(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 106295362 A
(43)申请公布日 2017.01.04

(21)申请号 201610614718.9

(22)申请日 2016.07.29

(71)申请人 福州瑞芯微电子股份有限公司
地址 350000 福建省福州市鼓楼区软件大道89号18号楼

(72)发明人 廖裕民

(74)专利代理机构 福州市鼓楼区京华专利事务所(普通合伙) 35212
代理人 王美花

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/79(2013.01)

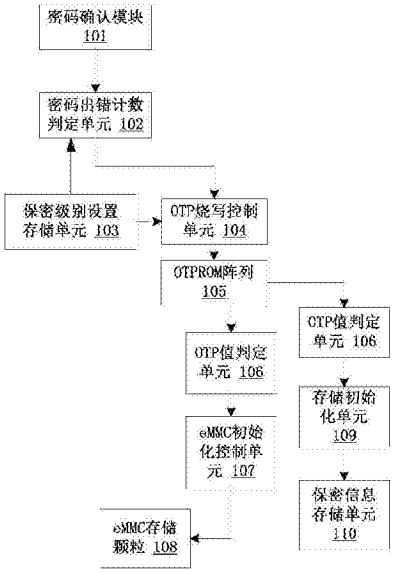
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种芯片自毁装置及方法

(57)摘要

本发明提供一种芯片自毁装置，包括密码确认模块、密码出错计数判定单元、保密级别设置存储单元、OTP烧写控制单元、OTPROM阵列、两个OTP值判断单元、EMMC初始化控制单元、EMMC存储颗粒、存储初始化单元以及保密信息存储单元；密码确认模块、密码出错计数判定单元、OTP烧写控制单元以及OTPROM阵列依次连接；保密级别设置存储单元分别连接所述密码出错计数判定单元和OTP烧写控制单元；OTPROM阵列通过其中一个所述OTP值判断单元依次连接EMMC初始化控制单元和EMMC存储颗粒，并通过另一个OTP值判断单元依次连接存储初始化单元和保密信息存储单元本发明在确认受到暴力破解的情况下可以让芯片自毁，或者只是完全消除保密数据而不损坏芯片。



CN 106295362 A

1.一种芯片自毁装置，其特征在于：包括密码确认模块、密码出错计数判定单元、保密级别设置存储单元、OTP烧写控制单元、OTPROM阵列、两个OTP值判断单元、EMMC初始化控制单元、EMMC存储颗粒、存储初始化单元以及保密信息存储单元；

所述密码确认模块、密码出错计数判定单元、OTP烧写控制单元以及OTPROM阵列依次连接；

所述保密级别设置存储单元分别连接所述密码出错计数判定单元和OTP烧写控制单元；

所述OTPROM阵列通过其中一个所述OTP值判断单元依次连接EMMC初始化控制单元和EMMC存储颗粒，并通过另一个所述OTP值判断单元依次连接存储初始化单元和保密信息存储单元。

2.根据权利要求1所述的一种芯片自毁装置，其特征在于：所述密码确认模块、密码出错计数判定单元、保密级别设置存储单元、OTP烧写控制单元、OTPROM阵列、两个OTP值判断单元、EMMC初始化控制单元、存储初始化单元以及保密信息存储单元均集成在芯片内，所述EMMC存储颗粒则设在芯片外部。

3.一种芯片自毁方法，其特征在于：提供如权利要求1所述的芯片自毁装置，并包括下述步骤：

(1)当本地使用者的密码输错次数大于预设的密码出错容忍门限值时，所述密码出错计数判定单元发出自毁命令送到OTP烧写控制单元；

(2)所述OTP烧写控制单元收到自毁命令后，会从保密级别设置存储单元中读取保密级别，并根据保密级别向OTPROM阵列写入特定值表示执行销毁操作；

(3)所述OTP值判定单元根据OTPROM阵列进行数值判断，并执行对应的销毁操作；

所述销毁操作包括：

通过所述EMMC初始化控制单元将芯片外部的Flash存储颗粒进行清零初始化；

通过所述存储初始化单元将芯片内的保密信息存储单元的存储内容清零初始化。

4.根据权利要求3所述的一种芯片自毁方法，其特征在于：

第一次使用设备时对存储保密级别和所述预设的密码出错容忍门限值进行设置并存储在一保密级别设置存储单元中，该保密级别设置存储单元分别连接所述密码出错计数判定单元和OTP烧写控制单元；供所述OTP烧写控制单元根据存储保密级别向OTPROM阵列写入特定值。

5.根据权利要求3所述的一种芯片自毁方法，其特征在于：

所述步骤(1)的具体过程是：

当本地密码确认模块收到本机使用者的密码输入确认请求后，会判断密码是否正确，如果正确则开启设备让本机使用者正常使用本设备；如果密码判断不正确，则要求使用者再次输入密码，同时将密码判定出错的结果送往密码出错计数判定单元进行记录；如果使用者多次输入密码出错，密码出错计数器的计数值已经达到保密级别设置存储单元中存储的密码出错容忍门限，则由密码出错计数判定单元发出自毁命令送到所述OTP烧写控制单元。

一种芯片自毁装置及方法

技术领域

[0001] 本发明涉及一种芯片自毁装置及方法。

背景技术

[0002] 随着移动电子设备的日益发展,手机和平板电脑等移动电子设备已经被广泛应用于电子支付和个人重要短信和邮件收发的功能,大量的用户个人隐私信息和保密信息都保存在移动电子设备上,因此移动电子设备的安全性能日益受到重视。在电子设备丢失或者被盗的情况下,如何保护电子设备中的保密数据是一个非常重要的课题。

[0003] 当前技术缺点:

[0004] 1.黑客可以通过暴力破解方式破解电子设备的保密数据,目前芯片保护技术不能在确认被暴力破解的情况下主动销毁数据,通常只能在软件层面锁定机器,在硬件和芯片层面,保密数据还是存在里面,黑客暴力破解时可以通过摘取电路板上的eMMC芯片或者其他flash存储芯片,虽然存在其中的保密数据通常有加密保护,但是黑客还是可以通过各种手段来破解并获取保密数据;

[0005] 2.黑客还可以通过剖片分析存储阵列的方式获取保密数据。

发明内容

[0006] 本发明要解决的技术问题,在于提供一种芯片自毁装置及方法,在确认受到暴力破解的情况下可以让芯片自毁,让黑客不能达到获取保密数据的目的。

[0007] 本发明的芯片自毁装置是这样实现的:一种芯片自毁装置,包括密码确认模块、密码出错计数判定单元、保密级别设置存储单元、OTP烧写控制单元、OTPROM阵列、两个OTP值判断单元、EMMC初始化控制单元、EMMC存储颗粒、存储初始化单元以及保密信息存储单元;

[0008] 所述密码确认模块、密码出错计数判定单元、OTP烧写控制单元以及OTPROM阵列依次连接;

[0009] 所述保密级别设置存储单元分别连接所述密码出错计数判定单元和OTP烧写控制单元;

[0010] 所述OTPROM阵列通过其中一个所述OTP值判断单元依次连接EMMC初始化控制单元和EMMC存储颗粒,并通过另一个所述OTP值判断单元依次连接存储初始化单元和保密信息存储单元。

[0011] 进一步的,所述密码确认模块、密码出错计数判定单元、保密级别设置存储单元、OTP烧写控制单元、OTPROM阵列、两个OTP值判断单元、EMMC初始化控制单元、存储初始化单元以及保密信息存储单元均集成在芯片内,所述EMMC存储颗粒则设在芯片外部。

[0012] 本发明的芯片自毁方法是这样实现的:一种芯片自毁方法,提供本发明所述的芯片自毁装置,并包括下述步骤:

[0013] (1)当本地使用者的密码输错次数大于预设的密码出错容忍门限值时,所述密码出错计数判定单元发出自毁命令送到OTP烧写控制单元;

[0014] (2)所述OTP烧写控制单元收到自毁命令后,会从保密级别设置存储单元中读取保密级别,并根据保密级别向OTPROM阵列写入特定值表示执行销毁操作;

[0015] (3)所述OTP值判定单元根据OTPROM阵列进行数值判断,并执行对应的销毁操作;

[0016] 所述销毁操作包括:

[0017] 通过所述EMMC初始化控制单元将芯片外部的Flash存储颗粒进行清零初始化;

[0018] 通过所述存储初始化单元将芯片内的保密信息存储单元的存储内容清零初始化。

[0019] 进一步的,第一次使用设备时对存储保密级别和所述预设的密码出错容忍门限值进行设置并存储在一保密级别设置存储单元中,该保密级别设置存储单元分别连接所述密码出错计数判定单元和OTP烧写控制单元;供所述OTP烧写控制单元根据存储保密级别向OTPROM阵列写入特定值。

[0020] 进一步的,所述步骤(1)的具体过程是:

[0021] 当本地密码确认模块收到本机使用者的密码输入确认请求后,会判断密码是否正确,如果正确则开启设备让本机使用者正常使用本设备;如果密码判断不正确,则要求使用者再次输入密码,同时将密码判定出错的结果送往密码出错计数判定单元进行记录;如果使用者多次输入密码出错,密码出错计数器的计数值已经达到保密级别设置存储单元中存储的密码出错容忍门限,则由密码出错计数判定单元发出自毁命令送到所述OTP烧写控制单元。

[0022] 本发明具有如下优点:

[0023] 1、在确认受到暴力破解的情况下可以让芯片自毁,让黑客不能达到获取保密数据的目的;

[0024] 2、自我保护时的自毁等级可配置,可以让芯片完全损坏,或者只是完全消除保密数据而不损坏芯片。

附图说明

[0025] 下面参照附图结合实施例对本发明作进一步的说明。

[0026] 图1为本发明方法执行流程图。

具体实施方式

[0027] 如图1所示,本发明的芯片自毁装置100包括密码确认模块101、密码出错计数判定单元102、保密级别设置存储单元103、OTP烧写控制单元104、OTPROM阵列105、两个OTP值判断单元106、EMMC初始化控制单元107、EMMC存储颗粒108、存储初始化单元109以及保密信息存储单110元;

[0028] 所述密码确认模块101、密码出错计数判定单元102、OTP烧写控制单元104以及OTPROM阵列105依次连接;

[0029] 所述保密级别设置存储单元103分别连接所述密码出错计数判定单元102和OTP烧写控制单元104;

[0030] 所述OTPROM阵列105通过其中一个所述OTP值判断单元106依次连接EMMC初始化控制单元107和EMMC存储颗粒108,并通过另一个所述OTP值判断单元106依次连接存储初始化单元109和保密信息存储单元110。

[0031] 所述密码确认模块101、密码出错计数判定单元102、保密级别设置存储单元103、OTP烧写控制单元104、OTPROM阵列105、两个OTP值判断单元106、EMMC初始化控制单元107、存储初始化单元109以及保密信息存储单元110均集成在芯片内，所述EMMC存储颗粒108则设在芯片外部。

[0032] 其中，

[0033] 所述密码确认模块102用于负责接收本地使用者的密码输入确认请求操作，并判断密码是否正确(此处的密码包含数字字母密码、手势密码、指纹密码等)，如果密码判断正确，则开启设备让本机使用者正常使用本设备，如果密码判断不正确，则要求使用者再次输入密码，同时将密码判定出错的结果送往密码出错计数判定单元102进行记录；

[0034] 所述密码出错计数判定单元102负责对本地使用者的密码输错次数进行记录，并把出错次数和保密级别设置存储单元103中存储的密码出错容忍门限进行比对判断；如果使用者多次输入密码出错，密码出错计数器的计数值已经达到保密级别设置存储单元103中存储的密码出错容忍门限，则发出自毁命令送到OTP烧写控制单元104；

[0035] 所述保密级别设置存储单元103负责存储保密级别设置和密码出错容忍次数设置，在第一次使用设备时需就要进行设置；

[0036] 所述OTP烧写控制单元104负责收到销毁命令后，从保密级别设置存储单元103中读取保密级别，并根据不同的级别向OTPROM阵列105写入特定值表示执行不同的销毁操作(这里的特定值就是指用来代表某种执行销毁操作的值)；

[0037] 所述OTP值判定单元106根据所述OTPROM阵列105进行数值判断是否执行对应的操作；

[0038] 所述EMMC初始化控制单元107负责将芯片外部的EMMC存储颗粒进行清零初始化；

[0039] 所述存储初始化单元109负责将芯片内的保密信息存储单元110的存储内容清零初始化。

[0040] 基于本发明所述的芯片自毁装置100，本发明的芯片自毁方法包括下述步骤：

[0041] 移动设备的初始设置，需要用户进行账户注册，并设置密码，然后还需要设置密码出错可以容忍的次数，以及芯片在收到销毁命令后的处理级别是彻底销毁芯片还是只销毁保密数据，设置好的存储保密级别和所述预设的密码出错容忍门限值并存储在保密级别设置存储单元103中，供所述OTP烧写控制单元104根据存储保密级别向OTPROM阵列105写入特定值。

[0042] 操作触发OTP烧写控制单元104进行熔断操作的条件：

[0043] 当密码确认模块101收到本机使用者的密码输入确认请求后，会判断密码是否正确(此处的密码包含数字字母密码，手势密码，指纹密码等密码输入方式)，如果正确则开启设备让本机使用者正常使用本设备；如果密码判断不正确，则要求使用者再次输入密码，同时将密码判定出错的结果送往密码出错计数判定单元102进行记录.如果使用者多次输入密码出错，且输错次数大于保密级别设置存储单元103中预设的密码出错容忍门限值时，所述密码出错计数判定单元102发出自毁命令送到OTP烧写控制单元104；

[0044] 销毁处理：

[0045] 所述OTP烧写控制单元104收到自毁命令后，会从保密级别设置存储单元103中读取保密级别；

[0046] 1、如果保密级别是只销毁保密数据,则执行以下的流程:

[0047] (1).向OTPROM阵列105写入特定值表示执行保密数据销毁操作(特定值比如是:32'h5a5a5a5a,(特定值是用于表示执行保密数据销毁操作的代码,因此不限于该数值);

[0048] (2).OTP值判定单元106会一直对OTP ROM阵列105的特定值进行判断,当特定值等于销毁保密数据级别的数值时,EMMC初始化控制单元107和存储初始化单元109会开始工作,将芯片内的保密信息存储单元110的存储内容清零初始化,和将芯片外部的eMMC存储颗粒108进行清零初始化。

[0049] 销毁保密数据的处理后,芯片还能继续使用,只是芯片内部和芯片外部的保密数据都已经被清零。

[0050] 2、如果保密级别设置存储单元中读取保密级别是芯片完全销毁,则执行以下的流程:

[0051] (a).向OTPROM阵列105写入特定值表示执行保密数据销毁操作(比如32'hdeaddead);

[0052] (b).OTP值判定单元106会一直对OTPROM阵列105进行数值判断,当特定值等于销毁芯片级别的数值时,EMMC初始化控制单元107和存储初始化单元109会开始工作,将芯片内的保密信息存储单元112的存储内容清零初始化,和将芯片外部的eMMC存储颗粒108进行清零初始化。

[0053] 销毁芯片的处理后,芯片将不能再继续使用,同时芯片内部和芯片外部的保密数据也会被清零。

[0054] 虽然以上描述了本发明的具体实施方式,但是熟悉本技术领域的技术人员应当理解,我们所描述的具体的实施例只是说明性的,而不是用于对本发明的范围的限定,熟悉本领域的技术人员在依照本发明的精神所作的等效的修饰以及变化,都应当涵盖在本发明的权利要求所保护的范围内。

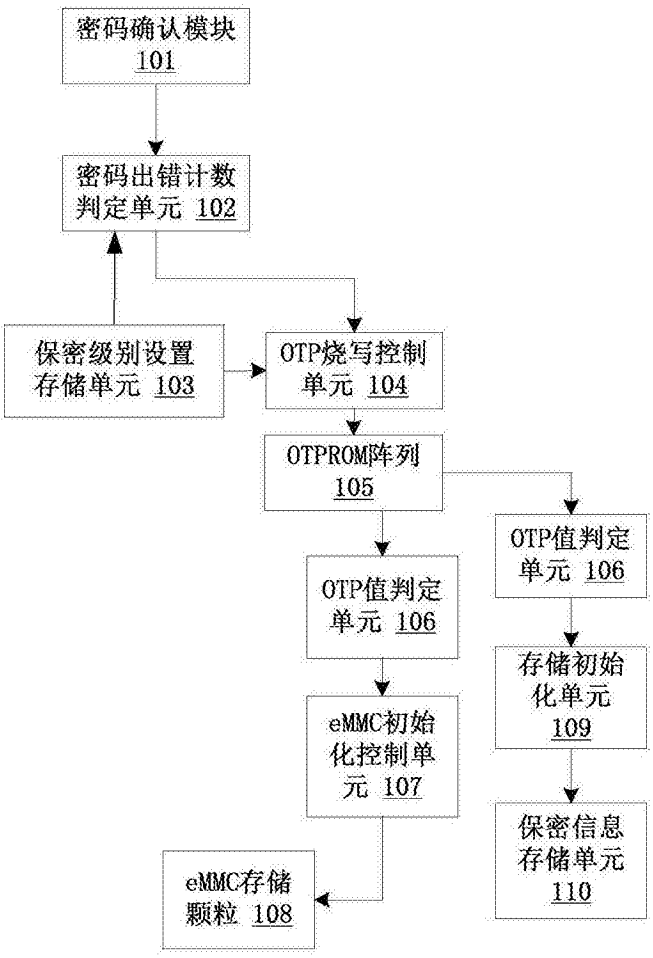

密码确认模块
101
密码出错计数
判定单元 102
保密级别设置
存储单元 103
OTP烧写控制
单元 104
OTPROM阵列
105
OTP值判定
单元 106
OTP值判定
单元 106
eMMC初始
化控制单
元 107
eMMC存储
颗粒 108
存储初始
化单元
109
保密信息
存储单元
110

图1