(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 103136830 A
(43)申请公布日 2013.06.05

(21)申请号 201310051994.5

(22)申请日 2013.02.18

(71)申请人 江苏省电力公司金湖县供电公司
地址 211600 江苏省淮安市金湖县建设东路2号
申请人 南京国网电瑞系统工程有限公司
江苏省电力公司
国家电网公司

(72)发明人 刘建戈 邵加武 邵青松 秦玥 居上 冯安金

(74)专利代理机构 淮安市科翔专利商标事务所 32110
代理人 韩晓斌

(51)Int.Cl.
G07C 9/00(2006.01)

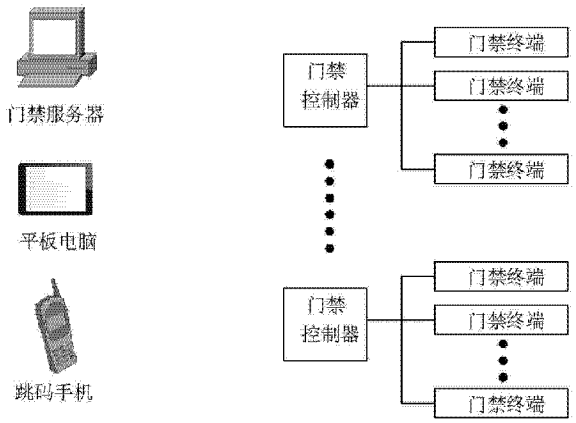
权利要求书1页 说明书4页 附图2页

(54)发明名称

无需通信的门禁系统跳码生成方法

(57)摘要

本发明公开了无需通信的门禁系统跳码生成方法，包括跳码终端和门禁控制器，一个跳码终端对应若干个门禁控制器，门禁控制器控制一个或若干个门禁终端；其中跳码终端安装了跳码生成程序，程序中有一组生成跳码的非线性算法和一个对应门禁控制器的加密算法调用规则表，每个时段对应每个门禁控制器的算法都不一样；其中门禁控制器的解密程序中有与跳码终端对应的一个解密算法调用规则表和一组密码解密的非线性算法，每个时段的算法与跳码终端的算法一致；本发明根据比对结果进行相应门禁控制终端授权，跳码终端与门禁控制器没有通信联系，实现门禁控制器不同时间不重复的密码。



CN 103136830 A

1. 无需通信的门禁系统跳码生成方法，其特征在于：该门禁系统跳码生成方法包括跳码终端和门禁控制器，一个跳码终端对应若干个门禁控制器，门禁控制器控制一个或若干个门禁终端；其中跳码终端安装了跳码生成程序，程序中有一组生成跳码的非线性算法和一个对应门禁控制器的加密算法调用规则表，每个时段对应每个门禁控制器的算法都不一样；其中门禁控制器的解密程序中有与跳码终端对应的一个解密算法调用规则表和一组密码解密的非线性算法，每个时段的算法与跳码终端的算法一致；跳码终端和门禁控制器以当前日期时间、门禁控制器编号和跳码生成程序的序列号为自变量，计算出当前时段跳码，与输入的跳码进行比对，根据比对结果进行相应门禁控制终端的授权。

2. 根据权利要求 1 所述的无需通信的门禁系统跳码生成方法，其特征在于：跳码终端是普通 PC 机、平板电脑或智能手机。

无需通信的门禁系统跳码生成方法

技术领域

[0001] 本发明涉及门禁系统的密码生成方法，尤其是一种无需通信的门禁系统跳码生成方法。

背景技术

[0002] 跳码技术又称滚码技术，是一种利用复杂的非线性加密算法实现编码的加密技术，其特点是编码多变化、抗截获、安全可靠，防范攻击和抵抗非法入侵能力强。目前，跳码技术主要用于汽车行业的遥控无钥门禁系统，以跳码技术通过发射无线信号来开关车门。跳码技术是通过硬件技术使钥匙每次发送的密码唯一而随机，入侵者无法预测，即使记录了原来的开锁密码也不能用于下次开锁，因此安全性极高。而门禁系统中主要采用RFID(无线射频)卡、生物识别、网络控制和密码技术。采用RFID卡时，卡片丢失时容易出现非授权的进入，无法做到远程的临时授权；生物识别更是无法做到远程的临时授权；网络控制的门禁虽然可以方便做到远程的临时授权，但对于分散不易于建立通信网络的场所是无法采用的；而密码技术的门禁系统，由于密码相对固定，不适合多人使用，更加容易出现失密事件。因此，对于一些分散的场所门禁系统，设计一种无需通信的门禁跳码生成方法是非常必要的。例如在电力系统中，变电站分布往往比较分散，其大门、控制室和开关制室等的门锁通常采用机械锁，各类人员需要频繁进出就不断进出变电站，必须往返于集控中心站取还钥匙，取还钥匙的时间远大于现场工作时间。门禁跳码技术可实现对各类人员的临时授权，保证各类人员的正常工作时间，也防止了使用已有密码随意进出变电站。

发明内容

[0003] 本发明的目的在于：提供一种无需通信的门禁系统跳码生成方法，跳码终端与门禁控制器没有通信联系，不依赖于通信网络实现门禁控制器不同时间不重复的密码。

[0004] 本发明的技术解决方案是：该门禁系统跳码生成方法包括跳码终端和门禁控制器，跳码终端是普通PC机、平板电脑或智能手机，一个跳码终端对应若干个门禁控制器，门禁控制器控制一个或若干个门禁终端；其中跳码终端安装了跳码生成程序，程序中有一组生成跳码的非线性算法和一个对应门禁控制器的加密算法调用规则表，每个时段对应每个门禁控制器的算法都不一样；其中门禁控制器的解密程序中有与跳码终端对应的一个解密算法调用规则表和一组密码解密的非线性算法，每个时段的算法与跳码终端的算法一致；

跳码终端和门禁控制器以当前日期时间、门禁控制器编号和跳码生成程序的序列号为自变量，计算出当前时段跳码，与输入的跳码进行比对，根据比对结果进行相应门禁控制终端的授权。

[0005] 工作时，门禁系统管理员在跳码终端上选择相应的门禁控制器及终端编号生成一个跳码，通过电话、短信或其他方式告知进站人员，进站人员通过门禁终端上的键盘输入跳码，门禁控制器进行运算解密确认；门禁控制器接受到键盘输入的密码，调用跳码解密程序，计算跳码的合法性；门禁控制器的解密程序中则有与跳码终端生成程序对应的一个解

密算法调用规则和一组密码解密算法，跳码正确且在时间范围内则由门禁控制器发出指令通过门禁终端打开电控锁。

[0006] 本发明具有以下优点：

1、在一个与门禁控制器无通信的跳码终端上通过软件产生一个带时效的不重复的密码，在对应的门禁控制器上输入该密码打开门锁，每个门禁每一个时段的密码算法都是不相同，同一时段控制器与跳码终端密码算法是一致的，且两者都是以当前日期时间、门禁编号和跳码生成程序序列号作为变量，即使算法重复的情况下所产生的密码也不会重复，跳码终端产生的一个跳码只会在一个时段内有效，跳码终端与门禁控制器之间无需任何通信或其他联系方式实现对跳码的解密和加密功能。

[0007] 2、跳码的加密和解密都以跳码生成程序序列号、当前日期时间和门禁控制器及终端编号为自变量，不同门禁控制器在不同时段对应不同的算法产生不同的跳码，即使相同时段不同禁控制器或同一禁控制器不同时段产生的跳码也不相同，门禁跳码随机变化，各个时段内不重复，通过复杂的非线性加密算法实现编码的加解密，所产生的跳码仅在一定的时间内有效，适合于各种门禁系统各类人员的临时授权。

附图说明

[0008] 图 1 为无通信跳码控制门禁系统的构成图

图 2 为跳码终端加密流程图

图 3 为门禁控制器解密流程图

具体实施方式

[0009] 结合附图对本发明作进一步说明。

[0010] 如图 1-3 所示，该门禁系统跳码生成方法包括跳码终端和门禁控制器，跳码终端是普通 PC 机、平板电脑或智能手机，一个跳码终端对应若干个门禁控制器，门禁控制器控制一个或若干个门禁终端；其中跳码终端安装了跳码生成程序，程序中有一组生成跳码的非线性算法和一个对应门禁控制器的加密算法调用规则表，每个时段对应每个门禁控制器的算法都不一样；其中门禁控制器的解密程序中有与跳码终端对应的一个解密算法调用规则表和一组密码解密的非线性算法，每个时段的算法与跳码终端的算法一致； 跳码终端和门禁控制器以当前日期时间、门禁控制器编号和跳码生成程序的序列号为自变量，计算出当前时段跳码，与输入的跳码进行比对，根据比对结果进行相应门禁控制终端的授权。

[0011] 以智能手机为例，将值班公用手机交由当值管理员使用，根据需要实现对门禁随时随地的授权。跳码终端中有一组跳码生成算法和有一个对应门禁控制器的加密算法调用规则表。

[0012] 表 1 跳码终端的算法调用规则

加密算法公式序号 i	加密算法	1 号站解密算法序号 k1	2 号站解密算法序号 k2	3 号站解密算法序号 k3	……
1	EN1 ()	42	15	2	……
2	EN2 ()	3	7	78	……
……	……	……	……	……	……

计算公式为

i = Fm(Tim,Cid)

其中 i 为非线性加密算法公式序号，Tim 为当前时间，格式为 yyyymmddhhmm，如 2012 年 12 月 12 日 15 时 30 分表示为 201212121530；Cid 为门禁控制器编号，范围为 01-99。

[0013] 每个 i 值对应一个非线性加密算法公式，非线性加密算法公式以当前时间 Tim、门禁控制器及门禁终端编号 CDid 和跳码程序序列号 Sn，公式如下：

Hcm =ENi (Tim, CDid,Sn) (i=1,2,3…99)

其中跳码程序序列号 Sn 固定不变，主要是防止跳码程序被非法拷贝后用来产生跳码；CDid 为门禁控制器及门禁终端编号，0100-9999，前两位表门禁控制器编号，后两位表示门禁控制器对应的门禁终端的编号，如编号为 6 的门禁控制器下的第二道门禁编号为 0602；通过加密算法程序产生的 Hcm 即为对应门禁控制器的跳码，通过电话或短信方式告知需要进站人员，进站人员在键盘上输入跳码 Hcm，由门禁控制器进行解密。

[0014] 门禁控制器的解密程序中则有与跳码终端中对应的一个解密算法调用规则和一组密码解密算法。

[0015] 表 2 门禁控制器的解密算法调用规则表

门禁控制器解密算法序号 K	解密算法公式	跳码终端加密算法序号 i
1	DE1 ()	15
2	DE2 ()	21
……	……	……

计算公式为

K = Fs(Tim)

其中 k 为非线性解密算法公式序号，Tim 的含义同加密算法；每个时段计算出的 k 值与跳码程序计算出的 i 值不完全一致，但非线性加密算法公式 ENi 与非线性解密算法公式 DEk 的表达是完全相同的，解密算法公式 DEk：

Hcc =DEk (Tim, CDid,Sn) (k=1,2,3…99)

自变量 Tim、CDid、Sn 含义与加密公式 ENi 基本一致；当计算出的 Hcc 等于输入的跳码 Hcm 时，打开相应的门禁。

[0016] 其中门禁编号 id 的后两位为 00 时，表示本次跳码对本门禁控制器对应的所有门禁终端通用，即可以打开站内所有门锁；后两位为 01 时只能打开大门门锁；因此，从某个场所大门门禁键盘输入的跳码时，门禁控制器必须进行两次计算；分别用门禁编号后两位为 00、01 计算出全站或大门的跳码，如用 00 计算出的跳码 Hcc 等于 Hcm，则开放全站门禁；若用 01 计算出的跳码 Hcc 等于 Hcm，则开放本站大门门禁；其他结果则为非法数据；跳码的时效性为 10 分钟，超过 10 分钟为新的算法产生的跳码；每 10 分钟内连续输入 5 次错误后不再接受跳码输入；通常一处场所只需安装一个门禁控制器，由控制器通过门禁终端对多个门实现控制；每个场所的门禁控制器每一个时段的密码算法都是不相同，同一时段门禁控制器与跳码终端算法一致的，且两者都是以日期时间作为变量之一，即使算法重复的情况下所产生的密码也不会重复，门禁跳码只会有一个时段内有效，有效防止了密码被他人盗用。

[0017] 下面以一个变电站门禁系统的跳码生成方法进行说明。

[0018] 电力系统中的变电站分布比较分散，通常是一个集控中心负责多个变电站的运维，日常巡视、操作和施工等各类人员需要频繁进出，就必须到集控中心不断取返相应变电

站的系列钥匙；采用无通信跳码门禁可方便管理人员不受时间和地点为需要进入变电站人员进行授权；在集控中心管理人员的手机上安装门禁跳码产生程序；如 2012 年 10 月 10 日 9 时 51 分有人需要进入 6 号变电站大门时，管理人员在手机选择所要产跳码的变电站及其大门，这是手机跳码产生程序内计算出

i= Fm(201010100951,06)=27

即调用加密算法公式 EN27，假定手机跳码程序序列号 526608，则计算出

Hcm=EN27(201010100951,0601,526608) ＝ 473453 进站人员在大门键盘上输入跳码后，门禁控制器根据当前时间计算出解密算法公式序号

K = Fs(201010100951) ＝ 3

根据解密算法调用规则，解密算法公式 DE3 等于加密算法公式 EN27，分别以全站门禁 0600 和大门门禁 0601 进行计算跳码

Hcm=DE3 ＝ EN27(201010100951,0601,526608) ＝ 321655（全站）

Hcm=DE3 ＝ EN27(201010100951,0601,526608) ＝ 473453（大门）

输入的跳码与本站大门门禁跳码相符合，开放大门门禁；当输入的跳码超过 10 时后，门禁控制器计算出的跳码出现变化；如果此时需要开门，必须由门禁系统管理员重新产生跳码方可。

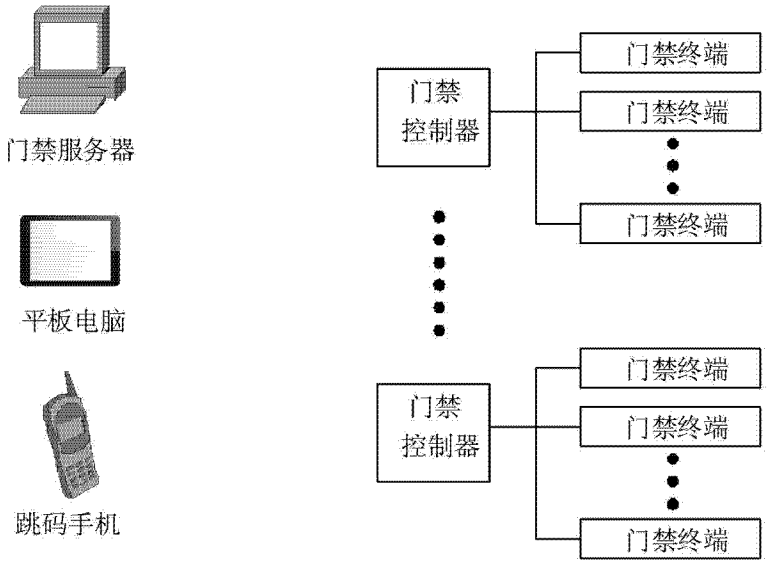

门禁服务器
平板电脑
跳码手机
门禁
控制器
门禁终端
门禁终端
门禁终端
门禁
控制器
门禁终端
门禁终端
门禁终端

图 1

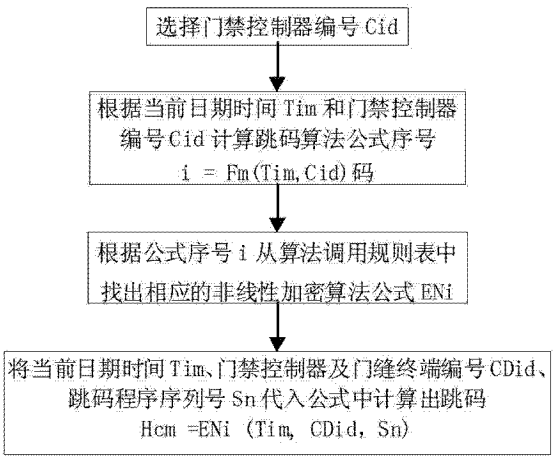

选择门禁控制器编号 Cid
根据当前日期时间 Tim 和门禁控制器编号 Cid 计算跳码算法公式序号 i = Fm(Tim,Cid) 码
根据公式序号 i 从算法调用规则表中找出相应的非线性加密算法公式 ENi
将当前日期时间 Tim、门禁控制器及门缝终端编号 CDid、跳码程序序列号 Sn 代入公式中计算出跳码 Hcm =ENi (Tim, CDid, Sn)

图 2

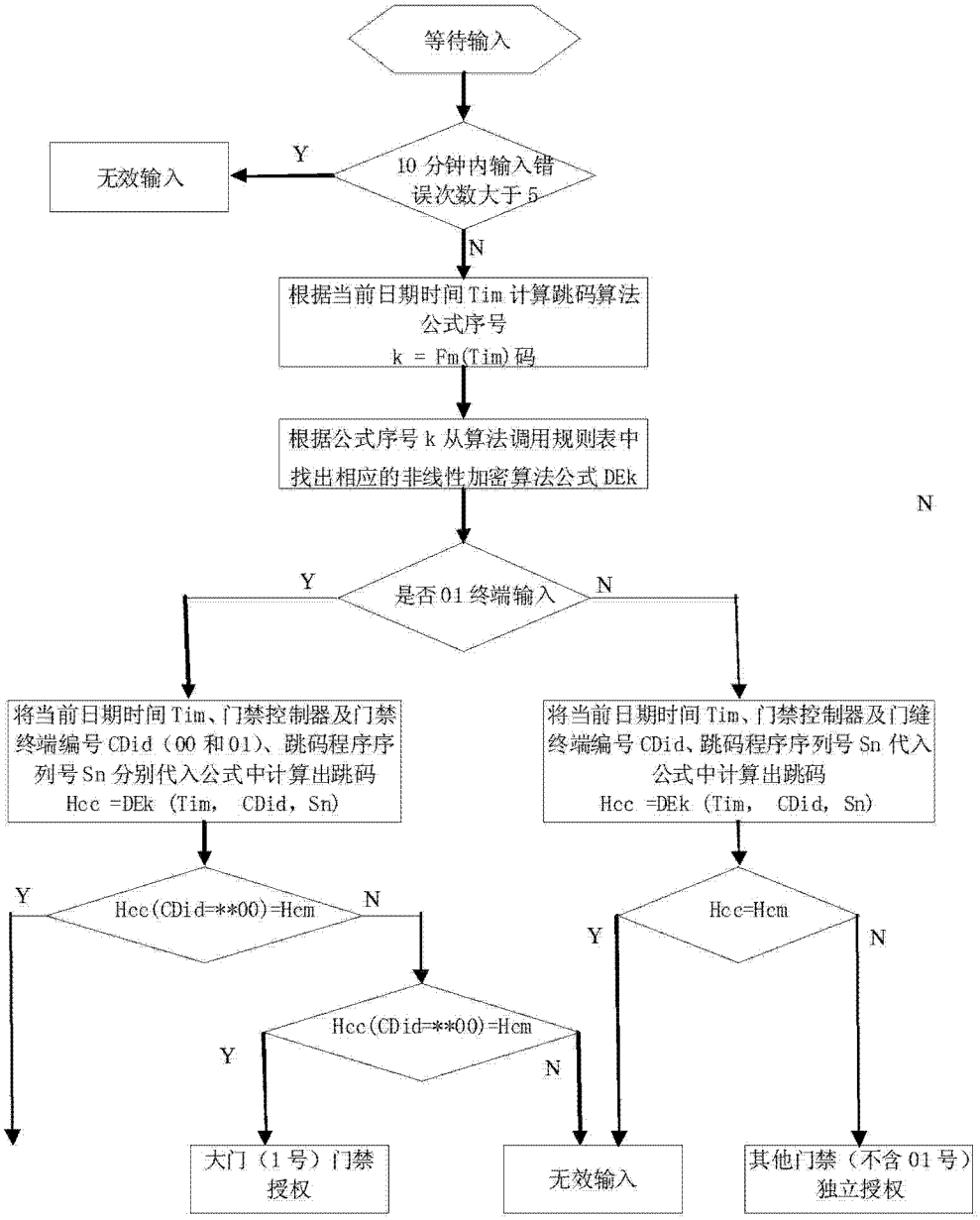

等待输入
10 分钟内输入错误次数大于 5
Y
无效输入
N
根据当前日期时间 Tim 计算跳码算法公式序号
k = Fm(Tim)码
根据公式序号 k 从算法调用规则表中找出相应的非线性加密算法公式 DEk
是否 01 终端输入
Y
N
将当前日期时间 Tim、门禁控制器及门禁终端编号 CDid（00 和 01）、跳码程序序列号 Sn 分别代入公式中计算出跳码
Hcc =DEk (Tim, CDid, Sn)
将当前日期时间 Tim、门禁控制器及门缝终端编号 CDid、跳码程序序列号 Sn 代入公式中计算出跳码
Hcc =DEk (Tim, CDid, Sn)
Hcc(CDid=**00)=Hcm
Hcc=Hcm
大门（1 号）门禁授权
无效输入
其他门禁（不含 01 号）独立授权

图 3