电路 21 中的安全功能分开。在另一种实施方案中，嵌入处理器 22 能够在用户被鉴权时启用主快速阵列 29 的全部或部分，

并且它能够在其它情况下停用主快速阵列 29 的全部或部分。

安全电路是提供围绕在安全功能周围的安全边界的一个集成电路，因为这些功能的操作不可从电路 21 的外部访问，并且包含在其中的安全数据只有在它控制的特定、有限的情况下才能被读或写。但是某些类型的初始用户信息必须写入电路 21 中，这对于该系统来说是有用的。为了提供用于输入用户信息的启动点，在一种实施方案中，在设备 2 开始运行前，有关用户数据最初可以在受控的情况下存储在快速存储器 27 中。例如该初始安装能够为系统管理员建立生物统计图以及功能性，该系统管理员就是以后能授权该新数据条目的唯一的人。作为选择，输入生物统计信息的第一个用户会被自动确定为系统管理员。在安全系统中输入初始用户信息的方法在本领域中是已知的。

一旦用户数据已经被输入该系统中，那么在一个潜在用户试图通过读出器接口 24 输入他或她的生物统计数据来使用该系统时，安全电路 21 会简单地把一个该用户的已验证或没有被验证的指示（以及可能还有一个经核准的特权）通过接口 28 提交给主机 20。因而没有暴露存储的用户参考数据，并且也不能通过电路 21 外部的任何设备来从电路 21 中读出该参考数据。

这大大优于图 1 的现有技术系统。在图 1 中，某种格式的安全数据，像指纹图存储在快速存储器中，其它设备可以通过接口 18 访问它。另外，主机处理器 12 是不安全的，并且可被篡改。这可被引导成通过接口 18 把安全数据暴露给外部设备，并且也会被引导成把伪造的用户文件存储在快速存储器中。如果快速存储器的控制电路可以通过共享总线访问，那么伪造的数据可以不用主机处理器 12 的知识或参与而直接写入快速存储器中。

比较起来，在图 2 的系统中，安全数据存储在隐藏的快速存储器 27 中，它不与任何外部接口共享总线，因而不可被任何外部设备读取。另外，嵌入处理器 22 完全用来提供安全电路 21 执行的安全功能。因此，嵌入处理器 22 由不可更改的代码控制，该代码不易遭受针对该安全功能的黑客攻击或其它篡改。主机处理器 20 执行所有的不安全功能，它不可访问安全电路 21 中的任何安全功能或安全数据。

在它的其它功能中，电路 21 基本上提供用于安全信息的只写存储设备。在初始数据在受控条件下被写入电路 21 之后，电路 21 不允许外

部设备读取任何安全数据，并且不允许另外的安全数据进入，除非是在
5 电路 21 的控制下。由于所有电路 21 都包含在单个集成电路中，所以没
有可访问的管脚或接口连接，而这种连接将暴露安全数据或者使得它能
够被外部设备读取或修改。这实际上使得安全攻击不能进入设备 2。这
不仅保护了安全数据，而且对输入数据的适当检查也可防止破坏性数据
被输入到电路 21 中。

图 3 显示了更详细的安全电路 21 的视图。嵌入处理器 22 通过一条
10 公共内部总线来与隐藏的快速存储器 27、程序存储器 26、RAM 25、随机
号码生成器 (RNG) 38、乘法器/累加器 39、运算加速器 37、生物统
计加速器 41、单调计数器 40 和监视计时器 36 对接，该公共内部总线对
外部设备而言不可访问。前三个设备与图 2 显示的设备一样；余下的设
备被用来执行有关安全的功能，并在下面更详细地描述了它。在图 2 中
还显示了处理器 22 与读出器接口 24 和主机接口 28 相耦合。

基准时钟 31 提供时钟源给电路 21。一种实施方案提供一个 70 兆赫
15 兹 (MHz) 的时钟给处理器 22。时钟分配电路 33 能够划分基准时钟直到
较慢的速率，以用作监视计时器 36 和其它功能诸如告警逻辑 34 的源时
钟。时钟检测器 32 能够确定基准时钟 31 是否有效以及是否在预先定义
的频率界限中，而电压不足/过电压 (UV/OV) 检测器 35 可以监控电路
21 中的电压电平。告警逻辑 34 可以从电路 21 的其它部分接收各种类型
20 的告警信号，并可以提供合并的告警指示给处理器 22 以及其它电路。

下面更详细地描述了电路 21 的功能：

处理器

嵌入处理器 22 可以处理命令并执行快速存储器管理。在一种实施
方案中，处理器 22 处理标准 SIM 命令，这样现有的传统软件在系统中
25 都可使用。处理器 22 也可以执行某些有关密码的处理，比如散列算法
或密码算法。该处理器有足够的性能来实时执行这些算法，而不影响性
能。处理器 22 也可并入存储器管理单元 (MMU)。MMU 在安全设计中是
一个非常必要的组件。它能够实施代码与数据的分离，并且能够把用于
30 一个处理上下文的数据与用于另一个处理上下文的数据分离。这种分离
可以用来确保私用数据不会因疏忽而与随后从安全电路 21 发送出的非
私用数据混合。

主机接口

主机接口 28 能够提供到图 2 的主机处理器的接口。该接口的类型有很多种，比如并行或串行接口、高速或低速接口等。为了保持与现有主机设备的兼容性，主机接口 28 可以复制当前在现有主机系统中使用的接口。

在一种实施方案中，在主机接口 20 和嵌入处理器 22 之间的传递能够以适当握手信号来执行，每次一个字节（或其它数据单元）。在另一种实施方案中，先进先出缓冲器（FIFO）能在接口 28 中被用来缓冲多个字节，这样就允许任一个或两个处理器以突发模式有效地运行。

主机接口 28 也可包括其它信号，像通过一个或多个管脚来传递从告警逻辑 34 来的告警信息，以及接收进入电路 21 的外部时钟信号（没有显示）。主机接口 28 的运行受嵌入处理器 22 的控制，该嵌入处理器能够启用或停用主机接口 28 的所有或一部分，以控制数据流及其它被传递给主机处理器 20 的或从主机处理器 20 传递来的信号。

程序存储器

程序存储器 26 包含用于执行处理器 22 所执行功能的指令。为了保护系统的安全性，程序存储器 26 可以被制成在系统中不可更改。它可以是像 PROM 的永久存储器，也可以是像 EEPROM 或快速存储器的半永久存储器。

快速存储器

快速存储器 27 被用来存储不断变化但是必须在功率损耗之后还存在的数据。在便携式设备中，快速存储器很好地适合于该目的，因为它能在便携式设备通常能获得的电压下运行。快速存储器只能以块的形式被擦除，所以足够的快速存储器的量被用来确保在数据变化时，包含该变化的整个块能够被复制到空白块中。而原来的块被擦除以提供给下一个变化一个空白块。

虽然在本公开内容中始终描述的是快速存储器，但是在电路内可编程的其它类型的非易失性存储器也能被使用，并包括在本发明的范围内。

主快速阵列 29 可以用于非安全信息，并且主机处理器 20 可以通过快速主机接口 30 来访问它。虽然主快速阵列 29 和它的接口 30 在功能上与电路 21 的其它部分分离，但是把它与隐藏的快速存储器 27 放在同一

一个集成电路中能够有效利用集成电路不动产，同时也能减少整个芯片量并提高生产效率。接口 30 可以是与主机接口 28 同一类型的接口，并且接口 30 甚至可以与公共总线相连，就像图 2 所描述的。接口 28 和 30 也可以是不同类型的，并且/或者在该系统中可以没有公共连接。

5 RAM 存储器

随机存取存储器 25 可以在系统运行时用作工作区存储器。由于在 RAM 电路断开电源时会丢失 RAM 存储器的内容，所以放在 RAM 中的数据不应该包括那些不能丢失的数据或者那些在重接电源后不能恢复的数据。

10 随机号码生成器

在安全电路 21 和其它设备之间的通信可以使用加密。多种类型的加密要求生成真正的随机号码。像 RNG 38 的硬件生成器能够提供比软件 RNG 更优越的性能。硬件 RNG 的性能在本领域中是已知的。一些标准要求将在电路内测试的 RNG 结果是随机的。这能够要求接近 2500 比特的 RAM 存储器（或作为选择可以是快速存储器）专用于分析功能。

15 乘法器/累加器

为了执行加密功能，乘法器/累加器 (M/A) 39 能够支持快速取幂和模数缩减，并且可以对这些功能最优化。它不必用于通用算术运算，通用算术运算可以在处理器 22 中执行。M/A 功能的设计与嵌入处理器的设计紧紧相关。如果处理器 22 是数字信号处理器 (DSP)，那么可以使用 DSP 的 M/A，并且可以不需要在总线上分离的 M/A 39。

算法加速器

20 算法加速器 37 对于使用的密码算法是特定的。该专用硬件执行该算法要求的处理时间比处理器的处理时间更短。算法加速器 37 在功能和实现上是与 M/A 39 分离的。M/A 可以被用来加速在不对称算法（比如公共钥加密）中使用的乘法运算和取幂运算。该算法加速器加速被频繁地用来提供消息保密的对称算法。对 M/A 39 和加速器 37 的需要及其特殊设计将依赖于要在该电路中使用的特定密码算法。RNG 38、M/A 39 和算法加速器 37 也能被用来鉴权和加密在电路 21 和生物统计读出器 23 之间任一方向传递的数据。

30 生物统计加速器

生物统计加速器 41 在功能上与算法加速器 37 相类似，但是它的目

的是加速生物统计数据的处理。原始生物统计数据到生物统计图的变换涉及深入的、重复的处理，该处理最好能够由为所要求的特定处理而特殊设计的硬件加速器执行。

电压不足/过电压检测器

5 电压不足/过电压 (UV/OV) 检测器 35 能够保护系统免受一种基于改变的电压输入的密码攻击。这些攻击驱使供应电压超出该设备规定的运行范围，而试图迫使该攻击下的主体误操作从而暴露明文或密钥。UV/OV 35 能够检测出溢出电压情况并警告处理器 22，处理器 22 可以在暴露保密信息之前采取措施来停止运行。这也保护系统在电源供应降级
10 或故障的情况下免受无控碰撞。在一种实施方案中，使用比较器来相对参考电压监控该输入电压。可以使用作为电压分配器的精密电阻器来设定参考电压以对一个运算放大器 (op amp) 加偏压。

时钟

基准时钟 31 可以提供时钟源给电路 21。在一种实施方案中，基准
15 时钟 31 是运行在 70MHz 的内部时钟。它可以作为处理器时钟而直接馈送给处理器 22。它也可以被时钟分配电路 33 分到较低频率以运行像监视计时器 36 和告警逻辑 34 的设备。使用内部时钟而不是外部时钟可以防止专业攻击者通过控制时钟来操纵电路。

时钟检测器

20 时钟检测器 32 能够监控时钟信号的频率。如果时钟频率超出预先设置的范围，那么将产生一个告警，因而处理器能采取适当措施来关机，或以其他方式保护私人信息。该检测器主要是在使用外部时钟源时使用。

监视计时器

25 监视计时器 36 能够监控程序执行和数据传送。程序可以设计成以周期性的时间间隔或在特定例程的开始给计时器预装入预定的值。如果程序按照预期的运行，那么在时间满期之前计时器总是被重载或停止。如果定时器满期，则它指示该程序执行时出现了一个意外的变化，并且将产生一个告警。监视计时器 36 也能被用来监控依赖于外部操作的事件，比如电路 21 和另一个设备之间的数据传送。因为监视计时器通常以毫秒来计时，而不是以微妙和纳秒，所以基准时钟 31 可以被减少为一个低频时钟以提供更有用的用于监视计时器的时间基准。

告警逻辑

告警系统对于任何安全设计来说都是关键性的，因为它通过警告系统以采取附加保护措施来防止故障或恶意攻击。告警逻辑 34 提供一个用于可产生的各种告警的集结点，并且发送适当信号给处理器 22，从而使得处理器 22 可以采取措施来防止专用信息或其它数据的丢失。就像图 3 显示的，告警信号也能被发送给主机接口 28，然后从接口 28 发送给主机系统，并且它们也可以直接提供给外部设备。

除了在前面的段落中描述的告警外，告警逻辑 34 也能处理下列告警：

- 10 1) 坏密钥告警——这监控密码密钥并在碰到坏密钥时产生告警。该坏密钥的特殊标识对于每个算法都是唯一的。
- 2) 人工密钥输入告警——这监控人工载入的密钥的精确性。人工载入密钥应该含有一个检错代码，像奇偶校验码，或者它们应该使用重复输入以验证该输入的密钥的准确性。
- 15 3) 随机数发生器告警——这检验 RNG 38 的输出，并且验证输出在统计上是随机的。在加电和运行期间的各个点都可以使用各种已知的测试来执行该验证。
- 20 4) 软件/固件告警——只要一加电，该程序就能被检验来验证它没有被破坏。这可以通过错误检测代码 (EDC) 或应用于程序内容中的数字签名来进行。
- 5) 自测试——可以在加电时、重置后或在主机发出命令时执行各种系统自测试。自测试包括指令集测试、快速存储器测试、RAM 测试和与 M/A 39 的已知应答测试。

单调计数器

25 单调计数器 40 被显示为与内部总线相连，但是它也能用其它连接来实施，或者可以在软件或固件中执行。单调计数器是只能增加（或只能减少）的计数器，并且从不重复一个数，这暗示了必须不允许它重置或循环回到它的开始计数值。单调计数器 40 可以被用来提供对于至/自电路 21 的每个通信的唯一的标识号。这防止一次通信被记录下来，并在以后重播而冒充合法的通信。由于与被记录通信一起使用的计数器值不再与当前计数器值匹配，所以被记录的通信一被发送给电路 21，这种类型的安全攻击就会被检测出。通过让计数器以非线形的方式增加可以

获得额外的安全，因此就不能通过对自从被记录的传送以来已经进行的通信次数进行计数而轻易地猜出当前的计数器值。

虽然电路 21 的安全内容通常是不能从电路外部进行访问和修改的，但是在一种实施方案中，嵌入 CPU22 的程序能够通过下载一个新程序到安全电路 21 中来修改或替换。在被接受并使用该下载的程序之前，
5 嵌入 CPU 22 鉴权该程序以防止非法程序被插入而危及系统的安全。下
载可以通过主机接口 28 进行，或者通过一个分离的安全接口（没有显
示）进行。

在一种实施方案中，如果被授权的用户已经被鉴权，那么该用户可
10 以被准许直接访问隐藏的快速存储器 27 的内容。

系统运行

快速存储器 27 可以用来存储识别每个授权用户的安全生物统计图。只要用户请求访问该系统，就可以通过生物统计读出器 23 读取她或他的生物统计数据，并且可以通过读出器接口 24 提供该数据。该生物统计数据与存储在系统中的所有授权用户的生物统计数据进行比较。
15 如果发现匹配，那么就可以通过主机接口 28 把‘用户已验证’消息发送给主机处理器 20，允许主机处理器 20 启动所请求的操作。在一种实施方案中，主机也被告知该特定用户被批准使用哪种功能或资源。

一旦安全用户数据被放置在隐藏的快速存储器 27 中的一个文件
20 内，该用户数据就不能被安全电路 21 周界之外的任何外部设备访问。与隐藏的快速存储器 27 相连的总线 29 没有外部端口。嵌入处理器 22 是与隐藏的快速存储器 27 和外部世界都耦合的唯一设备，并且可以通过把处理器 22 的运行代码放入 PROM 中来限制它的运行，因此该代码不能被修改以重定向处理器 22 的运行。作为选择，只要处理器 22 在接受
25 新运行代码或使用新运行代码之前鉴权了该新代码，处理器 22 就允许下载它。

多数生物统计读出器不会为了比较目的而发送原始生物统计数据，而是把它转换成集中在最有关的参数上的数据。例如，指纹的数字化图像可能需要好几千字节的数据。但是指纹技术集中在指纹特殊特征的位置、方向以及本质上，它可以缩减到几百个字节。这几百字节定义了指纹‘图’，并且它便是将被存储起来的图，以及在以后为了比较目的而作为参考。在用户请求访问系统时，他的最近输入指纹也被变换成

图，然后把它与当前存储在隐藏的快速存储器 47 中的图比较，以确定该用户是否被授权。

在常规系统中，用户的指纹图会在生物统计读出器 23 中产生。但是有关隐私问题的公共政策把该数据当作极为敏感的信息处理，并且应该只能在安全环境中产生该图。取决于该系统的结构，生物统计读出器 23 和读出器接口 24 之间的链路要受到监控，并且指纹图不应该在该链路上出现。由于该原因，所以本发明的一种实施方案在电路 21 中产生生物统计图，按需要可以使用处理器 22 以及总线 29 上的存储器。因而产生的图决不会暴露给安全电路 21 的任何外部接口，并且不能被任何外部设备读取。

其它类型的生物统计数据被类似处理。声音数据也能被转换成相关的频率、振幅和时间成分，然后它可以通过一个算法来被处理以产生说话者声音的声音图。视网膜扫描能够产生用户眼睛的图像，然后它可以被处理以产生描述用户视网膜的特征的视网膜图。虽然每种技术都有它自己的识别特征，但是本发明系统可以通过下列步骤来处理每种技术：1) 通过读取有关生物统计数据来注册一个用户，把该数据转换成图，并且把该图存储在非易失性存储器中，2) 通过读取请求者的有关生物统计数据来识别一个授权用户，把它转换成图，并且把该图与先前存储的图进行比较，3) 如果发现匹配，则发送一个消息给主机系统来指明该请求者是一个授权用户，并且在一些实施方案中识别该用户访问系统的范围，4) 如果没有发现匹配，则发送一个消息给主机系统来指明该请求者不是一个授权用户。

图 4 显示了一种特殊的系统级实施方案，其中前述安全系统被放在具有指纹读出器 23 的蜂窝电话 4 中，该指纹读出器 23 被集成到蜂窝电话 4 中来识别用户。该读出器被便利地放置在蜂窝电话上以读取持有该电话的人的指纹。该用户最初通过预先被授权的系统管理员在该电话中注册，该预先被授权的系统管理员引导该系统以把新用户的拇指指纹数据输入它的授权用户的数据库中。第一个把其指纹输入到该电话中的人被自动指定为系统管理员。作为选择，可以提供分离的工具来生成指纹图，然后通过指定通道把它下载到系统中。

不管数据库如何被装载，请求访问的用户能够把他们的拇指指纹放置在指纹读出器 23 上，读出器 23 将对该图像数字化并通过用户接口 24

把它发送给处理器 22。然后处理器 22 能够产生该图像的指纹图，并且把它与存储在非易失性存储器 27 中的一个图或多个图比较。存储的每个图也能含有该用户被授权使用的资源的有关列表。如果比较成功了（即如果该图与存储在存储器中的一个图匹配），那么处理器 22 会发送一个信号给主机处理器 20 来指示该请求者是一个授权用户，以及指示允许该用户使用哪种资源。接着主机处理器 20 使能该请求的服务，像从蜂窝电话小键盘 45 接受电话号码，并使用通信电路 46 来发送该号码给蜂窝电话网络。

在为声纹识别而设计的系统中，蜂窝电话中现有的麦克风能够用作生物统计读出器。为了避免使用已记录的声音从而不适当当地获得对系统的访问问题，某种格式的随机字提示是必要的。

本发明可以在硬件中和/或作为一种方法来实施。本发明也能作为存储在机器可读的媒体中的指令来实施，至少有一个处理器能够读取并执行该指令，以执行其中描述的功能。机器可读的媒体包括用于以机器（例如计算机）能读取的格式存储或发送信息的任何机制。例如机器可读的媒体能包括只读存储器（ROM）；随机存取存储器（RAM）；磁盘存储媒体；光存储媒体；快速存储设备；电信号、光信号、声音信号或其它格式的传播信号（例如载波、红外信号、数字信号等）以及其他类型。

前面的描述规定为说明性的而非限制性的。对于本领域的技术人员将出现变化。这些变化规定为包括在本发明中，它仅受到附加权利要求的精神和范围限制。

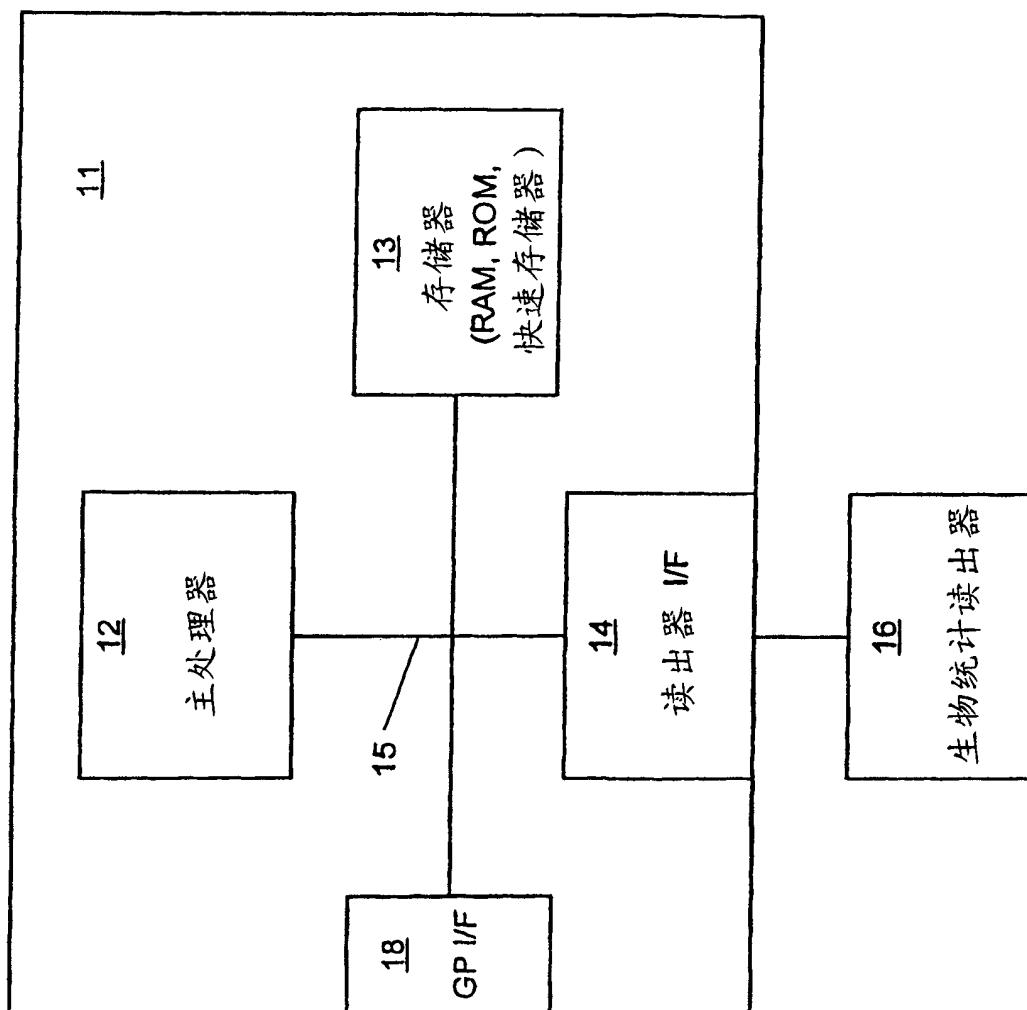
↗
1

图 1
现有技术

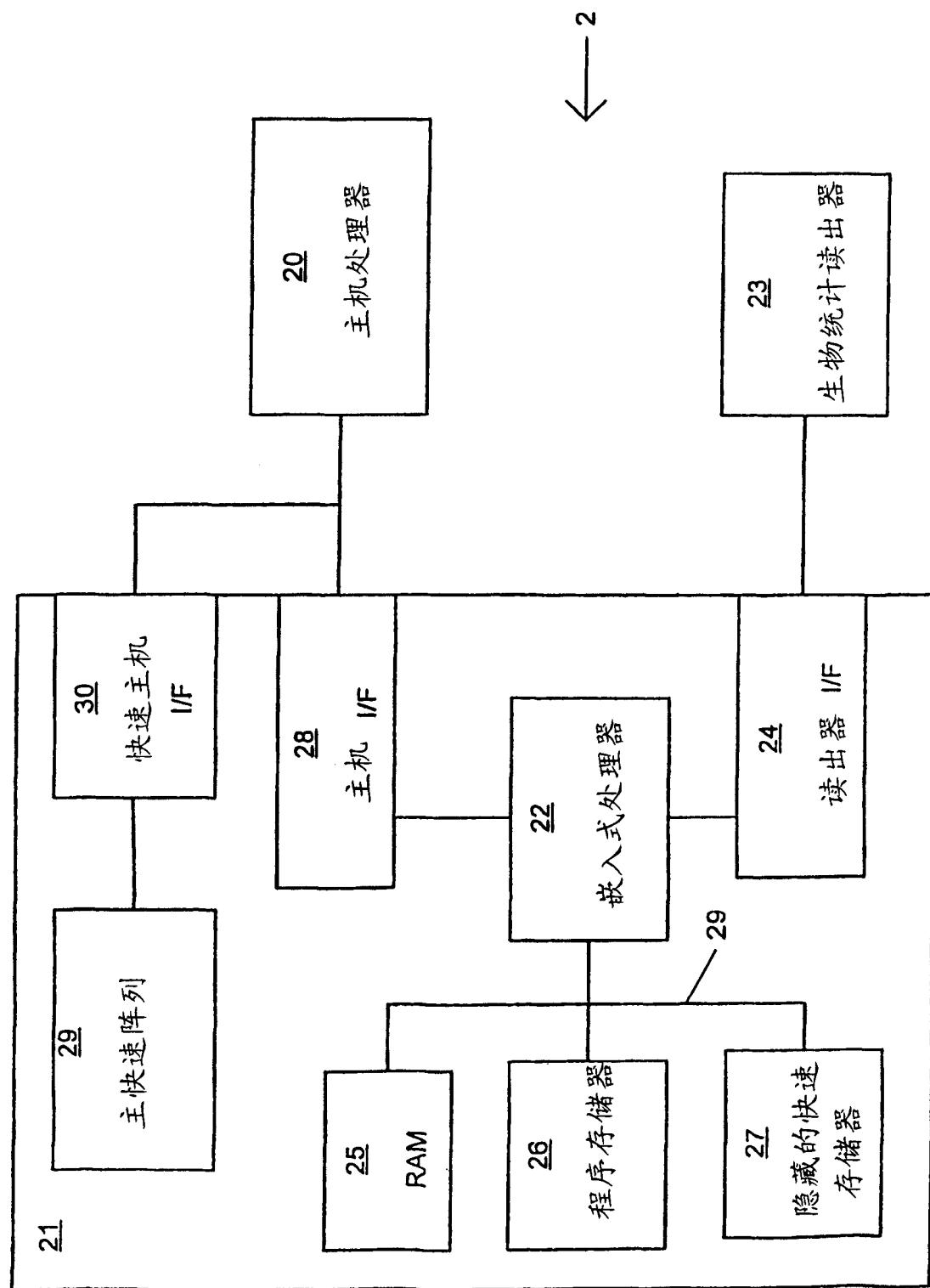


图 2

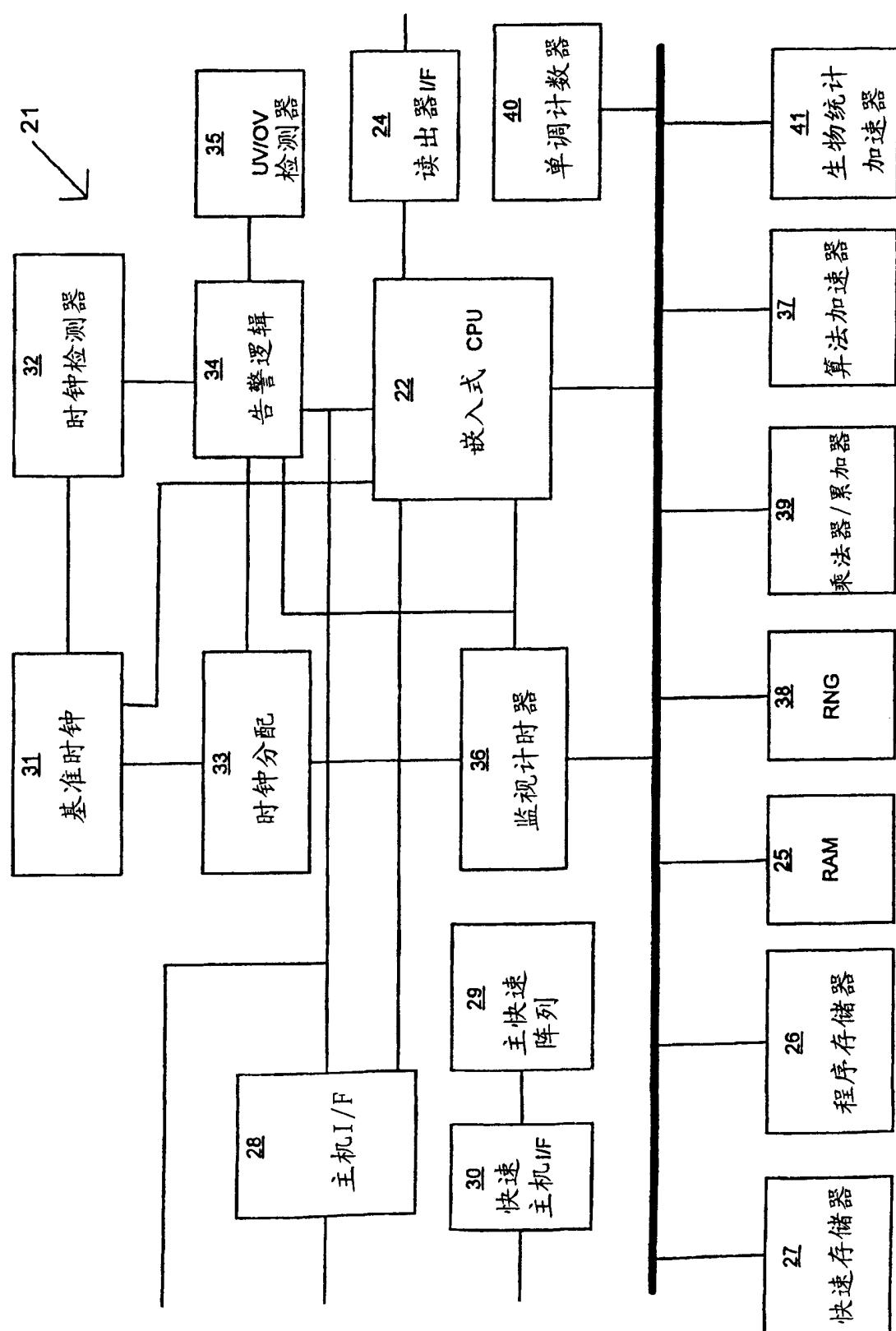


图 3

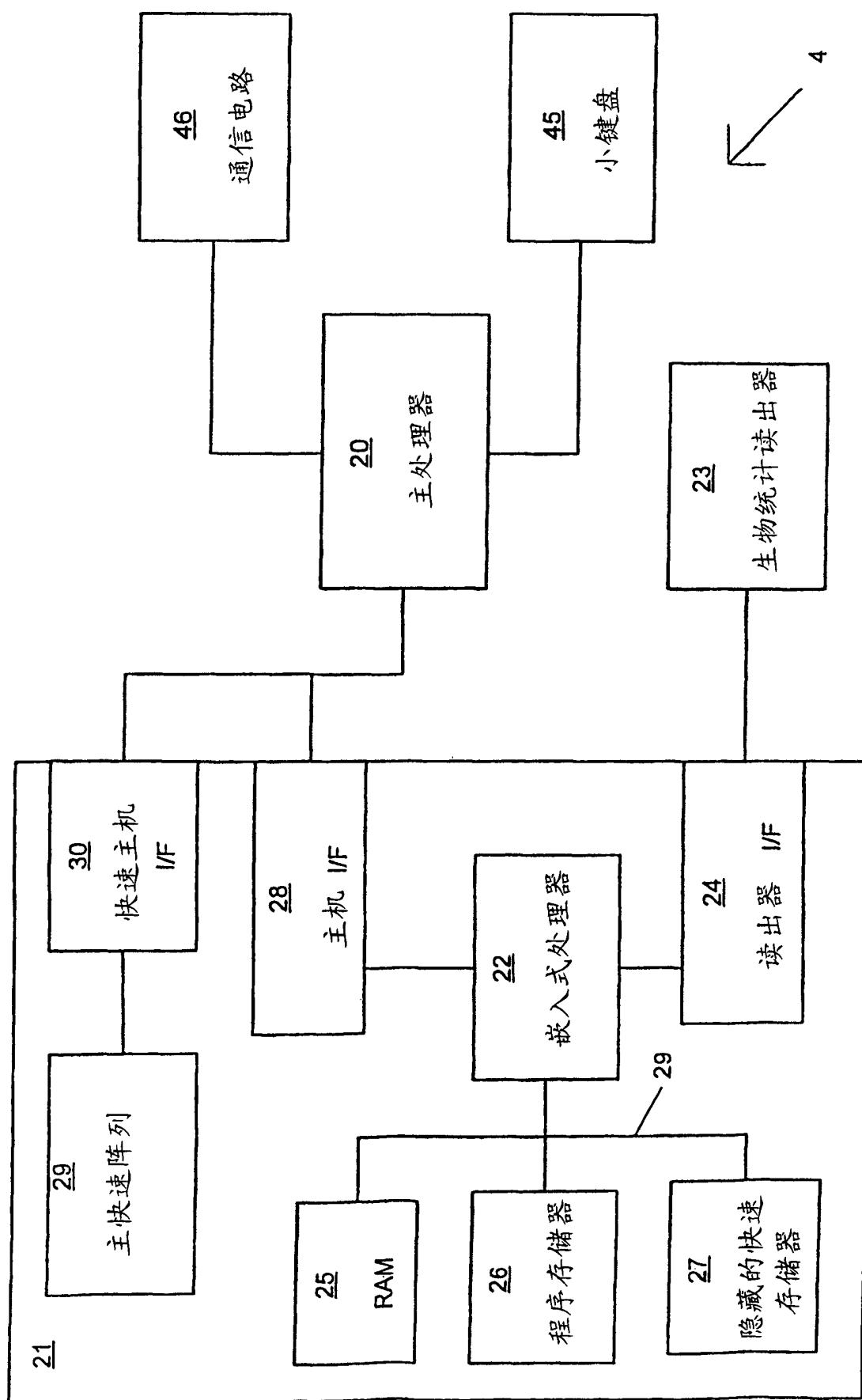


图 4