[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 21/00 (2006.01)
G06F 12/14 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200810082399.7

[43] 公开日 2008 年 9 月 10 日

[11] 公开号 CN 101261663A

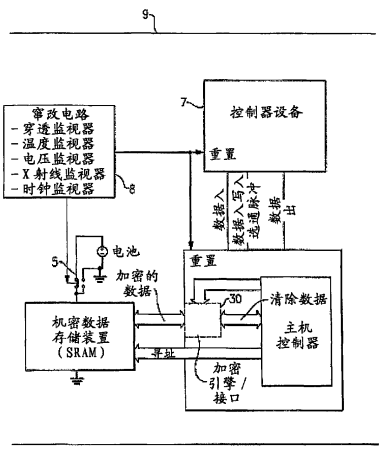
[22] 申请日 2008.3.4
[21] 申请号 200810082399.7
[30] 优先权
[32] 2007. 3. 6 [33] US [31] 11/682,349
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 C·U·布斯卡利亚 V·孔德雷利
K·C·格茨 N·哈季奇
D·W·普拉斯 T·维谢格拉迪
[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥
权利要求书 3 页 说明书 6 页 附图 3 页

[54] 发明名称

保护安全电子模块免受攻击的方法和系统

[57] 摘要

本发明涉及一种保护安全电子模块免受攻击的方法和系统。 披露了用于防止由安全电子模块中的首选状态/烧入导致的机密数据的非有意保留的方法和装置。 在交替的时钟周期顺序地存储所述数据及其反转，并通过主动地覆写数据以破坏数据来防止 SRAM 设备形成首选状态。 通过使用主加密密钥来加密相对大量的机密数据，并将所述主密钥存储在此非首选状态存储装置中，所述电子模块可方便地将此保护方案扩展到大量数据，而没有反转或主动擦除较大存储区域的开销。



1. 一种保护存储在电子存储装置中的机密信息的主密钥设备，所述设备包括:

具有寄存器的密钥存储装置，所述寄存器具有加密密钥以访问所述电子存储装置，所述密钥具有重置输入;

反相器，所述反相器连续地反转存储寄存器中的所述加密密钥；以及

窜改响应设备，所述窜改响应设备在启动和窜改事件时向所述密钥存储装置的所述重置输入提供输出信号以破坏所述加密密钥。

2. 如权利要求 1 中所述的主密钥设备，其中所述电子存储装置是易失性存储器。

3. 如权利要求 2 中所述的主密钥设备，其中所述易失性存储器是 SRAM。

4. 如权利要求 3 中所述的主密钥设备，还包括支持所述电子存储装置并在接收到窜改事件输出信号时关闭以便擦除所述机密信息的电源。

5. 如权利要求 1 中所述的主密钥设备，其中所述反相器在 50%或更多的工作循环时运行以防止印刻所述加密密钥中的首选状态。

6. 如权利要求 1 中所述的主密钥设备，还包括由所述加密密钥控制以对所述机密信息进行加密和解密的加密接口。

7. 如权利要求 6 中所述的主密钥设备，其中所述加密接口包括取回电路，所述取回电路读取所述密钥存储装置并将其写入密钥寄存器，以便可以将所述机密信息加密和解密到存储器控制器以及将所述机密信息读入和读出所述电子存储装置。

8. 如权利要求 1 中所述的主密钥设备，其中主机控制器读取所述加密密钥并对在所述主机控制器与所述电子存储装置之间交换的所述机密信息进行加密和解密。

9. 一种用于保护存储在电子电路中的机密数据的抗窜改系统，所述系统包括:

机密数据存储存储器;

一装置,用于对进出安全存储存储器的数据进行控制以及加密和解密;

抗窜改包,其感知对所述系统的入侵或中断并在感知到窜改事件之后生成输出信号;以及

具有加密密钥的主密钥存储装置,当生成来自所述抗窜改包的所述输出信号时将破坏所述加密密钥,由此防止访问所述机密数据。

10. 如权利要求 9 中所述的抗窜改系统,其中所述机密数据存储存储器是易失性存储器。

11. 如权利要求 10 中所述的抗窜改系统,其中所述易失性存储器是 SRAM。

12. 如权利要求 11 中所述的抗窜改系统,还包括独立的电源系统以支持所述 SRAM。

13. 如权利要求 12 中所述的抗窜改系统,其中在从窜改事件接收到所述输出信号时将关闭所述电源系统以破坏所述电子电路中存储的所有信息。

14. 一种用于保护存储在电子存储装置中的机密信息的方法,所述方法包括:

提供在窜改事件时生成输出信号或在启动时重置密钥存储装置的窜改设备;

将加密密钥加载到所述密钥存储装置中以访问所述电子存储装置;

连续反转所述密钥存储装置中的所述加密密钥;

使用所述加密密钥对电子存储存储器中的所述机密信息进行加密和解密;以及

在所述密钥存储装置接收到窜改事件信号时破坏所述加密密钥。

15. 如权利要求 14 中所述的方法,其中所述电子存储装置是易失性存储器。

16. 如权利要求 15 中所述的方法,其中所述易失性存储器是 SRAM。

17. 如权利要求 16 中所述的方法,还包括为所述电子存储装置提供电

源，在接收到窜改事件输出信号时将关闭所述电源以便擦除所述机密信息。

18. 如权利要求 14 中所述的方法，其中所述反转在 50%或更多的工作循环时运行以防止印刻所述加密密钥中的首选状态。

19. 如权利要求 18 中所述的方法，还包括读取所述密钥存储装置并将其写入密钥寄存器，以便可以将所述机密信息加密和解密到存储器控制器以及将所述机密信息读入和读出所述电子存储装置。

20. 如权利要求 14 中所述的方法，还包括主机控制器读取所述加密密钥并对在所述主机控制器与所述电子存储装置之间交换的所述机密信息进行加密和解密。

保护安全电子模块免受攻击的方法和系统

技术领域

本发明涉及物理上安全的加密硬件模块，具体地说，涉及用于保护所述模块中存储的敏感数据的窜改响应方法。

背景技术

通常，提供敏感数据（例如加密密钥）的物理安全性的系统需要包含存储和处理敏感数据的电路的外壳。专利 US4860351-“Tamper Resistence Packaging Protection of Information Store in Electronic Circuitry”描述了如何实现此类安全外壳并且其在此引入作为参考。对穿透物理外壳的窜改响应必须在一定时间内删除敏感数据，以使得外壳破坏或存储器设备中的数据检索或数据保留不可能进行。通常将 SRAM 存储器技术用于在安全模块中存储敏感数据的存储器应用。只要向设备（易失性存储器）施加电源并且没有使用写入启用信号来特意覆写数据，SRAM 数据就依然存储在存储器设备中。这种易失性存储器设备用于在安全外壳中存储敏感数据，因为当发生窜改事件时，可以通过切断设备的电源以相对快速的操作破坏整个存储器中的敏感数据。当系统电源没有为安全模块供电时，还将使用电池电源作为 SRAM 存储器的备用电源，因为要求在安全模块中保留某些安全数据。

当存储器设备或安全模块处于较低温度时，存储器单元在切断电源或电源接地时的放电（数据破坏）将花费较长时间。如果重新为设备供电时存储器单元中仍剩余一些电荷，则存储器单元将达到切断电源之前的状态。在这种情况下，将保留先前存储在存储器中的数据。在较低温度（但仍处于环境范围内的温度）下已观察到数据保留时间显著增加。

低温攻击尝试利用增加的数据保留时间来破坏外壳，并且在外壳破坏引起的窜改响应（切断存储器设备的电源）破坏存储器数据之前重新为存储器设备供电。

相反，长期对存储器设备施加高于设备最大指定工作电压的电压和/或长期将设备置于较高温度下会导致将首选状态（preferential state）‘烧入’存储器存储元件设备。在这种情况下，当在任何初始写入操作之前首次供电时，存储长期未被覆写的数据（例如加密密钥）的存储器设备可能会显示此长期数据。因此，窜改响应将变得无效，因为切断存储器设备的电源可能不会影响存储器设备内将在加电时显示的首选状态。

按照上面所述，在设计外壳和封闭式硬件的安全性时，必须考虑可以增加存储器中的数据保留时间的低温攻击以及可能会“烧入”存储器中的首选状态的高温/高压攻击。为了解决这些暴露的问题，可以使用温度和电压的最小/最大窜改限制，以便在外壳和存储器设备达到温度极限时调用窜改响应。但是，很难根据技术保留/烧入敏感性来确定温度和电压限制阈值。例如，不同存储器供应商提供的不同存储器技术可能会对较低温度具有较长或较短保留时间敏感性，并且随着技术的发展，对较低温度的保留时间敏感性可能会改变。此类电压和温度设置限制还将产生处理（静电放电）、运输以及产品存储限制。例如，在运输期间，飞机中的货物可以达到华氏温度 0 度以下而仓库温度可以达到华氏 100 度以上。因此，如果为了防止数据保留时间攻击，温度窜改限制需要高于或低于运输期间设备所处的温度，所以必须针对安全产品的运输做出特殊热量供应。此外，在具有电压窜改限制时，必须谨慎地将安全模块的所有部分绝缘以免意外地短路模块的配电系统，以便不会因在备用电池供电下处理安全模块而发生意外的电压窜改。

与切断电源相比，使用存储器的写入功能或写入使能主动地擦除存储器将提供更可靠的数据破坏并且对数据保留问题不敏感。但是，在具有存储安全数据所需的典型大小的大型存储器中，写入每一个存储单元以确保破坏（主动擦除）所有敏感数据无法在窜改响应的时间约束内完成。

在50%的工作循环时连续反转存储器存储位单元（将2状态元件从1状态更改为另一状态）以免印刻（imprinting）首选状态将防止SRAM设备的存储器单元的“数据印刻”或“烧入”，但是，在大型存储器中，由于其大小以及持续切换因素所消耗的功率，同样很难实现持续数据反转并且其非常耗时。

总而言之，对破坏敏感数据的典型窜改响应将触发穿透感应和温度/电压感应限制，并且响应以切断SRAM存储器的电源以破坏敏感数据。如先前所述，此数据擦除响应的质量和所需时间受温度和电压极限的影响。与仅切断存储器设备的电源（或使电源端子接地）相比，本发明提供了更好的保护以免在使用温度和电压极限（攻击）保持数据保留（时间）时破坏安全外壳。

发明内容

通过使用主密钥对安全存储易失性存储器中的敏感数据进行加密，克服了现有技术的缺点并提供了其他优点。此主密钥将变成可在窜改事件时被更安全地破坏的数据。由于已将敏感数据量减少到主密钥，因此可以使用主动擦除更快速地完成窜改响应窗口中的数据删除，并且可以轻松地实现主密钥数据的持续反转以减少暴露于存储存储器中的数据印刻。作为一种额外的措施，还可以在窜改事件时切断包含加密的安全数据的存储器的电源（使电源端子接地或颠倒电源端子的极性）。在此还描述和要求保护了对应于上述方法的系统和计算机程序产品。

通过本发明的技术实现了其他特性和优点。本发明的其他实施例和方面将在此详细描述并被视为所要求保护的发明的一部分。为了更好地理解本发明的优点和特性，可参考说明和附图。作为概述的发明的结果，在技术上已实现了一种解决方案，此解决方案为需要保护的数据提供了更好的安全性、在窜改事件时更快速和可靠地删除要保护的数据，以及对可能损害要保护的数据的删除的温度和电压影响（攻击）具有更好的免疫性。

附图说明

在说明书结尾处的权利要求中具体指出并明确要求保护了被视为本发明的主题。从以下结合附图的详细说明，本发明的上述和其他目标、特性和优点将是显而易见的，这些附图是:

图 1 是集成在物理安全数据系统内部的本发明的方块图;

图 2 示出了本发明的数据流; 以及

图 3 示出了具有非静态存储区（storage）的关键主密钥寄存器的实施例。

详细说明通过实例的方式参考附图解释了本发明的优选实施例及其优点和特性。

具体实施方式

现在转到更详细的附图，图 1 涉及根据本发明的存储器系统或安全模块 9，其在电子安全环境中运行，所述环境具有多个传感器，旨在检测各种形式的窜改以及温度、x 射线、电压波动以及功率波动。因此，模块 9 位于此安全窜改响应系统中。此模块 9 提供机密数据的加密、在窜改事件时主动擦除用于加密机密数据的密钥（多个），以及定期反转用于加密机密数据的密钥（多个）。系统 9 包括具有主密钥存储寄存器 71 的控制器设备 7, 寄存器 71 连接到定期反转或切换主密钥存储寄存器 71 的反相器 72。图 3 中示出了所述控制器设备的更详细说明。系统 9 可以使用软件或硬件加密引擎或接口 30 来执行和控制安全存储存储器 4 中的数据的加密和解密。窜改子系统 8 用于控制到控制器设备 7 和机密存储存储器 4 的电源 5（其可以包括电池）。窜改子系统 8 连接到控制器设备 7 以控制到主密钥存储区 71 和用于内部初始化的主机控制器 2 的重置输入以便生成和存储主密钥。窜改子系统 8 包括数个从温度传感器、电压传感器、物理穿透传感器以及其他未示出的环境和电子传感器接收信号的监视器。窜改子系统 8 还包括管理逻辑，所述管理逻辑根据来自窜改子系统监视器电路（多个）的信息来重置主密钥存储区 71、切断机密存储存储器 4 和包含主密钥 71

的控制器设备 7 的电源、使电源接地或颠倒电源极性。

在操作中，主密钥存储区 71 在系统初始化时生成并被加载到可以是低功率 CPLD 或微控制器的特殊安全存储区域。将存储主密钥中的数据寄存器位置的特征，以便可以使用一个简单的输入信号对其进行全局地重置。此主密钥用于在从安全存储器存储或检索敏感数据时对数据（例如加密密钥）进行加密/解密。安全存储存储器 4 可以采用诸如 SRAM 之类的易失性存储器实现。当加载敏感数据时采用硬件加密引擎 30 或通过软件快速进行加密，或在检索和需要敏感数据时采用硬件加密引擎 30 或通过软件进行解密。加密接口的典型软件实施方式包括主机控制器 2 从主密钥存储区 71 读取正确的加密密钥以及加密/解密到达/来自机密数据存储器 4 的数据流量。同一接口的硬件实施方式依赖于与用于连接机密数据存储器 4 的存储器控制器集成的硬件加密引擎或接口 30。

图 2 中示出了其中由加密引擎接口 30 过滤主机控制器 2 发出的写入事务的实施例。当控制和密钥取回单元 32 从主密钥存储区 71 读取并且将相应密钥写入密码引擎密钥寄存器 33 时，要写入的数据锁存在加密硬件路径 34 的输入处。一旦将正确的密钥加载到密钥寄存器 33，数据就被加密并通过 SRAM 接口控制器 31 移动到机密数据存储器 4。通过类似方式，主机控制器 2 读取请求被控制和密钥取回单元 32 拦截，单元 32 从主密钥存储区 71 使用相应密钥加载密钥寄存器 33，同时从机密数据存储器 4 执行数据读取。从机密数据存储器 4 读取的数据通过 SRAM 接口控制器 31 传递，并随后在到解密硬件路径 35 的输入中提供所述数据。然后将已解密的数据返回主机控制器 2。

当发生窜改事件时，响应将立即重置主密钥数据寄存器，从而主动地破坏主密钥，然后将主密钥存储区域切断电源（使存储主密钥的设备的电源端子接地）以及切断到已加密敏感/安全数据存储器（SRAM）设备的电源。由于保留在易失性 SRAM 存储器中的敏感数据被加密，因此即使 SRAM 中的数据由于低温时的数据保留时间增加或“烧入状态”而被恢复，也会防止数据免受未经授权的访问。只有主密钥需要在窜改响应时被可靠

地破坏。通过能够主动擦除主密钥以及在50%的工作循环时持续反转主密钥，缩短了切断电源时而可能保留的对温度或电压敏感的数据的暴露时间。主动重置主密钥防止了可在切断电源时较长时间保留数据并提供延长攻击时间窗口机会的低温攻击。此外，在50%的工作循环时连续反转主密钥数据位（将2状态元件从1状态更改为另一状态）以避免印刻主密钥存储元件中的首选状态。

图3示出了与数据翻转逻辑集成的主密钥存储寄存器的实施方式。如果写入选通脉冲中的数据是活动的，则在写入时钟的上升沿从‘数据入’输入加载密钥寄存器71。还使用同一条件将控制标志77设置为零，指示密钥寄存器71的内容正在被写入并包含有效数据。密钥寄存器71以及控制标志77中的值将（分别）通过反相器72和73反转，并且当‘数据入’写入选通脉冲为非活动时，在每个写入时钟将所述值写回密钥寄存器33和控制标志77。‘数据出’由多路复用器76驱动，当控制标志77等于0或者反相器72生成密钥存储区71中存储的数据的反转时，多路复用器76将输出密钥寄存器71中存储的数据。

此操作将提供保护以免受可在加电时将存储元件设置为首选状态并显示主密钥的高温或高压攻击。切断机密数据存储区域的电源将提供额外的一层保护，当确定要使用的加密模式的强度时可以考虑此保护。

可以采用软件、固件、硬件或它们的某种组合来实现本发明的功能。

在此示出的流程图仅为示例。这些附图或其中所述的步骤（或操作）可以具有许多变化而不偏离本发明的精神。例如，可以按照不同的顺序执行步骤，或者可以添加、删除或修改步骤。所有这些变化均被视为所要求保护的发明的一部分。

虽然已经说明了本发明的优选实施例，但是要理解的是，本领域的技术人员现在和将来可以做出各种落入以下权利要求的范围的改进和增强。这些权利要求应被理解为维持最初说明的本发明的正确保护。

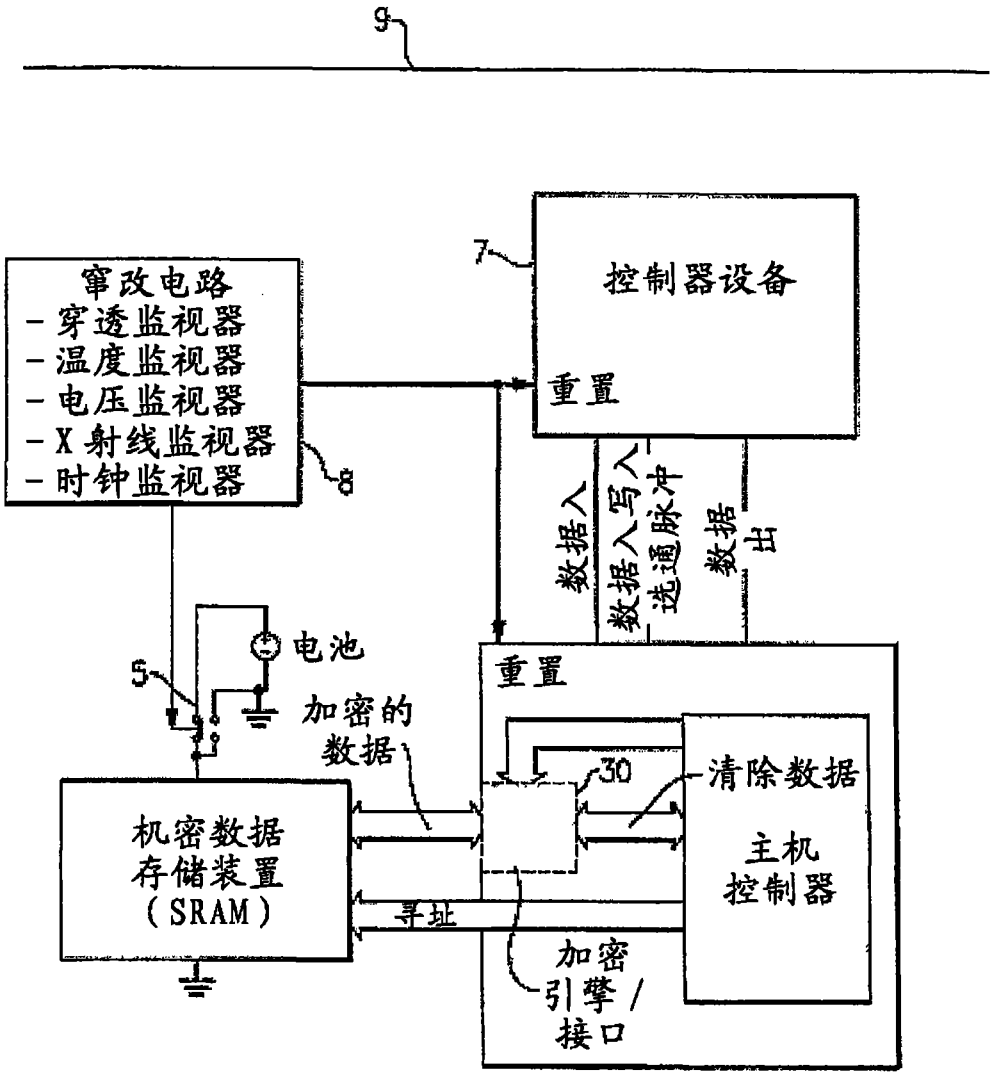

9
7
控制器设备
重置
窜改电路
- 穿透监视器
- 温度监视器
- 电压监视器
- X 射线监视器
- 时钟监视器
8
数据入
数据入写入选通脉冲
数据出
电池
5
加密的数据
重置
30
清除数据
主机控制器
机密数据存储装置（SRAM）
寻址
加密引擎/接口

图 1

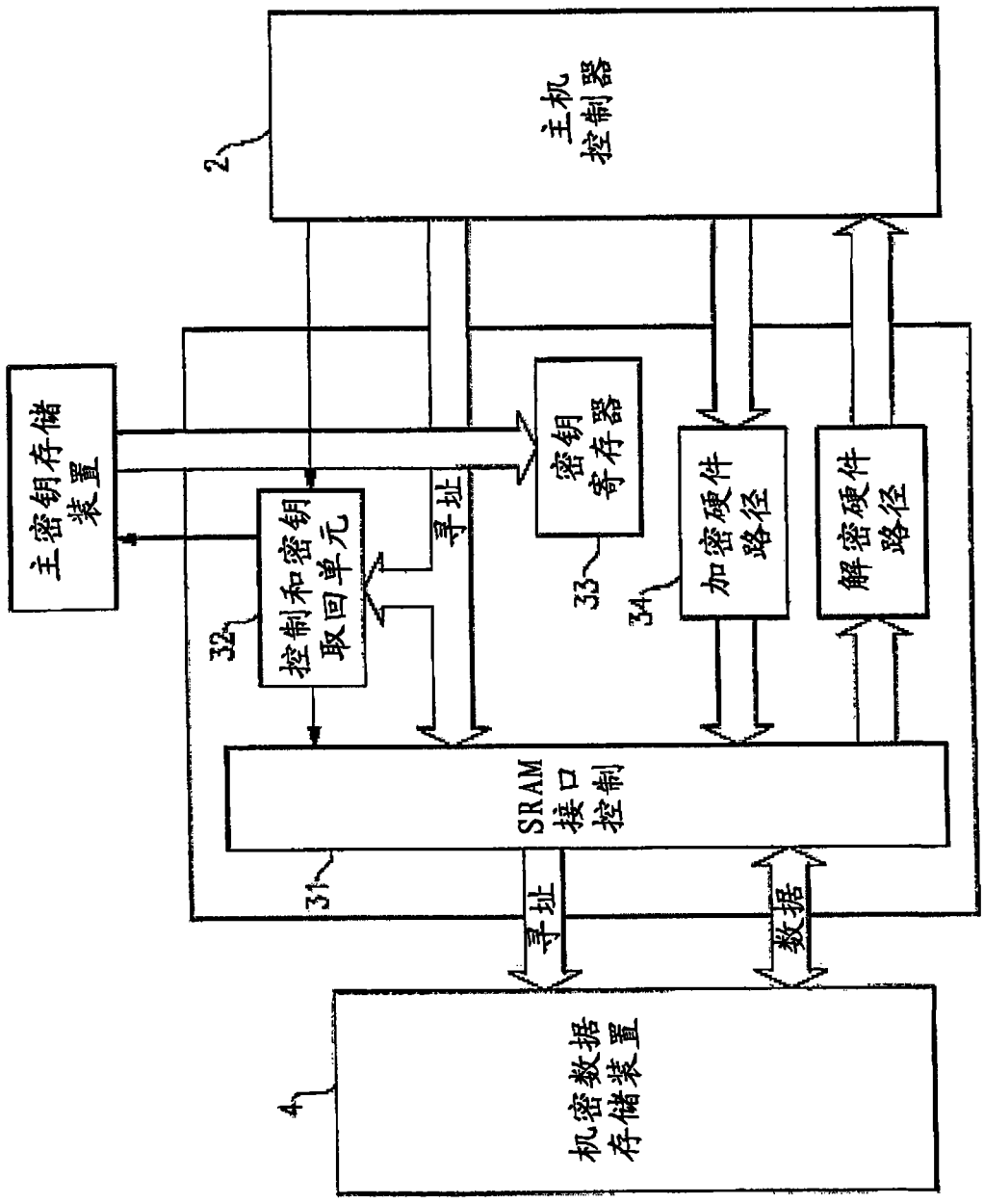

主机控制器
2
主密钥存储装置
密钥寄存器
33
加密硬件路径
34
解密硬件路径
控制和密钥取回单元
32
寻址
SRAM接口控制
31
寻址
数据
机密数据存储装置
4

图 2

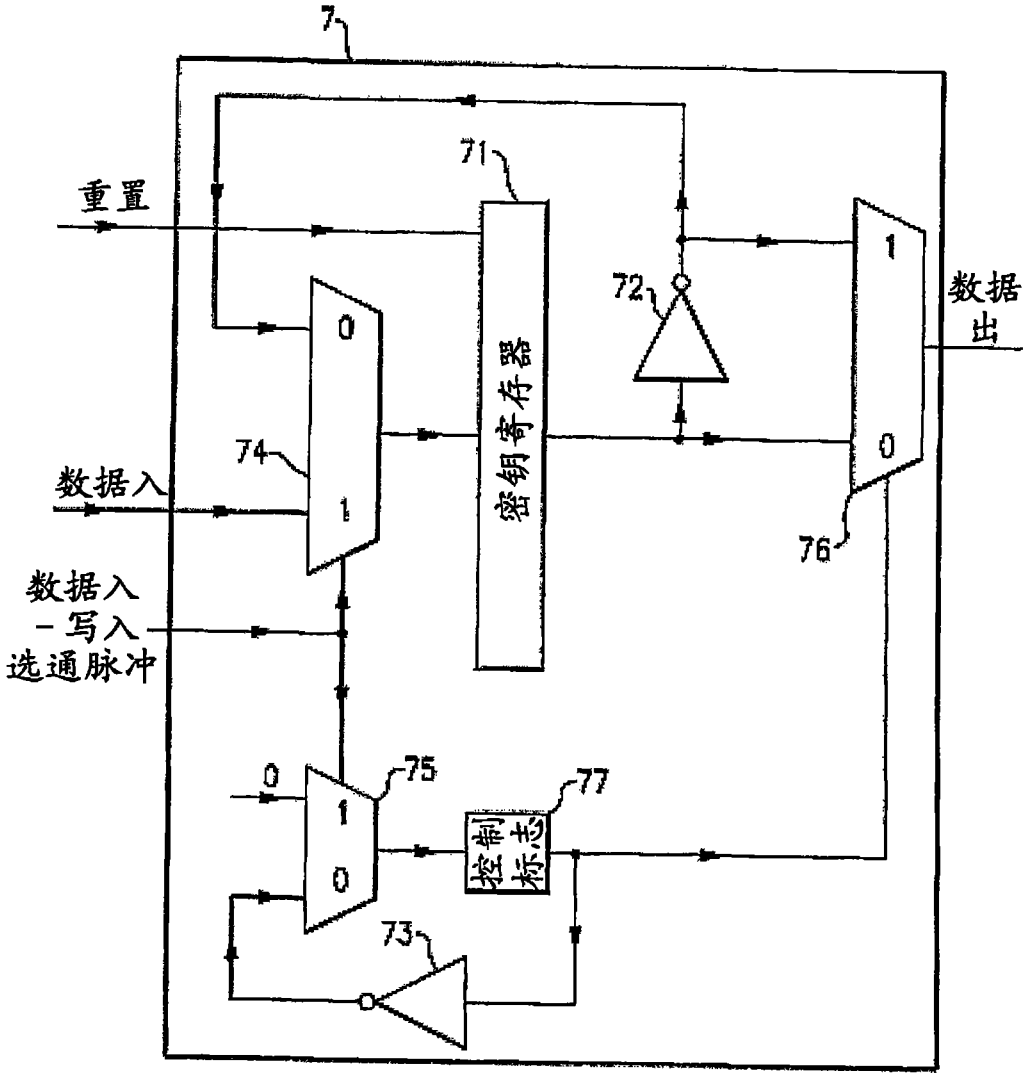


图 3