(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 105631362 A
(43)申请公布日 2016.06.01

(21)申请号 201410589729.7

(22)申请日 2014.10.29

(71)申请人 奇方科技有限公司
地址 中国台湾高雄市路竹区复兴路317号1楼

(72)发明人 黄智渊 杨明德

(74)专利代理机构 北京汇泽知识产权代理有限公司 11228
代理人 马廷昭

(51)Int.Cl.
G06F 21/71(2013.01)
G06F 21/73(2013.01)

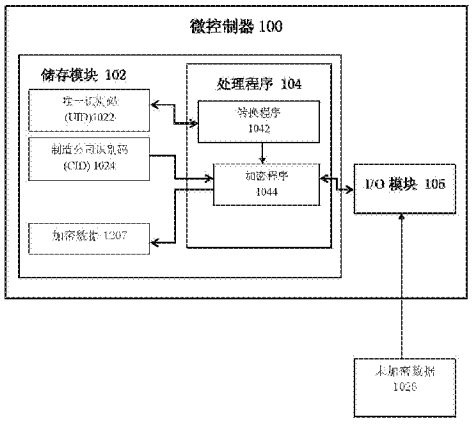
权利要求书1页 说明书5页 附图4页

(54)发明名称

微控制器加密的方法

(57)摘要

本发明提供一种微控制器(microcontroller unit)的加密方法，上述微控制器包含一储存模块以及一输入/输出模块，其中上述储存模块包含一唯一识别码(unique identifier, UID)以及一制造公司识别码(company identifier, CID)，上述储存模块更包括一处理程序，用以执行至少一转换程序以及一加密程序，执行下步骤如下：取得上述唯一识别码以及上述制造公司识别码；通过上述转换程序，以将上述唯一识别码转换为固定长度字节的数据；一未加密数据通过上述输入/输出模块传送至上述储存模块中；通过上述加密程序，以对经上述转换程序后的上述唯一识别码、上述制造公司识别码及上述未加密数据进行加密运算，以成为一加密数据；以及将上述加密数据储存于上述储存模块中。



CN 105631362 A

1.一种微控制器加密的方法，上述微控制器包括一储存模块以及一输入／输出模块，其中上述储存模块用以储存一唯一识别码以及一制造公司识别码，上述储存模块更包括一处理程序，用以执行至少一转换程序以及一加密程序，执行步骤如下：

取得上述唯一识别码以及上述制造公司识别码；

通过上述转换程序，将上述唯一识别码转换为固定长度字节的数据；

一未加密数据通过上述输入／输出模块传送至上述储存模块中；

通过上述加密程序，以对经上述转换程序后的上述唯一识别码、上述制造公司识别码及上述未加密数据进行加密运算，以成为一加密数据；以及

将上述加密数据储存于上述储存模块中。

2.如权利要求1所述的微控制器加密的方法，其特征在于，上述转换程序将上述唯一识别码转换为8个位元组的数据。

3.如权利要求2所述的微控制器加密的方法，其特征在于，上述唯一识别码于转换前是超过8个位元组的数据。

4.如权利要求2所述的微控制器加密的方法，其特征在于，上述唯一识别码于转换前是少于8个位元组的数据。

5.如权利要求1所述的微控制器加密的方法，其特征在于，上述转换程序是将上述唯一识别码排列成一n行8列的转换表格，其中n值大于或等于3 。

6.如权利要求1所述的微控制器加密的方法，其特征在于，上述未加密资料的字节长度与上述制造公司识别码及经上述转换程序后的上述唯一识别码的字节长度相同。

7.如权利要求6所述的微控制器加密的方法，其特征在于，上述字节长度为8个位元组。

8.如权利要求1所述的微控制器加密的方法，其特征在于，上述加密数据是将上述未加密数据、上述制造公司识别码和经上述转换程序后的上述唯一识别码，操作x次右循环、y次左循环及异或(XOR)运算所得到的加密结果。

9.如权利要求8所述的微控制器加密的方法，其特征在于，上述x介于0~8之间。

10.如权利要求8所述的微控制器加密的方法，其特征在于，上述y介于0~8之间。

11.如权利要求1所述的微控制器加密的方法，其特征在于，上述制造公司识别码是将足以辨识制造公司的资料，通过一字符编码表转换成为字节数据。

12.如权利要求11所述的微控制器加密的方法，其特征在于，上述字符编码表包含ASCII、Unicode、Big5、GB2312字符。

13.如权利要求1所述的微控制器加密的方法，其特征在于，上述储存模块包含ROM、PROMs、EPROMs、EEPROMs、闪存非挥发性存储器。

14.如权利要求1所述的微控制器加密的方法，其特征在于，上述唯一识别码及上述制造公司识别码是储存于上述非挥发性存储器中。

微控制器加密的方法

技术领域

[0001] 本发明关于一种加密方法，更特定而言，是关于防护微控制器中程式码的加密方法。

背景技术

[0002] 微控制器 (microcontroller unit, MCU) 是把中央处理器、存储器、定时 / 计数器、输入输出界面都整合在一块芯片上的微型计算机。与应用在个人计算机中的通用型微处理器相比，微控制器更强调不同外接硬件和节约成本。微控制器的最大优点在于体积小且硬件接线简单、易编写、保密性佳、输入输出界面简单，其发展非常迅速，可应用于多种领域，因而现今众多电子产品或高科技产品，如电子计算机、电子数字表、消费性电子产品等大多需仰赖微控制器方能执行。

[0003] 微控制器已与日常生活形影不离，其需求量与制造量相当可观，最典型的微控制器为八位元的 8051 微控制器。而近年来，由于消费性电子产品以及智能电子产品的崛起，早期简单性逻辑的微控制器已无法满足消费性电子产品以及智能电子产品的功能需求，因而开始朝向智能型演算的方向，且同时提升产品效能。

[0004] 于激烈的市场竞争压力下，除了针对硬件进行全面性的保护外，也同时须对软件或韧体进行保护，以防止不肖人士蓄意窃取重要机密，防止因非法拷贝而造成巨大的损失，因而，如何保护电子产业有关的内容和数据受到高度的关注。

[0005] 微控制器或 CPU 所执行的程序通常是储存于程序存储器 (ROM) 中，其扮演着系统运作的中枢，然而，信息科技的发达，复制工具（或程序）与技术也随之兴起，不肖人士将盗取后的微控制器，经过破解和复制工具（或程序）以获得公司重要机密并贩卖于市场中。有鉴于此，须对微控制器作进一步地防护，以防止他人蓄意盗取微控制器后，他人无法得知微控制器中重要机密，纵使被他人拷贝时，本发明的微控制器会产生错误的执行程序，使他人无法继续使用电子产品。

发明内容

[0006] 有鉴于此，本发明的主要目的在于提供一种微控制器加密的方法，其具简易且有效保护数据安全，同时降低成本的优点。

[0007] 综上所述，依据本发明的一观点，本发明提供一种加密方法，特别是对微控制器 (microcontroller unit) 进行加密的方法，上述微控制器包含一储存模块以及一输入 / 输出模块，其中上述储存模块包含一唯一识别码 (unique identifier, UID) 以及一制造公司识别码 (company identifier, CID)，上述储存模块更包括一处理程序，用以执行至少一转换程序以及一加密程序，执行下步骤如下 ：取得上述唯一识别码以及上述制造公司识别码 ；借由上述转换程序以将上述唯一识别码转换为固定长度字节的数据 ；一未加密数据通过上述输入 / 输出模块传送至上述储存模块中 ；借由上述加密程序以对上述唯一识别码、上述制造公司识别码及上述未加密数据进行加密运算，以成为一加密数据 ；以及将上述加密数

据储存于上述储存模块中。

[0008] 优选的是，上述转换程序将上述唯一识别码转换为 8 个位元组的数据。

[0009] 优选的是，上述转换程序是将上述唯一识别码排列成一 n 行 8 列的转换表格，其中 n 值大于或等于 3。

[0010] 优选的是，上述未加密数据的字节长度与上述制造公司识别码及经上述转换程序后的上述唯一识别码的字节长度相同。

[0011] 优选的是，上述加密数据是将上述未加密数据、上述唯一识别码和上述制造公司识别码，操作 x 次右循环、y 次左循环及异或 (XOR) 所得到的加密结果。

[0012] 优选的是，上述制造公司识别码是将足以辨识制造公司的资料，通过一字符编码表转换成为一字节数据。

[0013] 优选的是，上述储存模块包含 ROM、PROMs、EPROMs、EEPROMs、Flash 等非挥发性存储器。

[0014] 本发明的微控制器加密的方法，其具简易且有效保护数据安全，同时降低成本的优点。

附图说明

[0015] 上述元件，以及本发明其它特征与优点，借由阅读实施方式的内容及其附图后，将更为明显：

图 1 是根据本发明最佳实施例显示微控制器加密的系统结构图；

图 2 是根据本发明最佳实施例显示微控制器加密的步骤流程图；

图 3A 是根据本发明最佳实施例显示转换程序对唯一识别码的排列方式；

图 3B 是根据本发明最佳实施例显示转换程序对唯一识别码的演算方式；

图 4 是根据本发明最佳实施例显示加密程序的加密算法。

[0016] 附图标记说明

100 微控制器 102 储存模块 104 处理程序 105 I/O 模块

1022 唯一识别码 1024 制造公司识别码 1026 未加密数据

1027 加密数据 1042 转换程序 1044 加密程序

202-212 步骤。

具体实施方式

[0017] 本发明将配合其较佳实施例与随附的图示详述于下。应可理解为本发明中所有的较佳实施例仅为例示之用，并非用以限制。因此除文中的较佳实施例外，本发明亦可广泛地应用在其它实施例中。且本发明并不受限于任何实施例，应以随附的权利要求及其同等领域而定。

[0018] 以下，将搭配参照相应的附图，详细说明依照本发明的较佳实施例。关于本发明新颖概念的更多观点以及优点，将在以下的说明提出，并且使熟知或具有此领域通常知识者可了解其内容并且据以实施。

[0019] 参阅图 1，该图是根据本发明最佳实施例显示微控制器 100 加密的系统架构图。一微控制器 100 包含一储存模块 102 及一输入 / 输出 (I/O) 模块 105。于一实施例中，上述储

存模块102依照功能需求可为随机存取存储器(Random Access Memory, RAM),亦即数据存储器,为可读/写的记忆单元,用以存放数据或程序;以及上述储存模块102更可为程序存储器(program read only memory, ROM),本领域技术人员应当理解,现今大部分的程序存储器(ROM)为可读/写的记忆单元,其所储存的程序用以执行微控制器100,于此实施例中,上述储存模块102用以储存一唯一识别码(UID)1022以及一制造公司识别码(CID)1024,使用者仅能读取上述唯一识别码1022,其无法修改或删除。上述I/O模块105用以将外部的一未加密数据1026传送至上述储存模块102中,再通过上述处理程序104进行加密,以下将针对加密流程做进一步描述。

[0020] 所述储存模块102更包括一处理程序104,于一实施例中,上述处理程序104可为运算逻辑单元,用以执行逻辑运算(如加、减、乘、除等,但并不以此为限),并将运算后所得的数据传送至指定位置。上述处理程序104是执行运算的重要单元,其包含一转换程序1042以及一加密程序1044,以完成加、减、乘、除、与、或、异或等运算,或其他数学、逻辑、字符等运算或函数。于最佳实施例中,无须通过任一计算装置对上述微控制器100进行加密演算,直接利用上述微控制器100中韧体或软件径行加密演算;另一实施例中,亦可通过任一计算装置以对上述微控制器100进行加密演算。

[0021] 参阅图2,该图是根据本发明最佳实施例显示微控制器加密的步骤流程图。

[0022] 步骤202:取得上述唯一识别码1022。读取上述储存模块102中的上述唯一识别码1022。每一微控制器100制造出厂时,微控制器100制造商会对每一微控制器100直接写入识别码,每一微控制器100的唯一识别码1022皆为独一无二,使用者只可读取上述唯一识别码1022,但不可删除或更改上述唯一识别码1022,因此,于本发明的加密步骤中,无需通过任一装置即可进行读取,于另一实施例中,使用者可借由微控制器指令取得每一微控制器100的唯一识别码1022,以便于后续加密的步骤。微控制器100依照总线或数据暂存器的宽度,可分为四位元、八位元、十六位元和三十二位,于最佳实施例是采用具八位元的CMOS(互补式金属氧化物半导体)控制器以执行加密步骤,但并不以此为限。于一实施例中,使用者可通过一 RDMSR (read form MSR, 读取特别模块暂存器) 指令以读取上述唯一识别码1022。

[0023] 步骤204:转换上述唯一识别码1022的字节数据。借由上述处理程序104的上述转换程序1042,对上述唯一识别码1022进行演算操作,以转换为所需的字节。由于不同微控制器100制造商写入唯一识别码1022字节(Byte)皆不同,因此若小于八个位元组或超过八个位元组的唯一识别码1022,需转换成标准八个位元组的数据,或其他字节数,以利后续加密步骤。若转换前的唯一识别码1022即为标准的八个位元组,即可径行后续加密步骤。上述转换程序1042的排列方式如图3A所示,但不以此为限,实际的排列方式仍由制造公司自行决定。于此实施例中,转换前唯一识别码1022是由12个位元组所组成的数据,如UID(0)、UID(1)、...、UID(11),将12个位元组资料排列成n行8列的表格,n值大于或等于3,此实施例中n=3,需注意的是,表格的排列必须使用到唯一识别码1022的12个位元组,而每个字节皆可重复使用,最后将表格每一列的每一个字节做多个逻辑运算,如图3B所示的运算方式,即可得到转换后8个位元组的唯一识别码1022资料,如UID8(0)、UID8(1)...UID8(7), UID8资料。于图3B中,swap(Byte)为一种常见的逻辑运算,是将一个字节的高四位与下四位交换,如10100101经swap运算后得到01011010,或以另一方式表

示可为 B7B6B5B4B3B2B1B0 经 swap 运算后得到 B3B2B1B0B7B6B5B4，但并不以此为限。

[0024] 步骤 206：取得一制造公司识别码 (company identifier, CID)1024。除了制造商对微控制器 100 直接写入唯一识别码 1022 外，另外制造商亦将足以辨识制造商的文字、名称、简称或代码等资料，通过字符编码转换成电子储存或通讯使用的字节数据，以作为制造公司识别码 1024。上述字符编码表包含 ASCII、Unicode、Big5、GB2312 等字符。于一实施例中，使用者可通过一 RDMSR(read form MSR, 读取特别模块暂存器）指令以读取上述制造公司识别码 1024。一般而言，上述制造公司识别码 1024 无需经由上述转换程序 1042 以转换至所需的字节数据，因此，上述制造公司识别码 1024 可直接传送至上述加密程序 1044 中。于另一实施例中，亦可借由上述处理程序 104 的上述转换程序 1042，对上述制造公司识别码 1024 进行演算操作，以转换为所需的字节数据，其转换字节的方法可类比于上述唯一识别码 1022 的转换方法。由于不同制造公司识别码 1024 的字节 (Byte) 可能不尽相同，因此若小于八个位元组或超过八个位元组的制造公司识别码 1024，需转换成标准八个位元组的资料，或其他字节个数，以利后续加密步骤。若转换前的制造公司识别码 1024 即为标准的八个位元组，即可径行后续加密步骤。上述转换程序 1042 的排列方式可类比图 3A 所示，将 UID 修改为 CID 即可，但不以此为限，实际的排列方式仍由制造公司自行决定。此实施例中，转换前制造公司识别码 1024 是由 12 个位元组所组成的资料，如 CID(0)、CID(1)...CID(11)，将 12 个位元组资料排列成 m 行 8 列的表格，m 值大于或等于 3，此实施例中 m=3，需注意的是，表格的排列必须使用到制造公司识别码 1024 的 12 个位元组，而每个字节皆可重复使用，最后将表格每一列的每一个字节做多个逻辑运算，可类比图 3B 所示的运算方式，将 UID 修改为 CID，即可得到转换后 8 个位元组的制造公司识别码 1024 资料，如 CID8(0)、CID8(1)...CID8(7) 资料。swap(Byte) 为一种常见的逻辑运算，是将一个字节的高四位与下四位交换，如 10100101 经 swap 运算后得到 01011010，或以另一方式表示可为 B7B6B5B4B3B2B1B0 经 swap 运算后得到 B3B2B1B0B7B6B5B4，但并不以此为限。

[0025] 上述步骤 202-204 以及步骤 206 可同时进行，亦可分开进行，取得唯一识别码或制造公司识别码的先后顺序并无特别规定。

[0026] 步骤 208：转换后的上述唯一识别码 1022、上述制造公司识别码 1024 以及上述未加密数据 1026 同时（或分别）传送至上述加密程序 1044 中。上述唯一识别码 1022 经由上述转换程序 1042 转换至所需的字节数据后，并传送至上述加密程序 1044 中。上述制造公司识别码 1024 无需经由上述转换程序 1042 即可传送至上述加密程序 1044 中。来自外部的上述未加密数据 1026 则是通过上述 I/O 模块 105 以传送至上述加密程序 1044 中。

[0027] 步骤 210：借由上述加密程序 1044，对上述未加密数据 1026、上述制造公司识别码 1024 和经上述转换程序 1042 的上述唯一识别码 1022 进行加密运算，以成为一加密数据 1207。上述加密程序 1044 的运算方式如图 4 所示，但不以此为限，实际的排列方式仍由制造公司自行决定。将上述唯一识别码 1022 进行 x 次的右循环，以及上述制造公司识别码 1024 进行 y 次的左循环，再与上述未加密数据 1026 Dat(0)、Dat(1)…Dat(7) 进行多次运算，得到 Enc(0)、Enc(1)...Enc(7) 等资料，其总和即可为一加密数据 1207，其中 x 可大于或等于 0，y 可大于或等于 0。应当理解，上述未加密数据 1026 的字节长度为固定的长度，无需经过上述转换程序 1042 以进行转换，原则上，上述未加密数据 1026 的字节长度与上述制造公司识别码 1024 及经上述转换程序 1042 的上述唯一识别码 1022 的字节长度相同。

[0028] 步骤 212 :将上述加密数据 1207 储存于上述储存模块 102 中。将上述未加密数据 1026 经过多次运算即可得到上述加密数据 1207,其可储存非挥发性存储器,如 RAM、ROM、PROMs、RAMs、EPROMs、EEPROMs、快闪存储器等。

[0029] 综上所陈,本发明的执行与储存于储存模块 102 中进行,由上述步骤可知,虽唯一识别码 1022 或制造公司识别码 1024 易通过多种方式被他人取得,然而通过本发明的转换程序 1042 和加密程序 1044,将上述识别码进行多重加密,纵使他人虽易取得上述识别码,但却无法正确计算出加密后的数据,资料受到严密的保护,可有效防止他人窃取、删除、窜改保密资料,甚至,当不肖人士窃取上述微控制器时,上述微控制器会产生错误的执行程序,使他人无法继续使用电子产品,以防止资料外泄。

[0030] 本文与附图所述的算法或排列方式仅用以表达如何计算,实际应用不限于上述排列方式,实际排列方式由制造公司所决定,不对外公开。本文与附图所述的字节不限于 8 个位元组,本发明可广泛地应用至小于 8 个位元组或超过 8 个位元组,仍需依照实际状况而做调整。本文与附图所述的算法包括加、减、乘、除、与、或、异或 (XOR)、补码、左旋右旋、左移、右移、交换、错位等运算,或其他数学、逻辑、字符等运算或函数,计算出欲加密资料相同长度的加密资料,以作为加密的结果,储存于微控制器内的非挥发性存储器中,其中非挥发性存储器包括 ROM、PROMs、RAMs、EPROMs、EEPROMs、快闪存储器等。

[0031] 本发明可借由可输入指令的任一程序、软件或硬件进行加密步骤,如 C++ 通用程序设计语言、汇编语言 assembly 或其他语言程序,但并不以此为限。

[0032] 对熟悉此领域技术的人,本发明虽以较佳实例阐明如上,然而其并非用以限定本发明的精神。在不脱离本发明的精神与范围内所作的修改与类似的配置,均应包含在下述的权利要求内,此范围应覆盖所有类似修改与类似结构,且应做最宽广的诠释。

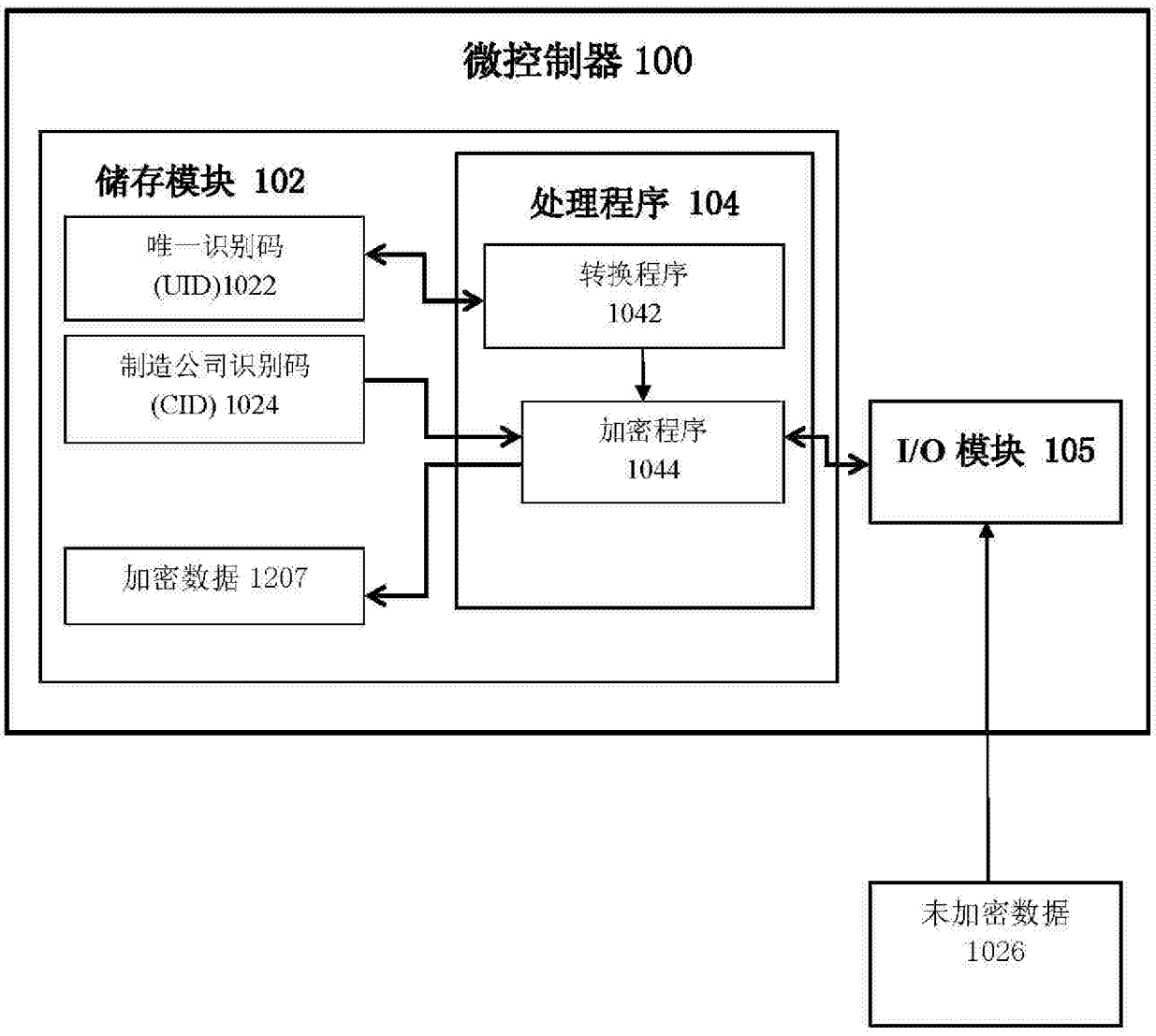

微控制器 100
储存模块 102
唯一识别码
(UID)1022
制造公司识别码
(CID) 1024
加密数据 1207
处理程序 104
转换程序
1042
加密程序
1044
I/O 模块 105
未加密数据
1026

图 1

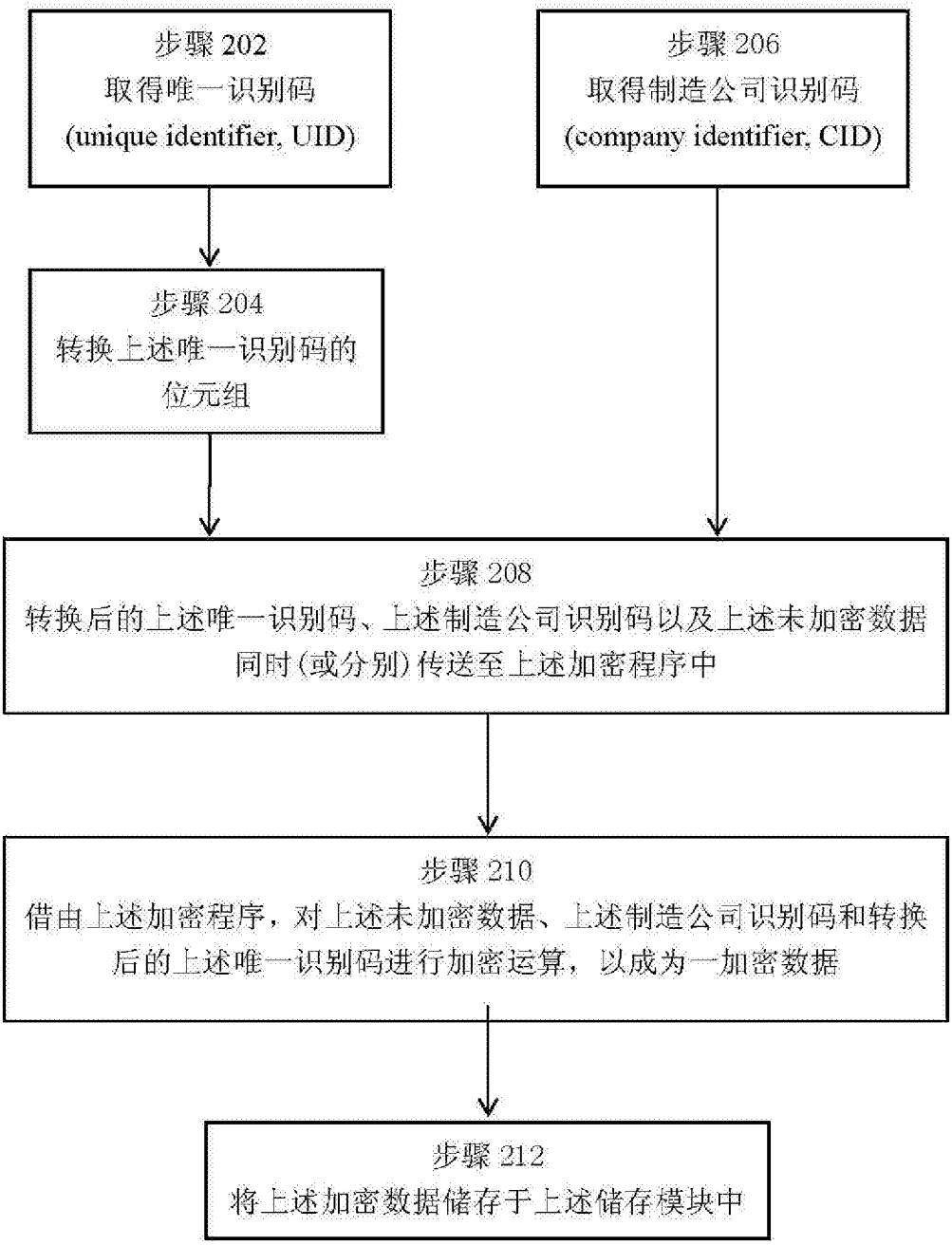

步骤 202
取得唯一识别码
(unique identifier, UID)
步骤 206
取得制造公司识别码
(company identifier, CID)
步骤 204
转换上述唯一识别码的
位元组
步骤 208
转换后的上述唯一识别码、上述制造公司识别码以及上述未加密数据
同时(或分别)传送至上述加密程序中
步骤 210
借由上述加密程序，对上述未加密数据、上述制造公司识别码和转换
后的上述唯一识别码进行加密运算，以成为一加密数据
步骤 212
将上述加密数据储存于上述储存模块中

图 2

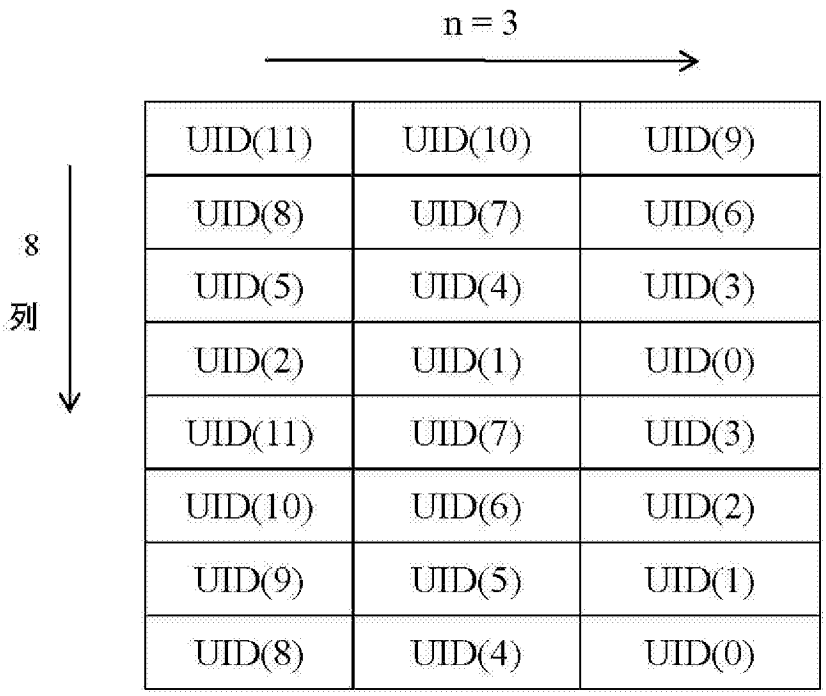


图 3A

UID8(0) = swap (UID(11) xor UID(10) xor UID(9))

UID8(1) = swap (UID(8) xor UID(7) xor UID(6))

UID8(2) = swap (UID(5) xor UID(4) xor UID(3))

UID8(3) = swap (UID(2) xor UID(1) xor UID(0))

UID8(4) = swap (UID(11) xor UID(7) xor UID(3))

UID8(5) = swap (UID(10) xor UID(6) xor UID(2))

UID8(6) = swap (UID(9) xor UID(5) xor UID(1))

UID8(7) = swap (UID(8) xor UID(4) xor UID(0))

图 3B

Enc(0) = Dat(0) xorrotateRight(CID8(0),y) xorrotateLeft(UID8(0),x)

Enc(1) = Dat(1) xorrotateRight(CID8(1),y) xorrotateLeft(UID8(1),x)

Enc(2) = Dat(2) xorrotateRight(CID8(2),y) xorrotateLeft(UID8(2),x)

Enc(3) = Dat(3) xorrotateRight(CID8(3),y) xorrotateLeft(UID8(3),x)

Enc(4) = Dat(4) xorrotateRight(CID8(4),y) xorrotateLeft(UID8(4),x)

Enc(5) = Dat(5) xorrotateRight(CID8(5),y) xorrotateLeft(UID8(5),x)

Enc(6) = Dat(6) xorrotateRight(CID8(6),y) xorrotateLeft(UID8(6),x)

Enc(7) = Dat(7) xorrotateRight(CID8(7),y) xorrotateLeft(UID8(7),x)

图 4